НАЦІОНАЛЬНИ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВА ОСВІТИ І НАУКИ УКРАЇНИ
Кафедра комп'ютерних інтелектуальних систем та мереж

ЧИФЛІКЛІЙ Іван Іванович

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

РОЗРОБКА ТА ДОСЛІДЖЕННЯ СИСТЕМИ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

Спеціальність 123 – Комп`ютерна інженерія

Спеціалізація – Комп'ютерні системи та мережі

Керівник: Шапорін Володимир Олегович,
кандидат технічних наук, доцент

Одеса – 2021

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Чифліклій Іван Іванович
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи)___ Розробка та дослідження системи запобігання витоку інформації

керівник проекту (роботи)_____Шапорін В.О., ктн, доцент_____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом ректора ОНПУ від "_10__"____11_____2021 _року №__420-В_

2. Строк подання студентом проекту (роботи)_____1_грудня_2021_року_____

3. Вихідні дані до проекту (роботи)___завдання на розробку

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)__1) Дослідження існуючих засобів забезпечення запобігання витоку інформації

___2) Дослідження системи запобігання витоку інформації доступом

___3) Розробка системи запобігання витоку інформації

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання_____1 вересня 2021 року_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Дослідження існуючих засобів забезпечення		
	запобігання витоку інформації		
2	Дослідження системи запобігання витоку		
	інформації доступом		
3	Розробка системи запобігання витоку інформації		

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ _____
(підпис) (прізвище та ініціали)

Відомість кваліфікаційної роботи магістра

№ рядка	Найменування	Кільк.	Примітка
1	Пояснювальна записка	76	
2	Дослідження існуючих засобів забезпечення запобігання витоку інформації	1	
3	Функціональна схема шлюзового виду DLP , що працює у режимі	1	
4	блокування	1	
5	Функціональна схема шлюзового виду DLP , що працює в режимі	1	
6	моніторингу	1	
7	Функціональна схема хостового виду DLP		
8	Інформаційні потоки контрольовані DLP-системою	1	
9	Загальна схема локальної мережі з проксі-сервером.	1	
10	Схема послідовності кроків для утворення та забезпечення мережевого	1	
11	об’єднання.	1	
12	Загальний алгоритм аутентифікації з логіном та паролем	1	
13	Алгоритм створення словника для морфологічного аналізу	1	
14	Алгоритм морфологічного аналізу	1	
15	Алгоритм симетричного шифрування	1	
16	Схема гібридної архітектури DLP	1	
17			
18			
19			
20			
21			
22			
23			
24			

				АМДП.АМ161.1919		
Зм. Лист	№ докум.	Підпис	Дата			
Розробив	Чифлклій І.І.			*Розробка та дослідження системи запобігання витоку інформації*	Літ.	Лист 1 / Листів 1
Перевірив	Шапорін В.О.					
Реценз.					«Одеська політехніка»	
Н. Контр.					ІКС КІСМ АМ161	
Затвердив						

АНОТАЦІЯ

Чифліклій І.І. Розробка та дослідження системи запобігання витоку інформації– Магістерська дипломна робота. Одеса, 2021: 76с. , 25 рис., 3таб., 14 джерел.

Об'єкт дослідження – Існуючі DLP-системи.

Предмет дослідження – Системи запобігання витоку інформації.

Мета роботи – проведення дослідження існуючих технологій запобігання витоку інформації, та розробка методів та моделей системи попередження втрати даних. Це є необхідним для запобігання втрати конфіденційних даних організації, що можуть понести матеріальних або фінансових втрат.

У роботі був проведений аналіз існуючих рішень. Було розроблено програмне та інформаційне забезпечення системи запобігання витоку інформації, в результаті чого з’являється можливість моніторингу та блокування документів отриманих з глобальної мережі в режимі реального часу, що відповідно, підвищує шанс на виявлення потенційних втручань у систему конфіденційних файлів та збір більшої кількості інформації щодо типу втручання та спроби навмисного викрадення даних.

Також було розроблено архітектурну та структурну схему , що надасть можливість швидшого та ефективнішого впровадження системи до мережі споживача.

СИСТЕМА ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ, DLP-СИСТЕМА, ПРОКСІ-СЕРВЕР, МОРФОЛОГІЧНИЙ АНАЛІЗ, ШИФРУВАННЯ

ABSTRACT

Chyfliklii I.I. Research of remote laboratory access technology - Master's thesis. Odessa, 2021: 76p., 16 figs., 3tab 25 sources.

Object of research - Existing DLP-systems.

Subject of research - Information leakage prevention systems.

The purpose of the work - research of existing technologies to prevent information leakage, and development of methods and models of data loss prevention system. This is necessary to prevent the loss of confidential data of the organization, which may incur material or financial losses.

The analysis of existing solutions was carried out in the work. Leak prevention system software and information software have been developed, making it possible to monitor and block documents received from the global network in real time, which increases the chance of detecting potential intrusions into the confidential file system and collecting more information about such as interference and attempted data theft.

An architectural and structural scheme has also been developed, which will enable faster and more efficient implementation of the system in the consumer network.

INFORMATION LEAK PREVENTION SYSTEM, DLP SYSTEM, PROXY SERVER, MORPHOLOGICAL ANALYSIS, ENCRYPTION

ЗМІСТ

ВСТУП

Ефективність бізнесу в багатьох випадках залежить від підтримки конфіденційності, цілісності та доступності інформації. Одна з найактуальніших загроз у сфері інформаційної безпеки є витік конфіденційних даних від несанкціонованих дій користувачів.

Це пов'язано з тим, що більшість традиційних засобів захисту, такі як антивіруси, брандмауери та системи аутентифікації не здатні забезпечити ефективний захист від інсайдерів. Ціль такого роду порушників (інсайдерів) є передача інформації за межі компанії з метою його подальшого несанкціонованого використання – продажу, оприлюднення його у відкритому доступі тощо.

Технології, які дозволяють запобігти витоку конфіденційної інформації активно розвиваються. Ринок використовує все більш розгалужену термінологію: Information Leak Protection (ILP), Information Leak Protection (ILP), Information Leakage Detection & Prevention (ILDP), Content Monitoring and Filtering (CMF), , Extrusion PreventionSystem (EPS) та інші. Остаточним і найточнішим вважається термін акронім DLP (Data Leak Prevention). За аналог прийнято вживати словосполучення «системи захисту конфіденційних даних від внутрішніх загроз». До внутрішніх загроз включають як навмисні, так і ненавмисні зловживання працівниками своїми правами доступу до даних.

Системи захисту від витоку конфіденційної інформації призначені для відстеження та блокування спроб несанкціонованої передачі даних для корпоративної мережі. Система DLP може виконувати функції відстеження дій користувача, запис та аналіз їх спілкування через електронну пошту, соціальні мережі, чати тощо. Основним завданням систем DLP є забезпечення реалізації організаціями політики конфіденційності (захисту інформації від витоку).

Використання системи DLP найбільш актуально для організацій, де є ризик витоку конфіденційної інформації, що спричинить серйозні фінансові або репутаційні збитки, а також для організацій, які насторожено ставляться до лояльності своїх співробітників. Рішення класу DLP забезпечує захист конфіденційної інформації, такої як умови тендерів, замовлення на послуги, номери пластикових карток, інформація про рахунки клієнтів, персональні дані співробітників і клієнтів, фінансові дані тощо.

Основні функції DLP-систем:

– контроль передачі інформації через Інтернет: електронна пошта, протоколи HTTP (HyperTextTransferProtocol гіпертекст), HTTPS (HyperTextTransferProtocolSecure - розширення протоколу HTTP, що підтримує шифрування), FTP (FileTransferProtocol) передача файлів), Skype, Інтернет-сервіс миттєвих повідомлень Zoom та інші програми та протоколи;

– контроль за збереженням інформації на зовнішніх носіях - CD, DVD, флеш-дисках, мобільних телефонах тощо.

– захист інформації від витоку шляхом контролю виходу даних на друк через порти принтера (LPT), а також витік через порти модему (COM);

– блокування спроб відправки/збереження конфіденційних даних, інформування адміністраторів ІБ про інциденти, створення тіньових копій, використання папки карантину;

– пошук конфіденційної інформації на робочих станціях і файли сервери за ключовими словами, тегами документів, атрибутами файлів та цифровими відбитками;

– запобігання витоку інформації шляхом моніторингу життєвого циклу і переміщення конфіденційної інформації.

Система класу DLP включає такі компоненти:

– центр контролю та моніторингу;

– агенти на робочих станціях користувачів;

– DLP мережевий шлюз, встановлений на периметрі Інтернету.

Результат застосування таких систем:

– запобігання витоку та несанкціонованої передачі конфіденційної інформації.

– мінімізація ризиків фінансової та репутаційної шкоди;

– підвищення дисципліни користувачів;

– матеріал для розслідування інцидентів та їх наслідків;

– усунення загроз безпеці персональних даних, відповідності вимоги щодо захисту персональних даних.

На ІТ ринку є багато продуктів, які сприяють виявленню та запобіганню витоку конфіденційної інформації на певних каналах. Комплексні рішення охоплюють всі існуючі канали набагато менше. У цих умовах стає надзвичайно важливим питання вибору технології, що забезпечує захист від витоку конфіденційної інформації та даних з максимальною ефективністю та мінімальним обсягом помилкового спрацьовування.

Причиною стає все більше витоків важливих документів, занепокоєння багатьох керівників компаній, і це пов'язано з потребою і актуальністю систем DLP в даний час. Багато постачальників вже давно мають подібні технології. Попередні завдання, які система DLP мала вирішити, вважалися нерозв'язними технічні засоби, а самі системи були занадто складними для реалізації. Тепер продукція повністю відповідає більшості вимог.

Популярність DLP-систем зростає закономірно. Більшість компаній захистилися від зовнішніх загроз надовго і всіма можливими способами. Але актуальність загроз зсередини зростає з кожним роком. Ефективність систем захисту даних дуже висока, однак як і будь-яку іншу технологію ряд систеим запобігання витоку слід вдосконалювати. Це стосується виконання поставленого першочергового завдання розробників для DLP - зменшити кількість помилкових спрацьовувань для випадків витоку інформації, спровокованого ненавмисною необережністю.

Системи DLP зазвичай використовують три методи ідентифікації: ймовірнісний, детермінований та комбінований. На основі систем за першим методом здебільшого використовують лінгвістичний аналіз вміст і цифрові

відбитки даних. Такі системи легко реалізувати, але недостатньо ефективні і характеризуються високим рівнем хибності позитиви.

Системи, що використовують детермінований підхід (мітки файли) дуже надійні, але їм не вистачає гнучкості.

Комбінований підхід поєднує обидва методи з аудитом середовища зберігання та обробки, що дає змогу досягти оптимального вирішення проблеми захисту конфіденційність інформації.

Існує два основних підходи до контент-аналізу. Перший підхід заснований на фільтрація вмісту, тобто багатозначної інформації. Це означає, що при перевірці таємності стандартні документи офісу у форматі .doc, система спочатку переведе їх у текстовий формат, а потім, використовуючи попередньо підготовлені дані, відобразить рішення відповідно до цього тексту.

Контекстна фільтрація використовує принципово іншу схему: система перевіряє контекст, у якому передається інформація: витягує файли-мітки, дивиться на його розмір або аналізує поведінку користувачів.

Системи DLP необхідні для всіх компаній, які прагнуть запобігти витік критично важливої для бізнесу інформації. В першу чергу можна згадати банки та страхові компанії, які змушені виконувати вимоги регуляторів. Особливо для їхнього бізнесу Витік конфіденційних даних є актуальним, оскільки загрожує серйозними репутаційними ризиками.

Існує чотири критерії оцінки програмних продуктів, які реалізують функціональність DLP, що були розроблені ForresterResearch (незалежна дослідницька фірма, яка забезпечує об'єктивні даних про ринок нових технологій, а також проведення спеціалізованих консультації):

Багатоканальний. Рішення DLP не повинно бути лише зосереджено на один канал витоку. Це має бути комплексне рішення, що покриває максимальну кількість каналів: електронна пошта, Інтернет та миттєві повідомлення (миттєві повідомлення – система обміну миттєвими повідомленнями), а також моніторинг операцій з файлами;

Эдине управління. Система повинна мати уніфіковані елементи керування для всіх компонентів, які вона включає. їх, зазвичай три: сервер керування, який зберігає групові політики користувачів; пристрій, що контролює витік мережі та агенти для робочих станції, сервери, сховище файлів. Основна вимога другого - можливість керувати цими трьома компонентами з однієї консолі;

Активний захист. Система повинна не тільки виявляти витік конфіденційної інформацію, але й дають можливість її заблокувати;

Класифікація інформації з урахуванням як змісту, так і контексту. Витоки конфіденційної інформації повинні базуватися не тільки на зміст інформації, що надсилається, а також контекст, у якому вона надсилається.

1 ДОСЛІДЖЕННЯ ІСНУЮЧИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

В цьому розділі проводиться дослідження систем запобігання витоку інформації, основні фактори та канали витоки даних. Загальні заходи для забезпечення безпеки. Дослідження існуючих сучасних видів систем запобігання витоку інформації. Освітлюється питання важливості DLP систем та їх призначення у політиках конфіденційності даних підприємств. Розглядаються переваги та недоліки загальної архітектури системи та розповідається про історію розвитку DLP.

1.1.Основні фактори та канали витоку інформації

Канали витоку інформації існують у будь-якому інформаційному просторі. Канал витоку в найзагальнішому розумінні тлумачаться як неконтрольований спосіб передачі інформації. В результаті зловмисник може отримати несанкціонований доступ до потрібних йому конфіденційних даних компанії.

Витік даних відноситься до:

– розголошення даних особами, які мають доступ до секретної інформації;

– втрата флешок та інших типів носіїв даних, на яких зберігалася конфіденційна інформація;

– навмисне викрадення секретної інформації з використанням шпигунства проти відкритих каналів витоку.

Факт витоку конфіденційної інформації стає відомим не відразу. У результаті отримання комерційної таємниці підприємства конкурент може тривалий час не видавати себе і не поширювати дані. Однак факт крадіжки з

часом «випливає», що виражається у вигляді серйозних фінансових або матеріальних втрат для організації.

Загальна класифікація каналів витоку. Існують непрямі або прямі канали витоку інформації. Непрямі канали означають, що зловмисник має прямий доступ до технічного середовища конкретної системи інформаційної безпеки.

Приклади непрямих витоків:

– Втрата флеш-носія або його навмисна крадіжка.

– Пошук конфіденційних даних через спроби дослідити сміття, викинуті документи тощо.

– Зчитування паразитного електромагнітного випромінювання та перешкод.

– Спроба викрадення інформації за допомогою оптичних засобів: фотографування об'єктів інформаційної системи, прослуховування приміщень.

При взаємодії з прямими каналами зловмисник має доступ до обладнання та інформації, яка використовується в інформаційній системі.

Прямі канали витоку – найпоширеніше середовище для втручання інсайдерів. Самі працівники компанії, в більшості випадків, стають засобом передачі інформації зловмиснику. Це може статися навмисно або випадково. У першому випадку працівник свідомо влаштовується на роботу в організацію з метою подальшого розкриття секретів, у другому — ненавмисне розкриття відбувається в неформальній атмосфері[1].

Пряме копіювання інформації також називають витоком через прямі канали.

Для захисту даних в компаніях найчастіше задіяна одна основна автоматизована система, тому важливо враховувати всі технічні канали витоку, які передбачають варіанти крадіжки даних з використанням фізичних властивостей системи.

Типи технічних каналів витоку включають:

– акустична – несанкціоноване зчитування звуку на об'єкті інформаційної діяльності, наприклад, прослуховування телефонних розмов у реальному часі або запис розмов;

– акустоелектричний – зчитування за допомогою звукових хвиль, після чого інформація передається по електромережі, а на стороні зловмисника перетворюється в читабельну форму;

– оптичний канал – це варіант крадіжки даних, при якому шкідник фотографує або проводить тривале візуальне спостереження за об'єктом тощо;

– віброакустичний – зчитування коливань, створених акустикою при впливі на стіни, вікна та інші архітектурні конструкції;

– електромагнітні – видалення індуктивних датчиків з полів інформаційної системи; бічне електромагнітне випромінювання, яке зловмисник видаляє і за допомогою спеціального обладнання перетворює в зрозумілу форму.

Канал акустичного витоку – найпоширеніший та найнебезпечніший з точки зору зберігання конфіденційної інформації. Зафіксовані тисячі випадків, коли конкурентна компанія намагалась встановити пристрої прослуховування та звукозапису на іншому об’єкті. За допомогою спрямованих мікрофонів зловмисник може отримати доступ до аудіоінформації в кімнаті на відстані до 200 метрів від будівлі[2].

Універсальним каналом витоку інформації є акустоелектричний, оскільки його можна використовувати на будь-якому рівні електричної мережі; зловмиснику не потрібно використовувати додаткові мікрофони або радіопатчі для зчитування даних. Інформація збирається без прямого підключення до мережі; використовується випромінювання у вигляді електромагнітних хвиль. У деяких випадках жучки-підсилювачі можуть бути встановлені в будівлі компанії. Під час їх роботи конкурент легко зчитує магнітні хвилі на відстані до 300 метрів від джерела даних. Захист від впливу на акустоелектричний канал забезпечується так званим транспортним перехрестям, яке здатне створювати перешкоди, так що шкідник не може повністю прочитати інформацію.

Зловмисник може прослуховувати телефонні розмови в компанії. Для реалізації цього каналу витоку використовуються високочастотні пристрої накладання. В результаті телефонна лінія генерує модульований сигнал, який перехоплюється конкурентом.

Оптичний канал доступний, якщо робочий процес компанії можна візуально контролювати, фотографувати та знімати на відео. Захист в цьому випадку забезпечується обробкою конфіденційної інформації тільки в закритих приміщеннях без вікон з міцною звукоізоляцією.

Крім технічних каналів, існує фізичний спосіб крадіжки, який передбачає вилучення матеріального носія з конфіденційною інформацією.

1.2 Дослідження загальних заходів для забезпечення безпеки

Технології захисту вдосконалюються, частково завдяки інноваціям у таких областях, як машинне навчання та автоматизація. Однак кіберзлочинці однаково вправно використовують технічні досягнення у своїх інтересах. Це робить надзвичайно важливим для підприємств, щоб усі їхні бази були охоплені найкращою практикою, щоб забезпечити відповідну політику, методологію та процедури для підтримки надійного захисту від загроз[3].

