Харківський національний університет імені В.Н. Каразіна
Факультет комп'ютерних наук
Безпека інформаційних систем і технологій

«Допущено до захисту»
Зав.кафедрою БІСТ

Сватовський І.І

« » червня 2023р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра
спеціальність: 125 Кібербезпека

на тему: «Дослідження методів і систем запобігання витокам даних»

оцінка « »
Голова ЕК
Лемешко О.В._____

Керівник Сватовський І.І
(прізвище та ініціали/підпис)
Рецензент Бакуменко Н.С.
(прізвище та ініціали/підпис)
Виконавець : студент групи КБ-41
Рекотов А.О.
(прізвище та ініціали/підпис)

Харків – 2023

РЕФЕРАТ

Пояснювальна записка містить 62 сторінки, 10 таблиць, 18 використаних джерел посилання.

Метою дослідження є аналіз та вивчення методів і систем запобігання витокам даних з метою забезпечення безпеки і конфіденційності інформації в сучасних інформаційних системах. Робота має на меті виявлення переваг, недоліків і особливостей різних систем запобігання витокам даних та надання рекомендацій щодо їх використання.

У процесі дослідження було застосовано методи аналізу літературних джерел, огляду існуючих систем запобігання витокам даних та аналізу переваг і недоліків цих систем. Для здійснення дослідження були використані наукові джерела, спеціалізовані публікації та інформація від провідних виробників систем запобігання витокам даних.

В результаті проведених досліджень були виявлені різні методи і системи запобігання витокам даних, такі як системи управління правами доступу (Access Rights Management Systems), системи запобігання вторгненням (Intrusion Prevention Systems), а також системи запобігання витокам даних (Data Loss Prevention Systems). Було проведено порівняльний аналіз цих систем.

Ключові слова: ВИТІК ДАНИХ, ШИФРУВАННЯ, КОНТРОЛЬ ДОСТУПУ, МОНІТОРИНГ, АУДИТУВАННЯ, ЗАПОБІГАННЯ ВТОРГНЕННЯМ, АНАЛІЗ СИСТЕМ.

ABSTRACT

The explanatory note contains 62 pages, 10 tables, 18 used references sources.

The purpose of the study is to analyze and study methods and systems for preventing data leaks in order to ensure the security and confidentiality of information in modern information systems. The work is aimed at identifying the advantages, disadvantages and features of various data leakage prevention systems and providing recommendations for their use.

In the process of research, the methods of literature analysis, review of existing data leakage prevention systems and analysis of the advantages and disadvantages of these systems were applied. The research was conducted using scientific sources, specialized publications and information from leading manufacturers of data leakage prevention systems.

As a result of the research, various methods and systems of data leakage prevention were identified, such as Access Rights Management Systems, Intrusion Prevention Systems, and Data Loss Prevention Systems. A comparative analysis of these systems was carried out.

Keywords: DATA LEAKAGE, ENCRYPTION, ACCESS CONTROL, MONITORING, AUDITING, INTRUSION PREVENTION, SYSTEMS ANALYSIS.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ 5

ВСТУП **7**

1 ТЕОРЕТИЧНИЙ АНАЛІЗ ПРОБЛЕМИ 8

1.1 Актуальність теми 8

1.2 Мета та завдання дослідження 8

1.3 Об’єкт та предмет дослідження 9

1.4 Методи дослідження 10

2 АНАЛІЗ МЕТОДІВ ЗАПОБІГАННЯ ВИТОКАМ ДАНИХ 11

2.1 Огляд існуючих методів запобігання витокам даних 11

2.2 Аналіз методів шифрування даних 17

2.3 Аналіз методів контролю доступу 21

2.4 Аналіз методів моніторингу та аудитування 26

3 АНАЛІЗ СИСТЕМ ЗАПОБІГАННЯ ВИТОКАМ ДАНИХ 31

3.1 Огляд існуючих систем запобігання витокам даних 31

3.2 Аналіз систем контролю доступу 33

3.3 Аналіз систем запобігання вторгненням 43

3.4 Аналіз систем запобігання витокам даних 50

ВИСНОВКИ 58

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ 60

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, ТЕРМІНІВ

VPN	–	Virtual Private Network
SHA	–	Secure Hash Algorithm
MD5	–	Message-Digest 5
SSL	–	Secure Sockets Layer
TLS	–	Transport Layer Security.
MAC	–	Mandatory Access Control
RBAC	–	Role-Based Access Control
ABAC	–	Attribute-Based Access Control
DAC	–	Discretionary Access Control
ІКСМ	–	Інформаційно-комунікаційні системи і мережі
ICMP	–	Internet Control Message Protocol
TCP	–	Transmission Control Protocol
UDP	–	User Datagram Protocol
MIB	–	Management Information Database
NMS	–	Network Management Systems
SNMP	–	Simple Network Management Protocol
RMON	–	Remote Network Monitoring
IDS	–	Intrusion Detection System

IPS	–	Intrusion Prevention System
DLP	–	Data Leak Prevention
ARMS	–	Access Rights Management Systems
AD	–	Active Directory
AWS	–	Amazon Web Services
USB	–	Universal Serial Bus
DoS	–	Denial of Service
NIPS	–	Network-based Intrusion Prevention System
WIPS	–	Wireless Intrusion Prevention System
NBA	–	Network Behavior Analysis
HIPS	–	Host-based Intrusion Prevention System
WLAN	–	Wireless Local Area Network

ВСТУП

Захист інформації є важливим завданням будь-якої організації, незалежно від її розміру та сфери діяльності. Однак із розвитком технологій і збільшенням кількості каналів передачі даних стає все важче захистити інформацію від несанкціонованого доступу та розголошення.

Метою даної роботи є вивчення методів і систем запобігання витоку даних. Для досягнення цієї мети аналізуються існуючі методи та системи запобігання витоку даних і визначаються їхні сильні та слабкі сторони.

Для досягнення поставленої мети визначено кілька завдань, які включають аналіз існуючих методів і систем запобігання витоку даних, оцінку їх ефективності та придатності для застосування в захисті інформації в різних сферах діяльності. Крім того, проводиться порівняльний аналіз методів і систем захисту інформації, щоб можна було визначити їх сильні та слабкі сторони. Особливу увагу приділено системам контролю доступу, запобігання вторгненням, моніторингу активності користувачів та виявлення загроз інформаційній безпеці.

Після аналізу систем і методів захисту інформації, були сформульовані рекомендації щодо вибору та використання систем і методів запобігання витокам даних в залежності від особливостей діяльності організацій, рівня конфіденційності інформації, бюджету на захист інформації, кваліфікації персоналу та інших чинників. Дані рекомендації набудуть практичного значення для організацій, що прагнуть забезпечити надійний захист своєї інформації від несанкціонованого доступу та витоку, а також можуть використані для подальших досліджень в цій області.

1 ТЕОРЕТИЧНИЙ АНАЛІЗ ПРОБЛЕМИ

1.1 Актуальність теми

У сучасному світі інформаційні технології є невід'ємною частиною бізнесу та повсякденного життя людей. Організації будь-якої форми власності, незалежно від їх розміру та напрямку діяльності, мають значну кількість даних, які потрібно захищати від несанкціонованого доступу та витоку.

Зростання кількості каналів передачі даних та швидкий розвиток технологій вимагають постійного вдосконалення методів та систем захисту інформації. Захист даних стає все складнішим завданням, адже зловмисники шукають нові способи для витоку інформації та несанкціонованого доступу до неї. У зв'язку з цим, дослідження в галузі захисту даних та розробка нових систем є надзвичайно важливою задачею для бізнесу та організацій будь-якої форми власності. Розробка ефективних методів та систем захисту даних дозволить зберегти довіру клієнтів та зберегти конкурентні переваги організацій у майбутньому. Таким чином, тема захисту даних є надзвичайно актуальною та потребує подальших досліджень та розробок.

Отже, актуальність теми полягає в необхідності розробки та використання методів та систем запобігання витокам даних, які забезпечать ефективний захист інформації від несанкціонованого доступу та витоку. Такі методи та системи повинні бути адаптовані до різних типів організацій та їх потреб, з урахуванням сучасних вимог безпеки даних.

1.2 Мета та завдання дослідження

Метою дослідження є аналіз та оцінка сучасного стану методів і систем запобігання витокам даних. Для досягнення цієї мети необхідно буде виконати такі завдання:

1) Проаналізувати стан захисту інформації в організаціях різних форм власності, включаючи державні установи, комерційні компанії та неприбуткові організації

2) Оцінити ефективність застосовуваних методів та систем захисту інформації від несанкціонованого доступу та витоку.

3) Вивчити основні методи та системи захисту інформації від несанкціонованого доступу та витоку, що застосовуються в сучасному світі.

4) Розробити рекомендації щодо покращення захисту інформації в організаціях, включаючи рекомендації щодо впровадження нових методів та систем захисту інформації від несанкціонованого доступу та витоку.

Результатом дослідження будуть рекомендації щодо покращення захисту інформації в організаціях різних форм власності, що забезпечать ефективний захист даних. Ці рекомендації допоможуть організаціям вибрати найбільш підходящі методі та системи захисту інформації від несанкціонованого доступу та витоку, за метою забезпечення максимальної безпеки даних.

1.3 Об’єкт та предмет дослідження

Об'єктом дослідження є системи запобігання витокам даних в організаціях різних форм власності від несанкціонованого доступу та витоку.

