Вісник ЛДУБЖД
Bulletin of Lviv State University of Life Safety
https://journal.ldubgd.edu.ua/index.php/Visnuk
ISSN 2078-4643 (print), ISSN 2708-1389 (online)

UDC 004.056.53
DOI: 10.32447/20784643.30.2024.13

О. І. Полотай, А. О. Пузир
Львівський державний університет безпеки життєдіяльності, м. Львів, Україна
Національний університет «Львівська Політехніка», м. Львів, Україна
ORCID: https://orcid.org/0000-0003-4593-8601 – О. І. Полотай
orest.polotaj@gmail.com

АНАЛІЗ ЗАСОБІВ ЗАПОБІГАННЯ ВИТОКУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВАХ, НА ПРИКЛАДІ СИСТЕМИ DLP

Постановка проблеми. В умовах цифровізації сучасного бізнес-середовища питання безпеки інформації стає критично важливим. Конфіденційні дані, такі як фінансова інформація, персональні дані клієнтів і внутрішні корпоративні документи, є цінним активом для будь-якого підприємства. Витоки такої інформації можуть призвести до серйозних наслідків, включаючи фінансові збитки, репутаційні втрати, штрафи з боку регуляторів та навіть юридичні наслідки. Сучасні загрози інформаційній безпеці, такі як кібератаки, фішинг, ненавмисне розголошення даних співробітниками та зовнішніми контрагентами, лише підвищують ризики.

Мета. Метою статті є дослідження особливостей DLP-систем, які виконують ключову роль у забезпеченні інформаційної безпеки на підприємстві, надаючи можливості для моніторингу, виявлення та захисту конфіденційної інформації в реальному часі.

Результати. У статті детально описано переваги використання на підприємствах систем запобігання витоку даних DLP, які забезпечують три основні сфери IT-безпеки організації: захист персональних даних та дотримання встановлених вимог, захист інтелектуальної власності та видимість даних. Описано та показано сфери та потоки даних, на які спрямована робота DLP-систем. Серед них можна виділити весь вихідний трафік, такий як HTTP, SMTP тощо. Наводиться характеристика двох груп, на які поділяються DLP-системи: шлюзові та вузлові. Наводиться порівняльна характеристика деяких представлених на ринку DLP-систем. Детально описано методики аналіз потоку даних з метою виявлення конфіденційної інформації підприємства, які використовуються сучасними DLP-системами. Представлено етапи впровадження DLP-систем. Більш детально описуються особливості роботи американської DLP-системи Symantec на прикладі реального підприємства.

Висновки. Системи запобігання витоку даних DLP відіграють важливу роль у сучасній інформаційній безпеці підприємств. Вони пропонують цілісний підхід до захисту конфіденційної інформації, зокрема захист активів, відповідність нормативним вимогам, зниження ризиків та покращення культури безпеки. Системи запобігання витоку даних стають невід'ємною частиною стратегії інформаційної безпеки на підприємствах.

Ключові слова: система DLP, конфіденційна інформація, підприємство, кібербезпека, інформаційна безпека, загрози.

O. I. Polotai, A. O. Puzyr
Lviv State University of Life Safety, Lviv, Ukraine
Lviv Polytechnic National University, Lviv, Ukraine

ANALYSIS OF MEANS OF PREVENTION OF LEAKAGE OF CONFIDENTIAL INFORMATION AT ENTERPRISES, ON THE EXAMPLE OF THE DLP SYSTEM

Introduction. In the conditions of digitization of the modern business environment, the issue of information security becomes critically important. Sensitive data such as financial information, personal customer data, and internal corporate documents are a valuable asset to any business. Leaks of such information may lead to serious consequences, including financial losses, reputational losses, fines from regulators, and even legal consequences. Modern threats to information security, such as cyber-attacks, phishing, and inadvertent leakage of data by employees and external contractors, only increase the risks.

Purpose. The purpose of the research is to explore the features of DLP systems, which play a key role in ensuring information security at the enterprise, providing opportunities for monitoring, detecting, and protecting confidential information in real-time.

Results. The article describes in detail the benefits of using DLP data leakage prevention systems in enterprises, which provide three main areas of IT security for an organization: personal data protection and compliance, intellectual property protection, and data visibility. The article describes and shows the areas and data flows that DLP systems are aimed at. These include all outgoing traffic, such as HTTP, SMTP, etc. The article describes the two groups into which DLP systems are divided: gateway and node. A comparative description of some DLP systems on the market is given. The methods of data flow analysis to identify confidential information of an enterprise used by modern DLP systems are described in detail. The stages of DLP systems implementation are presented. The features of the American Symantec DLP system are described in more detail on the example of a real enterprise.

Conclusion. Data Loss Prevention (DLP) systems play an important role in modern enterprise information security. They offer a holistic approach to protecting confidential information, including asset protection, regulatory compliance, risk mitigation, and improving security culture. Data leakage prevention systems are becoming an integral part of an enterprise's information security strategy.

Keywords: DLP system, confidential information, enterprise, cyber security, information security, threats.

Вступ. У сучасному цифровому світі, де інформація є важливим активом для підприємств та організацій, захист конфіденційної інформації має вирішальне значення. В умовах глобалізації, стрімкого технологічного розвитку і збільшення обсягу оброблюваних даних, питання безпеки даних виходять на перший план. Конфіденційна інформація, така як персональні дані, фінансова інформація, комерційна таємниця і інтелектуальна власність, стає мішенню кіберзлочинців, конкурентів і зловмисників.

Загрози кіберзлочинності, такі як фішинг, вірусні атаки, порушення даних через вразливості системи та загрози інформації в локальній мережі [19, 20], загрожують не лише конфіденційності інформації, але й безпеці всього бізнесу. Згідно з дослідженнями, більшість компаній стикаються з кіберінцидентами, які призводять до витоку конфіденційної інформації. Така втрата даних може призвести до серйозних фінансових втрат, починаючи від витрат на відновлення системи і закінчуючи штрафами, накладеними за недотримання нормативних вимог.

Погіршення репутації компанії також є серйозним наслідком витоку конфіденційної інформації. Втрата довіри з боку клієнтів і партнерів може призвести до зниження продажів, відтоку клієнтів і зниження конкурентоспроможності. Наприклад, вузькоспеціалізовані компанії, схильні до порушення даних, часто втрачають частину своєї клієнтської бази, оскільки споживачі не хочуть, щоб їхні дані були скомпрометовані.