З цією метою найефективніші IT-організації використовують найкращі методи безпеки мережі, щоб максимально підвищити ефективність своєї безпеки та захистити свої активи. Нижче наведено 10 основних найкращих практик, які кожна організація має використовувати для захисту своїх підприємств. Всі ці практики повинні підтримуватися постійно для забезпечення захисту своєї інформації. Цю практику слід регулярно переглядати для оцінки їх ефективності та, за потреби, коригувати, якщо обставини змінюються.

1. Аудит мережі та контроль безпеки.

Знання необхідні для підтримки безпечного середовища. Щоб мати точне уявлення про безпеку даного підприємства, IT-організації необхідно провести аудит мережі. За допомогою аудиту IT-фахівці можуть досягти наступного:

– визначити потенційні вразливості, які необхідно виправити;

– знайти невикористані або непотрібні програми, що працюють у фоновому режимі, які можна усунути;

– визначити потужність брандмауера та валюту його налаштування;

– вимірювати стан мережевих серверів, обладнання, програмного забезпечення та додатків;

– підтвердити загальну ефективність інфраструктури безпеки;

– і оцінити стан резервних копій сервера.

Аудит не повинен бути одноразовою подією. Це діяльністю, яка постійно проводиться протягом певного часу.

2. Дослідження політики безпеки.

Наявність прагматичної та дієвої політики безпеки є важливою для забезпечення міцної позиції безпеки. Часто організації не переглядають політику, щоб переконатися, що вони відповідають поточним вимогам бізнесу та умовам безпеки. І, на жаль, підприємства занадто часто не повідомляють про ці правила як до IT-персоналу, так і, якщо це можливо, до кінцевих користувачів. Такі організації, як SANS Institute, публікують довідкові документи, які IT-спеціалісти можуть використовувати під час перегляду й оновлення політики, наприклад, наявність офіційної директиви щодо введення та виконання змін.

3. Створення резервних копій даних і створення плану відновлення.

На підприємствах існують ситуації, коли їх безпека знаходиться під постійною загрозою, це зумовлено слабкою або взагалі відсутністю системи безпеки та захисту інформації. Важливо створювати резервні копії як важливих для роботи, так і дуже конфіденційних даних. Оскільки атаки програм-вимагачів стають все більш загрозливими, що впливають на організації в різних галузях, не менш важливо мати в межах найкращих методів безпеки мережі стратегію відновлення, яка мінімізує час простою та обмежує витрати.

4. Шифрування критичних даних.

Шифрування даних є ще одним важливим елементом захисту найціннішої та конфіденційної інформації організації. IT-організаціям необхідно періодично оцінювати класифікацію даних і використовувати шифрування, якщо це необхідно. VPN можуть забезпечити ще один рівень захисту для співробітників, яким, можливо, доведеться отримати доступ до конфіденційних файлів з віддалених місць.

5.Оновлення програмного забезпечення для захисту від шкідливих програм.

Застаріле антивірусне програмне забезпечення є одним із найпоширеніших недоліків у безпеці підприємства. Він також є одним із найпростіших для вирішення. Фахівці з безпеки повинні періодично перевіряти своє програмне забезпечення для захисту від шкідливих програм, щоб переконатися, що на всіх пристроях запущено найновіший програмне забезпечення безпеки. ІТ також має автоматизувати управління виправленням, коли це можливо.

6. Встановлення відповідних засобів контролю доступу та використовуйте багатофакторну аутентифікацію.

Ефективне керування доступом починається з наявності правильних політик, що визначають які користувачі та пристрої мають право доступу до певних ресурсів. Використання систем управління загальним доступом і привілейованого права для контролю того, хто може отримувати інформацію, є важливим. Ефективне керування паролями також є частиною найкращих методів безпеки мережі. Паролі мають містити не менше 10 символів і часто змінюватися. Системи керування паролями можуть допомогти спростити цей процес. Багатофакторна аутентифікація є ще одним важливим інструментом, який перевіряє, що лише відповідний користувач має доступ до належного ресурсу.

7. Створення структури управління безпекою.

Дотримання не обов’язково означає безпеку, але воно може дати важливі вказівки щодо захисту від ризиків. Регулюючі органи, такі як Міжнародна організація зі стандартизації та Рада зі стандартів безпеки індустрії платіжних карток, підкреслюють важливість створення організації, яка визначає, хто відповідає за управління безпекою та реагування на події кібербезпеки. ІТ-організаціям необхідно визначити відповідні обов’язки окремих осіб щодо управління ризиками та реагування на інциденти. Виконання періодичної оцінки ризику може допомогти організаціям визначити пріоритети усунення вразливості і мінімізувати час простою.

8. Розвідок рівня свідомості кінцевих користувачів.

Фішингові атаки є перевагою методології багатьох кібератак, підвищення обізнаності кінцевих користувачів має вирішальне значення. У 2017 році в опитуванні корпоративних співробітників, проведеному Dell, понад 75% визнали, що за певних обставин охоче поділилися б конфіденційними даними. Кінцеві користувачі мають схильність ставати жертвами певних типів атак, які імітують звичайне спілкування. Кіберзлочинці стають все більш вправними у використанні електронної пошти та інших форм-факторів для точного відображення професійної взаємодії, ймовірність того, що співробітник піддасться загрозі, зростає. Щоб інформувати співробітників про мінливе середовище загроз і пов'язану з ними політику корпоративної безпеки, навчання кінцевих користувачів має бути постійним процесом, який є невід'ємною частиною культури компанії.

9.Система обслуговування інфраструктури безпеки.

IT-організаціям слід підходити до безпеки як до безперервної роботи, яка вимагає постійних перевірок, щоб переконатися, що всі системи та засоби контролю працюють належним чином. Наслідком таких дій є організація підприємств, що повинні мати процедури, щоб їх інфраструктура була актуальною та в належному робочому стані. Системи безпеки необхідно контролювати та регулювати, коли трапляються інциденти. IT-організації повинні прийняти механізми, які схвалюють і повідомляють про зміни в політиках і практиках безпеки.

10.Організація DLP системи

Запобігання витоку даних (DLP) – це підхід, який спрямований на покращення інформаційної безпеки та захисту інформації від її витоку або викрадення. Це запобігає переміщенню кінцевих користувачів ключової інформації за межі мережі. DLP також відноситься до інструментів, які дозволяють адміністратору мережі контролювати дані, до яких мають доступ кінцеві користувачі.

1.3.Поняття DLP-систем та їх призначення

Запобігання втраті даних є одним із найбільш розповсюджених і найменш зрозумілих інструментів в арсеналі безпеки. Кінцева цінність DLP систем може бути недооцінена в залежності від розуміння функціонала, що він охоплює та можливості зменшення збитків компанії залежно від цінності її конфіденційних даних.

Діяльність сучасних організацій вимагає зберігання та використання все більших обсягів інформації, чому сприяє зниження вартості обчислювальної потужності, пропускної. Можливості мереж та систем зберігання. Зростають ризики витоку інформації, тиск з боку регулюючих органів та очікування зацікавлених осіб щодо захищеності інформації. Розголошення конфіденційної інформації може призвести до збитків, спричинити собою передбачену законодавством відповідальність, а також пошкодити репутації за рахунок публікацій у ЗМІ та широкого суспільного розголосу. З урахуванням зростаючих ризиків промислового шпигунства та крадіжки інтелектуальної власності організаціям необхідно вжити наступні негайні заходи[4]:

– визначити інформацію, що використовується;
– оцінити наслідки та ймовірність витоку;
– виробити стратегію запобігання витоку;
– впровадити засоби, що бракують захисту інформації.

Розуміння технології та потреб свого підприємства може дати більшу повноту картини у якості вибору щодо конкретної DLP системи.

DLP – це підліткова технологія, яка забезпечує значну цінність для тих організацій, які її потребують, незважаючи на продукти, які для багатьох сучасних компаній дані є, мабуть, найціннішим товаром.

Методи запобігання втрати даних (DLP) – це методи, які компанія або організація використовує для захисту даних. Часто це передбачає використання програмного забезпечення для запобігання втраті даних у поєднанні з роботою мережевих адміністраторів і технічних спеціалістів[5].

В назві даного підходу є слово «втрата», однак методи DLP зосереджені на запобіганні викрадення даних кіберзлочинцями через порушення даних. Вони також працюють, щоб запобігти переміщенню даних із мережі без дозволу співробітникам та іншим особам у мережі компанії.

Організації покращать безпеку своїх мереж, встановлюючи системи DLP на своїх підприємствах. У той же час адміністратори мережі матимуть можливість контролювати використання даних, гарантуючи, що ніхто не має неналежного доступу до певних типів даних.

Одним з ключових аспектів систем запобігання втраті даних є сканування файлів і даних для визначення найбільш чутливих елементів. Адміністратор мережі може використовувати програмне забезпечення DLP для забезпечення додаткового захисту цих елементів.

Система запобігання витоку даних (або запобігання втраті даних) — це програмне забезпечення, яке визначає, виявляє та відстежує конфіденційні дані та запобігає їх виходу з локального середовища. Впровадження рішення DLP вимагається такими галузевими стандартами безпеки, як HIPAA, GLBA, PCI DSS, SOX і FISMA.

Рішення DLP забезпечує активний або пасивний моніторинг. Існує три основних типи активних DLP залежно від середовища розгортання: мережа, кінцева точка або хмарний сервіс.

Мережевий DLP розгортається на сервері або постачається як фізична коробка і контролює все, що відбувається всередині мережі.

DLP кінцевої точки розгортається на кожній кінцевій точці і контролює лише одну машину.

Хмарний DLP розгортається на віртуальному сервері і контролює діяльність організації у приватній хмарі.

Усі три типи сканують середовище (мережу, кінцеву точку або хмарний сервер) для виявлення конфіденційних даних. Кожне рішення DLP має свій власний алгоритм виявлення на основі політики класифікації даних. Ця політика визначає типи та формати даних, які вважаються конфіденційними для певної

організації. Програмне забезпечення DLP шукає такі типи даних і контролює їх [6].

Деякі рішення DLP можуть самостійно ідентифікувати поширені типи конфіденційної інформації (наприклад, облікові дані, номери кредитної картки та соціального страхування, особисту інформацію). Таке рішення забезпечує вам ретельне сканування мережі, однак це може залишити конфіденційні дані непоміченими.

Пасивне рішення DLP відстежує та записує мережеву активність замість моніторингу даних. Він надає адміністраторам об’ємні журнали всіх дій у мережі. Такі рішення корисні для моніторингу активності, розслідування інцидентів та усунення проблем у мережі.

NIST окреслює такі типи втрати даних, які покриваються рішенням DLP:

Витік даних – найпоширеніший тип втрати даних, витік даних є порушенням конфіденційності, коли конфіденційні дані стають загальнодоступними. Це відбувається, коли хакери розміщують конфіденційні дані компанії в Інтернеті [7].

Зникнення даних – це коли інформація видаляється з серверів компанії. Наприклад, незадоволений співробітник з привілейованим обліковим записом може стерти важливі дані.

Пошкодження даних – це коли інформація змінена або зашифрована. Найпоширенішим сценарієм цієї форми втрати даних є атака програмного забезпечення шляхом шифруванням.

Згідно з документацією NIST, DLP захищає дані в одному з таких станів:

– У стані спокою – дані, що зберігаються на жорсткому диску, сервері, базі даних тощо.

– На кінцевій точці – дані, які використовуються співробітниками на своїх пристроях.

– У русі – дані, що надсилаються за межі мережі компанії будь-яким способом зв’язку.

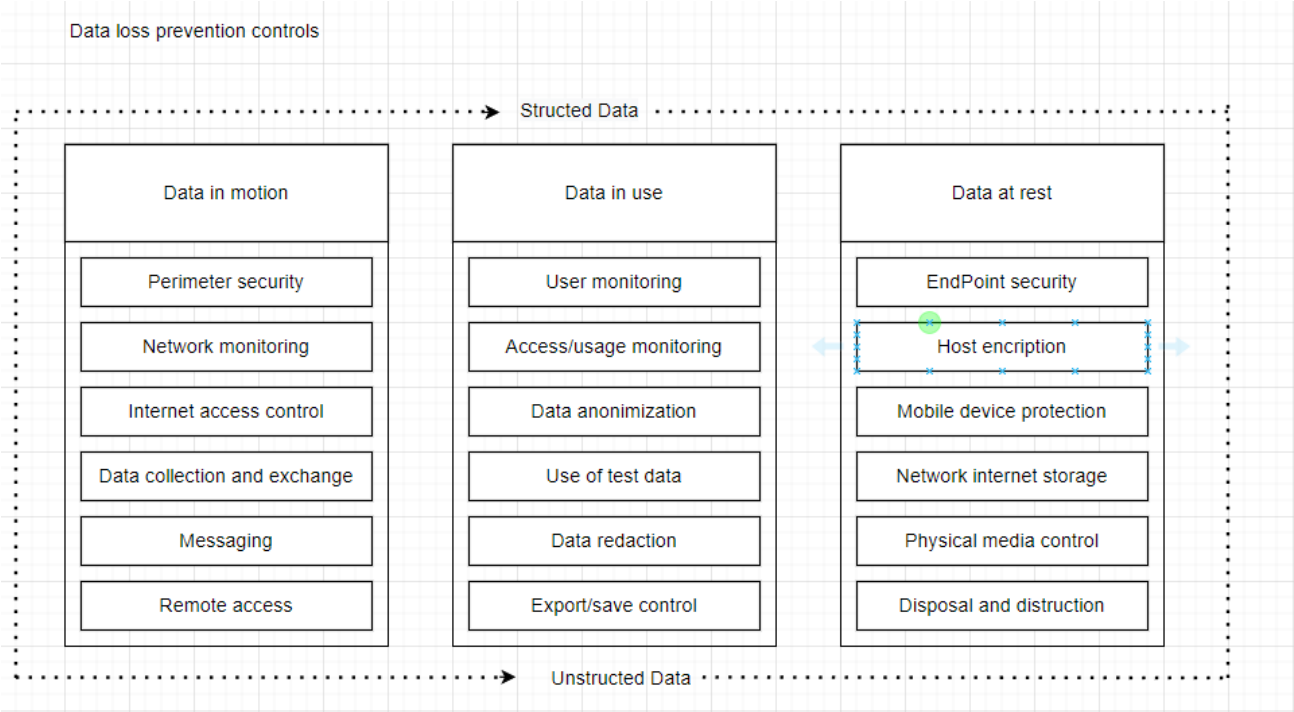

Рисунок 1.1 Контроль запобігання втраті даних

1.3.1 Переваги DLP системи

Стандартні заходи безпеки включають брандмауер, систему виявлення вторгнень і антивірусне програмне забезпечення. Це механізми, які захищають комп'ютери від внутрішніх і зовнішніх атак.

Додавання рішення DLP до вашої системи кібербезпеки надає вам наступні переваги:

1. DLP ефективний для виявлення зовнішніх і внутрішніх загроз. Він використовує брандмауер для обмеження зовнішнього доступу до внутрішньої мережі. Зовнішні атаки можуть бути виявлені програмним забезпеченням DLP за допомогою антивірусного сканування, щоб знайти троянські програми, встановлені на кінцевих точках, і зловмисне програмне забезпечення, яке проникає в мережу компанії через вкладення електронної пошти. Він пом'якшує інсайдерські загрози шляхом постійного моніторингу даних, виявляючи випадки, коли зловмисники порушують дані. Він також шифрує всі дані, скопійовані на USB-пристрої або відправлені за межі мережі[8].

2. Рішення DLP запобігають спробам копіювати чи надсилати конфіденційні дані без авторизації. Інформацію, яка класифікується як конфіденційна, можна

3.Системи DLP надають корпораціям бачення того, що відбувається з будівлі. Вони забороняють користувачам надсилати конфіденційні дані. Маючи систему DLP, ви можете побачити, хто намагається надіслати інформацію, і, можливо, зупинити злом даних, перш ніж він може завдати занадто великої шкоди.

4.Деякі DLP використовують алгоритми машинного навчання для визначення нових конфіденційних даних. Постійний аналіз внутрішнього вмісту допомагає точно визначити всі дані, які потрібно захистити. Ця ж технологія дозволяє виявляти незвичайні запити на доступ і обмін даними між співробітниками. Для цього найкраще використовувати спеціальне рішення для моніторингу активності користувачів або аналітики поведінки користувачів і сутностей.

1.3.2. Недоліки DLP системи

Якщо у вашій компанії є програмне забезпечення DLP, є ризик, що воно може залишити прогалини у вашій корпоративній безпеці. Ви можете відчути, що все захищено, тому не потрібно застосовувати інші заходи безпеки; але це відчуття насправді може бути помилковим відчуттям безпеки.

Використовуючи рішення DLP, необхідно звернути увагу на наступні фактори:

1. Система DLP не принесе користі компанії, якщо не знати, де зберігаються ваші дані. Для того , щоб мати все під контролем потрібно провести інвентаризацію як секретних, так і несекретних даних. Потім перерахуйте, хто має доступ до секретних даних. Деякі рішення DLP пропонують автоматичне сканування та виявлення конфіденційних даних у корпоративній мережі. Але через специфічні робочі процеси та типи даних у кожній компанії, можливо, краще позначати дані вручну.

2. Система DLP – це бізнес-продукт, а не технологічний проект. Після того, як ваша компанія зобов’язується придбати систему DLP, починається важка робота, оскільки рішення DLP важко розгорнути. Щоб зрозуміти, які дані варто

відстежувати, вашому IT-відділу потрібен вичерпний огляд потоків даних у вашій компанії.

3. Користувачам у вашій мережі призначаються різні привілеї доступу. Вам потрібно перевірити всі рівні привілеїв і переконатися, що рішення DLP здатне відрізнити звичайного користувача від привілейованого.

4. Якщо компанія не витрачає час на визначення стратегії захисту даних і розробку основних технічних і бізнес-вимог, система DLP не буде ефективною. Визначення та впровадження комплексної політики запобігання витоку даних займає багато часу. Нечітка політика спричиняє проблеми з інтеграцією DLP у вашу систему кібербезпеки та додає накладні витрати.

5. Немає стандартного набору функцій. Деякі рішення не відстежують обмін файлами через Dropbox або месенджери, але інші роблять. Розгортання мережевого DLP допомагає захистити інформацію всередині локальної мережі. Але якщо співробітникам потрібно брати свої ноутбуки у відрядження або працювати з дому, дані на цих машинах не будуть захищені.

1.4.Дослідження видів DLP-систем та принципи їх функціонування

Сучасні DLP-системи мають величезну кількість параметрів і характеристик, які необхідно враховувати при виборі рішення для захисту конфіденційної інформації від витоку. Але, найважливішим з них є використовувана мережева архітектура. За цим параметром продукти розглянутого класу поділяються на дві великі групи: шлюз і хост.

У першому використовується єдиний сервер, на який спрямовується весь вихідний мережевий трафік корпоративної інформаційної системи. Цей шлюз обробляє його для виявлення можливих витоків конфіденційних даних.