Предметом дослідження є методи та системи захисту інформації від несанкціонованого доступу та витоку, які використовуються в цих організаціях. Дослідження включає аналіз сучасних методів та систем захисту інформації, їх ефективності та придатності для різних типів організацій. Також, дослідженням охоплюється розробка рекомендацій щодо використання методів та систем захисту інформації в різних типах організацій.

У процесі дослідження буде звернена увага на такі аспекти предмета дослідження, як технічні та організаційні методи захисту інформації, якість та ефективність різних систем захисту, а також ризики витоку та несанкціонованого

доступу до інформації. Результати дослідження дозволять зрозуміти, які методи та системи захисту інформації найбільш підходять для цього, як зменшити ризики витоку та несанкціонованого доступу до інформації, та як забезпечити ефективний захист інформації в цілому.

1.4 Методи дослідження

Для досягнення мети дослідження та вирішення поставлених завдань будуть використовуватися наступні методи:

1) Аналіз наукової літератури, який дозволить оцінити стан сучасних систем та методів захисту інформації від несанкціонованого доступу та витоку. Для цього будуть використовуватися наукові джерела, бази даних, електронні ресурси та інші документи, які містять інформацію про цю тему.

2) Експериментальні дослідження, які дозволять перевірити ефективність розроблених методів та систем захисту інформації від несанкціонованого доступу та витоку.

3) Статистичний аналіз, який дозволить здійснити порівняння ефективності різних методів та систем захисту інформації від несанкціонованого доступу та витоку. Для цього будуть зібрані та проаналізовані дані про ефективність різних методів та систем захисту інформації на різних етапах дослідження. Далі будуть застосовані статистичні методи аналізу даних для порівняння ефективності різних методів та систем захисту інформації. В результаті проведення порівняльного аналізу будуть визначені найбільш ефективні методи та системи захисту інформації, які можна рекомендувати для використання в різних типах організацій.

2 АНАЛІЗ МЕТОДІВ ЗАПОБІГАННЯ ВИТОКАМ ДАНИХ

2.1 Огляд існуючих методів запобігання витокам даних

В останні роки зростає кількість витоків даних, що стає серйозною проблемою для компаній та організацій. Це пояснюється тим, що збільшується кількість даних, які зберігаються в електронному вигляді, а також збільшується кількість шляхів доступу них.

Існує багато методів запобігання витокам даних, які використовуються організаціями для захисту своєї інформації. Ось деякі з них:

1) Шифрування даних - це метод захисту інформації, що полягає в перетворенні звичайного тексту на шифр за допомогою алгоритмів шифрування. Шифрування даних забезпечує безпеку та конфіденційність інформації, що передається через мережі зв'язку, такі як Інтернет[1].

Один з головних принципів шифрування даних полягає у тому, що лише отримувач повинен мати ключ для дешифрування зашифрованої інформації[1]. Це означає, що в будь-якому місці на шляху передачі даних (наприклад, на мережевому роутері) інформація залишається зашифрованою і недоступною для зловмисників. Шифрування даних використовується для запобігання витоку даних в різних ситуаціях, наприклад:

- Під час передачі даних через мережі зв'язку, такі як Інтернет. Шифрування даних забезпечує конфіденційність та захист від перехоплення даних зловмисниками.
- Під час зберігання даних на комп'ютерах та інших пристроях. Шифрування даних забезпечує захист від несанкціонованого доступу до даних, які зберігаються на комп'ютері або іншому пристрої.

- Під час передачі даних між різними додатками та системами. Шифрування даних забезпечує захист від несанкціонованого доступу до даних, які передаються між різними додатками та системами[1].
- Під час роботи з електронною поштою та месенджерами. Шифрування даних забезпечує конфіденційність та захист від перехоплення даних зловмисниками[1].

Загалом, шифрування даних є важливим методом захисту інформації в сучасному світі. Використання цього методу дозволяє забезпечити конфіденційність інформації, що передається через мережі зв'язку, та зменшити ризик її витоку. Проте, важливо пам'ятати, що шифрування даних не є універсальним методом захисту інформації і може мати свої обмеження та вразливості. Тому, для забезпечення найвищого рівня захисту даних, необхідно поєднувати шифрування даних з іншими методами захисту, такими як захист від вірусів та шкідливих програм, бекапи даних та інші.

2) Використання біометричних методів ідентифікації є одним з методів запобігання витоку даних, який полягає у використанні фізіологічних або поведінкових рис особи для ідентифікації її особистості[2].

Фізіологічні риси включають такі параметри як[2]:

- Відбитки пальців;
- Розпізнавання обличчя;
- Розпізнавання ірису ока;
- Сканування вен та інші.

Поведінкові риси включають такі параметри як:

- Розпізнавання голосу;
- Стиль письма;
- Особливості походження та інші.

Використання біометричних методів ідентифікації може запобігти витоку даних за рахунок забезпечення високого рівня автентифікації особи, яка намагається отримати доступ до інформації. За допомогою біометричних методів можна переконатися, що особо, яка намагається отримати доступ до інформації, дійсно має право на цей доступ, тому що її ідентичність підтверджена на основі її унікальних фізіологічних або поведінкових рис.

Одним із прикладів використання біометричних методів ідентифікації є використання системи розпізнавання обличчя для отримання доступу до комп'ютера або мобільного пристрою. Коли користувач підходить до пристрою, система розпізнає його обличчя та автоматично розблоковує пристрій[2].

Іншим прикладом використання біометричних методів ідентифікації є використання системи розпізнавання відбитків пальців для авторизації операцій з банківськими рахунками, доступу до приміщень або для відкриття доступу до комп'ютерів або мобільних пристроїв. За допомогою сканера відбитків пальців можна ідентифікувати особу, яка намагається отримати доступ, та перевірити, чи має вона право на такий доступ[2].

Однак, варто мати на увазі, що жоден метод ідентифікації не є 100% надійним. Біометричні системи можуть бути обмануті, наприклад, шляхом використання моделей обличчя або пальців, які були створені на основі отриманих раніше даних. Також, біометричні дані можуть бути викрадені або використані незаконно.

Тому, наряду з використанням біометричних методів ідентифікації, необхідно застосовувати й інші методі захисту даних, такі як шифрування, двофакторна автентифікація, мережеві заходи безпеки та інші.

3) Контроль доступу до даних є важливим методом запобігання витоку даних, який полягає у забезпеченні обмеженого доступу до конфіденційної інформації тільки тим особам, які мають право на її отримання.

Цей метод базується на принципі "необхідності знання", що означає, що тільки ті особи, які потребують доступу до інформації для виконання своїх обов'язків, повинні мати доступ до неї. Для забезпечення контролю доступу до даних, організації використовують різноманітні методи, такі як авторизація та аутентифікація користувачів, захист мережі та фізичний контроль доступу до обладнання.

Одним з основних методів контролю доступу до даних є авторизація та аутентифікація користувачів. Авторизація полягає у визначенні того, чи має користувач право на доступ до конкретної інформації. Аутентифікація, з іншого боку, є процесом перевірки того, що користувач, який намагається отримати доступ до інформації, дійсно є тим, за кого він себе видає.

Для забезпечення більшого рівня безпеки, організації використовують різноманітні методи аутентифікації, такі як паролі, карти доступу, біометричні методи ідентифікації та інші. Наприклад, використання двохфакторної аутентифікації забезпечує більшу безпеку, оскільки вимагає перевірки не тільки чогось, що користувач знає (такого як пароль), але й чогось, що він має (такого як карта доступу або токен).

Захист мережі також є важливим методом контролю доступу до даних. Захист мережі включає в себе застосування мережевих заходів безпеки, таких як брандмауери та віртуальні приватні мережі (VPN), для обмеження доступу до мережі ззовні та контролю потоку даних між різними вузлами мережі. Додатково, захист мережі може включати моніторинг мережевої активності та виявлення потенційних загроз безпеці.

Фізичний контроль доступу до обладнання також є важливим методом контролю доступу до даних. Він включає застосування методів фізичного захисту, таких як замки на дверях, контроль доступу до серверних кімнат та інше. Ці заходи

можуть допомогти забезпечити те, що тільки авторизовані користувачі мають доступ до обладнання, на якому зберігається конфіденційна інформація.

Контроль доступу до даних є важливим методом запобігання витоку даних, який включає в себе різноманітні техніки та заходи безпеки для забезпечення того, що тільки авторизовані користувачі мають доступ до конфіденційної інформації.

4) Моніторинг дій користувачів - це метод контролю дій користувачів в системі, який використовується для виявлення та запобігання витоку даних. Цей метод передбачає систематичний аналіз дій користувачів, щоб відстежувати, які файли, папки, програми або ресурси вони відкривають, копіюють, переміщують або видаляють.

Моніторинг дій користувачів дозволяє виявляти неправомірні дії, такі як спроби викрадення конфіденційної інформації, втручання у систему або виконання неповноважних операцій. Цей метод дозволяє оперативно виявляти та реагувати на можливі загрози безпеці даних.

Для реалізації моніторингу дій користувачів використовують спеціальні програмні засоби, які реєструють дії користувачів в системі. Ці засоби можуть бути розгорнуті на окремих комп'ютерах або на всій мережі організації. При виявленні підозрілих дій, система може надсилати повідомлення адміністратору або автоматично виконувати певні заходи безпеки, наприклад, блокувати доступ до конфіденційної інформації або вимагати додаткової аутентифікації користувача.