Правові наслідки витоку конфіденційної інформації також можуть бути серйозними. Багато країн, включаючи країни-члени Європейського союзу, прийняли законодавство про захист даних, наприклад, Загальний регламент про захист даних (GDPR). Цей регламент передбачає значні штрафи для компаній, які не дотримуються вимог щодо захисту даних. Таким чином, порушення закону може призвести до фінансових санкцій та судових розглядів, що ще більше ускладнює ситуацію для компаній.

У контексті недобросовісної конкуренції захист конфіденційної інформації стає ще більш важливим. Конкуренти можуть намагатися отримати доступ до важливих даних підприємства, що може призвести до неправомірних дій і втрати конкурентних переваг. Для запобігання таким ситуаціям організації повинні впроваджувати ефективні механізми захисту даних, зокрема використання систем запобігання витоку даних, які допоможуть виявити, запобігти та реагувати на потенційні загрози.

Отже, актуальність теми захисту конфіденційної інформації обумовлена численними факторами, такими як зростаючі загрози кіберзлочинності, фінансові та юридичні наслідки витоку даних, а також потреба у збереженні довіри клієнтів і партнерів. У цьому контексті запровадження комплексних стратегій захисту інформації стає обов'язковим для забезпечення стабільності та успішності бізнесу в умовах сучасних викликів.

Методи досліджень. Методологічну основу дослідження становлять принципи та основні категорії діалектичного пізнання соціальних явищ і процесів, розвитку та взаємозв'язку об'єктів реальної дійсності, системи загальнонаукових та спеціальних методів, які є засобами наукового пошуку в арсеналі гуманітарних, у тому числі й юридичних наук.

Результати досліджень. Абревіатура DLP означає Data Loss Prevention або «запобігання втраті даних». Це підхід або набір стратегій, що складається з інструментів і процесів, які мережеві адміністратори можуть використовувати для забезпечення захисту конфіденційних даних від несанкціонованого доступу, крадіжки або втрати. Це запобігає передачі користувачами конфіденційної або критично важливої інформації за межі мережі компанії. Користувачі можуть через недбалість або зловмисні наміри передавати дані, що може завдати шкоди організації, яка володіє мережею. Приклади включають пересилання ділових електронних листів за межі корпоративного домену або завантаження конфіденційних файлів до комерційних хмарних

сховищ, таких як Dropbox. DLP-системи категоризують та захищають чутливі дані незалежно від їхньої категорії – робочі, конфіденційні або захищені за законодавством.

DLP дає змогу вирішити три болісних питання в IT-безпеці організації: захист персональних даних/дотримання встановлених вимог, захист інтелектуальної власності та видимість даних.

Захист персональних даних/комплаєнс: організації, які збирають і зберігають персональні ідентифікаційні дані, дані про стан здоров'я та платіжні дані, швидше за все, підпадають під дію таких нормативних актів, як HIPAA та GDPR. Це означає, що їм доведеться вжити заходів для захисту конфіденційної інформації своїх клієнтів.

Захист інтелектуальної власності: якщо підприємство має цінну інтелектуальну власність, об’єкти комерційної або навіть державної таємниці, то втрата або викрадення таких даних може поставити їх під загрозу. Рішення DLP, що використовують контекстну класифікацію, можуть класифікувати інтелектуальну власність як структурованим, так і неструктурованим способом. Політика та запобіжні заходи можуть допомогти запобігти витоку даних.

Видимість даних: комплексне корпоративне DLP-рішення здатне бачити та відстежувати дані на кінцевих точках, в мережах та у хмарі. Ви побачите, як здійснюється взаємодія користувачів організації із даними.

DLP-рішення є також ефективними для протидії несанкціонованим діям користувачів, захисту даних Office 365, аналізу поведінки користувачів і структурних підрозділів та захисту від комплексних загроз.

Основне призначення DLP-систем – забезпечувати захист від випадкового або навмисного поширення конфіденційної інформації з боку співробітників, що мають доступ до неї в силу своїх службових обов’язків [16].

Серед потоків даних, на які спрямована робота DLP-систем можна виділити вихідні повідомлення електронної пошти, вихідний HTTP трафік, тіньові копії файлів, файли друку, тощо [22].

Системи запобігання витоку даних (DLP) стають невід'ємною частиною стратегії інформаційної безпеки на підприємствах. Вони виконують три основні функції, які дають можливість організаціям ідентифікувати, захищати та реагувати на загрози, пов'язані з конфіденційною інформацією.

Такі системи створюють безпечний «цифровий периметр» навколо організації та аналізують усю вихідну, а іноді й вхідну інформацію. Інформація, якою керують, включає не лише інтернет-трафік, але й багато інших інформаційних потоків. Наприклад, документи, винесені за межі контуру безпеки, захищені зовнішніми носіями, документи, роздруковані на принтерах, і документи, надіслані на мобільні носії через Bluetooth або WiFi і т.д.

DLP-система аналізує потік даних, що проходить через периметр інформаційної системи, яка захищається. Якщо в цьому потоці виявляється чутлива інформація, спрацьовують активні компоненти системи і передача повідомлень (пакетів, потоків, сеансів) блокується. Виявлення чутливої інформації в потоці даних відбувається шляхом аналізу вмісту та виявлення особливих ознак, таких як печатки документів, спеціально введені мітки або значення хеш-функції з певного набору.

DLP-системи поділяються на три групи: на основі використання агента (agent based), без використання агента (agentless) та гібридні або змішані (hybrid). Системи на основі агента потребують обов’язково встановлення програмного забезпечення на кожний кінцевий пристрій, в той час як системи без агента моніторять трафік мережі. Гібридні, своєю чергою, можуть працювати в обох режимах.

Сучасні DLP-системи мають величезну кількість параметрів і характеристик, які обов'язково необхідно враховувати під час виборів рішення організації захисту конфіденційної інформації від витоків. Мабуть, найважливішим з них є мережева архітектура. Відповідно до цього параметра продукти класу, що розглядається, поділяються на дві великі групи: шлюзові (рис. 1) і хостові (рис. 2) [17].