Другий варіант заснований на використанні спеціальних програм - агентів, які встановлюються на кінцевих вузлах мережі - робочих станціях, серверах додатків і т. д.

Системи DLP хоста і шлюзу розвивалися паралельно, не заважаючи одна одній. При цьому вони були призначені для захисту від різних типів загроз: шлюзові використовувалися для контролю мережевого трафіку, а хости використовувалися для моніторингу локальних пристроїв, які можна використовувати для передачі інформації. Таким чином, для повного захисту корпоративної мережі необхідно було використовувати два рішення разом.

1.5.Шлюзові DLP-системи

Шлюзові DLP-системи базуються на використанні шлюзів-централізованих серверах для обробки мережного трафіку. Область застосування таких рішень значно обмежена у зв’язку з принципом даного підходу. Системи шлюзів дозволяють захиститися від зловмисників лише при умовах витоку інформації через традиційні інтернет протоколи: HTTP, FTP, POP3 та SMTP, які ця система контролює. Також ця система не має можливості контролювати процес обміну інформації на кінцевих точках.

Почати треба з простоти введення в експлуатацію, обслуговування та управління. Шлюзова система може бути підключена до віддаленого сервера або звичайного ПК (у невеликих мережах), який може бути встановлений між робочими станціями корпоративної мережі та проксі-серверами. При цьому весь мережевий трафік спочатку йде до системи DLP, тому ви маєте контроль над цим аспектом: пропустити або заблокувати. Пропущені пакети надсилаються на проксі-сервери а згодом і в Інтернеті. Тому IT-персонал повинен налагодити DLP продукт і пере скорегувати напрям трафіку з робочих станцій до нього. Функціональна схема шлюзового рішення, що працює в режимі блокування, представлена на рисунку 1.2.

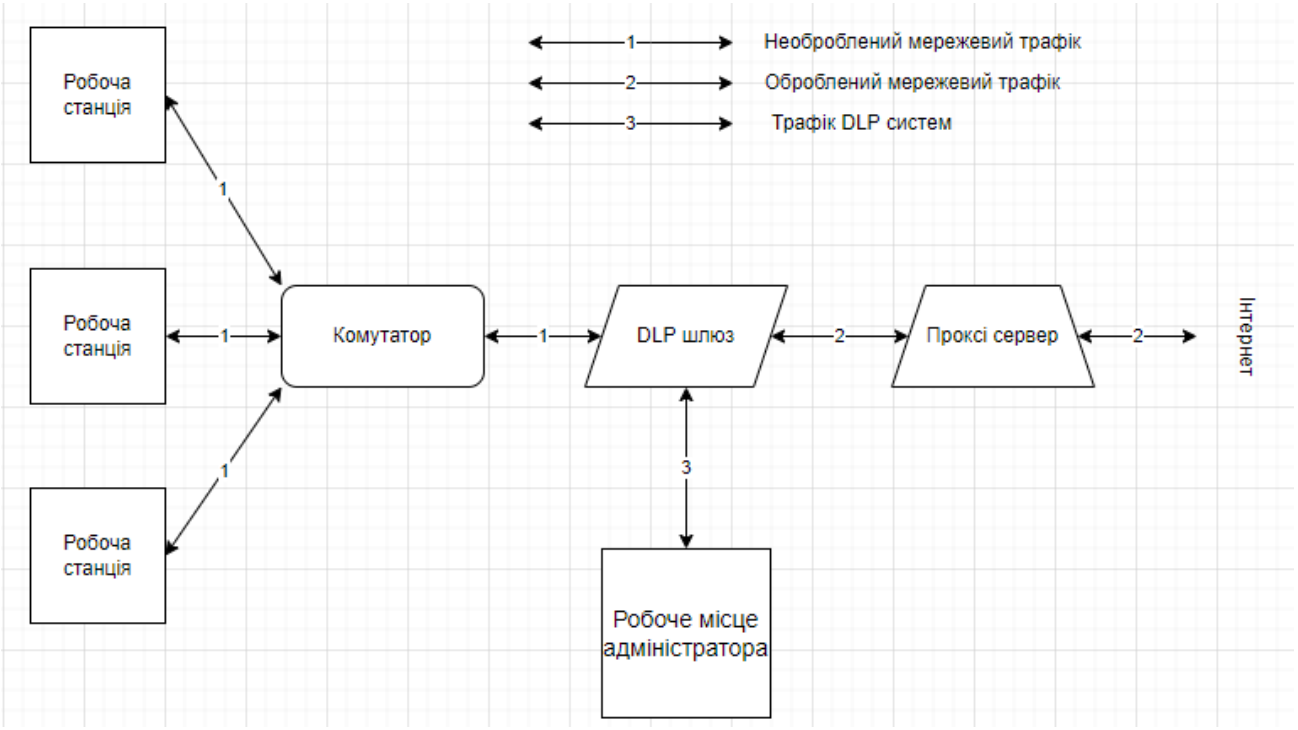

Рисунок 1.2 Функціональна схема шлюзового рішення, що працює у режимі блокування

Існує ще один варіант реалізації системи шлюзу DLP. Принцип даного підходу базується на тому, що він обробляє не прямий, а дубльований трафік. У цьому випадку система захисту може працювати тільки в режимі моніторингу. У ньому підозрілий трафік не блокується, а зберігається в журналі для подальшого аналізу працівниками відділу інформаційної безпеки. У цьому випадку процес реалізації ще простіше. Вам просто потрібно налаштувати систему DLP і направити до неї трафік, наприклад, за допомогою керованого комутатора з портом дублювання.

Функціональна схема рішення шлюзу, що працює в режимі моніторингу, показано на рисунку 1.3.

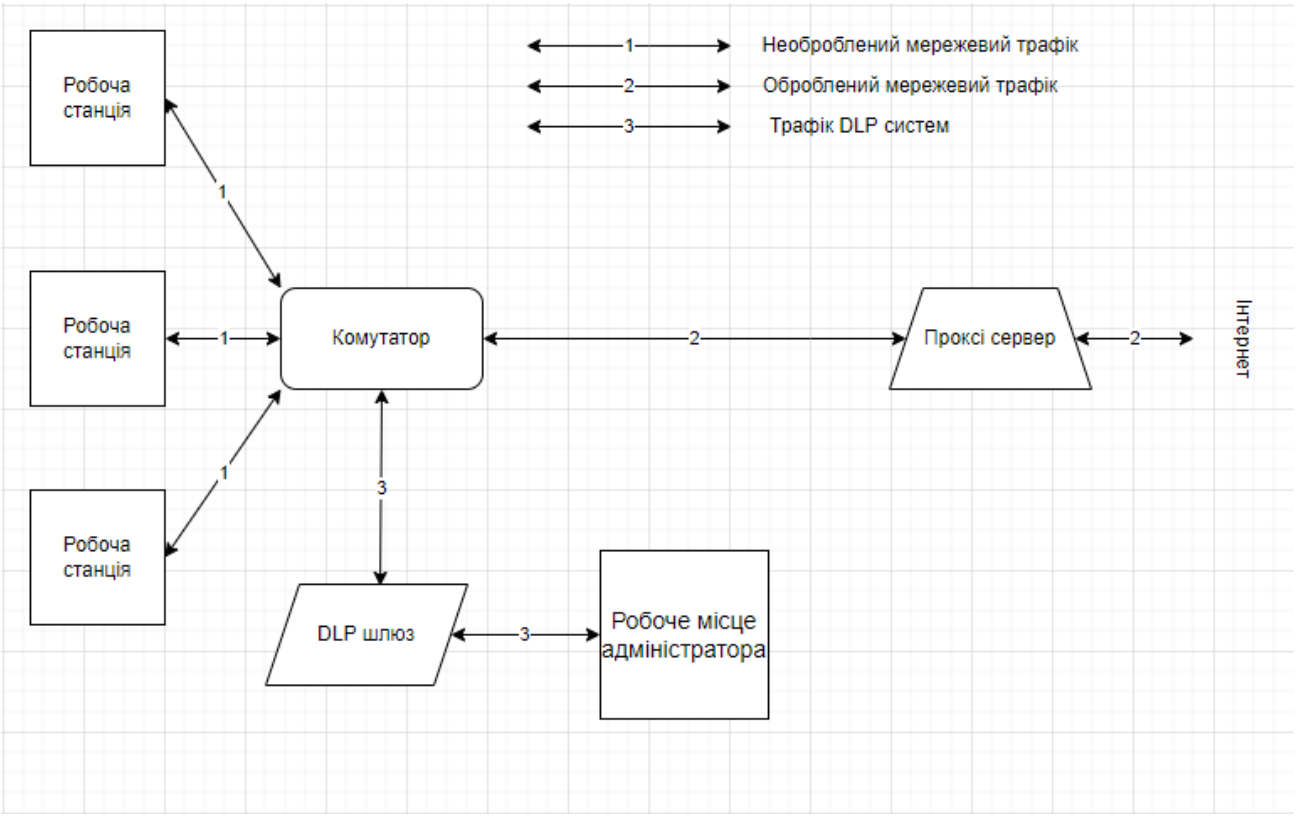

Рисунок 1.3 Функціональна схема шлюзового рішення, що працює в режимі моніторингу.

Перша схема, яка дозволяє не тільки ідентифікувати, а й запобігти витоку конфіденційної інформації, однозначно краща. Однак вона використовується відносно рідко. Проблема полягає в значному скороченні каналу зв'язку, який контролюється системою DLP. Тут є два ризики. По-перше, це можливість помилкових спрацьовувань при блокуванні легально переданих даних. По-друге, ризик виходу з ладу самої системи DLP (а це трапляється, особливо при високих навантаженнях), при якій буде заблокований весь канал.

Перша схема може вплинути на безперервність бізнес-процесів компанії. Саме тому такий підхід використовується значно рідше, ніж простий моніторинг мережевого трафіку, і майже ніколи не використовується у великих організаціях.

Використання лише одного комп'ютера в системі DLP-шлюзу значно полегшує його обслуговування. Усі використовувані правила та політики обробки трафіку застосовуються одноразово, після чого вони негайно вступають в силу для всіх співробітників організації.

Ще однією перевагою систем DLP-шлюзу є високий ступінь захисту від несанкціонованого втручання в його роботу з боку користувачів корпоративної мережі - відключень, зміни політик безпеки тощо. Працюючи на окремому сервері, він недоступний нікому, крім обслуговуючого персоналу та працівники відділу інформаційної безпеки.

Недоліки систем DLP-шлюзу. Крім обмеженої області застосування, вони включають проблемне управління деякими типами мережевого трафіку. Особливо великі труднощі виникають із зашифрованими мережевими пакетами, що передаються за протоколами сімейства SSL. Також можна відзначити неможливість перехоплення трафіку системи Skype (вона також використовує шифрування трафіку), яка останнім часом набирає популярності в нашій країні.

1.6.Дослідження хостових DLP систем

Основні системи DLP базуються на використанні спеціальних агентів, які встановлюються на кінцевих точках корпоративної мережі. Ці програми відіграють відразу дві ролі.

Вони контролюють діяльність користувачів комп’ютерів, не дозволяючи їм виходити за межі встановленої політики безпеки (наприклад, забороняючи копіювати будь-які файли на «флешки»). Вони реєструють всі дії операторів і переносять їх у централізоване сховище, дозволяючи відділу інформаційної безпеки отримати повну картину того, що відбувається.

Використання програм-агентів обмежує сферу дії хост-систем DLP: вони можуть бачити лише локальні або мережеві пристрої, підключені безпосередньо до комп’ютерів, на яких вони працюють. Функціональна схема основного рішення DLP показана на малюнку 1.4.

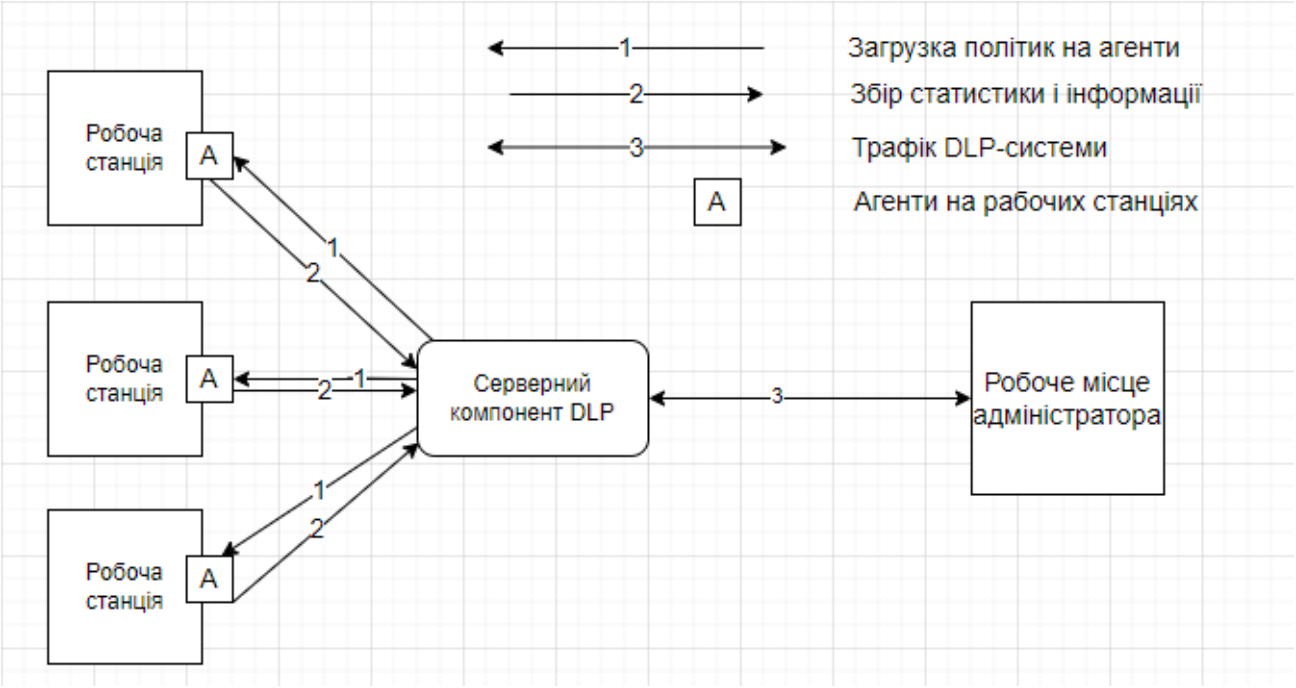

Рисунок 1.4 Функціональна схема хостового DLP-рішення

Переваги хост-систем DLP включають широкі можливості керування користувачами. Працюючи безпосередньо на кінцевих станціях корпоративної мережі, вони можуть не тільки контролювати «поза мережеві» канали витоку конфіденційної інформації, але й виконувати цілий комплекс інших функцій. Деякі розробники системи DLP використовують цю функцію, наприклад, для виявлення випадків неправомірного використання комп'ютерів співробітниками.

Основним недоліком хост-систем DLP є більш складний процес впровадження та подальшого адміністрування. При їх розгортанні необхідно не тільки встановити і налаштувати серверний компонент, але і встановити програму-агент на кожен комп’ютер корпоративної мережі. Не обов’язково обходити кожен ПК і вручну запускати на ньому дистрибутив. Розробники системи DLP пропонують способи автоматичної установки агента. Найбільш часто використовувані функції серверного компонента або групової політики Windows.

Усі вищеописані поняття розповсюджуються і на адміністраторів. Для роботи агенти використовують політики, завантажені безпосередньо на локальні комп’ютери, на яких вони встановлені.

Щоразу, коли правила безпеки змінюються, адміністратор повинен переконатися, що вони поширюються на всі кінцеві точки в мережі. Зазвичай це робиться за допомогою серверного компонента або групових політик Windows.

Хост-системи DLP менш захищені від несанкціонованого втручання в їх роботу з боку користувачів мережі. Працюючи на комп'ютері, до якого співробітник організації має прямий доступ (а часто і права локального адміністратора), програма агента потенційно може бути вивантажена з пам'яті. У цьому випадку ПК випадає з-під контролю системи DLP. Розробники намагаються захистити свою продукцію від такого втручання. Для цього використовуються різні інструменти для контролю завантаженості та безперервності всіх встановлених агентів, надсилання сповіщень адміністраторам безпеки при виникненні потенційно небезпечної ситуації. Проте повністю усунути ризик втручання неможливо.

DLP-системи також існують і в універсальній формі для розширення власних функціональних можливостей. На ринку не залишилося або майже не залишилося рішень, які можна було б назвати суто рішеннями хоста або шлюзу. Навіть ті розробники, які тривалий час розвивали лише один напрямок, додають до своїх рішень модулі іншого типу. Наприклад, три роки тому, на додаток до суто хост-рішення Zlock, Zecurion (раніше SecurIT) випустила продукт керування мережею Zgate. Обидва вони керуються з єдиної консолі управління (як і інші продукти Zecurion, це одна з особливостей цього виробника). Не відстає від своїх конкурентів і DeviceLock, який доповнив своє рішення модулем управління мережею[9].

Один з останніх кроків до універсалізації зробили виробники рішення Dozor Jet DLP. Це одна з провідних систем на нашому ринку, яка донедавна була виключно мережевою. Але він також придбав програму агента в її останній версії.

Існує дві причини переходу до універсалізації рішень DLP.

Перший – це різні сфери застосування для різних типів систем. Як ми вже говорили, хост-рішення DLP дозволяють контролювати всі види локальних і мережевих – Інтернет каналів витоку конфіденційної інформації. Оскільки в

переважній більшості випадків організація потребує повного захисту, вона потребує і того, і іншого. Продаючи тільки «чисті» DLP-системи певного типу, розробники самостійно обмежують свій ринок і, як наслідок, отримують менший прибуток. Зрештою, компанії зазвичай намагаються придбати відповідні системи захисту від одного виробника і, бажано, з одним керівництвом, оскільки це робить процес обслуговування легшим і дешевшим. Універсалізація дозволяє розробникам збільшити продажі своєї продукції.

Другою причиною універсалізації є деякі технологічні особливості та обмеження, які не дозволяють суто шлюзовим DLP-системам повністю контролювати всі необхідні Інтернет канали. Прикладом є Zoom. Цей комунікаційний засіб останнім часом все частіше використовується в бізнес-процесах, в деяких випадках навіть повністю (або майже повністю) замінюючи Skype. Однією з ключових особливостей Zoom є передача трафіку по закритому протоколу в зашифрованому вигляді. Як наслідок, системи DLP суто шлюзів не можуть контролювати цей потенційно небезпечний канал - вони просто не можуть розшифрувати перехоплений мережевий трафік. У цьому випадку на допомогу приходить програма-агент, встановлена на клієнтських комп'ютерах. Володіючи широкими правами, він може грати роль «шпигуна», перехоплюючи не тільки текст повідомлень, а й голосовий трафік і передаючи все це безпосередньо на базу системи DLP. Такий підхід використовується.