Щоб забезпечити ефективність моніторингу дій користувачів, необхідно правильно налаштувати програмні засоби і визначити список дій, які будуть відстежуватися. Крім того, необхідно забезпечити конфіденційність зібраних даних та дотримуватися законодавства щодо зберігання та обробки персональних даних.

5) Навчання користувачів є важливим методом запобігання витоку даних, який полягає в підвищенні рівня освіченості користувачів з питань безпеки даних

та попередженні неправильних дій, які можуть призвести до витоку конфіденційної інформації.

Цей метод може бути спрямований на забезпечення безпеки даних як в робочому, так і в особистому контексті. В організаціях, де відбувається обробка конфіденційної інформації, навчання користувачів може включати в себе такі теми як:

- Безпека електронної пошти;
- Безпека паролів;
- Захист від фішингу;
- Використання зашифрованих каналів зв’язку;
- Правила зберігання конфіденційної інформації;
- Процедури повідомлення про можливі витоки даних та інші.

Крім того, навчання користувачів може включати в себе інформування про найновіші загрозі безпеці даних та оновлення політик безпеки. Навчання може відбуватися за допомогою онлайн-курсів, вебінарів, тренінгів та інших форм навчання

У побутовому контексті, навчання користувачів може включати в себе такі питання як:

- Безпека використання інтернету;
- Захист пристроїв від кібератак;
- Безпека використання соціальних мереж;
- Забезпечення безпеки особистої інформації

Вивчення принципів та практик безпеки може допомогти користувачам зрозуміти ризики, пов’язані з неправильним використанням технологій та роботою с конфіденційною інформацією, та допоможе вжити заходів для забезпечення безпеки своїх даних. Це може бути використання сильних паролів, перевірку достовірності електронної пошти та посилань, зберігання даних в безпечних місцях,

використання антивірусного програмного забезпечення та оновлення його на пристроях.

Загальна мета цього методу полягає у створенні культури безпеки даних, коли користувачі свідомо вживають заходів для захисту своїх даних, які є невід'ємною частиною їх особистого та професійного життя. Це допомагає попередити витоки даних та зменшити ризик збитків, пов'язаних з ними.

2.2 Аналіз методів шифрування даних

Шифрування даних - це процес перетворення звичайного тексту в код, який можна розшифрувати тільки з ключем. Це дозволяє зберегти дані в безпечному стані, навіть якщо вони будуть викрадені. Існує декілька методів шифрування даних, які використовуються для захисту інформації:

1) Симетричне шифрування - це метод шифрування, при якому використовується один ключ як для шифрування, так і для розшифрування повідомлення. Це означає, що якщо одна сторона використовує певний ключ для шифрування повідомлення, то інша сторона може використати цей же ключ для розшифрування його[4].

Процес шифрування зазвичай складається з таких кроків: спочатку повідомлення перетворюється на послідовність бітів, які потів перетворюються на інші біти, що є шифрованими даними, за допомогою ключа. Розшифрування даних відбувається за допомогою того ж самого ключа. який був використаний для шифрування. Отже, щоб відновити початкові дані, потрібно мати доступ до ключа.

Симетричне шифрування широко використовується в сферах, де швидкість обробки даних та простота використання є найважливішими. Наприклад, в банківський сфері для шифрування транзакцій, а також в бездротових мережах для захисту передачі даних.

Однак, симетричне шифрування має певні недоліки. Найбільш очевидним з них є потреба в обміні ключами між сторонами, які хочуть здійснити шифрування

та розшифрування. Крім того, зберігання ключів також стає проблемою, особливо якщо ключі використовуються для багатьох цілей. З цієї причини, у більш складних системах зазвичай використовують асиметричне шифрування, яке дозволяє вирішити ці проблеми[4].

Серед найпопулярніших алгоритмів симетричного шифрування можна виділити DES, AES, Blowfish, RC5 та інші.

2) Асиметричне шифрування - це метод шифрування даних, який використовує два ключі: публічний та приватний. Публічний ключ доступний всім, і його можна використовувати для шифрування повідомлень, які можуть бути розшифровані лише за допомогою приватного ключа, який належить власнику[3].

Асиметричне шифрування також відоме як криптографія з відкритим ключем, оскільки публічний ключ використовується для шифрування даних, які можуть бути розшифровані за допомогою відповідного приватного ключа, який залишається в руках власника.

Цей метод шифрування дозволяє забезпечити безпеку передачі даних в мережі, оскільки він дозволяє відправнику шифрувати повідомлення з використанням публічного ключа отримувача, а отримувач може розшифрувати повідомлення за допомогою свого приватного ключа[3].

Крім того, асиметричне шифрування використовується для створення цифрових підписів, які забезпечують цілісність повідомлення та перевіряють автентичність відправника. Для створення цифрового підпису відправник використовує свій приватний ключ, а отримувач може перевірити цифровий підпис за допомогою публічного ключа відправника.

Асиметричне шифрування є безпечнішим методом шифрування, ніж симетричне шифрування, оскільки воно не вимагає передачі приватного ключа. Однак, воно може бути менш ефективним за часом та обчислювальною складністю, оскільки процес шифрування та розшифрування може бути повільним для обробки

великих обсягів даних. Серед найпопулярніших алгоритмів асиметричного шифрування можна виділити RSA, ElGamal, DSA та інші[3].

3) Хеш-функція - це математична функція, яка приймає на вхід будь-який рядок довільної довжини і повертає фіксований вихід, який називається хеш-значенням. Цей вихід може бути використаний для перевірки цілісності даних або для їх ідентифікації[5].

Хеш-функції застосовуються для шифрування даних в тих випадках, коли не потрібно відновлювати початкові дані з їх хеш-значення, але потрібно перевірити, чи були вони змінені. Наприклад, хеш-функції можуть бути використані для перевірки цілісності файлів після їх завантаження з Інтернету або для захисту паролів.

Один і той же вхід завжди дає той самий вихід у випадку використання однієї і тієї ж хеш-функції. Це дозволяє легко порівнювати хеш-значення для перевірки, чи збігаються два рядки. Але зворотний процес - відновлення початкових даних з хеш-значення неможливий[5].

Основні властивості хеш-функцій - це відсутність залежності вихідного значення від розміру вхідних даних (фіксований розмір хеш-значення), однозначність (один і той же вхід завжди дає одне і те ж хеш-значення) та незворотність (неможливість відновити початкові дані з хеш-значення).

Хеш-функції можуть бути підвергнуті атакам, таким як зіткнення (collision), коли два різні рядки дають одне і те ж хеш-значення. Це може дозволити зловмисникам змінювати дані, зберігаючи при цьому той самий хеш. Для захисту від таких атак використовуються криптографічні хеш-функції, які мають велику довжину хеш-значення та спеціальні алгоритми для запобігання зіткненням[5].

Найпоширеніші криптографічні хеш-функції - це SHA (Secure Hash Algorithm) та MD5 (Message-Digest Algorithm 5). Однак, MD5 вже вважається

небезпечною і не рекомендується для використання, тому що відомі вразливості в її алгоритмі зроблюють її вразливою до атак.

Хеш-функції також можуть бути використані для створення цифрових підписів, які можуть підтверджувати автентичність даних та авторства документа. У такому випадку хеш-функція застосовується до даних, які підписуються, і результат зашифровується приватним ключем користувача. При перевірці підпису хеш-функція застосовується до підписаного документа, а результат розшифровується за допомогою відкритого ключа автора. Якщо результати співпадають, це підтверджує автентичність та цілісність документа.

4) SSL (Secure Sockets Layer) і його наступник TLS (Transport Layer Security) - це протоколи криптографічного захисту, які забезпечують безпечну передачу даних через Інтернет.

SSL/TLS забезпечує захист від шпигунського або неправомірного доступу до інформації, а також захист від підробки і перехоплення даних, що передаються між комп'ютерами.

SSL/TLS працює на рівні транспортного протоколу (наприклад, на рівні HTTP), і використовує симетричне та асиметричне шифрування для забезпечення конфіденційності, цілісності та аутентифікації даних.

У SSL/TLS взаємодія між сервером і клієнтом складається з кількох етапів, у тому числі:

- Встановлення зв'язку і обмін інформацією про підтримувані криптографічні алгоритми і версії протоколів.
- Аутентифікація сервера за допомогою цифрових сертифікатів.
- Генерація спільного ключа для симетричного шифрування даних.
- Захищена передача даних між сервером і клієнтом з використанням симетричного шифрування та контролю цілісності даних за допомогою хеш-функцій.

SSL/TLS є надійним і популярним методом шифрування даних, і використовується для захисту веб-сайтів, електронної пошти, мобільних додатків та інших додатків, що працюють через мережу Інтернет.

У загальному, вибір методу шифрування даних залежить від конкретної ситуації та потреб безпеки. Кожен метод має свої переваги та недоліки, і важливо розуміти їх, щоб правильно вибрати метод, який найкраще підходить для ситуації.

2.3 Аналіз методів контролю доступу

Контроль доступу - це процес встановлення правил та обмежень, які визначають, хто може отримувати доступ до певної інформації або ресурсів та яким способом. Це важлива складова частина забезпечення безпеки інформації в будь-якій організації.

Нижче описані деякі з найпоширеніших методів контролю доступу.