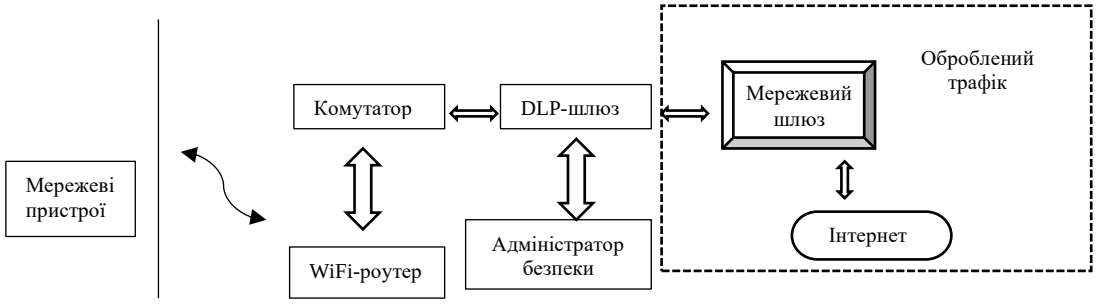

Рисунок 1 – Функціональна схема шлюзового DLP-рішення

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

Другий варіант заснований на використанні спеціальних програм – агентів, які встановлюються на кінцевих вузлах мережі – робочих станціях, серверах додатків та ін.

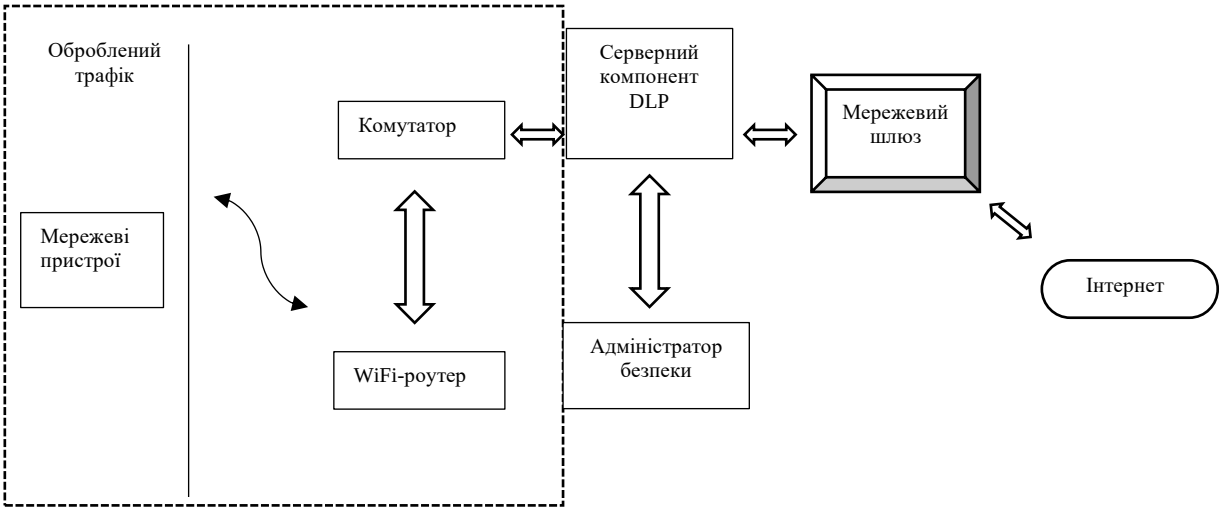

Рисунок 2 – Функціональна схема вузлового DLP-рішення

Останнім часом спостерігається стійкий перехід до універсалізації DLP-систем. На ринку залишилося мало або зовсім не залишилося рішень, які називаються чисто хостинговими або шлюзовими рішеннями. Навіть розробники, які довгий час розвивали лише один напрямок, додають в рішення модулі 2-го типу.

Завдання аналізу потоку даних для виявлення конфіденційної інформації можна назвати нетривіальним, оскільки пошук потрібних даних ускладнюється безліччю факторів, які необхідно враховувати. Тому на сьогодні розроблено кілька технологій для виявлення спроб передачі конфіденційних даних. Кожна з них відрізняється від інших своїм принципом роботи.

Традиційно всі методи виявлення витоків можна розділити на 2 групи. До першої категорії відносяться технології (морфологічний і статистичний аналіз, шаблони), засновані на аналізі тексту відправленого повідомлення або самого документа. За аналогією з антивірусним захистом їх можна назвати проактивними. 2-у групу складають реактивні методи (цифровий друк і бирки). Вони визначають витік за характеристиками документа або наявності спеціальних міток.

Морфологічний аналіз. Це один з найпоширеніших контент-орієнтованих методів виявлення витоків конфіденційної інформації. Суть цього методу полягає в пошуку певних слів або фраз у тексті, що передається [13].

Статистичний аналіз. Принцип статистичних методів ґрунтується на імовірнісному аналізі текстів, що дає змогу припускати конфіденційність і відкритість. Алгоритми зазвичай потребують попереднього навчання. Обчислюється ймовірність знаходження певного слова або фрази в конфіденційному документі.

Регулярні вирази (шаблони). Менеджер безпеки визначає шаблон рядка (кількість символів та їх тип (буква або цифра)) для конфіденційних даних. Потім система шукає в аналізованому тексті комбінації, які йому задовольняють, і застосовує до знайдених файлів і повідомлень дії, зазначені в правилах.

Цифрові відбитки. У цьому випадку цифровий відбиток – це набір характерних елементів документа, які можуть бути ідентифіковані з високою достовірністю в майбутньому. Сучасні DLP-рішення можуть виявляти як цілі файли, так і їх фрагменти. Вони також можуть обчислювати ступінь відповідності. Такі рішення можуть створювати диференційовані правила, які описують різні дії для різних відсотків збігів.