Універсалізація рішень DLP вигідна всім. Розробники отримують додатковий ринок і можуть збільшити продажі своєї продукції. Ну а кінцеві користувачі, тобто організації, які потребують захисту від витоку конфіденційної інформації, отримують системи, які простіші в розгортанні та експлуатації та можуть контролювати всі потенційно небезпечні канали передачі даних.

На ринку не існує «чистих» систем DLP через їх неповноцінність, які використовують лише шлюз або хост. Всі найпопулярніші рішення в світі є універсальними. Це вигідно всім. І розробники, які отримують можливість збільшити свій дохід, і споживачі, які отримують більш зручні та надійні системи захисту.

Проте в деяких випадках дійсно можна обмежити систему захисту лише однією частиною. Це стосується ізольованих мереж, які не підключені до Інтернету. Вони можуть використовувати лише розміщене рішення DLP. Це також можливо, якщо використання глобальної мережі в організації суворо обмежено як адміністративними заходами, так і технічними засобами. Тому існує можливість надана розробниками дозволяється купувати системи DLP хостів і шлюзів незалежно один від одного. На щастя, вони випускаються у вигляді додаткових модулів, або як окремі продукти з єдиним управлінням.

1.7.Етапи розвитку DLP-систем

Ринок DLP систем почав формуватися вже цього століття. саме поняття "DLP" поширилося приблизно 2006 року. Найбільше компаній, створювали DLP системи, виникло США. Там був найбільший попит на ці рішення та сприятлива обстановка для створення та розвитку такого бізнесу[10].

Згодом змінилися і характер загроз, і склад замовників та покупців DLP-систем. Сучасний ринок пред'являє до цих систем такі вимоги:

– підтримка кількох способів виявлення витоку даних (Data in Use, Data - in Motion, Data-at Rest);

– підтримка всіх популярних мережевих протоколів передачі: HTTP, SMTP, FTP, OSCAR, XMPP, MMP, MSN, YMSG, Skype, різних P2P протоколів;

– наявність вбудованого довідника веб-сайтів і коректна обробка трафіку, що передається на них (веб-пошта, соціальні мережі, форуми, блоги, сайти пошуку роботи і т.д.);

– бажана підтримка тунелюючих протоколів: VLAN, MPLS, PPPoE, та їм подібних;

– прозорий контроль захищених SSL/TLS протоколів: HTTPS, FTPS, SMTPS та інших;

– підтримка протоколів VoIP телефонії: SIP, SDP, H.323, T.38, MGCP, SKINNY та інших;

– наявність гібридного аналізу - підтримки кількох методів розпізнавання цінної інформації: за формальними ознаками, за ключовими словами, збігом вмісту з регулярним виразом, на основі морфологічного аналізу;

– бажана можливість вибіркового блокування передачі критично важливої інформації з будь-якого контрольованого каналу в режимі реального часу; виборче блокування (для окремих користувачів, груп або пристроїв);

– бажаною є можливість контролю дій користувача над критичними документами: перегляд, друк, копіювання на зовнішні носії;

– бажаною є можливість контролювати мережеві протоколи роботи з поштовими серверами Microsoft Exchange (MAPI), IBM Lotus Notes, Kerio, Microsoft Lync і т.д. для аналізу та блокування повідомлень у реальному часі за протоколами: (MAPI, S/MIME, NNTP, SIP тощо);

– бажаний перехоплення, запис та розпізнавання голосового трафіку: Skype,Zoom, IP-телефонія, Microsoft Lync;

– наявність модуля розпізнавання графіки (OCR) та аналізу вмісту;

– підтримка аналізу документів кількома мовами;

– ведення докладних архівів та журналів для зручності розслідування інцидентів;

– бажано наявність розвинених засобів аналізу подій та їх зв'язків;

– можливість побудови різної звітності, включаючи графічні звіти.

Завдяки новим тенденціям у розвитку інформаційних технологій стають затребуваними і нові функції DLP продуктів. З широким розповсюдженням віртуалізації в корпоративних інформаційних системах виникла потреба її підтримки та в DLP рішеннях. Повсюдне використання мобільних пристроїв як інструмент ведення бізнесу стало стимулом для виникнення мобільного DLP. Створення як корпоративних, і публічних " хмар " зажадало їх захисту, зокрема і DLP системами. І як логічне продовження призвело до появи "хмарних" сервісів інформаційної безпеки[11].

Ринок DLP-систем почав формуватися вже в цьому столітті. саме поняття "DLP" поширилося приблизно 2006 року. Найбільше компаній, створювали DLP системи, виникло США.

Однією з компаній лідерів виробників DLP-систем із зарубіжних компаній є Symantec Corp., На російському ринку популярні продукти розробників DLP-систем: SearchInform, InfoWatch EndPoint Security, Solar Dozor[12].

1.8.Висновки до розділу 1.

Проведено дослідження існуючих актуальних систем запобігання витоку інформації, в результаті якого було виявлено, що вони класифікуються непрямими та прямими каналами витоку інформації, також найбільш розповсюджені методи її викрадення.

Були розглянуті основні фактори витоку даних, а також наведено приклади загального походження захисту інформації.

Було проведене дослідження щодо запобігання викрадення інформації та можливість витоку даних із зовнішніх та внутрішніх носіїв.

Проаналізовано найбільш поширені види DLP-систем, їх переваги та недоліки. Виявлено, що найбільш розповсюдженими DLP-системами є гібридний тип змішаної архітектури шлюзового та хостового підходів реалізації.

Розглянуті загальні засоби безпеки від стороннього втручання у обмін даними всередині корпорації та способи попередження викрадення конфіденційних даних.

Описані етапи розвитку DLP систем та їх важливість у питанні збереження конфіденційної інформації на підприємстві.

2.ДОСЛІДЖЕННЯ СИСТЕМ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

Для того, щоб провести дослідження систем запобігання витоку потрібно виконати основні кроки:

– Провести аналіз актуальності DLP-систем
– Провести аналіз кількості витоку інформації за минулі роки
– Провести загальний систем та визначити їх основне призначення
– Дослідити та описати основні функції системи
– Розглянути основні рішення систем, їх переваги та недоліки

Виконання всіх вищеперерахованих кроків дозволить чітко визначити актуальність та значення систем запобігання витоку інформації та систематизувати необхідність функціоналу даних систем.

2.1.Актуальність DLP-систем інформаційних технологій

Витік інформації – це подія, коли конфіденційна інформація стає відома не уповноваженим особам. Будь-яке поверхневе сканування джерел новин показує, що витік даних відбувається із загрозливою швидкістю. Якщо витік інформація щодо проектних операцій або інформація про тендери, це може призвести до втрати прибутку для бізнесу, а витік інформації також тягне за собою непрямі наслідки для бізнесу. Витік конфіденційної інформації про клієнтів може зашкодити репутації вашої компанії на ринку, оскільки потенційні клієнти будуть обережно працювати з вами або надавати особисту інформацію вашої компанії [13].

Основні причини витоку інформації:

1. Обмін інформацією за допомогою незахищених інструментів
2. Співробітники крадуть інформацію про компанію
3. Співробітники випадково передають конфіденційну інформацію

4. Інформація була випадково надіслана не тим адресатам

5. Фішингові шахрайства

ІТ-фахівці часто працюють, використовуючи технічну термінологію, яка не завжди доступна іншим. Ця проблема може призвести до напруженості між лідерами та відповідальними за забезпечення безпеки. Це природний опір керівництва організації, оскільки вище керівництво є джерелом і «охоронцями» важливої інформації. Конфіденційна інформація про клієнтів недоступна співробітникам на нижчих рівнях ієрархії компанії. Це відкриває можливість витоку інформації з топ-менеджменту. Ще одна причина, чому це завжди корисно ретельно керувати і контролювати клімат у колективі, стежачи за цим щоб співробітники, які залишають вашу організацію, робили це на позитивній ноті. Якщо співробітник задоволений, він менше ймовірно поділиться інформацією, яка може поставити під загрозу ваш бізнес.

Компанії зазвичай зосереджуються на захисті від зовнішнього середовища загрози, тоді як аналітики відзначають, що більше половини випадків порушення безпеки відбуваються з вини самих працівників або інших осіб особи, які мають законний доступ до інформації. Протягом кількох останніх років середній збиток від внутрішніх витоків інформації у світі склав понад три десятки мільярдів доларів (на рік). Дослідження компанії InfoWatch заявляє про кількість внутрішніх витоків щороку продовжує зростати, і це наочно показано на рисунку 2.1.

Рисунок 2.1 Кількість витоку інформації і об’єм скомпрометованих даних (записів), 2011-2017

Це пов’язано як із повсюдним поширенням інформації систем, що використовуються для обробки даних, і зі збільш вартість самих інформаційних активів компаній. Один з найефективніших елементів безпеки даних у корпоративних інформаційних системах залишається використання насамперед засоби запобігання витоку даних (системи DLP).

У корпоративних інформаційних системах повідомлення можуть містити захищену інформацію в її оригінальному вигляді (як вона є зберігаються у вигляді документів та інших носіїв захищеної інформації), а в зміненому - перетворено в інше формулювання, що містять скорочення, галузеві терміни та сленгові вирази тощо[16].

Система DLP — це рішення, яке поєднує в собі контроль над переміщення інформації як на рівні зв'язку із зовнішньою мережею, і на рівні пристроїв користувача (Рисунок) для того, щоб протидії витоку інформації.

Важлива функція класичного рішення DLP — це можливість сканувати збережені файли та бази даних для виявлення місць розташування конфіденційної інформації.

Основне призначення систем DLP – забезпечити захист від випадкового або цілеспрямованого поширення конфіденційної інформації від співробітників, які мають законний доступ інформації.

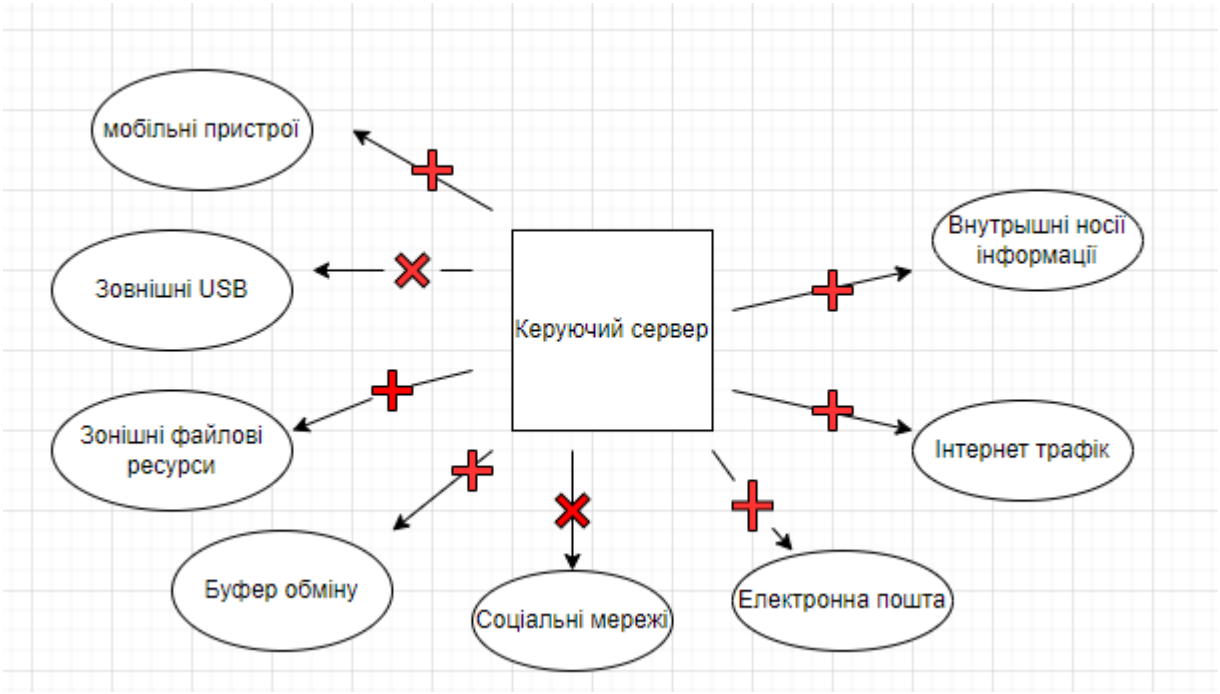

Рисунок 2.2 Інформаційні потоки контрольовані DLP-системою

Основні функції систем DLP:

– контроль передачі інформації через Інтернет з використанням різних протоколів;

– контроль передачі та збереження інформації на зовнішні носії тощо;

– захист інформації від витоку шляхом контролю виведення даних на

– печатка;

– блокування спроб пересилання/збереження конфіденційних даних, інформування адміністраторів ІБ про інциденти;

– пошук конфіденційної інформації на робочих станціях та файлові сервери;

– запобігання витоку інформації шляхом контролю життєвого циклу та руху конфіденційних відомостей.

У таблиці розглянуто основні особливості технологічних рішень, що використовуються для захисту від витоків, а також їх переваги та недоліки.

Таблиця 2.1 Технологічні рішення, що використовуються для захисту від витоку даних

	Орієнтованість рішення на боротьбу з втратою даних	Можливість блокування витоку	Наявність механізмів аналізу контенту	Захист даних від розповсюдження	Повність охвату більшості каналів витоку
Антивіруси		+-	+-		+-
Сканери вразливості					+-
IDS			+-		
Контроль доступу до мережі					+
Розмежування доступів		+-			
Захист каналів зв’язку	+-	+-		+-	+-
Контроль звернень до захисних ресурсів	+-			+-	
Контроль портів і пристроїв	+-	+-		+-	
Аудит дій користувача	+-				+-
DLP	+	+	+	+-	+
SIEM			+-		+
Фільтрація трафіку	+-		+-		
Шифрування даних	+	+-		+	

Проаналізувавши результати таблиці зроблено висновок, що оптимальне рішення для забезпечення ефективного захисту від витоків інформація буде системою DLP.

Для того, щоб система DLP функціонувала ефективно необхідно, щоб вона вміла розрізняти конфіденційні та відкриті інформації, необхідно передати певну логіку, на основі якої він повинен розрізняти ці два види інформації. Є кілька вбудованих механізмів для класифікації даних в системах DLP.

Основні методи класифікації інформації.

1. привласнення грифа секретним документам (потрібно було додати текстову мітку або змінити властивості кожного окремого документа вручну);

2. аналіз шаблонів (вимагалося скласти словник спеціалізованих для організації термінів, на підставі яких має реагувати система).

Останнім часом у сучасні DLP системи стали також впроваджувати цифрові відбитки.

Цифрові відбитки пальців - технологія, призначена для виявлення рідко змінені або незмінні (статичні) документи, дозволяє автоматично виявляти в аналізованому тексті цитати із зразків документів, що містять конфіденційну інформацію. Заслуги цього методу є висока точність виявлення статичності документів, але недоліком є те, що потрібна попередня індексація зразки документів, а також чутливість до змін тексту.

Основні переваги систем DLP:

– здатність виділяти важливі для захисту дані;

– орієнтованість на повне охоплення потоків інформації в організації;

– налаштовування під існуючі бізнес-процеси організації (позитивного ефекту від використання DLP систем можна досягти без організаційних перетворень та збільшення штату працівників).

Рішення DLP добре підходять для великих організацій де постійно активний, але погано керований обмін документами зі зовнішніми контрагентами, і при цьому є завдання забезпечення конфіденційності цього процесу.

Рішення DLP найкращим чином показують себе, саме коли відбувається високочастотний обмін документами у великій організації, якими важко керувати, однак потрібно забезпечити конфіденційність інформації.

Система DLP буде постійно контролювати трафік і надсилання самої інформації, яка копіюється на зовнішній носій, поштою або текстовими повідомленнями, ідентифікує конфіденційну інформацію, дані та реагує на спроби їх передачі чи розповсюдження. Працівник компанії не зможе безперешкодно відправити персональні дані клієнтів і компанія не може зробити випадкові копії важливих документів.

Використання систем DLP значно знизить ймовірність виникнення витоку конфіденційних даних, а про всі інциденти, які виникають, ви будете попереджені і зможете вжити заходів запобігання витоку. Ефективності системи DLP залежить від того, наскільки вона правильно налаштована.

2.2.Дослідження і аналіз систем захисту від витоку даних

2.2.1 Дослідження платформи Authentica ARM

Authentica ARM Platform контролює електронні документи та поштові повідомлення. Додаткові модулі інтегруються з настільними додатками (Microsoft Office і Outlook, Lotus Notes, Adobe Acrobat, Microsoft Explorer і Netscape) і засобами зовнішньої аутентифікації (LDAP, єдиний вхід Windows, X.509, RSA SecurID). Функціональність захисних активних прав передбачає аутентифікацію користувачів та їх авторизацію на перегляд інформації, контроль за друком документи та стандартні операції (копіювання, редагування, читання). Вся конфіденційна інформація є у зашифрованому вигляді і розшифровується тільки в момент роботи з ним. Обмін інформацією також підлягає шифруванню між сервером політики ARM і компонентами клієнта[17].

Інсайдер з правами доступу до конфіденційного документа має обхідний шлях для викрадення інформації. Для цього потрібно створити новий документ і перейти до налаштування конфіденційної інформації.

2.2.2 Дослідження технології PortAuthority

PortAuthority 5.0 призначений для комплексного захисту конфіденційної інформації. Зона покриття продукту включає такі канали: SMTP / ESMTP,

HTTP / HTTPS, ICQ, FTP і т. д. Крім того, виробник заявляє про підтримку протоколів Microsoft Exchange і Lotus Notes та про контроль друку на мережевих принтерах. Рішення PortAuthority також дозволяє контролювати переміщення чутливої інформації на змінних пристроях. PortAuthority 5.0 базується на трирівневій архітектурі та включає PortAuthority Enterprise Manager - пристрій, що реалізує централізоване управління; PortAuthority Protector Appliance - пристрій, відповідальний за моніторинг і контроль мережевого трафіку; Агент сервера PortAuthority - програмний модуль для моніторингу і запобігання витоку через внутрішні комунікації (контроль над MS Exchange, Lotus Notes і мережеві принтери); PortAuthority Endpoint Protection — це програмний модуль для контролю конфіденційної інформації, скопійованої на знімний пристрій, пристрої (USB тощо) на робочих станціях, ноутбуках та серверах. Аналіз переданого через контрольовані канали інформації здійснюється з використанням власної технології PreciseID, заснованої на використанні цифрових відбитки пальців (цифр відбитки пальців). Крім методу цифрових відбитків пальців, Технологія PreciseID включає більш знайомі способи аналізу переданого вмісту та дозволяє відстежувати канали, що відстежуються за ключовими словами та словосполучення, за словниками, до відповідності зі зразками. Рішення передбачає можливість аналізувати трафік за допомогою регулярних виразів, а також типів файлів і підписів[18].