1) Контроль доступу на основі ролей (RBAC) - це метод управління доступом до ресурсів в комп'ютерних системах, де доступ до ресурсів (таких як файли, папки, програми тощо) призначається користувачам на основі їхніх ролей в системі. Кожна роль має свій набір дозволів на доступ до ресурсів, а користувачі можуть бути призначені для однієї або більше ролі[6].

RBAC дозволяє управляти доступом користувачів до різних ресурсів в системі, зокрема забезпечувати контроль доступу до конфіденційних даних або функцій, що вимагають певних прав.

Основні компоненти RBAC включають ролі, користувачів та ресурси. Ролі визначаються відповідно до обов'язків та функцій користувачів у системі, а користувачі можуть бути призначені для однієї або більше ролі. Кожна роль має свій набір дозволів на доступ до ресурсів, які можуть бути змінені адміністратором системи. Дозволи включають дії, які користувачі можуть виконувати з ресурсами, наприклад, перегляд, редагування або видалення файлів. Ресурси можуть включати

файли, директорії, пристрої, мережеві з'єднання, програми та інші компоненти системи.

В RBAC визначаються правила, які встановлюють, які ролі мають доступ до яких ресурсів. Наприклад, правило може визначати, що роль "адміністратор" має повний доступ до всіх ресурсів системи, тоді як роль "користувач" може мати обмежений доступ до деяких ресурсів.

RBAC також включає механізми аутентифікації та авторизації, що забезпечують, що користувач, який намагається отримати доступ до ресурсів, має право на цей доступ[6].

Узагалі, RBAC є потужним інструментом для забезпечення безпеки та контролю доступу до ресурсів в комп'ютерних системах.

2) Контроль доступу на основі атрибутів (ABAC) - це метод управління доступом до ресурсів в комп'ютерних системах, де доступ до ресурсів призначається користувачам на основі їхніх атрибутів. Кожен користувач має набір атрибутів, які описують його характеристики, такі як ідентифікатор, посада, місцезнаходження, відділ тощо. Рішення про надання доступу до ресурсу приймається на основі зіставлення атрибутів користувача з вимогами, встановленими для цього ресурсу[6].

ABAC дозволяє ефективно управляти доступом користувачів до різних ресурсів в системі на основі їхніх характеристик та вимог до ресурсу. Цей підхід до контролю доступу є більш гнучким та масштабованим, ніж традиційні методи контролю доступу, які засновані на ідентифікації користувачів та наданні їм окремих дозволів на доступ до кожного ресурсу.

Крім того, ABAC дозволяє легко керувати доступом великої кількості користувачів до ресурсів в складних системах. Наприклад, велика компанія може мати тисячі користувачів, кожен з яких має свої власні характеристики та вимоги

до ресурсів. ABAC дозволяє управляти цими характеристиками та вимогами централізовано, що спрощує адміністрування системи.

Основні компоненти ABAC включають атрибути, політики та ресурси. Атрибути визначаються відповідно до характеристик користувачів у системі, політики встановлюють вимоги до доступу до ресурсів на основі атрибутів користувачів, а ресурси - це об'єкти, до яких потрібно контролювати доступ. Політики можуть бути визначені на різних рівнях, таких як рівень системи, додатку або ресурсу. Крім того, ABAC може бути інтегрований з іншими методами контролю доступу, такими як Role-Based Access Control (RBAC) або Mandatory Access Control (MAC), що дозволяє створювати більш складні та точні системи контролю доступу[6].

Однією з переваг ABAC є можливість динамічно змінювати вимоги до доступу до ресурсів в реальному часі на основі зміни характеристик користувачів або зміни вимог до ресурсів. Наприклад, якщо користувач переходить на нову посаду, його атрибути можуть змінитися, що автоматично впливає на його доступ до ресурсів в системі.

Крім того, ABAC дозволяє застосовувати політики до груп користувачів, що спрощує управління доступом до ресурсів для цілих відділів або підрозділів. ABAC також забезпечує більш високий рівень безпеки, оскільки вимоги до доступу до ресурсів можуть бути дуже точними та детальними, що дозволяє уникнути несанкціонованого доступу до важливих ресурсів в системі.

У загальному ABAC є ефективним та гнучким методом контролю доступу до ресурсів в комп'ютерних системах. Він дозволяє управляти доступом користувачів до ресурсів на основі їхніх атрибутів та вимог до ресурсу, що спрощує управління доступом в складних системах з великою кількістю користувачів та ресурсів.

3) Контроль доступу на основі маркерів (MAC) - це метод управління доступом до ресурсів, який використовує систему маркерів для встановлення

дозволів на доступ до ресурсу. Цей метод зазвичай використовується в системах, де безпека є основним аспектом, наприклад, в урядових та військових системах.

У системі контролю доступу на основі маркерів кожен об'єкт та користувач має свій унікальний маркер безпеки, який визначає рівень доступу до об'єкта. Ці маркери призначаються системою або адміністратором та зберігаються в системі. Для доступу до ресурсу користувач повинен мати маркер безпеки, який має відповідний рівень доступу до цього ресурсу[6].

Система контролю доступу на основі маркерів дозволяє забезпечити високий рівень безпеки, оскільки дозволи на доступ до ресурсів залежать від рівня маркерів безпеки, а не від ідентифікації користувача. Це означає, що навіть якщо хакер отримає доступ до системи, він не зможе отримати доступ до ресурсів, які мають маркер безпеки, що перевищує його рівень маркера безпеки.

Однак, використання системи контролю доступу на основі маркерів може бути складним та обтяжливим, оскільки кожен об'єкт та користувач має свій унікальний маркер безпеки, що потребує багато ресурсів для зберігання та обробки. Крім того, встановлення маркерів безпеки для кожного ресурсу та користувача може бути складним та часом затратним процесом.

4) Дискреційний контроль доступу (Discretionary Access Control або DAC) - це метод управління доступом до ресурсів в комп'ютерних системах, де власник ресурсу може самостійно встановлювати права доступу до своїх ресурсів.

У DAC, кожен об'єкт (файл, папка, документ тощо) має власника, який визначає права доступу до нього. Власник може призначити доступ до свого об'єкта іншим користувачам або групам користувачів та визначити, які операції дозволені для кожного з них. Наприклад, власник може дозволити іншому користувачеві читати вміст файлу, але не дозволяти йому редагувати його.

Принцип DAC полягає у тому, що власник ресурсу може самостійно встановлювати права доступу до своїх ресурсів без втручання адміністратора

системи. Це дозволяє більш гнучко керувати доступом до ресурсів та забезпечити більш високий рівень безпеки. Однак, такий підхід також може призвести до невірної конфігурації прав доступу, якщо власник не має достатньої експертизи щодо безпеки та управління доступом[6].

DAC є одним з найбільш розповсюджених методів контролю доступу. Він використовується в багатьох операційних системах та додатках, включаючи Windows та Unix/Linux. Однак, з ростом складності систем та збільшенням кількості користувачів та ресурсів, DAC може стати непрактичним, тому що він не забезпечує достатнього рівня гнучкості та масштабованості.

5) Ідентифікація та автентифікація - це методи контролю доступу, що використовуються для підтвердження ідентичності користувача та перевірки його прав на доступ до ресурсів комп'ютерної системи.

Ідентифікація - це процес визначення ідентичності користувача шляхом представлення унікального ідентифікатора або ім'я користувача. Це може бути логін, номер працівника, адреса електронної пошти, номер паспорту тощо. Кожен користувач має унікальний ідентифікатор, який служить для його ідентифікації в системі.

Автентифікація - це процес перевірки ідентичності користувача шляхом підтвердження правильності введеного ним пароля, ключа або іншого виду ідентифікаційних даних. Коли користувач вводить свої ідентифікаційні дані, система перевіряє їхню відповідність збереженим у базі даних даним, які вказані при реєстрації. Якщо дані відповідають, користувач автентифікується і отримує доступ до системи.

Ідентифікація та автентифікація використовуються в комплексі з іншими методами контролю доступу, такими як ролевий контроль доступу (RBAC) та контроль доступу на основі атрибутів (ABAC), для забезпечення безпеки в комп'ютерних системах. Використання ідентифікації та автентифікації дозволяє

забезпечити безпеку доступу до ресурсів системи та захистити їх від несанкціонованого доступу користувачів.

Методи контролю доступу можуть бути застосовані окремо або в поєднанні один з одним. Важливо пам'ятати, що контроль доступу - це процес, який потребує постійного оновлення та адаптації до змін у вимогах безпеки інформації та внутрішніх процесів організації.

2.4 Аналіз методів моніторингу та аудитування

Різноманіття засобів, що використовуються для контролю та аналізу ІКСМ поділяються на декілька класів:

1) Системи керування мережею – централізовані програмно-апаратні системи, що збирають дані про стан вузлів та комунікаційних пристроїв мережі, дані про трафік, що циркулює у мережі. Особливістю даних систем є, те що вони в автоматичному або напівавтоматичному режимах виконують дії з керування мережею – увімкнення або відімкнення портів приладів, зміна змісту маршрутизуючих таблиць, правил брандмауерів, тощо[7-8].

2) Засоби керування системою – виконують функцію, що аналогічні до систем керування мережею, але по відношенню до комунікаційного обладнання. Також вона здатна виконувати найпростіший аналіз мережевого трафіка.

3) Вбудовані системи діагностики та управління – дані системи реалізуються шляхом використання програмних модулей у комунікаційному обладнанні. Вони направлені на виконання функцій діагностики та керування лише над одним пристроєм. На даний час вбудовані системи також виконують роль SNMP-агентів, що постачають дані для систем керування мережею.