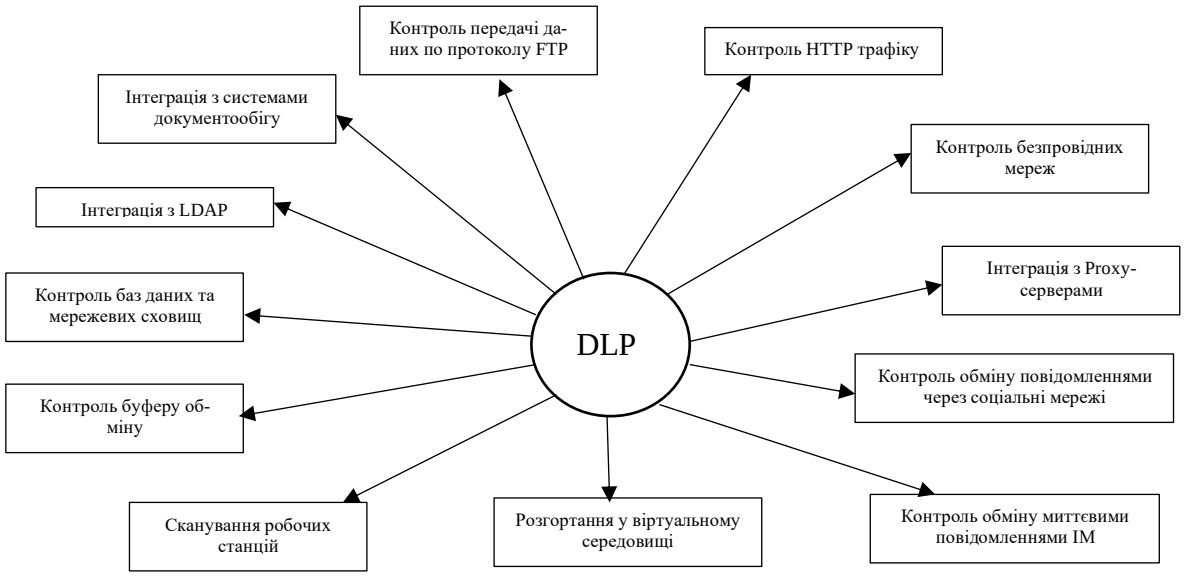

Рисунок 3 – Основні функції DLP-систем

Цифрові мітки. Принцип дії цього методу такий: до обраного документа наноситься спеціальна мітка. Вона відображається лише в клієнтському модулі DLP, який і є використовуваним рішенням. Залежно від доступності система дозволяє або забороняє певні дії з файлом. Основні функції DLP-систем представлені на рисунку 3.

Впровадження системи запобігання витоку даних є складним і багатоступеневим процесом, що потребує ретельного планування і координації. Щоб забезпечити успішну інтеграцію DLP-системи, організації повинні пройти такі ключові етапи (рис. 4).

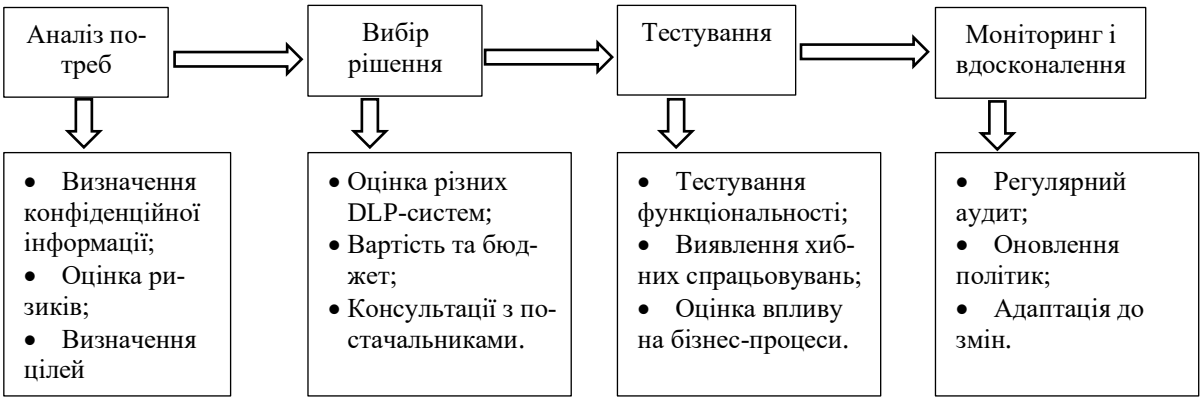

Рисунок 4 – Етапи впровадження DLP-систем [15]

В таблиці 1 наводиться порівняння сучасних DLP-систем.

Таблиця 1

Порівняння характеристик сучасних DLP-систем

Назва	**Symantec**	**Comodo MyDLP**	**Cocosys Endpoint Protector**	**InfoWatch Traffic Monitor**
Складність в роботі	середня	легка	середня	середня
Керування ролевим доступом	+	+	+	+
Підтримка мобільних пристроїв	+	-	+	+
Шифрування USB	+	-	+	-
Додаткові функції	DLP End User Remediation	-	контроль пристроїв	криміналістичний аналіз
Пробна версія	30 днів	30 днів	1 рік, до 5 пристроїв	30 днів, до 100 користувачів

Головне вікно DLP-системи на прикладі Symantec представлене на рисунку 5. Symantec DLP дає можливість виявляти конфіденційну інформацію, яка розташована в хмарних сховищах, файлових і веб-серверах, базах даних і кінцевих точках (настільних і портативних системах), захищати конфіденційну інформацію за допомогою карантину і відстежувати мережевий трафік на предмет передачі конфіденційних даних.