Захист цієї системи можна обійти, передаючи інформацію в зашифрованому вигляді, в результаті чого система не зможе розпізнати в ній слова і фрази, що сигналізують про конфіденційність інформації.

2.2.3 Дослідження системи моніторингу та контролю дій користувачів Verdasys

Verdasys - Американська компанія, що пропонує рішення Digital Guardian, призначене для моніторингу та контролю дій користувачів на рівні робочої станції.

Функціональність рішення Digital Guardian включає виявлення операцій з файлами, включаючи відкриття, копіювання та модифікацію файлів, передача файлів по FTP та надсилання даних через веб-пошту. Рішення дозволяє контролювати копіювання конфіденційної інформації на різні пристрої (CD / DVD, USB, FireWire, PCMCIA, Bluetooth, Wi-Fi), виведення скріншотів та друк на принтері.

Цифровий The Guardian складається з центрального сервера, відповідального за зберігання та керування політикою безпеки і за накопичення інформації про всі порушення та агентів, розташованих на всіх робочих станціях, ноутбуках і серверах, де необхідно захистити дані. Система керується за допомогою спеціальної консолі керування Digital Guardian, що підключена до центрального сервера.

Вся діяльність користувача реєструється. У разі порушення агент політик безпеки Digital Guardian дозволяє блокувати заборонену операцію, надсилати сповіщення, а також відображати відображається попередження про порушення політики безпеки або запит на виправдання провести операцію.

Щоб обійти цю систему, достатньо передрукувати інформацію з конфіденційного документа в новий без використання операції з буфером обміну. Система не виявить передачу конфіденційних даних, що містяться в новому документі, оскільки не має механізму фільтрації вмісту.

2.2.4 Дослідження комплексної системи рішень Vontu

Vontu 7.0- комплексне рішення для запобігання витоку конфіденційних даних. Vontu 7.0 заснований на одиночній платформі Vontu Enforce, що складається з п'яти програмних продуктів для захисту конфіденційної інформації: Vontu Discover, Vontu Protect, Vontu Monitor, Vontu Prevent і Vontu Endpoint

Monitor. Продукція Vontu Discover і Vontu Protect створені для того, щоб захистити конфіденційні дані на місцях роботи кінцевих користувачів. Vontu Discover відповідає за виявлення конфіденційної інформації. Vontu Protect розроблено для захисту конфіденційних даних на робочих станціях і ноутбуках. Це дозволяє вам ізолювати, переміщувати або копіювати конфіденційні документи, знайдені за допомогою Vontu Discover, у визначене безпечне місце. Продукт також підтримує можливість шифрування незахищених конфіденційних даних[19].

Vontu Monitor і Vontu Prevent призначені для моніторингу та контролю даних, передаються по мережі. Vontu Monitor відповідає за виявлення витоків конфіденційної інформації даних через електронну пошту, веб-пошту та FTP. Vontu Prevent дозволяє блокувати несанкціоновану передачу конфіденційних даних, шифрувати дані, передається відкритим текстом. Монітор Vontu у поєднанні з Vontu Prevent автоматично пригнічує можливість витоку конфіденційних даних через мережу. Vontu Endpoint Monitor - продукт, призначений для моніторингу даних, скопійованих на знімні пристрої (USB, CD/DVD тощо). Це дозволяє відстежувати, які конфіденційні дані були завантажені на локальні диски. Контент-аналіз здійснюється на основі запатентованих технологій. До них відноситься технологія розпізнавання структурованих даних Vontu Exact Data Matching і аналіз неструктурованих даних за допомогою цифрових відбитків пальців за допомогою зіставлення індексованих документів Vontu. Крім того, технологія Vontu Described Content дозволяє розпізнавати вміст на основі ключових слів і фраз, словників відповідності зразків.

Інсайдер може подолати захист даної системи за допомогою шифрування. Неможливо виявити зашифрований текст слова та фрази, що сигналізують про конфіденційність інформації.

2.2.5 Дослідження хостової агентської системи McAfee Data Loss Prevention (DLP)

Система захисту від витоків на основі агентського контролю за використанням конфіденційної інформації. Продукт дозволяє:

1. Контролювати доступ користувачів до конфіденційної інформації;

2. Блокувати копію буфер обміну для певного вмісту;

3. Аналізувати вихідні повідомлення в електронному листі та заблокуйте витік конфіденційна інформація; відстежувати переміщення конфіденційної інформації між комп'ютерами, що контролюються, а також його копіювання на знімний носій;

4. Блокувати передачу інформації через мережеві протоколи TCP \ IP;

5. Аналізувати блокування друку документи, якщо вони містять конфіденційну інформацію;

6. Виявляти та блокувати передачу на зовнішні конфіденційні носії інформація;

7. Блокувати операцію «Print Screen» для певних програм;

8. Перехоплювати пост-запити в Інтернеті Explorer - наприклад, вихідні повідомлення електронної пошти в Інтернеті.

Інсайдер може обійти цю систему передруком конфіденційної інформації з оригінального документа на новий. Немає використання операцій буфера обміну.

2.2.6 Дослідження DLP-системи InfoWatch Enterprise Solution

Рішення InfoWatch Enterprise (IES) дозволяє контролювати поштовий канал і веб-трафік, а також комунікаційні ресурси робочих станцій. Рішення включає такі програмні компоненти: InfoWatch Traffic Monitor, InfoWatch Net Monitor і InfoWatch Mail Storage, які також поставляються як окремі розчини. InfoWatch Traffic Monitor — розподілена багатокомпонентна система для фільтрації пошти та веб-трафіку. Продукт класифікує інформаційні об'єкти за змістом морфологічного аналізу і різних формальних атрибутів, а потім відповідно до політики безпеки вирішує про можливість переміщення інформації в межах корпоративної мережі. InfoWatch Enterprise Solution – централізований збір

статистичних даних і інтегрується з електронним сховищем. Повідомлення InfoWatch Mail Storage використовується для розслідування інцидентів і виявлення інсайдерів[20].

Для перевірки всіх повідомлень використовується технологія фільтрації вмісту Morpho-Logic, яка аналізує вміст повідомлення та файли вкладених документів. InfoWatch Net Monitor — це програмний продукт для контролю за поведінкою робочих станцій, файлів та серверів з конфіденційною інформацією. Продукт відстежує транзакції з файлів (читання, змінювання, копіювання, копіювання в буфер обміну, друкування тощо) і інформує адміністратора з IT-безпеки про ті, які не відповідають прийнятій політиці безпеки IT. Продукт надає можливість контролю доступу користувачів до комунікаційних портів і пристроїв введення-виведення на робочих станціях (CD, дискети, знімні накопичувачі, порти COM, LPT, USB та IrDA, Bluetooth, FireWire, Wi-Fi). Операції, які не відповідають вказаним правилам, блокуються. Рішення надає можливості для детальної реєстрації всі дії з файлами.

Інсайдер може використовувати шифрування, щоб обійти цю систему. Слова та фрази, що сигналізують про конфіденційність інформації, не будуть виявлені.

2.2.7 Дослідження апаратного програмного забезпечення Sure View

Oakley Networks надає апаратний продукт Sure View, який забезпечує комплексне виявлення та запобігання витоків конфіденційної інформації. Продукт дозволяє фільтрувати веб-трафік, електронну пошту і миттєві повідомлення (IM), стежити за активністю користувачів на рівні робочої станції.

Рішення SureView складається з трьох компонентів:

– Агенти (розташовані на робочих станціях)

– Апаратне ядро (виконує основні функції фільтрації)

– Виділений сервер (використовується для централізованого керування політикою).

Продукт Oakley Networks використовує кілька технологій і алгоритми, заснованих на ймовірнісних і статистичних методах. Апаратне програмне

забезпечення аналізує поведінку користувачів з урахуванням чутливості оброблюваних документів, але не виконує функції фільтрації змісту в загальному розумінні.

Слабким місцем цього рішення є неповне охоплення комунікаційних ресурсів робочих станцій. Інсайдери мають можливість перезаписувати дані на мобільні пристрої через бездротові інтерфейси IrDA, Wi-Fi, Bluetooth.

2.2.8 Дослідження системи DLP Hackstrike

Hackstrike надає багатофункціональний апаратний продукт Fortress-1, орієнтована на середній та малий бізнес.

Типова архітектура включає кілька комбінованих модулів: маршрутизатор, брандмауер, антивірус, фільтр спаму, фільтр вмісту, фільтр URL-адрес, VPN, система виявлення та запобігання вторгненням, формувач трафіку для підтримки необхідного рівня якості обслуговування та модуль захисту документів.

Модуль захисту документів запобігає витоку даних. Цю функціональну систему SDAS (Secure Digital Asset System) розробила компанія Hackstrike. Продукт може знаходити конфіденційні документи в потоці даних, надіслані за допомогою цієї технології. Метод пошуку включає аналіз цифрових водяних знаків і підпис порівняння. Розміщення цифрових водяних знаків і зняття підписів відбувається за допомогою спеціального додаткового модуля, який підключається до Microsoft Office і дозволяє одним клацанням на панелі інструментів позначити документ як конфіденційний. Додаткові технології SDAS дозволяє здійснювати пошук за ключовими словами[22].

Ресурси робочої станції не перевіряються. Користувач може обійти цифрові водяні знаки та підписи шляхом копіювання даних через буфер обміну в нових документах і перетворення його в інший формат (наприклад, Adobe PDF).

2.2.9 Дослідження програмного забезпечення Tablus

Tablus Content Alarm Solution програмне забезпечення для виявлення та запобігання витоків.

В продукт включає апаратні модулі:

– Content Alarm NW

– Моніторингова мережа каналів

– Проведення DT Content Alarm моніторингу робочих місць.

Змістовий модуль Alarm NW призначений для виявлення витоків через мережеві канали. Він включає засоби контролю політики та класифікації даних, пасивні датчики моніторингу, поштовий фільтр для запобігання витоків з електронної пошти, фільтри пересилання та клієнт для централізованого керування.

Процес виявлення витоків заснований на фільтрації контенту, під час якої виконується лінгвістичний аналіз, пошук конфіденційних даних за підписами, аналіз ключових слів і фраз, пошук за шаблонами, аналіз атрибутів даних, що надсилаються.

Агенти, розміщені на робочих станціях, дозволяють керувати наступними операціями користувача: запис даних до CD, копіювання файлів на USB-пристрої, виведення інформації на принтер, робота з буфером обміну (операції копіювання та вставки), створення знімку екрана, відправка повідомлень електронною поштою, вкладення файлів до засобів обміну миттєвих повідомлень (IM)[23].

Продукт має ряд недоліків: неповний контроль за АРМ (повністю бездротові можливості не охоплені. Не підтримується моніторинг передачі даних через IrDA, Bluetooth, Wi-Fi та усіх інших портів, крім USB).

2.2.10 Дослідження поштового захисника Proofpoint Messaging Security

Proofpoint Messaging Security – дозволяє забезпечити повний контроль над електронними поштою . За допомогою цього пристрою ви можете перевіряти повідомлення на наявність вірусів і спаму, запобігати зловживанню поштовими ресурсами та витоку конфіденційної інформації через них. Захист від витоку конфіденційних даних заснований на механізмі фільтрації контенту. Вся передана інформація попередньо розподілена на кілька тематичних категорій. Фільтр здатний аналізувати більше 300 типів вкладень, включаючи популярні формати Word, Adobe PDF, ZIP тощо.

Рішення Proofpoint призначеного для захисту одного конкретного каналу передачі дані електронної пошти.

Недоліком даного рішення є: можливість інсайдера скопіювати конфіденційну інформацію на знімний носій.

2.2.11 Дослідження системи моніторингу FalconGaze SecureTower

Програма дозволяє стежити за діяльністю користувачів всередині компанії локальної мережі, що перехоплює весь інтернет-трафік, у тому числі передається по зашифрованим каналам, а також передає дані до зовнішніх пристроїв та принтерів. Програма автоматично повідомляє службу безпеки у разі виявлення факту передачі конфіденційні дані будь-якими каналами. Функціональність SecureTower:

– Перехоплення мережевого трафіку.
– Комплексний контроль роботи пристроїв і принтерів.
– Можливості для перегляду інформації.
– Автоматична доставка повідомлень порушення даних.
– Перегляд статистики в режимі реального часу.
– Повідомлення про роботу системи перехоплення.

Цю систему можна обійти за допомогою шифрування. Аналіз вмісту зашифрованого тексту не виявить слів і фраз, які сигналізують конфіденційність.

2.2.12 Дослідження комплексної системи DLP Peremetrix Safestore

Peremetrix Safestore є комплексним рішенням для захисту корпоративної таємниці від витоку. Частина SafeSpace складається з трьох основних продуктів, Perimetrix SafeStor, Perimetrix Safeus, Perimetrix SafeEdge та ядро системи Perimetrix ShadowCore. ShadowCore містить архів дій користувача при роботі з конфіденційними документами для подальшого аналізу та аудиту.

Захист даних на стадії зберігання забезпечує продукт Perimetrix SafeStore. SafeStore — це централізоване сховище зашифрованих документів з обмеженим доступом.

Захист інформації під час використання реалізується Perimetrix Safeuse. Safeuse створює середовище для перевірки розподіленого зберігання та обробки конфіденційної інформації відповідно до політики безпеки компанії. Агенти Safeuse запобігають витоку даних через знімні носії, принтери та локальні порти

комп'ютерів. SafeEdge перехоплює, фільтрує, а також здійснює автоматична класифікація вихідного трафіку. SafeStore — це централізоване сховище зашифрованих документів з обмеженим доступом[24].

Інсайдер може передрукувати конфіденційні дані в новий документ, зашифрувати їх і надіслати електронною поштою. Якщо використовується шифрування, система фільтрація вмісту не працюватиме.

2.2.13.Дослідження модульної DLP-системи SearchInform

Модульний продукт для запобігання витоку інформації. Модулі циклу включають:

– NetworkSniffer – дозволяє перехоплювати дані, надіслані користувачами через популярні мережеві протоколи. Це єдина консоль, яка включає наступне продукти:

– MailSniffer – дозволяє перехоплювати всі вхідні та вихідні електронні листи.

– IMSniffer – дозволяє перехоплювати повідомлення Інтернет-пейджера (ICQ, QIP, MSN, JABBER).

– HTTPSniffer дозволяє перехоплювати інформацію, що надсилається на інтернет форуми, блоги та інші веб-сервіси.

– SkypeSniffer – дозволяє перехоплювати голосові та текстові повідомлення Skype.

– 3.DeviceSniffer – дозволяє перехоплювати відомості, записані на різні зовнішні пристрої (наприклад, USB-накопичувачі, CD/DVD диски).

– PrintSniffer – дозволяє перехоплювати зміст документів, надісланих користувачем для друку.

– Сервер робочих станцій індексації дозволяє відстежувати появу конфіденційної інформації на комп'ютерах користувачів, ресурсах загальнодоступної мережі та в інших місцях, не призначених для цього.

– DataCenter – здійснює зберігання даних і контролює стан усіх компонентів «Схема захисту інформації SearchInform» та надсилає повідомлення про несправності.

– AlertCenter – це програма, яка опитує всі модулі, перехоплює і при необхідності негайно повідомляє відповідальних за інформацію безпека людей.

Ця система використовує контент аналіз переданої інформації. З використання шифрування викраденої інформації можна обійти систему сповіщень витоку даних.

2.2.14. Аналіз розгляданих DLP-систем.

Функції системи DLP, наведені нижче були обрані через відсутність будь-якої іншої існуючої можливості викрадення конфіденційної інформації. Міцність всього ланцюга дорівнює міцності його самої слабкої ділянки. Не володіючи принаймні одною із перерахованих характеристик, система DLP не зможе захистити секретну інформацію від витоку повністю[25].

Продукція розглядалася за такими показниками:

1. Наявність змістового механізму фільтрації. Наявність механізму фільтрації контенту є обов'язковою для системи DLP, оскільки за її відсутності користувач з доступом до секретної інформації зможе передати її за межі мережі компанії, просто «передрукувавши» його та відправивши електронною поштою або іншим способом. Якщо існує система фільтрації змісту, система DLP може запобігти спробі передачі секретної інформації.

2. Виявлення спроб передачі секретної інформації за допомогою стенографії. Система DLP повинна контролювати і запобігання спробам передачі інформації через приховані в медіа файлах.

3. Виявлення спроб передачі зашифрованої інформації. Інсайдер може зашифрувати секретну інформацію, а потім передати його електронною поштою або іншим існуючим способом. Система DLP повинна контролювати і запобігти цим спробам.

4. Розпізнавання тексту в зображеннях, надісланих електронною поштою і іншими канали. Інсайдер може фотографувати екран із секретними документами та передайте їх за межами компанії.

5. Підтримка всіх мов світу. Інсайдер може перекладати текст секретних документів на мову, яка не підтримується системою DLP в результаті система фільтрації контенту не працюватиме.

6. Підтримка всіх форматів документів. Інсайдер може конвертувати секретний документ у формат, який не підтримується DLP системою, внаслідок чого може не працювати система фільтрації контенту.

7. Підтримка всіх протоколів передачі даних. Система DLP повинна відстежувати всі спроби передачі інформації доступні інсайдеру через технічні канали (передача на знімний носій, передача електронною поштою, передача інформації за протоколи http, https, tcp \ ip, ftp, udp, transfer через bluetooth тощо).

Результати перевірки наявності вищеописаних показників у DLP системи, що розглядаються, наведено в таблиці

Таблиця 2.2. Результати перевірки DLP системи

Продукт	Країна	Показники						
		1	2	3	4	5	6	7
Authentica ARM Platform	США	-	-	-	-	-	-	-
PortAuthority Technologies	США	+	-	-	-	-	+	+
Verdasys	США	-	-	-	-	-	-	-
Vontu	США	+	-	-	-	-	+	+
McAfee Data Loss Prevention	США	+	-	-	-	-	+	+
InfoWatch Enterprise Solution	Росія	+	-	-	+	-	+	+
PC Acme	Великобританія	-	-	-	-	-	-	-
Oakley Networks Sure View	США	+	-	-	-	-	-	-

Hackstrike	Ізраїль	+	-	-	-	-	-	-
Tablus	США	+	-	-	-	-	+	-

Продовження таблиці 2.2.