4) Аналізатори протоколів – програмні або програмно – апаратні системи, що виконують лише функції моніторингу та аналізу трафіку. Характеристикою аналізатора є здатність до виявлення певного числа протоколів. Аналізатори

встановлюють логічні умови з метою перехоплення пакетів для визначених протоколів.

5) Експертні системи – даний вид систем акумулює людські знання про виявлення причин аномальної роботи мережі та можливих способах повернення мережі до нормального режиму функціонування. Експертні системи часто реалізуються у вигляді підсистем засобів моніторингу та систем керування мережею. Функціональною основою складних експертних систем є так звані бази знань, що володіють елементами штучного інтелекту.

Розглянемо найбільш поширені методи проведення моніторингу доступності та цілісності інформаційних потоків. До основних методів моніторингу відносяться: активний моніторинг, пасивний моніторинг, моніторинг мережі базований на маршрутизації, моніторинг за аномальною поведінкою.

Активний моніторинг. Суть активного моніторингу полягає у передачі в інформаційну мережу пакетів з метою вимірювання параметрів між двома кінцевими точками корпоративної мережі. Вимірюються такі параметри: доступність, маршрут, затримка пакетів, зміна порядку пакетів, втрата пакетів, пропускна здатність каналу. Базовими інструментами, що здатні допомогти у вимірюванні вищезгаданих параметрів є ping, що вимірює затримки та втрату пакетів, traceroute– допомагає побудувати топологію мережі. Ці інструменти використовують ICMP пакети. Також даний метод аудиту реалізується з використанням інструменту iperf, що генерує TCP та UDP трафік для вимірювання пропускної здатності мережі та втрати пакетів. Недоліком активного моніторингу є те, що згенерований трафік завантажує мережу під час її експлуатації.

Пасивний моніторинг. На відміну від активного моніторингу, пасивний метод не генерує надлишкового трафіку, та вимірює параметри продуктивності лише в одній точці мережі. Даний метод знайшов застосування у пакетних сніферах.

Результати пасивного моніторингу можуть бути досліджені лише постфактум, при цьому ніякого навантаження на мережу не має.

Моніторинг мережі, що базується на маршрутизації. Такі методи зазвичай реалізуються програмно-апаратними засобами мережевих пристроїв.

Simple Network Management Protocol. Даний протокол є протоколом прикладного рівня стеку TCP/IP. Його використання надає адміністратору мережі можливості з керування та контролю над пристроями (комутаторами, маршрутизаторами, серверами, модемами, робочими станціями) та додатками у мережі шляхом обміну інформацією між агентами, що встановлені у мережевих пристроях та менеджерами, що встановлені на станціях керування (Network Management Systems) [7]. Агенти є програмним забезпеченням, здатним перетворювати дані протоколу SNMP у команди керування пристроями, та навпаки. Станції керування є програмним забезпеченням, що здійснюють моніторинг та контроль за керованими пристроями. Обробка всіх даних,

отриманих з агентів, виконується на станціях. Станції керування здатні виконувати 4 базові операції: read – зчитування значень змінних, що знаходяться у пам’яті керованих пристроїв; write – змінює значення змінних; traversal operations – накопичення інформації щодо доступних змінних керованого пристрою; trap – повідомляє NMS про певну подію, що сталася з керованим пристроєм. Недоліком використання SNMP у мережі, є те що даний протокол є вразливим, оскільки жодних процедур з аутентифікації користувачів не виконується.

Remote Monitoring (RMON). RMON включає в собі різні мережеві монітори та системи для обміну інформацією мережевого моніторингу. Даний метод моніторингу є розширенням Management Information Database (MIB). На відміну від SNMP, коли NMS повинна власноруч надсилати запити на отримання інформації, RMON дозволяє налаштовувати обробники подій, що будуть спрацьовувати за певних критеріїв. Іншою відміною від SNMP є те, що агенти RMON збирають та

зберігають інформацію самостійно. Агентами можуть бути мережеві пристрої зі вбудованим програмним забезпеченням та комп'ютери. Агенти здатні бачити трафік лише всередині певного сегменту. Роль клієнта виконує станція керування, що взаємодіє з агентами з використанням SNMP [8]. Дана технологія функціонує на мережевому рівні та нижче.

Моніторинг за аномальною поведінкою. Суть даного методу полягає у моніторингу стану мережі та виявлення значних відхилень параметрів у порівнянні зі значеннями цих параметрів при стабільному функціонуванні. Наприклад, для виявлення аномальної динаміки мережевого трафіку використовується штучний інтелект та статистичні показники. Для ефективного застосування даного методу, спочатку необхідно зафіксувати контрольні значення важливих параметрів функціонування мережі. Виявлення аномалій запускає модуль для подальшого аналізу трафіку або спричинює повідомлення для аналітика безпеки [8].

Базовими вимогами, що ставляться до систем моніторингу є:

- масштабованість та розподіленість. Дані властивості є взаємопов'язаними, оскільки високий рівень здатності до масштабування досягається за рахунок розподіленості системи управління. Під розподіленістю будемо розуміти те, що система може включати декілька серверів та клієнтів. Сервери (менеджери) накопичують дані про поточний стан мережі з встановлених у ній агентів у власній базі даних. Клієнти використовують інтерфейси для доступу до накопиченої інформації серверу;
- відкритість, що дозволяє використовувати систему з різнотипним обладнанням від різних виробників. [8];
- ступінь завантаженості ІКСМ. Функціональні компоненти, що входять до складу систем контролю здатні генерувати трафік для вимірювання показників продуктивності мережі, що впливає на пропускну здатність каналів передачі;
- кількість вузлів, що може аналізуватися та контролюватися системою;

- можливість встановлення клієнтів та серверів на робочі станції з різними операційними системами;
- отримання інформації про динаміку трафіку у режимі реального часу;
- здатність системи до конфігурації контролю окремих програмних додатків;
- наявність централізованого місця накопичення службової інформації, з можливістю індексування для прискорення витягу потрібних даних;
- можливість створення реєстру наявних у мережі програмних та апаратних ресурсів.

Виділення вимог дозволило сформувати критерії оцінки якості системи аудиту та моніторингу інформаційних потоків: підтримка різних операційних систем; можливість аудиту та контролю різних за призначенням серверів; можливість аудиту та контролю СУБД; виявлення відхилень функціонування мережі від норми (поява незареєстрованих вузлів, втрата зв’язку з окремими вузлами, втрата пакетів, перенавантаження комунікаційних пристроїв); підтримка графічних інтерфейсів для перегляду звітів, можливості конфігурування параметрів налаштувань .

3 АНАЛІЗ СИСТЕМ ЗАПОБІГАННЯ ВИТОКАМ ДАНИХ

В сучасному цифровому світі, де зберігається велика кількість цінної та конфіденційної інформації, запобігання витокам даних стає надзвичайно важливою задачею. Існує ряд систем та інструментів, призначених для виявлення, запобігання та відстеження витоків даних. У цьому розділі будуть розглянуті деякі з них.

3.1 Огляд існуючих систем запобігання витокам даних

Системи запобігання витокам даних:

1) Системи управління правами доступу (Access Rights Management Systems): Ці системи встановлюють та керують правами доступу до різних ресурсів у комп'ютерній мережі або інформаційній системі. Вони дозволяють визначати, які користувачі мають доступ до яких даних, і контролюють цей доступ з урахуванням рівня авторизації та політик безпеки[9].

2) Системи виявлення вторгнень (Intrusion Detection Systems, IDS): Ці системи призначені для виявлення незаконних або шкідливих активностей у комп'ютерній мережі або системі. Вони моніторять мережевий трафік та системні журнали, аналізують їх і сповіщають про можливі вторгнення або аномальні дії, що можуть призвести до витоку даних.

3) Системи запобігання вторгненням(Intrusion Prevention System, IPS). Є програмою мережевої безпеки, яка відстежує системну або мережеву активніть на предмет зловмисної діяльності. IPS розглядаються як доповнення до IDS, оскільки вони обидві відстежують мережевий трафік і системну активність. Виявлення зловмисної активності, сповіщення про неї, збір інформації с приводу неї та спроби заблокувати або зупинити її – основні функції IPS[10].

4) Системи запобігання витокам даних (Data Loss Prevention, DLP): Ці системи виявляють та запобігають витокам конфіденційної або важливої

інформації з комп'ютерної системи. Вони встановлюють правила та політики щодо використання, передачі та зберігання даних, моніторять ці дії та вживають заходів для запобігання неправомірному витоку даних[11].

5) Системи криптографічного захисту (Cryptographic Protection Systems): Ці системи використовують криптографію для захисту даних від несанкціонованого доступу та витоку. Вони використовують алгоритми шифрування для перетворення даних у незрозумілу форму, яку можуть розшифрувати лише авторизовані особи або системи. Криптографічні системи забезпечують конфіденційність та цілісність даних, унеможливлюючи їх розкриття навіть у випадку втрати або крадіжки.

6) Системи моніторингу та аудитування (Monitoring and Auditing Systems): Ці системи відіграють важливу роль у виявленні та відстеженні витоків даних. Вони моніторять активність користувачів, доступ до ресурсів, мережевий трафік та інші параметри системи з метою виявлення підозрілих або некоректних дій. Крім того, системи аудитування збирають та зберігають журнали подій для подальшого аналізу та встановлення причин витоків даних.