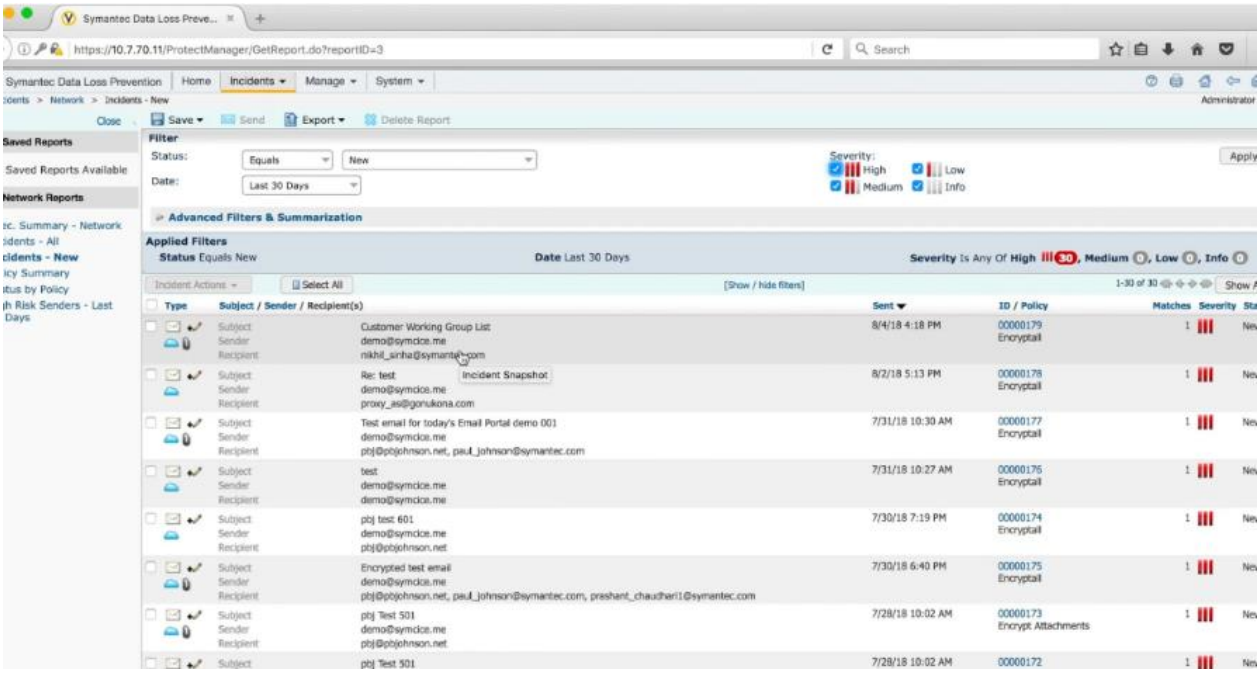

Рисунок 5 – DLP-система Symantec [9, 10]

Система DLP від Symantec надає широкий спектр функцій для захисту конфіденційної інформації (рис. 6).

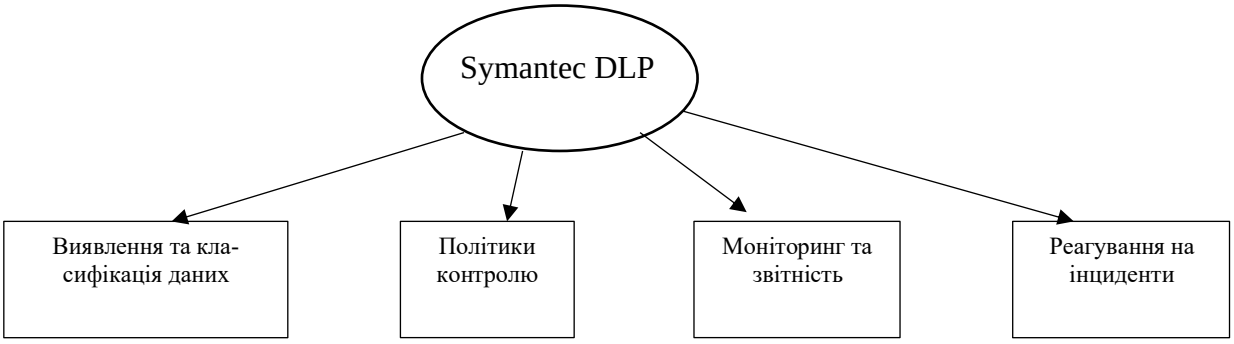

Рисунок 6 – Функції Symantec-DLP [6]

Однією з важливих особливостей програмного забезпечення Symantec-DLP є можливість її інтеграції з іншими системами інформаційної безпеки, такими як SIEM [19], для покращення виявлення загроз і реагування на інциденти.

Обговорення результатів досліджень. Перед впровадженням системи захисту даних від Symantec важливо провести детальний аналіз потреб компанії. Необхідно визначити, які дані є критичними для бізнесу. На прикладі досліджуваного підприємства це такі дані, як:

•Фінансова інформація: банківські рахунки, фінансові звіти.

•Особисті дані: інформація про співробітників, клієнтів.

•Конфіденційна інформація: патенти, торгові секрети.

•Інформація про проекти: дані про розробки, плани, контракти.

Визначивши, які дані потрібно захищати, можна переходити до створення політик, що регулюють їх обробку та зберігання (рисунок 7).

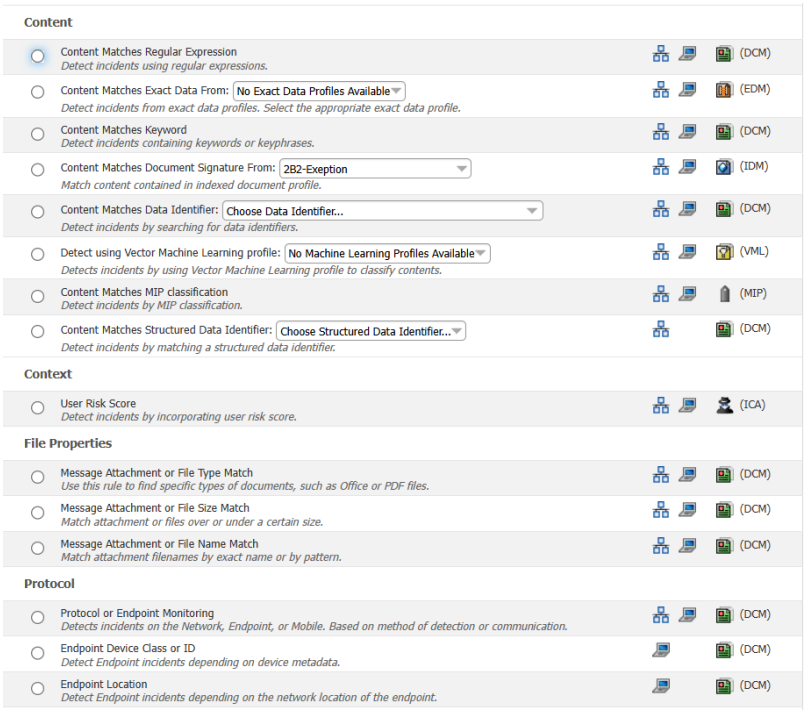

Рисунок 7 – Можливості для створення політик

На цьому етапі система пропонує достатню базу можливостей для створення правил та політик зберігання даних. Серед них варто виділити такі:

•Правило для виявлення контенту використовуючи регулярні вирази.

•Правило для виявлення контенту використовуючи заздалегідь створений відбиток структурованої таблиці.

•Правило для виявлення контенту використовуючи словники.

•Правило для виявлення контенту, використовуючи заздалегідь створені цифрові відбитки документів.

•Правила, розроблені вендорами Symantec для виявлення конфіденційної та персональної інформації, такі як: номери карток, ідентифікатори американських та європейських стандартів.

•Правила для виявлення за параметрами файлів, такі як: виявлення файлів за їхнім типом, за розміром та за назвою.