Proofpoint Messaging Security	США	+	-	-	-	-	+	+
FalconGaze SecureTower	Росія	+	-	-	-	-	+	+
Perimetrix Safestore	Росія	+	-	-	-	-	+	+
SearchInform	Росія	+	-	-	-	-	+	+

З даної таблиці видно, що серед розглянутих продуктів немає системи, які мають усі необхідні характеристики. Це пов’язано насамперед з тим, що деякі з них практично неможливі. Виробники систем DLP важко підтримувати всі мови світу, особливо якщо інсайдер використовує маловідомий діалект. Будь-яке зображення з текстом можна легко привести до такого вигляду, що впізнати його буде практично неможливо. Надайте підтримку всім форматів документів також неможливо, оскільки нове програмне забезпечення програмне забезпечення з'являється щодня і його неможливо відстежити, а тим більше впровадити аналізатори файлів для цих програм.

Усі розглянуті системи запобігання витоку інформації здатні захистити від випадкового витоку інформації, що передається відкритим текстом. За допомогою контент-аналізу вони можуть виявити спробу передачі конфіденційної інформації. Однак у тому випадку, якщо витік здійснюється навмисно, із шифруванням або інше перетворення переданого інформації до типу, що не дозволяє аналізувати контент, системи безпеки не зможе виявити та запобігти витоку інформації.

Системи захисту від витоку інформації можна і потрібно покращити, щоб значно підвищити ефективність запобігання навмисних витоків.

2.3.Висновки розділу

У даному розділі була розглянута актуальність систем запобігання конфіденційної інформації на підприємстві, а також проведений загальний аналіз методів та існуючих систем запобігання втрати даних.

Розглянуті системи мають змогу попередження витоку інформації у вигляді відкритого тексту та виявлення пристроїв з яких було проведено копіювання.

Дослідивши статистику випадків втрати даних зроблено висновок, що основною причиною втрати даних являються «інсайдери». На даний час не існує ідеальної системи, що змогла би попередити усі можливі види витоку, адже завжди присутній людський фактор.

3.РОЗРОБКА СИСТЕМИ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

Створена система запобігання витоку інформації призначена для застосування на підприємстві, а також для вільного користування приватним особам. Особливістю системи є ефективність попередження витоків відносно існуючих систем; та автоматизована організація адміністративного доступу до інформації, що забезпечує контрольований обмін інформацією між співробітниками В даному розділі розглядається принцип роботи комплексу механізмів ,моделей та методів. Описані способи його впровадження на підприємстві.

В ході проведення дослідження існуючих систем запобігання витоку інформації було прийнято рішення розробити наступні моделі та методи:

– модель фільтрації контенту,
– метод виявлення спроб передачі зашифрованої інформації,
– модель проксі-серверу,
– модель морфологічного аналізу

Першим етапом побудови DLP системи є представлення моделі обміну даними на проксі-сервері. Такий підхід задовольняє потрібність розмежування зовнішньої мережі від локальної. Використовуючи найновіший протокол SOCKS5 дає можливість використовувати методи аутентифікації та авторизації.

Для реалізації моделі обміну даними було обрано трирівневу ієрархічну модель. На кожному рівні моделі мережі буде виконуватися певна ділянка цієї мережі.

Перший рівень – це рівень організації всіх робочих станцій у рамках однієї мережі на одному рівні доступу, а програмне забезпечення буде використано, як агенти для організації мережевого обміну даними.

Другий рівень – це рівень розподілу – середній рівень ієрархії який забезпечує виконання комутаційних функцій на кінцевих пристроїв.

Третій рівень – рівень ядра – який забезпечує надійність передачі трафіку шляхом між мережевого екрану. Роль ядра у даній системі виконує маршрутизатор який об’єднує усі канали мережі та передає проксі-серверу, який у свою чергу їх аналізує. Якщо виникає потрібність у проксі-сервера у отриманні якоїсь інформації про рівень аутентифікацію, метадані або доступ до якогось файлу він має можливість прямого доступу до бази даних локальної мережі через роутер.

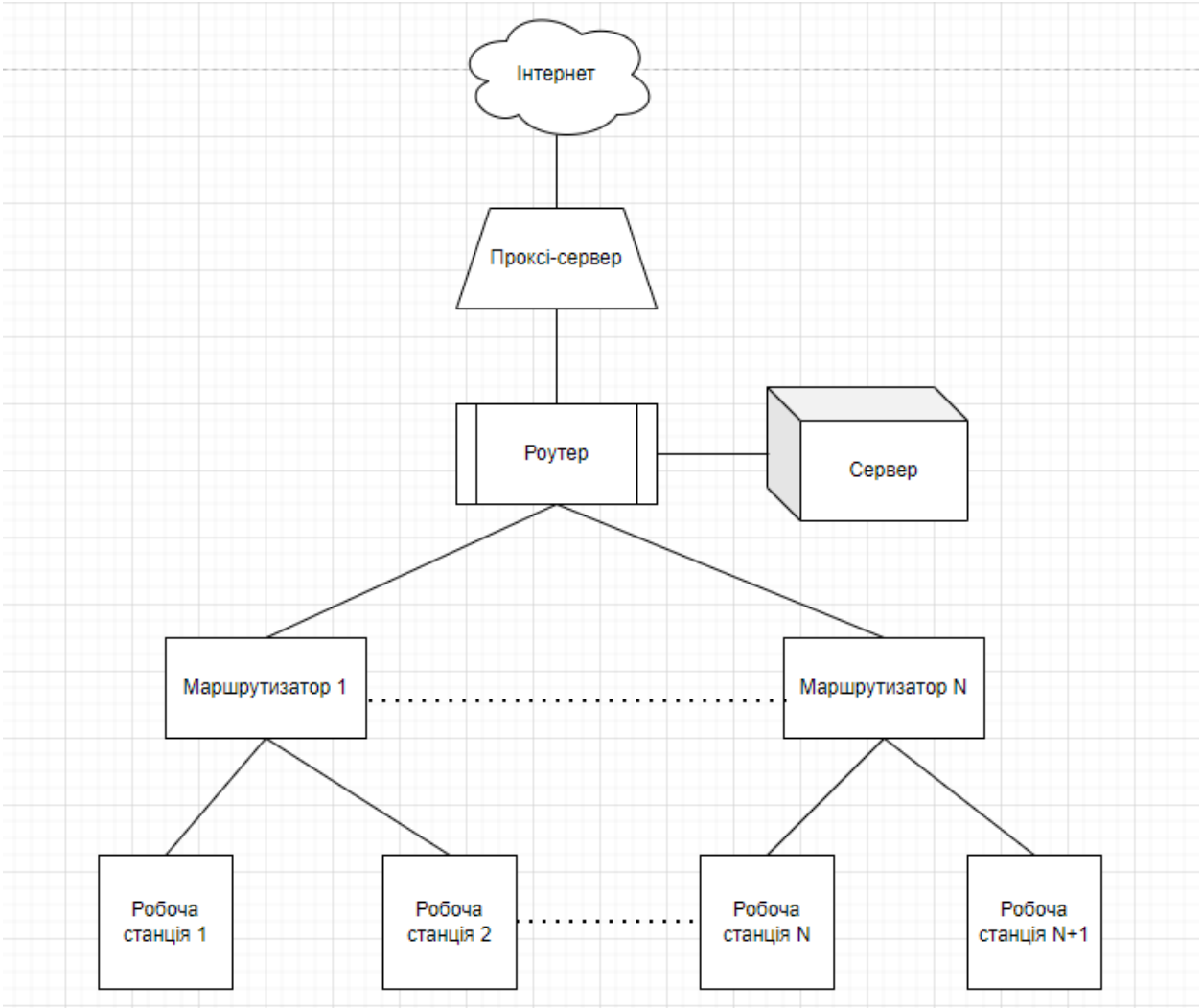

Рисунок 3.1. Локальна мережа з проксі-сервером.

Ефективність даного підходу можна розрахувати, взявши за основу розроблену мережу локального підключення за участі проксі-серверу. Система витрачає певний час для обробки одного запиту на відправлення до мережі

Інтернет. Визначивши цей час, можна зробити висновок щодо ефективності даного підходу.

Дана структурна мережа з використанням проксі-сервера потребує розробки моделі проксі-сервера з урахуванням використовуваних даних для комунікації з мережею Інтернет. Інформація, яка потрібна для налаштування обміну даними між клієнтом та сервером та метадані.

3.1.Визначення моделі проксі-сервера

Розробка моделі проксі-серверу базується на означенні, специфічних даних, що використовуються під час налаштування обміну даними між споживачем та постачальником.

Зв’язок між клієнтом і сервером для організації потоку даних виконується за допомогою TCP-з’єднання. В разу вдалої сесії зв’язку, клієнт із сервером обмінюються даними для аутентифікації. Клієнт надсилає серверу запит на визначення методу аутентифікації, а сервер в свою чергу повинен відповісти на запит клієнта або відхилити його.

Структура аутентифікації повинна підтримувати чотири основні типи з’єднання для клієнтів:

$$\text{Authentification} = < \text{N}, \text{G}, \text{P}, \text{B} >, \text{де}$$

N – доступ до серверу не потребує аутентифікації;

G – використання GSS-API;

P – доступ до серверу через передачу логіну та паролю;

B – тип доступу, який не підтримується сервером.

Завдяки визначеній структурі налаштування проксі-серверу визначається спосіб аутентифікації до зазначеного серверу. Таким чином отримується

інформація щодо того, хто намагається авторизуватися й мати доступ до мережі Інтернет та внутрішнього серверу.

Реалізація методу розділення мереж та методу аутентифікації у комбінації з DLP-системами підвищує рівень безпеки обміну даними у системі. Метод аутентифікації дає змогу ідентифікувати інсайдерів всередині мережі під час потенційного витоку конфіденційних даних. Налагоджена система аутентифікації дозволяє визначити рівень можливого доступу користувача та за рахунок системи ідентифікації логіна та пароля визначити групу компанії до якої відноситься співробітник. Також система рівнів доступу розповсюджується і на файли у базі даних. Та завдяки даним щодо рівня конфіденційності документа і рівня доступу користувача можна побудувати матричну таблицю доступу(табл. 1).

Таблиця 3.1 – визначення рівня аутентифікації клієнтів

Рівень доступу користувача(групи)/ Рівень доступу до файла	Рівень 0	Рівень 1	Рівень 2	Рівень 3	Рівень 4	Рівень 5
Рівень 0 (Гість)	1	0	0	0	0	0
Рівень 1 (HR)	1	1	0	0	0	0
Рівень 2 (Менеджери)	1	1	1	0	0	0
Рівень 3 (Розробники)	1	1	1	1	0	0
Рівень 4 (Адміністратори)	1	1	1	1	1	0
Рівень 5 (Керівники)	1	1	1	1	1	1

При виконанні команди для визначення типу зв’язку передається одна із трьох констант від 1 до 3:

– Базову з’єднання із зовнішнім сервісом.
– Приєднання певного IP адресу до сокета.
– Утворення UDP зв’язку.

Після успішного встановлення зв’язку, для виконання з’єднання із зовнішньою мережею клієнт та сервер повинні почати обмін пакетами.

$$\text{Request} = < \text{V}, \text{C}, \text{T}, \text{AD}, \text{PD} >, \text{ де}$$

V – версія протоколу;

C – команда для визначення типу зв’язку;

T – тип адреси;

A – адреса провайдера сервісу із зовнішньої мережі;

P – порт провайдера сервісу із зовнішньої мережі.

Структура запиту слугує для виконання функцій визначення типу адреси, переслати його до клієнту з метою утворення мережі обміну даними з сервісами мережі Інтернет.

Адреса сервісу та порт передачі даних клієнт отримує завдяки отриманню пакету-запиту для того, щоб утворити об’єднання. Наступна структура описує метод відповіді проксі-сервера на запит клієнта у вигляді пакету, після його обробки

$$\text{Reply} = < \text{V}, \text{R}, \text{T}, \text{AB}, \text{PB} >, \text{ де}$$

V – версія протоколу;

R – поле для коду відповіді;

T – тип адреси до якої приєднався сервер;

AB – адреса сервісу до якого звернувся сервер;

PB – порт за яким звернувся сервер до сервісу;

Відповідь сервера на запит користувача може бути будь якою, це залежить від списку правил, що були задані кінцевим сервером для надання послуг. У

випадку перевищення часу з’єднання до зовнішніх даних, у доступі до них може бути відмовлено. Проксі-сервер має декілька обов’язкових задач:

- Розпізнавання існування адреси до якої будуть передані дані.

- Визначення типу підтримуваної команди, що була передана через пакет-запит.

У випадку невідповідності зазначених вище умов, проксі сервер має як найшвидше повідомити користувача про потенційну помилку та перервати сесію із ним.

Обмін пакетів даних забезпечує об’єднання клієнта з глобальною мережею, однак для організації зв’язку існує необхідність забезпечення усіх з’єднань зі глобальною мережею на сервері. У цих з’єднаннях повинні зберігатися адреси відправника та клієнта. З цією метою сервер записує структурований список класів, де описані усі зв’язки клієнта у вигляді запропонованому, як модель:

$$\text{Connection} = < \text{CA}, \text{BA}, \text{S}, \text{B}, \alpha, \beta, \mu >, \text{де}$$

CA – адреса клієнта, який намагається отримати доступ до зовнішньої мережі;

BA – адреса сервісу із зовнішньої мережі;

S – стан зв’язку між клієнтом та зовнішньою мережею;

B – буфер обміну між клієнтом та зовнішньою мережею через проксі-сервер;

α – операція для обробки відного з’єднання;

β – операція для закриття з’єднання;

μ – обробка та відправлення вхідного буфера.

Зі сторони сервера повинні виконуватися дві основні функції:

– Підтримка списку клієнтів

– Наявність структури даних для аналізу потоку інформації

Ощадна функція сервер також включає в себе список заданої архітектури мережі.

Модель проксі-серверу слугує для виконання визначеного функціоналу в залежності від конкретизації об’єкта обробки. З цього слідує, що функціонал проксі-серверу можна поділити на три основні підрозділи.

Перший з них відповідає за аутентифікацію споживача та утворення мережевих об’єднань за допомогою протоколу TCP.

Другий підрозділ покриває функціонал підтримки з’єднання для мережевого каналу та роботи буферу обміну, який посилає дані цим каналом.

Третій – організовує аналіз інформації, що приходить з буферу.

Таким чином, можна представити загальну модель проксі-серверу у вигляді вхідних та вихідних даних, а також операції, які він уповноважений виконувати:

$$\text{Proxy} = < \text{H}, \text{P}, \text{CL}, \text{Buff}, \text{NN}, \text{NT}, \alpha, \beta, \mu > \text{, де}$$

H – набір адрес, які прослуховує проксі-сервер;

P – порт, який прослуховує проксі-сервер;

CL – список з’єднань усіх клієнтів із зовнішньою мережею;

Buff – буфер даних, який передається у зовнішню мережу;

NN – об’єкт нейронної мережі як вхідний параметр;

NT – лист для задання топології та навчальних вибірок нейронної мережі;

α – операції для створення TCP-з’єднань та аутентифікації клієнтів;

β – операції для підтримки з’єднань та роботи з буфером;

μ – операцій для аналізу потоку даних.

Крім того слід виділити, що проксі-сервер отримує порт та адресу опціональними параметрами, який потрібно оброблювати на наявність виявлення запиту для утворення мережевого зв’язку за допомогою протоколу TCP. Також модель проксі-серверу включає в себе багато поточну обробку для аналізу ряду мережевих зв’язків одночасно.

Отже, реалізація представленого методу проксі-серверу та додавання усіх заявлених вхідних даних буде забезпечувати утворення потоку мережі та

відповідного аналізу цієї мережі, згідно з основними поняттями, які заявлені у документації мережевого протоколу SOCKS5.

3.2.Визнаення алгоритму реалізації потоку даних

Для реалізації потоку даних, що потрібно аналізувати між локальною та глобальною мережами потрібно скористуватися протоколом SOCKS5. На рисунку 3.2 відображена схема послідовності кроків для утворення та забезпечення відповідного мережевого об’єднання.

Рисунок 3.2 Схема послідовності кроків для утворення та забезпечення мережевого об’єднання.

За допомогою брандмауера виконується передача потоку даних між клієнтом та сервером відповідно. У ролі брандмауера реалізований проксі-сервер з системою запобігання витоку інформації. Для встановлення мережевого об’єднання проксі-сервер повинен мати не зайнятий порт відповідний до зазначеного протоколу. В даній системі це - SOCKS5. Для сервісу SOCKS використовується окремий TCP порт - 1080.

Першим кроком для передачі даних від клієнта потрібно запросити створення з’єднання за допомогою протоколу TCP з проксі-сервером, який виконує функціонал підтримки цього каналу та комутує з буфером обміну для відправки даних до глобальної мережі. Ініціація утворення мережевого каналу починається з відповідного запиту клієнта до проксі-серверу. В свою чергу сервер організовує необхідний канал для обміну даними на певному сокеті. Після створення сокету, сервер повинен ініціалізувати даний сокет із відповідним дескриптором для його ідентифікації.

Якщо з’єднання клієнта та проксі-сервера пройшло успішно, сервер змінює статус запиту на «Очікування», що сигналізує про заняту чергу на доступ до глобальною мережі конкретним клієнтом. Також слід виокремти той факт, що проксі-сервер має власний зв’язний список усіх з’єднань та їх статуси.

Після об’єднання клієнта з сервером починається процес аутентифікації. Цей процес проходить завдяки обміну запитами між клієнтом та сервером щодо визначення конкретного метода аутентифікації на сервері. Сервер має обробити усі запити і встановити відповідний зв’язок з клієнтом або скасувати його.

Рисунок 3.4. описує загальний алгоритм пошагової аутентифікації методом вводу логіну та паролю. В залежності від обраного методу ауетентифікації клієнт надсилає свої дані логіну та паролю. Якщо цей запит позитивно приймається сервером, то ініціюється TCP-з’єднання для обміну пакетами даних. Визначений пакет даних, що надсилає клієнт показаний на рисунку 3.3.

Версія	Довжина логіну	Логін	Довжина паролю	Пароль
1	1	Від 1 до 255	1	Від 1 до 255

Рисунок 3.3. Пакет для передачі логіну та паролю

Цей спосіб обміну підтримує різні варіанти обміну пакетами, тож клієнт разом із запитом повинен надіслати інформацію щодо типу цього запиту. Наступним кроком є встановлення та визначення довжини логіну та паролю, а також безпосередньо сам логін та пароль у форматі строки. Після успішного

комутування сервер розпочинає пошук відповідного логіну на його наявність. У разі не існування введеного логіну у базі даних сервер у якості відповіді надсилає помилку. Після перевірки логіну наступним кроком виконується процес перевірки відповідності пароля. Якщо пароль введено не вірно, або він не існує у базі сервер надсилає помилку.