7) Системи боротьби зі шкідливим програмним забезпеченням (Malware Defense Systems): Ці системи спеціалізуються на виявленні та блокуванні шкідливих програм, які можуть бути використані для отримання та передачі конфіденційної інформації. Вони використовують антивірусні програми, файрволи та інші заходи для забезпечення безпеки системи та запобігання витоку даних через шкідливе програмне забезпечення.

Ці системи запобігання витокам даних використовуються як окремо, так і в комбінації, для створення комплексних заходів безпеки даних. Вони допомагають попереджати витоки даних, виявляти потенційні загрози, реагувати на інциденти та забезпечувати захист інформації в комп'ютерних системах. Деякі системи мають вбудовані функції аналізу поведінки, машинного навчання та інтелектуального

аналізу даних для виявлення аномальних патернів та неправильних дій, що можуть вказувати на витік або небажану активність.

Крім цього, системи запобігання витокам даних можуть мати можливості контролю доступу, шифрування, маркування даних, контролю вихідних точок, моніторингу передачі даних та інші функції, що сприяють запобіганню витокам даних на різних рівнях системи.

Важливим елементом систем запобігання витокам даних є постійне оновлення та покращення заходів безпеки з урахуванням нових загроз, уразливостей та технологічних розвитків. Це дозволяє підтримувати високий рівень захисту даних та зменшувати ризик витоку інформації.

Загалом, системи запобігання витокам даних відіграють критичну роль у забезпеченні безпеки даних та зменшенні ризику витоку цінної інформації. Їх використання сприяє підвищенню довіри до комп'ютерних систем, захисту бізнесу від фінансових втрат, репутаційних збитків та правових проблем, пов'язаних з витоками даних

3.2 Аналіз систем контролю доступу

Системи управління правами доступу (Access Rights Management Systems, ARMS) - це програмні рішення, які дають змогу ефективно керувати правами доступу користувачів до різноманітних ресурсів, таких як: файли, папки, додатки, бази даних та інші об'єкти в системах. ARMS забезпечують контроль, надання та управління правами доступу відповідно до політик безпеки організації.

Основною метою ARMS є забезпечення контролю доступу до ресурсів і належної організації. Адміністратори систем можуть встановлювати, змінювати та вилучати права доступу в залежності від обов'язків та потреб окремих користувачів або груп користувачів. ARMS забезпечують детальний контроль над тим, хто може отримати доступ до яких ресурсів, які дії можуть вони виконувати з цими ресурсами та в який час[10].

Основні компоненти ARMS включають:

1) Механізм автентифікації: ARMS забезпечують ідентифікацію користувачів та перевірку їхньої автентичності перед наданням доступу до ресурсів. Це може включати використання логінів, паролів, біометричних даних або інших методів автентифікації[9].

2) Управління ролями: ARMS базуються на концепції ролей, де користувачам призначаються відповідні ролі з набором прав доступу. Це спрощує процес управління доступом, оскільки права надаються на рівні ролей, а не на індивідуальних користувачів[9].

3) Правила і політики: ARMS дозволяють встановлювати правила та політики доступу до ресурсів. Це включає встановлення обмежень щодо типів дій, які можуть виконувати користувачі з ресурсами, обмеження доступу на основі рівня конфіденційності даних, контроль часових рамок доступу та інші параметри. Правила і політики ARMS можуть бути налаштовані з урахуванням внутрішніх політик безпеки організації.

4) Аудит та журналювання: ARMS забезпечують моніторинг та журналювання дій користувачів щодо доступу до ресурсів. Це дозволяє виявляти потенційні порушення безпеки, визначати вразливі місця та вживати відповідних заходів для запобігання витоку даних або несанкціонованого доступу[9].

5) Централізоване управління: ARMS надають централізований механізм управління правами доступу. Це дозволяє адміністраторам легко керувати правами користувачів, розподіляти ролі та права доступу, змінювати налаштування і відслідковувати доступ користувачів до ресурсів з одного місця[10].

6) Інтеграція з іншими системами: ARMS можуть інтегруватися з іншими системами безпеки, такими як системи ідентифікації та аутентифікації, системи моніторингу подій, системи управління інцидентами та інші. Це забезпечує

комплексний підхід до управління безпекою і забезпечує спрощення адміністративних процесів.

7) Забезпечення дотримання регуляторних вимог: ARMS дозволяють організаціям виконувати вимоги щодо безпеки та конфіденційності, встановлені регуляторними органами. Вони надають можливість встановлювати політики та контролювати доступ до ресурсів відповідно до законодавства та нормативних актів.

8) Управління життєвим циклом доступу: ARMS дозволяють ефективно управляти життєвим циклом доступу до ресурсів. До цього входить: надання прав доступу новим користувачам, зміну прав доступу під час зміни ролей або обов'язків, призначення тимчасового доступу та вилучення прав доступу після припинення робочого відносин.

9) Звітність і аналітика: ARMS забезпечують можливість створення звітів та аналізу доступу користувачів до ресурсів. Цей компонент дозволяє виявляти аномалії, проводити аудит безпеки, виявляти порушення політик доступу та приймати відповідні заходи для запобігання інцидентам безпеки.

Крім основних компонентів, ARMS можуть мати додаткові функціональності, такі як:

1) Автоматизація процесів: ARMS можуть використовувати автоматизовані процеси для надання та зняття прав доступу, що спрощує управління правами користувачів та зменшує витрати часу та зусиль[10].

2) Самообслуговування користувачів: ARMS можуть мати функціонал, що дозволяє користувачам самостійно запитувати та керувати своїми правами доступу до ресурсів. В результаті це полегшує процес зміни доступу та зменшує навантаження на адміністраторів системи.

3) Інтеграція зі сторонніми додатками: ARMS можуть бути інтегровані з різноманітними сторонніми додатками та сервісами, такими як хмарні платформи,

електронні поштові системи, системи керування ідентифікацією та інші. Забезпечується більш широкий спектр функціональних можливостей та сумісність з існуючою інфраструктурою.

4) Групове управління: ARMS можуть дозволяти адміністраторам групово призначати права доступу для груп користувачів, що полегшує управління доступом для більшого обсягу користувачів та забезпечує єдинообразність налаштувань для груп користувачів зі схожими обов'язками або потребами[10].

5) Мобільний доступ: ARMS можуть надавати можливість управління правами доступу через мобільні додатки або веб-інтерфейси. Це дасть змогу адміністраторам контролювати доступ користувачів навіть поза офісом та підвищує зручність управління правами доступу.

ARMS відіграють важливу роль у забезпеченні безпеки інформації, ефективного управління правами доступу та дотримання внутрішніх та зовнішніх регуляторних вимог. Вони допомагають організаціям зменшити ризики, пов'язані з несанкціонованим доступом, витоком даних, зловживанням привілеями та недостатнім контролем доступу.

Завдяки ARMS організації можуть:

- Ефективно керувати правами доступу користувачів до різних ресурсів, встановлювати, змінювати та вилучати права доступу відповідно до обов'язків та потреб користувачів.
- Забезпечити обмеження доступу до ресурсів на основі політик безпеки, рівня конфіденційності даних, контролю часових рамок доступу та інших параметрів.
- Запобігти витокам даних та зловживанню привілеями, забезпечуючи централізований контроль над правами доступу та аудит дій користувачів.
- Дотримуватися регуляторних вимог та нормативів, встановлених регуляторними органами, шляхом налаштування політик та контролю доступу.

- Покращити ефективність та зручність управління правами доступу шляхом автоматизації процесів, самообслуговування користувачів та інтеграції з іншими системами безпеки та інфраструктурою.

В результаті, ARMS допомагають організаціям забезпечити високий рівень безпеки, ефективність та контроль над правами доступу, що є критичними аспектами в сучасному цифровому середовищі.

Розглянемо кілька прикладів систем управління правами доступу.

SolarWinds Access Rights Manager. SolarWinds є провідним виробником інструментів управління IT-ресурсами, а Менеджер прав доступу є гарним рішенням для контролю Active Directory. Цей інструмент доступний лише для середовища Windows Server. Однак він може отримати доступ до каталогів AD для ряду служб, включаючи Microsoft Exchange Server і NTFS[11].

Основні можливості:

- Створює простіший інтерфейс для AD;
- Уніфікує керування багатьма екземплярами AD;
- Аудит прав доступу;
- Керує правами доступу до NTFS і Exchange Server.

SolarWinds Access Rights Manager є одним с найкращіх пакетом для управління Active Directory. Ця система забезпечує інтерфейс для багатьох рутинних завдань, необхідних для координації облікових записів між центрами управління доступом. Вона пропонує автоматизовані утиліти для тих стандартних завдань, які багато системних адміністраторів часто не помічають, наприклад, перевірка покинутих облікових записів. Дуже мало компаній можуть дозволити собі мати експерта, який працює лише над правами доступу, тому системним адміністраторам, які займаються багатьма питаннями, потрібна автоматизована система управління правами доступу, і пакет SolarWinds є найкращим на ринку.

Менеджер прав доступу відстежує дії, що впливають на контролери домену, які працюють у мережі. Він сповістить про будь-які зміни в записах в базах даних AD. Це дуже важливий монітор, оскільки доступ до Active Directory для зміни дозволів - це стратегія, яку використовують хакери та шкідливе програмне забезпечення. Функції аудиту поширюються на список змін у поштових скриньках, календарях і спільних папках Microsoft Exchange[11].