•Правила виявлення за такими параметрами, як розташування робочої станції користувача, протоколами передачі інформації та типами змінних носіїв.

На цьому етапі розглянемо можливість створення політики за принципом виявлення контенту, використовуючи словники (рисунок 8).

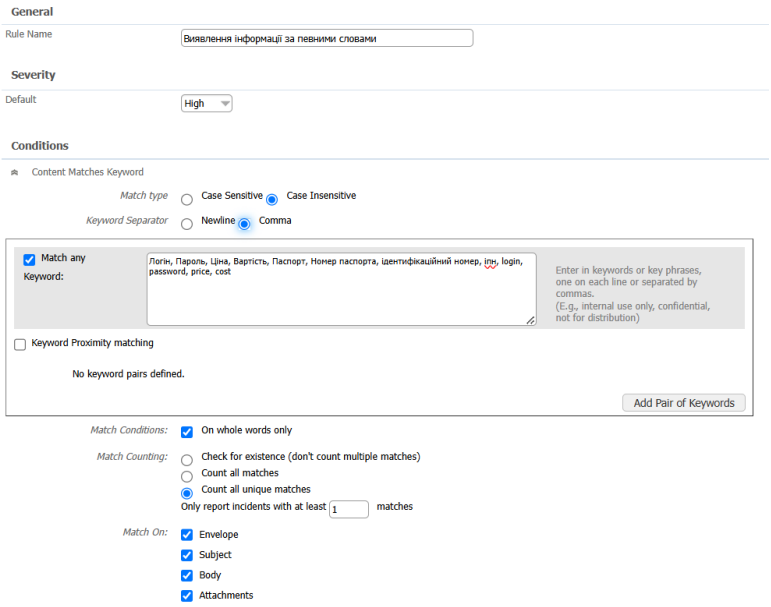

Рисунок 8 – Створення політики використовуючи словники

Політика виявлення ключових слів у системі DLP дає змогу організаціям захищати чутливі дані, визначаючи конкретні терміни або фрази, які мають критичне значення для бізнесу. Коли користувачі взаємодіють із даними, система автоматично сканує вміст на наявність цих ключових слів.

Після створення політики потрібно дати системі зрозуміти як діяти після виявлення інцидентів, згідно з політикою. У таких випадках існують Response Rules, тобто правила, які вказують на певні дії в разі виявлення, згідно з політикою (рисунок 9).

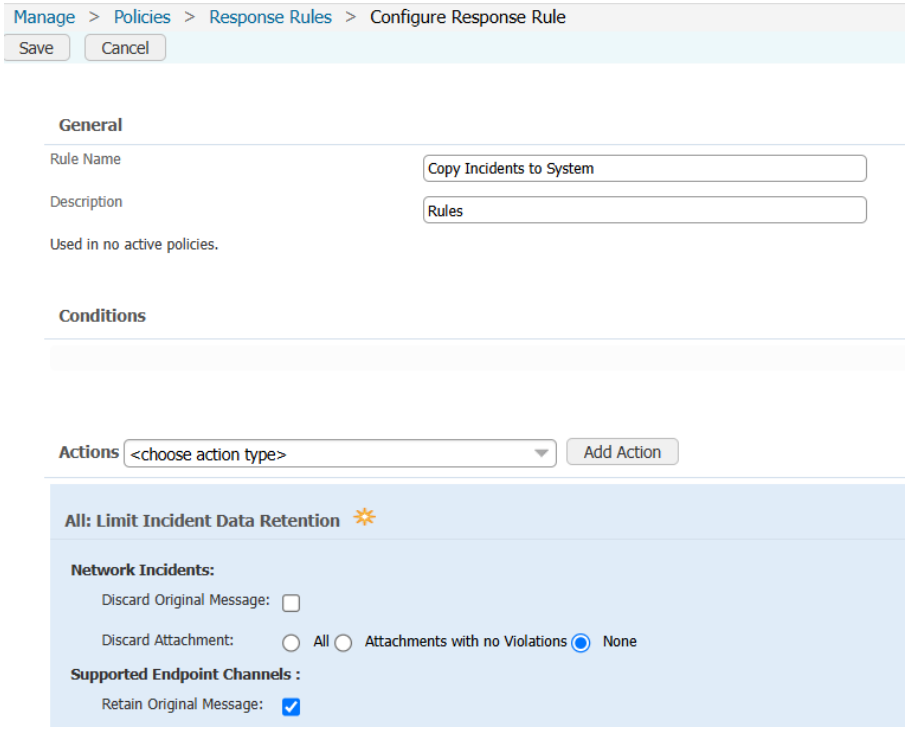

Рисунок 9 – Створення правила для відпрацювання згідно політики.

На рисунку 10 зображено створення правила відпрацювання. Якщо згідно із створеною політикою для виявлення інформації за ключовими словами агент DLP, котрий стоїть на кінцевій точці (вузлі), має надіслати даний інцидент у нашу систему.

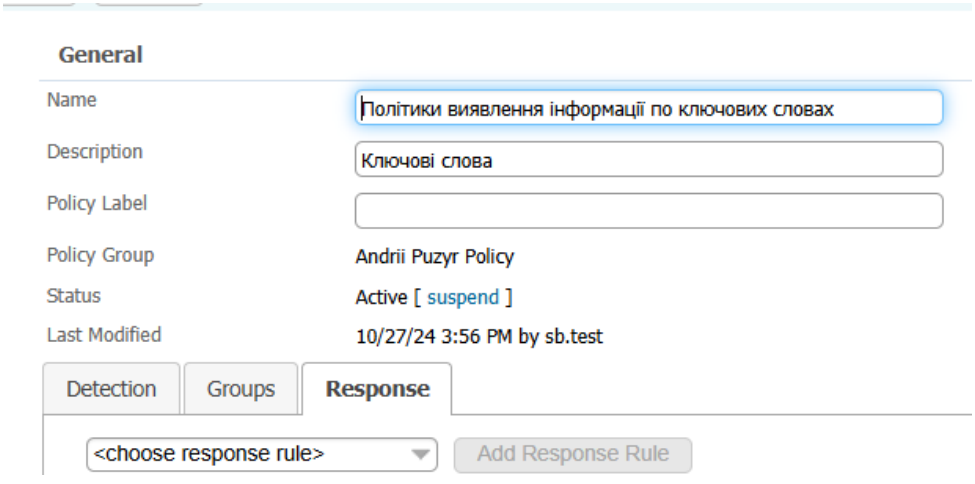

Рисунок 10 – Створення правила для відпрацювання, згідно з політикою

Для тестування запрограмованих політик необхідно створити файл типу *.doc, який буде містити хоча б одне слово, згідно з нашою політикою. Це такі слова як «номер, пароль, ідентифікаційний код» тощо. І спробуємо надіслати цей файл зі станції, на якій стоїть агент DLP, та залогований користувач у пошті на іншу скриньку.