У випадку коректно заповненої форми аутентифікації проксі-сервер дозволяє авторизуватися користувачу з певним рівнем можливостей в залежності від того, який обліковий запис було аутентифіковано. Додатковою функцією проксі-серверу є зберігання інформації щодо користувача: рівень доступу, id номер, логін, пароль та дату створення облікового запису. Дана інформація використовується при аналізі запитів створених цим клієнтом.

Після успішно створеного зв’язку з сервером та аутентифікації клієнту дозволяється надіслати запит для створення відповідного зв’язку зі зовнішньою або глобальною мережею. Найважливішими даними при передачі мережевого пакету – це IP адреса та порт провайдера потрібного ресурсу. У разі не повного заповнення форми бракуючі поля заповнюються за замовченням. Якщо поля не були заповнені з будь-якої причини клієнтом або сервером запит не буде оброблюватись, а канал передачі буде закритий.

Якщо клієнт створив валідний запит до сервера відповідний до протоколи SOCKS5. У свою чергу проксі-сервер створює мережеве з’єднання через відповідний сокет із відповідним сервісом зовнішньої мережі та пересилає запит для отримання доступу.

Якщо зовнішній сервіс відмовляє у доступі, час доступу перевищується або не під'єднатись неможливо через недоступність сервісу, запит клієнта буде відповідно оброблений і проксі-сервер повідомить про помилку з’єднання, а утворені сокетні канали закриються у найкоротший час.

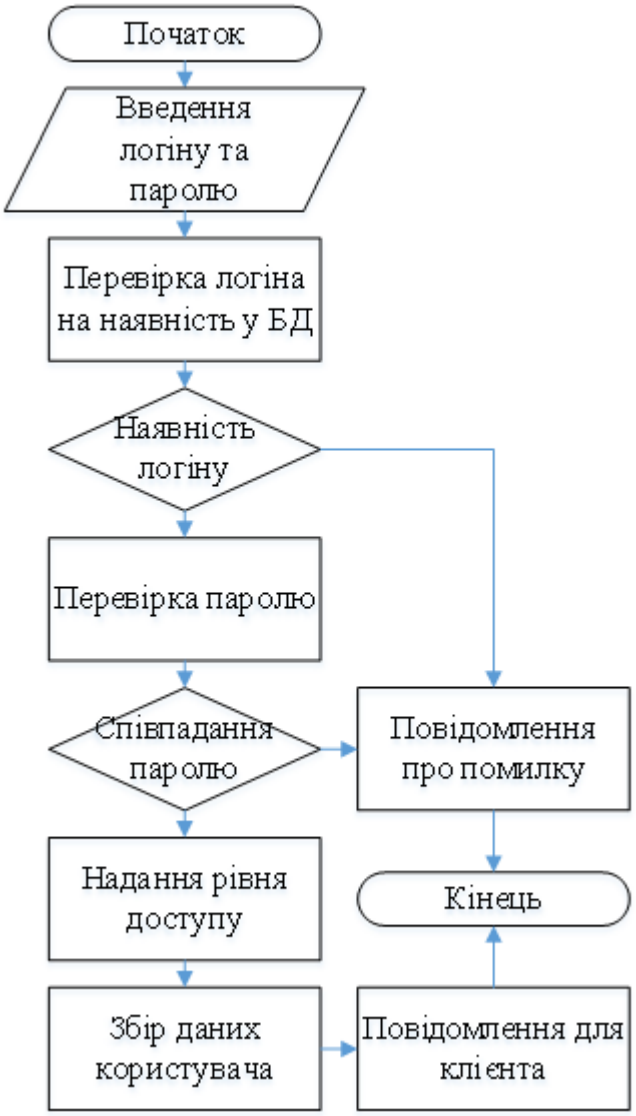

Рисунок 3.4. Загальний алгоритм аутентифікації з логіном та паролем

У разі задовільного з’єднання клієнта зі зовнішньою мережею, проксі-сервер розпочинає ряд синхронних процедур для утримання позитивного статусу підтримки мережі. Першою процедурою запускається процес оновлення хеш-таблиці з’єднань, де записується при відповідних значень IP адрес та портів під’єднаних один до одного зовнішнього до внутрішнього ресурсу. Даний функціонал потрібен для збереження даних на випадок багато поточного підключення. У разі обірванця зв’язку одною зі сторін буде виконуватися спроба повторного підключення. Завершення оновлення хеш-таблиці дає змогу проксі-серверу оновити статус черги користувача з «Очікування» на «Підключено».

Після оновлення статусу зв’язку сервер надсилає сповіщення про задовільне з’єднання з глобальною мережею.

Послідовність таких дій призводить до утворення об’єднання клієнта з Інтернетом за допомогою проксі-серверу, який аналізує інформацію обміну запитами та відповідями між сервером та споживачем.

3.3.Визначення методу фільтрації контенту

Існує декілька основних принципів фільтрації контенту у рамках інформаційної безпеки. Кожен з цих принципів повинен підтримуватися функціонуючою DLP:

– Блокування веб-сторінок за критеріями – дане рішення базується на ведені бази даних інтернет ресурсів, які користувачі можуть відвідувати з робочих станцій. Адміністратор мережі може корегувати даний список або базу даних в залежності від його репутації та чистоти з точки зору вірусних програм.

– Антіспам – принцип функціонування даного модуля базується на корисності інформації отримуваної користувачем, залежно від деяких факторів: алгоритм фільтрації спаму сортує листи та контент, кінцевою точкою яких є робоча станція.

– Блокування електронних листів або веб-сторінок в залежності від наявності ключових слів – це механізм фільтрації, який контролює адміністратор. Використовуючи дану методику адміністратор може встановити ряд заборонених слів. Якщо ці слова використовуються в листах або на сайтах, то ці ресурси негайно блокуються.

– Блокування файлів та додатків вкладених у електронний лист або завантажуваних з веб-сторінок по назві або формату – адміністратор може заблокувати доступ скачування деяких документів в залежності від частини їх назви або формату документа.

– Блокування листів або веб-сторінок і файлів не відповідних до чіткого формату – при поширенні шкідливих програм зловмисники часто використовують невідомий формат даних для DLP.

Розроблювальна система має гібридний вид архітектури організації, що дає можливість делегувати функції механізму фільтрації між DLP сервером, безпосередньо контрольованим адміністратором, та агентами на робочих станціях: програмне забезпечення, що контролює процес обміну даними саме з робочих комп'ютерів. В даній схемі об'єднано шлюзовий та хостовий підходи реалізації DLP на підприємстві, що дає широкий спектр можливостей контролювати обмін даними, як у середині системи так і проводити фільтрацію контенту поза її межами. Загальна схема змішаної архітектури DLP зображена на рисунку.

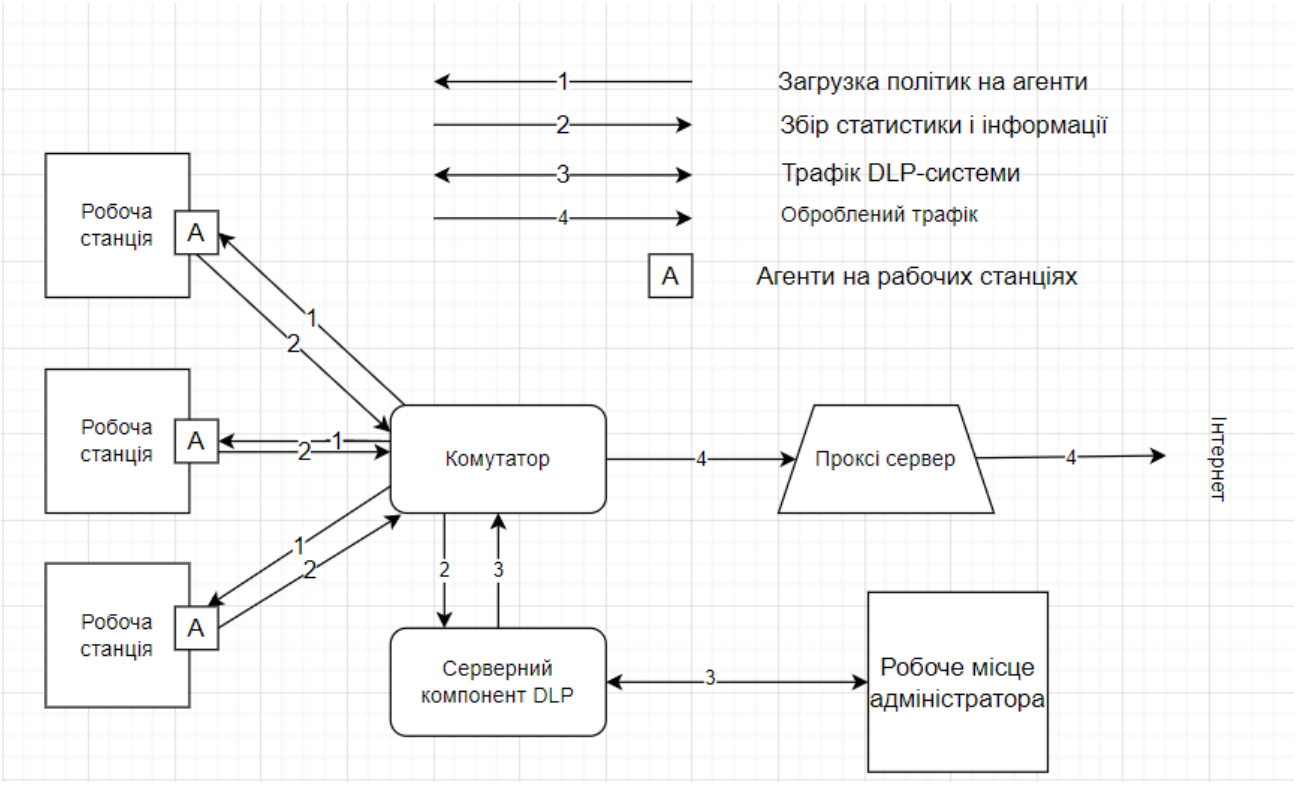

Рисунок 3.5. Схема гібридної архітектури DLP

На даній схемі присутні 3 види передачі мережевих даних:

– 1: Загрузка політик фільтрації та конфіденційної інформації – цей мережевий маршрут являє собою набір попереджень та обмежень, що

завантажуються на агенти робочих станцій згідно з вказівкою DLP серверу. Надалі частину фільтрації контенту можливо проводити відразу на робочих станціях, а не відправляти окремий запит до серверу.

– 2: Збір статистики та інформації – цей мережевий маршрут слугує для збору інформації та статистики відносно заблокованих та попереджених ресурсів та для запиту до DLP серверу, якщо агент не мав чітких вказівок на блокування або дозволу контенту, однак порахував його підозрілим

– 3: Трафік DLP системи – цей мережевий трафік слугує для передачі установ по ланцюгу Адміністратор – Сервер – Агент. Його основною метою є передача усього контенту, що не відфільтрувався на робочих станціях, однак пройшов обробку збоку сервера та адміністратора.

– 4: Оброблений трафік – фінальна ступінь передачі даних від робочої станції до мережі Інтернет, де присутній вже від фільтрований трафік агентами та адміністратором.

3.3. Визначення методу виявлення спроб передачі зашифрованої інформації

Була розроблена концепція, яка включає в себе наявність власної системи шифрування посилань між робочими станціями мережі та поза її межами. Такий підхід було реалізовано з метою виокремлення зашифрованих посилань всередині мережі від шифрування невідомого походження.

Кожен файл або інший вид даних переданий в межах системи, що охороняється проходить шифрування власними ключами DLP. В ході розробки було прийнято рішення використовувати симетричний підхід шифрування інформації.

Симетричне шифрування – це спосіб шифрування даних, при якому один і той же ключ використовується і для кодування, і відновлення інформації.

Вихідні дані нічого не повинні містити статистичних патернів вихідних даних: найбільш частотні символи осмисленого тексту нічого не винні відповідати найбільш частотним символам шифру.

Шифр має бути нелінійним: у шифрованих даних не має бути закономірностей, які можна відстежити, маючи на руках кілька відкритих текстів і шифрів до них.

Використовуючи комбінацію операцій підстановки (заміна фрагментів вихідного повідомлення, наприклад літер, інші дані, наприклад цифри, за певним правилом або за допомогою таблиці відповідностей) і перестановки (перемішування частин вихідного повідомлення за певним правилу), по черзі повторюючи їх можна досягти більшої ймовірності захисту від зловмисників. Алгоритм симетричного шифрування зображений на рисунку 3.5.

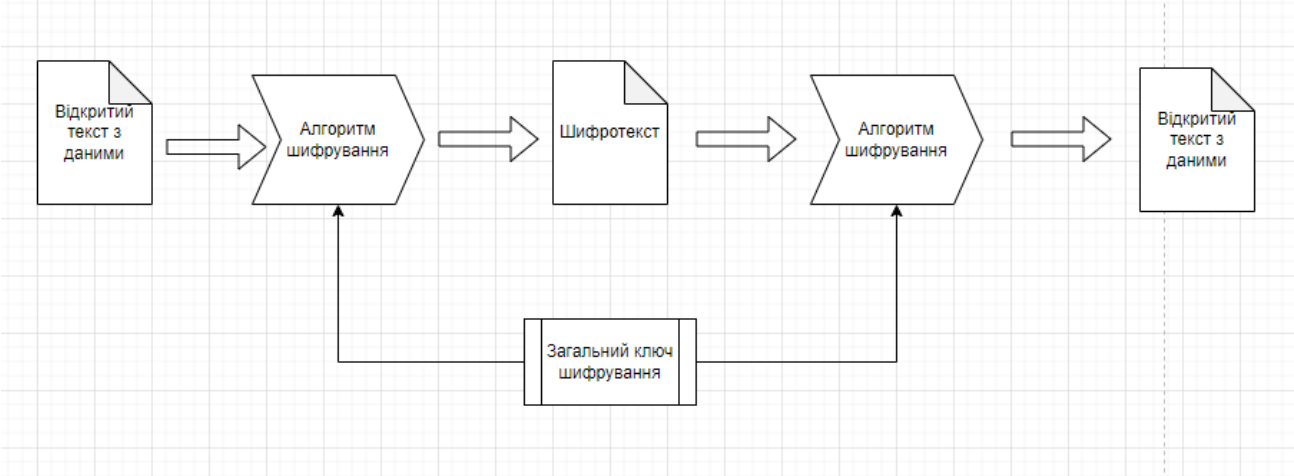

Рисунок 3.6. Алгоритм симетричного шифрування

Перевагами симетричних алгоритмів є те, що вони вимагають менше ресурсів і демонструють більшу швидкість шифрування, ніж асиметричні алгоритми. Більшість симетричних шифрів імовірно стійка до атак за допомогою квантових комп'ютерів, які теорії представляють загрозу для асиметричних алгоритмів.

3.4. Визначення методу морфологічного аналізу

Морфологічний аналіз – це механізм аналізу контенту інформації, який забезпечує виявлення каналів витоку конфіденційної інформації. Головною метою

запропонованого методу є виявлення конкретних наборів букв у документі або файлі, які надсилаються до Інтернету. Цей механізм є одним з основних у реалізації системи запобігання витоку інформації.

Аналіз даних морфологічним методом дає можливість контролювати усі можливі потоки даних у мережевих каналах. Таким чином цей метод виконує одночасно дві основні функції: аналіз контенту файлів та повідомлень, і аналіз мережевих об’єднань.

Розробка цієї моделі необхідна для створення універсального словника для аналізу файлів та документів компанії. Цей словник потрібен для зберігання слів, які найчастіше зустрічаються у документах. Реалізація цього методу буде застосовуватися на проксі сервері як прикладний модуль.

В даному випадку хеш-таблиці слугують для утворення даних у вигляді схеми, що собою формують спеціалізований словник. Хеш-таблиця – це певна структура даних, яка використовується для візуалізації наглядного асоціативного масиву, в якій зберігаються дані о парах мережевих об’єднань у вигляді ключ-значення. Дана таблиця виконує три основні функції:

– Функція додавання нової пари
– Функція операції пошуку
– Функція операції існуючої пари

$$\text{Hash} - \text{Table} = < \text{K}, \text{V1}, \text{V2}, \dots, \text{VN}, \alpha, \beta, \mu, \Omega >, \text{ де}$$

K – ключ з пари, в якості якого виступає ключове слово для пошуку;

$\text{V1}, \text{V2}, \dots, \text{VN}$ – значення до ключового слова пари, в якості якого виступають додаткові слова словника;

α – операція додавання нового слова до словника;

β – операція пошуку певного слова у словнику;

μ – операція видалення ключового слова разом із усіма іншими словами ланцюга;

Ω - об'єднання пари за ключем.

Даний вид представлення метода пояснюється наявністю ключових слів або слово утворень на базі яких визначається статус документу: конфіденційний він чи загальнодоступний. Загалом, на підставі єдиного слова не можливо визначити статус документа, через це механізм аналізу базується на використанні хеш-таблиць.

Ключем зазвичай визначається слово, яке найчастіше використовується у певному документі. Після отримання ключа документа потрібно визначити набір слів, який з найбільшою вірогідністю присутній у документі у порядку спадання кількості разів використовування та зазначити їх у таблиці, як значення певного ключа(візуалізація підходу зображена на рисунку 3.5.)

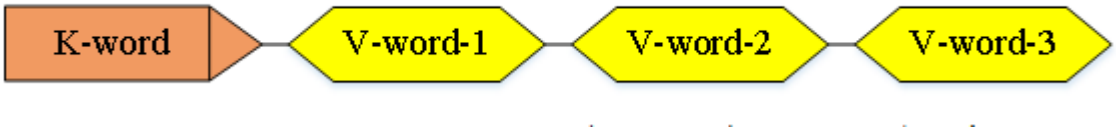

Рисунок 3.7. – Приклад пари ключ-значення у хеш-таблиці

Використовуючи такий підхід отримується заповнена пара ключ-значення усіх слів з документу у порядку спадання кількості разів використовування. Також треба визначити, що дана система враховує за слово будь-який набір більше ніж трьох символів, що дозволяє ігнорувати більшість сполучників збільшуючи вірогідність визначення ключового слова.

Даний підхід дозволяє аналізувати канали потоку даних та організовувати їх у певні хеш-таблиці, що структурують таблицю парами єдиного розуміння.

Об’єднання пар однакових ключових слів утворює послідовний ланцюг, де механізм розглядає основу слова, як ключ. А всі додаткові слова – значення (рисунок 3.6.). Об’єм виділеної пам’яті для додаткових слів обмежує запис до максимального значення у п’ять наборів символів (строк), а згодом об’єднуються у єдиний ланцюг.