Є можливість змінювати дозволи в записах AD за допомогою диспетчера прав доступу. Інтерфейс також дозволяє додавати, призупиняти і видаляти дозволи. Інструмент включає в себе модуль самообслуговування, який базується на веб-технологіях і дозволяє користувачам створювати або змінювати власні облікові записи.

Інструмент має модуль аналізу, який звітуватиме про всі дії зареєстрованих користувачів. Це ще одна важлива функція, оскільки вона допоможе виявити аномальну поведінку, яка може свідчити про злом облікового запису, що використовується хакером.

Цей інструмент особливо корисний для підприємств, яким необхідно забезпечити аудит відповідності та звітність, оскільки система SolarWinds бере на себе цю відповідальність автоматично. Програмне забезпечення для SolarWinds Access Rights Manager працює на Windows Server.

Переваги та недоліки SolarWinds Access Rights Manager приведені в таблиці 3.1.

Таблиця 3.1 – Переваги та недоліки використання SolarWinds Access Rights Manager

Переваги використання SolarWinds Access Rights Manager	Недолікі використання SolarWinds Access Rights Manager
• Забезпечує чітке уявлення про дозволи та файлові структури завдяки	• SolarWinds Access Rights Manager - це поглиблена платформа, призначена для системних адміністраторів, для

Продовження таблиці 3.1

Переваги використання SolarWinds Access Rights Manager	Недолікі використання SolarWinds Access Rights Manager
автоматичному відображенню та візуалізації; • Попередньо налаштовані звіти дозволяють легко продемонструвати відповідність вимогам; • Будь-які проблеми з відповідністю виявляються після сканування і супроводжуються діями по їх усуненню; Системні адміністратори можуть налаштовувати права доступу і контроль в Windows та інших додатках.	повного вивчення якої може знадобитися час

ManageEngine AD360. ManageEngine пропонує кілька систем моніторингу автентифікації користувачів. Всі вони засновані на Active Directory. Орієнтація на Active Directory означає, що цей інструмент буде корисним тільки в середовищі Windows Server, хоча ManageEngine зазвичай пише все своє програмне забезпечення так, щоб воно могло працювати і в Linux. Це дуже комплексна система керування AD, яка не тільки отримує доступ до файлів AD, але й стежить за ними, щоб захистити їх від хакерського втручання[11].

Основні можливості:

- Аудит Active Directory;
- Відстежування локальних та хмарних впроваджень AD;
- Керує єдиним входом.

ManageEngine AD360 - це фактично пакет із семи інструментів ManageEngine, які стосуються Active Directory. Чотири з них - ADManager Plus, Exchange Reporter Plus, M365 Manager Plus і SharePoint Manager Plus - забезпечують краще керування Active Directory. Три інструменти для відновлення - RecoveryManager Plus, ADAudit Plus і ADSelfService Plus - надають послуги моніторингу та управління системою, які працюють з даними, що зберігаються в екземплярах Active Directory. Отже, це дуже великий набір послуг, і можуть знадобитися не всі модулі. Наприклад, система ADAudit Plus займається управлінням відповідністю нормативним вимогам, моніторингом цілісності файлів і аналізом поведінки користувачів. Пакет RecoveryManager Plus займається лише резервним копіюванням Active Directory у всіх його різних реалізаціях, наприклад, для мережевого доступу, Azure і елементів Microsoft 365[11].

AD360 контролює покриття Active Directory файлових систем, мережевих ресурсів, Microsoft Office і поштових систем Microsoft Exchange Server. Він також може відстежувати доступ до хмарних сервісів через віддалені контролери доменів. Інтерфейс цього інструменту керування надає доступ до записів AD. За допомогою AD360 можна додавати, видаляти, змінювати і призупиняти права доступу.

За допомогою AD360 можна створити середовище єдиного входу і використовувати можливості управління багатофакторною автентифікацією. Макет консолі керування можна адаптувати. Це дає змогу надавати часткові види молодшому персоналу та співробітникам служби підтримки, щоб вони могли виконувати делеговані завдання, не отримуючи повного доступу до системи дозволів користувачів.

Дії, необхідні для створення нового облікового запису користувача, спрощуються за допомогою шаблонів користувачів. Вони також контролюють створення груп користувачів. Нові облікові записи також можна створювати

масово, завантажуючи дані з файлу CSV. Призупинення та видалення облікових записів також можна здійснювати масово.

Переваги та недоліки ManageEngine AD360 приведені в таблиці 3.2.

Таблиця 3.2 – Переваги та недоліки використання ManageEngine AD360

Переваги використання ManageEngine AD360	Недоліки використання ManageEngine AD360
• Значно покращує зручність використання Active Directory, спрощуючи виконання та автоматизацію рутинних завдань; • Може відстежувати зміни в локальних і хмарних середовищах AD; • Підтримує SSO та MFA, що підходить для захисту керування доступом за допомогою багаторівневої автентифікації.	• Працює тільки на Windows Server в середовищі Active Directory.

AWS(Amazon Web Services) Directory Service. Цей провідний хмарний провайдер пропонує простір для зберігання даних, веб-хостинг і дуже широкий спектр послуг, включаючи хмарний менеджер Active Directory. Служба каталогів - чудовий варіант для тих, хто розміщує свої Amazon Web Services або сервери додатків і файлів на AWS.

Основні особливості:

- Інтегрована в платформу AWS;
- Відповідність стандартам HIPAA та PCI DSS;
- Реалізує Active Directory.

AWS Directory Service - це хмарна реалізація Active Directory, розміщена на платформі Amazon Web Services. Пакет може керувати правами доступу до

Windows та обліковими даними для інших систем Microsoft, незалежно від того, чи працюють вони на сайті або на інших хмарних платформах. Великою перевагою цього сервісу перед запуском власної Active Directory на базі Windows є те, що він є керованим сервісом[11].

Реалізація Active Directory від AWS відповідає вимогам HIPAA та PCI DSS, оскільки включає в себе функції аудиту для забезпечення цілісності даних. Знімки системи створюються щодня, також можна отримувати їх на вимогу в критичні моменти, наприклад, безпосередньо перед оновленням програми[12].

Цей AD дозволяє впроваджувати групові політики, а також керувати стратегією єдиного входу.

До онлайн-платформи можна отримати доступ через браузер, що робить її інтерфейс нейтральним до операційної системи, служба управління доступом взаємодіє лише з Active Directory, тому вона може бути корисною лише для тих, хто працює в середовищі Windows.

Переваги та недоліки AWS Directory Service приведені в таблиці 3.3.

Таблиця 3.3 – Переваги та недоліки використання AWS Directory Service

Переваги використання AWS Directory Service	Недоліки використання AWS Directory Service
• Простий і зручний інтерфейс для управління AWS; • Підтримує управління цілісністю даних для таких стандартів, як PCI DSS або HIPAA; • Веб-інтерфейс доступний з будь-якої операційної системи • Розроблений для масштабування з середовищем AWS.	• Для використання потрібно мінімум два доменних середовища; • Погана візуалізація даних.

3.3 Аналіз систем запобігання вторгненням

Система запобігання вторгненням(Система запобігання вторгненням, IPS) – компонент безпеки мережі, спрямований на виявлення й блокування зловмисних атак та вторгнень в мережу. Забезпечення захисту мережевих ресурсів та безпеки даних за допомогою активного виявлення та блокування небезпечного трафіку є основною цілю IPS[13].

Основні характеристики та функції системи IPS:

1) Виявлення загроз: Система IPS виявляє загрози на основі попередньо визначених правил та сигнатур. Вона аналізує мережевий трафік, детектує небезпечні шаблони, атаки або аномалії, ідентифікує вразливості та сповіщає про можливі вторгнення[14].

2) Блокування атак: Система IPS приймає активні заходи для блокування атак та забезпечення безпеки системи. Вона використовує різні методи, такі як фільтрація пакетів, відмова в обслуговуванні (Denial of Service, DoS) або проти-експлойти, щоб запобігти успішному вторгненню[14].

3) Аналіз поведінки: Система може використовувати аналіз поведінки для виявлення відхилень в роботі мережі або системи. Вона порівнює активність з стандартними шаблонами та алгоритмами, виявляє аномальні зміни і сповіщає про можливі загрози.

4) Реагування на інциденти: Можливість реагувати на виявлені інциденти безпеки. Автоматичне заблокування IP-адрес, відправку сповіщень адміністратору, генерацію журналів або запуск додаткових захисних механізмів як варіанти реагування.

5) Інтеграція з іншими системами безпеки: Система IPS може бути інтегрована з іншими системами безпеки, такими як системи управління інцидентами (Security Information and Event Management, SIEM), системи виявлення

вторгнень (Intrusion Detection System, IDS) та інші. За допомогою цього отримуємо комплексний підхід до захисту мережі та системи.

Причини для використання IPS:

- Захист від відомих і невідомих загроз: IPS може блокувати відомі загрози, а також виявляти і блокувати невідомі загрози, які раніше не зустрічалися.
- Захист в режимі реального часу: IPS може виявляти і блокувати шкідливий трафік в режимі реального часу, не даючи атакам завдати шкоди.
- Відповідність вимогам: У багатьох галузях існують нормативні вимоги, які вимагають використання IPS для захисту конфіденційної інформації та запобігання витоку даних.
- Економічна ефективність: IPS - це економічно ефективний спосіб захисту вашої мережі в порівнянні з витратами на усунення наслідків порушення безпеки.
- Підвищена видимість мережі: IPS забезпечує підвищену прозорість мережі, дозволяючи вам бачити, що відбувається у вашій мережі, і виявляти потенційні ризики для безпеки.