Після надсилання файлу, котрий містить дані, згідно з політикою можна побачити всю інформацію про цей інцидент (рисунок 11).

Рисунок 11 – Відпрацювання надсилання, згідно з політикою

Для прикладу, на цьому рисунку можна побачити, яка політика та дані спрацювали при надходженні трафіку. Дата та час, коли відбулося це надсилання, вкладення, а також куди надсилався цей лист.

Висновки. Витік конфіденційних даних може призвести до величезних збитків для компанії і, що найголовніше, вплинути на бізнес компанії в довгостроковій перспективі, а не відразу. Для збереження власних даних, фінансових ресурсів та репутації, зменшення ймовірності настання інцидентів кібербезпеки, підприємствам в умовах сучасних реалій необхідно дотримуватися сучасних правил забезпечення інформаційної безпеки, використовуючи при цьому як технічні, програмно-апаратні, так і програмні засоби досягнення згаданих вище цілей. Одним з таких засобів виступають DLP-системи. У цій статті розглянуто особливості впровадження таких DLP-систем на прикладі системи Symantec DLP. Проведене дослідження сучасних DLP-систем дало змогу обгрунтувати вибір оптимальної серед них для аналізу особливостей впровадження та роботи з нею.

Список літератури:

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

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

3. An enterprise DLP that's easy to learn, deploy, and manage [Електронний ресурс].- Режим доступу: acronis.com/en-us/products/devicelock

4. Bader S. What Is Data Loss Prevention and How Does It Work? 2022. URL: https://rewind.com/blog/data-loss-prevention/

5. Chapple M., Stewart J. M., Gibson D. (ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide. – John Wiley & Sons, 2018

6. Factum. Колегія детективів і фахівців безпеки бізнесу. Витік інформації. URL: http://ukr.detectiveua.com/vitik-inform

7. Features of modern DLP systems. URL: forbes.com/sites/davidbalaban/2021/11/12/all-features-of-moderndlp-systems/?sh=27666e2e7618

8. Gurpreet Dhillon, Tiago Oliveira, Santa Susarapu, and Mario Caldeira. Decidingbetween information security and usability: Developing value based objectives.Computers in Human Behavior, 61:656–666, 08 2016.

9. Luther Martin. Understanding DLP. Auerbach Publications, (n.d).

10. McAfee Data Loss Prevention Endpoint. 2024. URL: softlist.com.ua/catalog/product-mcafee-dlp/

11. Reasons Why Your Business Needs (DLP) Data Loss Prevention. 2022 URL. https://uniserveit.com/blog/reasons-why-your-business-needs-dlp-data-lossprevention.

12. Symantec Data Loss Prevention Solution. URL: https://docs.broadcom.com/doc/data-loss-prevention-solution-en

13. Symantec Data Loss Prevention. URL: static.carahsoft.com/concrete/files/9814/4734/5158/Data_Loss_ Prevention_Data_Insight_Enterprise.pdf

14. Tanaka K. Transformer-based Models in Data Loss Prevention Systems. 2023. URL: https://www.cyberdatascience.com/transformers-dlp/

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

16. Zvit «Rozrobka ta vprovadzhennia typovykh rishen shchodo kompleksnoi systemy zakhystu informatsii v AIS NANU» (KSZI AIS NANU): Systema upravlinnia intsydentamy informatsiinoi bezpeky. Kerivnytstvo administratora. (2009). Kyiv: НАН України 2009. 149 p.

17. Близнюк А.В. Дослідження алгоритмів морфологічного аналізу у DLP-системах для запобігання витоку інформації. Інфокомунікаційні та комп'ютерні технології. 2022. №2 (04). С. 143-148.

18.Вовчановський П.П., Демчинський В.В. Архітектура DLP-систем в умовах політики BYOD. Системи та технології кібернетичної безпеки. 2020. С. 151-154.

19.Впровадження DLP-систем. (2024). URL: https://techexpert.ua/our-services/implementation-of-dlp-systems/

20.Гержан С. Г., Масальска Е. А. (2020). Попередження витоку даних з допомогою DLP-систем. URL http://ir.nmu.org.ua/bitstream/handle/123456789/148756/masalska_gerjan.pdf.

21.Запобігання витоку даних — DLP. (2023). URL: https://www.kingston.com/ua/blog/data-security/data-loss-prevention-dlp

22.Кучменко М. В., Грайворонський М. В. Аналіз концпепції BYOD та архітектура для її впровадження. Теоретичні і прикладні проблеми фізики, математики та інформатики: матеріали XV Всеукраїнської науково-практичної конференція студентів, аспірантів та молодих вчених (м. Київ 25-27 травня 2017 р.). Київ: 2017. С. 147.

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

24.Полотай О.І., Довнаник С. SIEM-системи, як елемент аналізу та управління подіями CSOC. Матер. Всеукр. наук.-практ. Internet-конф. "Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку" (м. Черкаси, 16–22 березня 2020 р.). Черкаси : ЧНУ ім. Б. Хмельницького, 2020. С. 60–61.

25.Полотай О.І., Дубик А.-О.Ю. Загрози інформації в комп'ютерних мережах на канальному рівні. "Світ наукових досліджень" (матеріали Міжнародної мультидисциплінарної наукової інтернет-конференції (м. Тернопіль, Україна, м. Ополе, Польща, 21-21 березня 2024 р.). Вип. 28. С. 185-187.

26.Полотай О.І., Федінець Н.І., Кухарська Н.П. Дослідження загроз інформаційної безпеки та способів їх вирішення в комп'ютерних мережах на канальному рівні. Вісник Львівського державного університету безпеки життєдіяльності. 2024. № 29. С. 65–71.