Дана реалізація поєднує усі додаткові слова, що пов’язані з ключовим словом та дозволяє проаналізувати більшу кількість інформації зі збіглим контентом.

Створення словника потребує обробки системою певну кількість конфіденційних даних. Згодом, після утворення словника на базі заповненої хеш-таблиці він слугує для структурування даних та аналізу контенту мережевих потоків у DLP-системі та впровадження у різноманітні алгоритми, що використовують дану хеш-таблицю.

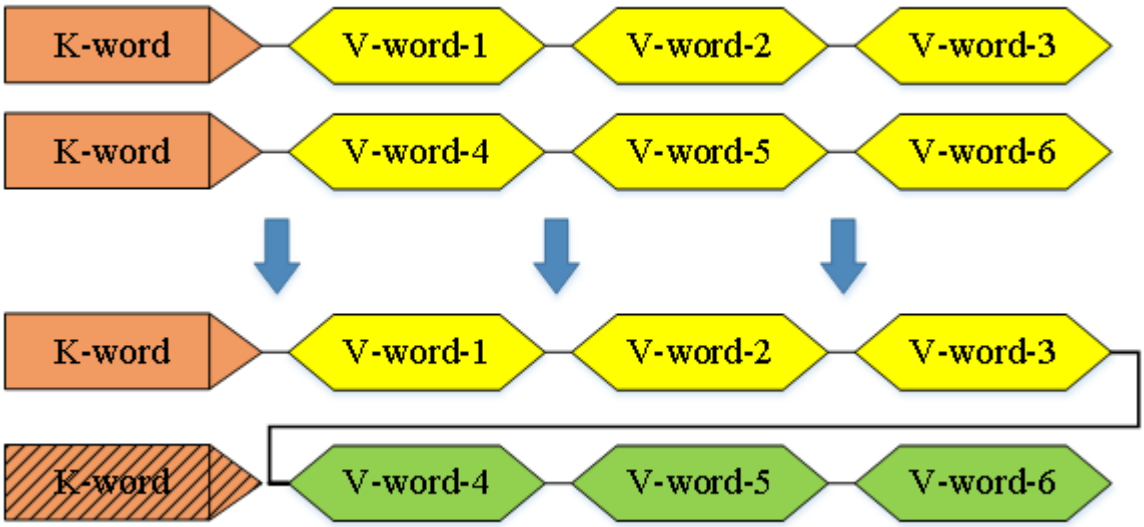

Рисунок 3.8. – Операція об’єднання двох пар хеш-таблиці у єдиний ланцюг

3.5. Алгоритм створення словника для морфологічного аналізу

Цей алгоритм – візуалізація покрокової реалізації словника для морфологічного аналізу (рисунок 3.7.). Його побудова потрібна для визначення функцій, які виконуються використанні хеш-таблиць, які мають вплив на побудову словника.

Даний алгоритм має послідовність кроків, які необхідно реалізувати до того, як зорганізується кінцевий словник ключових слів, що виконує ключову роль у морфологічному аналізі мережевого потоку.

Першим кроком реалізації алгоритму є отримання інформації на базі яких будуть утворюватись ключові слова. В залежності від кількості оброблювальних документів буде варіювати точність цього алгоритму. Чим більше документів використаних аналізатором – тим більше похибка і тим більша кількість ключових слів у морфологічному словнику.

Після вводу даних, алгоритм починає аналізувати слова, які найчастіше зустрічаються у документах відносно загальної кількості слів у них.

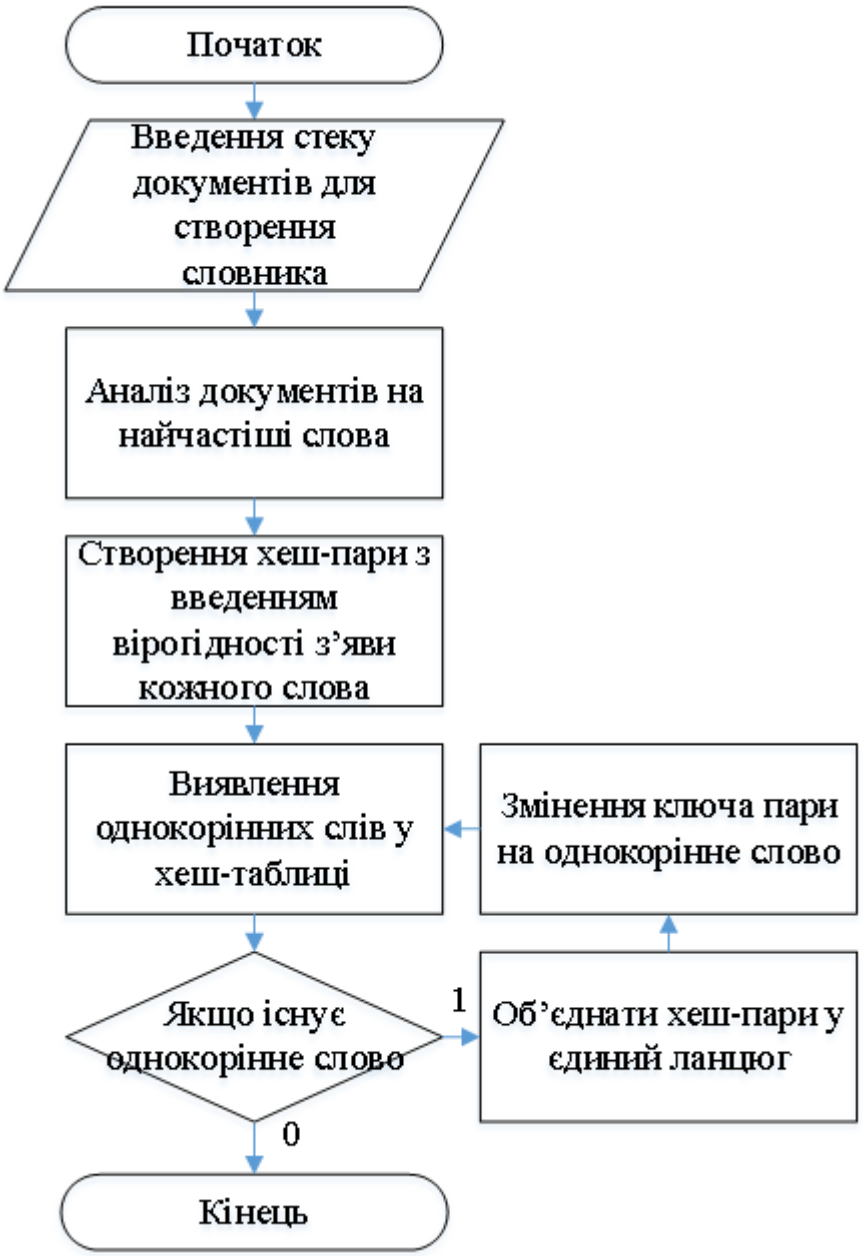

Рисунок 3.9. – Алгоритм створення словника для морфологічного аналізу

Наступним кроком необхідно утворити у хеш-таблиці пари. У ролі ключа пари запропоновано набір символів, яких вживається найбільше. У ролі значення виступають набори символів з меншою частотою використання у файлі. Додатковим параметром записується до кожного ключа вірогідність вживання слів з меншою частотою у якості метаданих.

Аналіз системою на пари зі схожими словами проводиться після утворення кожної нової пари у хеш-таблиці. Існування таких пар призводить до утворення значення зі зміною ключового слова на схоже спільне. Утворена пара у хеш-таблиці повинна забезпечувати аналіз якомога більшої кількості файлів зі схожим контекстом і дає можливість мінімізувати словник.

3.6. Алгоритм морфологічного аналізу

Представлений алгоритм – візуалізація покрокового виконання функцій морфологічного аналізу. Головною метою цього алгоритму є визначення певних слів у мережевому потоці інформації та базуючись на них розрахувати ймовірність приналежності до конфіденційної інформації.

Кроки виконання функціоналу морфологічного аналізу у загальному вигляді описані у алгоритмі на рисунку 3.8.

У якості вхідних даних для алгоритму надається інформація, що підлягає морфологічному аналізу. Зазвичай ця інформація представлена у вигляді контенту певного файлу.

Першим етапом алгоритму є визначення ключових слів наданого контенту, що зберігаються у хеш-таблиці. У випадку відсутності наявності таких слів алгоритм припиняє своє функціонування у зв’язку з тим, що надана інформація не несе у собі конфіденційних даних. У випадку наявності відповідного слова алгоритм запускає механізм аналізу контенту на базі значень до відповідних ключових слів у хеш-таблиці.

Система морфологічного аналізу виконує ретельний аналіз контенту на наявність усіх наборів символів із списку хеш-таблиці. При виявлені певних слів з ланцюга,

алгоритм автоматично вносить вірогідність даного слова до загальної вірогідності δ.

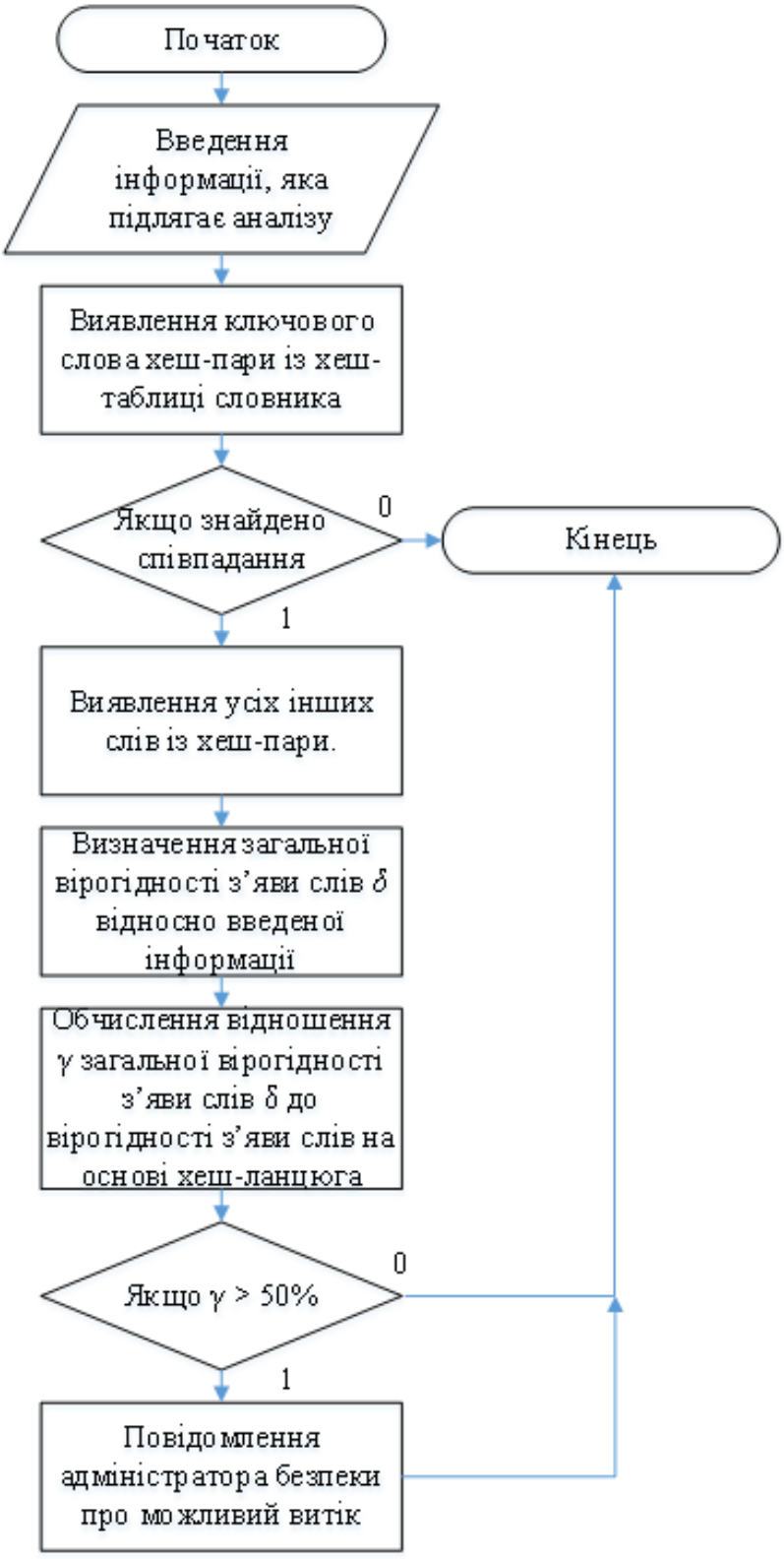

Рисунок 3.10 – Алгоритм морфологічного аналізу

Закінчення розрахунку вірогідності δ компрометує виконання наступного кроку – розрахунок відношення γ, яке відповідає відношенню загальної вірогідності δ до загальної вірогідності з’яви усіх слів із хеш-таблиці. На підставі результатів розрахунку відношення γ робиться висновок щодо статусу даних: конфіденційні чи загальнодоступні.

Адміністратор має можливість н підставі отриманого значення залежності γ робити висновки щодо цілісності інформації. Якщо показник вірогідності сягає відмітки більш ніж у 50%, то адміністратор отримує відповідне повідомлення про можливий витік даних.

ВИСНОВОК

В дипломній роботі були виконані дослідження та розробка системи запобігання витоку, призначеного для запобігання втрати конфіденційних даних та зменшенню ймовірності викрадення особистих або корпоративних даних.

Для досягнення мети дипломної роботи було проведено аналіз існуючих DLP систем, дослідження їх видів та типів, розглянуті аналоги уже існуючих програм для проектування системи. На підставі зазначеного аналізу в дипломній роботі були виконані етапи розробки системи попередження втрати даних та представлений комплекс механізмів для забезпечення максимально можливого захисту інформації. Розроблено загальну структуру системи, яка призначена для впровадження на робочі станції. Вона складається з трьох основних частин: агентська, адміністраторська та набору правил політики конфіденційності.

При цьому було визначено необхідні функціональні можливості та загальну структурну схему системи попередження витоку, що необхідно при розробці програмного продукту, який забезпечить безпеку конфіденційної інформації компанії.

Розроблено архітектурну та структурну схему програмного продукту, що наддасть можливість швидшого та ефективнішого впровадження системи до мережі споживача. Для досягнення більшої ефективності було прийнято рішення побудувати систему з об’єднаною архітектурою шлюзового та хостового типів систем.

Було розроблено програмне та інформаційне забезпечення системи запобігання витоку інформації, в результаті чого адміністратор матиме можливість контролювати можливості робочих станцій: доступу на веб сторінки, можливість листування з обмеженим колом осіб, можливість моніторингу та блокування документів приходячих з глобальної мережі в режимі реального часу, що відповідно, підвищує шанс на виявлення потенційних втручань у систему

конфіденційних файлів та збір більшої кількості інформації щодо типу втручання та спроби навмисного викрадення даних.

Визначено, що за допомогою програмного продукту споживач матиме можливість використовувати функціональні можливості системи, а також взаємодіяти з системою у вповноваженому режимі маючи адміністраторський доступ до системи.

Проведено дослідження поведінки DLP при роботі у режимах блокування та моніторингу, які забезпечують можливість повного контролювання обміну даними як всередині мережі так і з усіма зовнішніми носіями та ресурсами.

Практичне застосування запропонованого комплексного апаратного продукту та політик конфіденційності запобігання та попередження витоку даних дозволить повне попередження усіх ймовірних існуючих способів витоку конфіденційних даних.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛИТЕРАТУРИ

1. Автоматизовані інформаційні технології, [електронний ресурс], https://studfile.net/

2. Режим комерційної таємниці. захист конфіденційності інформації, [електронний ресурс], https://ips.ligazakon.net/

4. Програмно-апаратний захист інформації, [електронний ресурс], https://works.doklad.ru/

5. ГОСТ SOCKS5, [електронний ресурс], https://v2.gost.run/en/socks/6. Завгородній, В.І. Комплексний захист інформації у комп'ютерних системах [Текст]: навчальний посібник. / В. І. Завгородній. – М.: Логос, 2011. – 264 с.

6. Порівняння DLP-систем, [електронний ресурс], https://searchinform.ru/

7. «Об'єктні моделі. Стратегії, шаблони та програми» , [електронний ресурс], http://dspace.wunu.edu.ua/

8. Соціальні засади інформаційної безпеки ділової організації:, [електронний ресурс], https://ips.ligazakon.net/document/JG3TH00A

9. McAfee, [електронний ресурс], https://www.mcafee.com/enterprise/ru-ru/products/dlp-endpoint.html

10. Проблеми сучасних систем запобігання витоку даних з кінцевих точок мережі, [електронний ресурс], http://integritysys.com.ua/security/dlp/

11.SearchInforrm official library, [електронний ресурс], https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/

12.Посібник із захисту від внутрішніх загроз інформаційної безпеки, [електронний ресурс], https://er.dduvs.in.ua/bitstream

13. Як працюють DLP-системи: розуміємось на технологіях запобігання витоку інформації, [електронний ресурс], https://secretmag.ru/enciklopediya/chto-takoe-dlp-sistema-obyasnyaem-prostymi-slovami.htm

14. Онтології у комп'ютерних системах, [електронний ресурс], http://nzp.tnpu.edu.ua/article/view/65226

15. Семантичний аналіз на службі, [електронний ресурс], https://pidru4niki.com/1246122040309/logika/logiko-semantichniy_analiz_movi

16. All Technical Assistance , [електронний ресурс], http://allta.com.ua/nashi-resheniya/informacionnaya-bezopasnost/dlp-systems

17. Infowatch, [електронний ресурс], http://www.infowatch.ru/

18. Byte – онлайн-видання для IT-фахівців, [електронний ресурс], http://www.bytemag.ru/

19. Основи інформаційної безпеки, [електронний ресурс], http://www.intuit.ru/

20. Гарант Інформаційно-правовий портал, [електронний ресурс], http://base.garant.ru

21. Як працюють DLP-системи: розуміємося на технологіях запобігання витоку інформації, [електронний ресурс],. http://www.xakep.ru/

22. Захист від витоку конфіденційних даних Symantec DLP, [електронний ресурс], http://computel.ru/decision/ssb/Symantec/

23. DLP-системи-вибір, порівняння, рекомендації, [електронний ресурс], http://www.anti-malware.ru/dlp.

24. Впровадження DLP систем, [електронний ресурс], https://techexpert.ua/ru/our-services/implementation-of-dlp-systems/

25. Data Leak Protection, [електронний ресурс], https://www.kickidler.com/ru/dlp.html