27.Що робити компанії в разі витоку інформації? 2015. URL: uteka.ua/publication/news-14-delovye-novosti-36-shhorobiti-kompanii-v-razi-vitoku-informacii

28.Що таке DLP-система і навіщо вона потрібна? 2020. URL: https://falcongaze.com/ua/pressroom/publications/dlp-sistemy/what-is-dlp.html

References:

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

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

3. An enterprise DLP that's easy to learn, deploy, and manage URL: https://www.acronis.com/en-us/products/devicelock

4. Bader S. What Is Data Loss Prevention and How Does It Work? 2022. URL: https://rewind.com/blog/data-loss-prevention/

5. Chapple M., Stewart J. M., Gibson D. (ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide. – John Wiley & Sons, 2018

6. Factum. Kolehiia detektyviv i fakhivtsiv bezpeky biznesu. Vytik informatsii. [Board of Detectives and Business Security Specialists. Information Leak] URL: ukr.detectiveua.com/vitik-inform [in Ukrainian].

7. Features of modern DLP systems. URL: forbes.com/sites/davidbalaban/2021/11/12/all-features-of-moderndlp-systems/?sh=27666e2e7618

8. Gurpreet Dhillon, Tiago Oliveira, Santa Susarapu, and Mario Caldeira. Deciding between information security and usability: Developing value based objectives. Computers in Human Behavior, 61:656–666, 08 2016.

9. Luther Martin. Understanding DLP. Auerbach Publications, (n.d).

10.McAfee Data Loss Prevention Endpoint. 2024. URL: https://softlist.com.ua/catalog/product-mcafee-dlp/

11.Reasons Why Your Business Needs (DLP) Data Loss Prevention. 2022 URL. https://uniserveit.com/blog/reasons-why-your-business-needs-dlp-data-lossprevention.

12.Symantec Data Loss Prevention. URL: static.carahsoft.com/concrete/files/9814/4734/5158/Data_Loss_ Prevention_Data_Insight_Enterprise.pdf

13.Symantec Data Loss Prevention Solution. URL: https://docs.broadcom.com/doc/data-loss-prevention-solution-en

14.Tanaka K. Transformer-based Models in Data Loss Prevention Systems. 2023. URL: https://www.cyberdatascience.com/transformers-dlp/

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

16.Zvit «Rozrobka ta vprovadzhennia typovykh rishen shchodo kompleksnoi systemy zakhystu informatsii v AIS NANU» (KSZI AIS NANU):

Systema upravlinnia intsydentamy informatsiinoi bezpeky. Kerivnytstvo administratora. (2009). Kyiv: 2009. 149 p.

17. Blyzniuk A.V. (2022). Doslidzhennia alhorytmiv morfolohichnoho analizu u DLP-systemakh dlia zapobihannia vytoku informatsii. [Research of morphological analysis algorithms in DLP systems to prevent information leakage]. Infokomunikatsiini ta kompiuterni tekhnolohii - Information communication and computer technologies, 2 (04), 143-148 [in Ukrainian].

18. Vovchanovskyi P.P., Demchynskyi V.V. (2020) Arkhitektura DLP-system v umovakh polityky BYOD. [Architecture of DLP-systems in terms of BYOD policy]. Teoretychni ta prykladni problemy fizyky, matematyky ta informatyky - Theoretical and applied problems of physics, mathematics and computer science, 151-154 [in Ukrainian].

19. Vprovadzhennia DLP-system. [Implementation of DLP systems]. (2024). Retrieved from https://techexpert.ua/our-services/implementation-of-dlp-systems/ [in Ukrainian].

20. Herzhan S. H., Masalska E. A. (2020). Poperedzhennia vytoku danykh z dopomohoiu DLP-system. [Prevention of data leakage with the help of DLP]. URL: ir.nmu.org.ua/bitstream/handle/123456789/148756/masalska_gerjan.pdf [in Ukrainian].

21. Zapobihannia vytoku danykh DLP. [Preventing data leakage DLP]. (2023). URL: https://www.kingston.com/ua/blog/data-security/data-loss-prevention-dlp [in Ukrainian].

22. Kuchmenko M.V., Hraivoronskyi M.V. (2017). Analiz kontspeptsii BYOD ta arkhitektura dlia yii vprovadzhennia. [Analysis of the BYOD concept and architecture for its implementation]. Teoretychni i prykladni problemy fizyky, matematyky ta informatyky - Theoretical and applied problems of physics, mathematics and computer science, 147 [in Ukrainian].

23. Pestierieva S.Ie., Chebotarova D.V. (2021). Analiz tekhnolohii zapobihannia vytoku informatsii. [Analysis of information leakage prevention technologies]. Problems of informatization - Problems of informatization, 67 [in Ukrainian].

24. Polotai O.I., Dovnanyk S. (2020). SIEM-systemy, yak element analizu ta upravlinnia podiiamy CSOC. [SIM-system, as an element of analysis and management of events of CSOC]. Avtomatyzatsiia ta kompiuterno-intehrovani tekhnolohii u vyrobnytstvi ta osviti : stan, dosiahnennia, perspektyvy rozvytku - Automation and computer-integrated technologies in production and education: status, achievements, development prospects, 60–61 [in Ukrainian].

25. Polotai O.I., Dubyk A.-O. (2024). Zahrozy informatsii v kompiuternykh merezhakh na kanalnomu rivni. [Information threats in computer networks at the channel level]. Svit naukovykh doslidzhen – The world of scientific research, 28, 185-187 [in Ukrainian].

26. Polotai O.I., Fedynets N.I., Kukharska N.P. (2024). Doslidzhennia zahroz informatsiinoi bezpeky ta sposobiv yikh vyrishennia v kompiuternykh merezhakh na kanalnomu rivni. [Studies of threats to information security and ways to solve them in computer networks at the channel level]. Visnyk Lvivskoho derzhavnoho universytetu bezpeky zhyttiediialnosti - Bulletin of the Lviv State University of Life Safety, 29, 184-187 [in Ukrainian].

27. Shcho robyty kompanii v razi vytoku informatsii? [What to do companies in the event of leakage of information?]. (2015). URL: https://uteka.ua/publication/news-14-delovye-novosti-36-shhorobiti-kompanii-v-razi-vitoku-informacii [in Ukrainian].

28. Shcho take DLP-systema i navishcho vona potribna? [What is a DLP system and why is it needed?]. (2020). URL: https://falcongaze.com/ua/pressroom/publications/dlp-sistemy/what-is-dlp.html [in Ukrainian].

Оглядова стаття.
Надійшла до редакції 30.10.2024.
Прийнято до публікації 18.12.2024.