Системи запобігання вторгненням (IPS) поділяються на 4 типи:

1) Мережева система запобігання вторгненням (NIPS): Контролює всю мережу на предмет підозрілого трафіку, аналізуючи активність протоколів[13].

2) Бездротова система запобігання вторгнень (WIPS): Відстежує бездротову мережу на наявність підозрілого трафіку, аналізуючи протоколи бездротових мереж[13].

3) Аналіз мережевої поведінки (NBA): Вивчає мережевий трафік для виявлення загроз, які генерують незвичайні потоки трафіку, такі як розподілені атаки на відмову в обслуговуванні, специфічні форми шкідливого програмного забезпечення та порушення політик[13].

4) Система запобігання вторгненням на основі хоста (HIPS): Це вбудований програмний пакет, який працює на одному хості для виявлення сумнівної активності, скануючи події, що відбуваються на цьому хості[13].

Особливості технологій IPS наведені у таблиці 3.4 .

Таблиця 3.4 – Технології IPS та їх особливості

Тип технології IPS	Типи виявленої зловмисної активності	Обсяг за кожним датчиком	Сильні сторони
NIPS	• Активність мережевого, транспортного та прикладного TCP/IP рівнів.	• Кілька мережевих підмереж і груп хостів.	• Єдиний IDPS, який може аналізувати найширший спектр прикладних протоколів.
WISP	• Активність бездротового протоколу; використання несанкціонованих бездротових локальних мереж (WLAN).	• Кілька WLAN і груп бездротових клієнтів.	• Єдиний IDPS здатний передбачити активність бездротового протоколу.
NBA	• Активність мережевого, транспортного та прикладного TCP/IP рівнів що	• Кілька мережевих підмереж і груп хостів.	• Зазвичай ефективніше за інших виявляє розвідувальне сканування та

Продовження таблиці 3.4

Тип технології IPS	Типи виявленої зловмисної активності	Обсяг за кожним датчиком	Сильні сторони
	спричиняє аномальні мережеві потоки.		DoS-атаки, а також реконструює серйозні зараження шкідливим програмним забезпеченням.
HIPS	Діяльність хост-додатків та операційної системи (ОС); діяльність мережевого, транспортного та прикладного рівнів TCP/IP.	Окремий хост.	Може аналізувати активність, яка передавалася в наскрізних зашифрованих каналах зв'язку.

Розглянемо декілька прикладів систем запобігання вторгненням та визначимо їх сильні та слабкі сторони.

Check Point Quantum IPS. Це система запобігання вторгненням компанії Check Point Software Technologies. Призначена для виявлення та блокування потенційних вторгнень у реальному часі[15].

Check Point Quantum IPS включає:

1) Виявлення вторгнень. Базуючись на широкому спектрі виявлення атак система виявляє загрози та аномалії в мережевому трафіку.

2) Блокування атак. За допомогою блокування атак і застосуванню відповідних заходів безпеки для запобігання компрометації системи Check Point Quantum IPS має можливість одразу реагувати на загрози.

3) Керування загрозами. Системою надається централізований інтерфейс для керування загрозами, який включає можливість налаштування правил та політик безпеки, аналіз журналів подій, моніторинг загроз та створення звітів[15].

Переваги та недоліки використання Check Point Quantum IPS наведені в таблиці 3.5.

Таблиця 3.5 – Переваги та недоліки Check Point Quantum IPS

Переваги Check Point Quantum IPS	Недоліки Check Point Quantum IPS
• Система може виявляти різні типи атак, включаючи відомі та нові; • Має високу точність виявлення атак, знижує ймовірність помилкових спрацьовувань і покращує ефективність системи; • Негайне реагування на виявлені загрози та їх блокування, завдяки роботі у режимі реального часу; • Вбудований антивірус, анти-бот і пісочниця; • Наявність централізованого інтерфейсу для керування загрозами, політиками безпеки та моніторингу.	• Відсутність підтримки зовнішніх ресурсів, які не перенаправляються через шлюз; • Висока вартість в порівнянні з іншими системами запобіганню вторгнень; • Внутрішній мережевий трафік повинен перенаправлятися через шлюз для захисту.

Cisco NGIPS (Next-Generation Intrusion Prevention System). Система запобігання вторгненням компанії Cisco Systems. Розроблена для виявлення та захисту від потенційних загроз та атак у мережевому середовищі[15].

Cisco NGIPS включає в себе:

1) Виявлення вторгнень. Використовуючи різноманітні техніки, такі як сигнатурний аналіз, аналіз вмісту, аналіз поведінки та машинне навчання Cisco NGIPS легко виявляє великий спектр вторгнень та загроз у реальному часі.

2) Блокування атак. Застосування різних методів блокування, таких як відмову в обслуговуванні(DoS) й блокування шкідливого трафіку дає можливість системі одразу реагувати на виявлені атаки[15].

3) Управління загрозами. Надається централізований інтерфейс для керування загрозами, включаючи налаштування правил та політик безпеки, моніторинг та аналіз журналів подій, а також створення звітів про загрози та атаки.

Переваги та недоліки використання Cisco NGIPS наведені в таблиці 3.6.

Таблиця 3.6 – Переваги та недоліки Cisco NGIPS

Переваги Cisco NGIPS	Недоліки Cisco NGIPS
• Використання розширених методів аналізу та машинного навчання для виявлення складних атак і загроз; • Можливість розгортання в різних мережевих середовищах, такі як фізичні, віртуальні та хмарні інфраструктури. • Здатність системи інтегруватися з іншими продуктами Cisco, для забезпечення комплексного захисту мережі.	• Незручний інтерфейс для користувача, складність налаштування та управління системою; • Для малих і середніх підприємств Cisco NGIPS може бути дуже дорогим в розгортанні та підтримці.

Snort. Є відкритим програмним забезпеченням та однією за найпопулярніших системи виявлення вторгнень(IDS) та систем запобігання вторгненням(IPS), розробленим на базі правил(rule-based)[15].

Snort включає в себе:

1) Аналіз трафіку. Система аналізує мережевий трафік, шукає відповідність правилам(сигнатурам) та виявляє підозрілі активності та атаки.

2) Система правил. Використання правил, які визначають патерни або сигнатури атак, що потрібно виявити. Правила можна налаштовувати та оновлювати за необхідністю відповіді на нові загрози[15].

3) Логування та сповіщення. Система здатна вести журнал подій та повідомляти адміністратора про загрози та атаки які виявила.

Переваги та недоліки використання Snort наведені в таблиці 3.7.

Таблиця 3.7 – Переваги та недоліки Snort

Переваги Snort	Недоліки Snort
• Система є відкритою та безкоштовною, це дозволяє користувачам використовувати її без обмежень та модифікувати за необхідністю; • Можливість налаштування та адаптації для різних мережевих середовищ та вимог безпеки; • Величезна спільнота користувачів, це забезпечує підтримку, оновлення правил та спільний обмін знаннями; • Велика бібліотека готових правил виявлення.	• Складності в налаштуванні для некваліфікованих користувачів та для мереж зі складною інфраструктурою; • Використання не налаштованих та не оновлених належним чином правил для виявлення атак може спричинити велику кількість помилкових позитивних або негативних результатів.

Незважаючи на недоліки, Snort залишається ефективною та потужною системою запобіганню вторгненням, особливо для організацій з обмеженим

бюджетом та тих, хто шукає відкрите та гнучке програмне забезпечення для безпеки мережі.

3.4 Аналіз систем запобігання витокам даних

Система запобігання витокам даних(Data Loss Prevention, DLP) – комплексна інфраструктура, яка призначена для запобігання втрати, неправильному використанню або доступу до конфіденційних даних неавторизованими користувачами. Захист інформації від витоку, збереження конфіденційності та забезпечення відповідності нормативним вимогам – все це мета DLP[16].

Ключові компоненти систем DLP:

1) Виявлення чутливої інформації. Використання методів для ідентифікації конфіденційних даних(персональна інформація, фінансові дані, комерційна інформація тощо) таких як аналіз зразків даних, ключових слів, шаблонів та аналізу контексту[16].

2) Моніторинг активності. Системи DLP проводять моніторинг за активністю користувачів та мережевим трафіком, для виявлення несанкціонованої передачі даних. Аналізуючи поведінку користувачів, вони виявляють незвичайні активності, великий обсяг передачі даних або некоректну взаємодію з конфіденційною інформацією[16].

3) Контроль доступу та політики. Встановлюються правила та політики доступу до конфіденційної інформації. Здійснюється контроль за тим, хто має доступ до даних, які дії можуть бути виконані с цими даними та як вони можуть буду передані.

4) Захист кінцевих пристроїв. DLP системи використовують методи шифрування, блокування USB-портів та контролюють виконання певних дій на пристроях.

5) Звітність та аудит. Щодо використання та передачі конфіденційної інформації забезпечується аудит та збір логів. Це дозволяє відстежувати події, виявляти порушення безпеки та аналізувати потенційні ризики витоку даних[17].

6) Інтеграція з іншими системами безпеки. Системи DLP можуть бути інтегровані з іншими системами безпеки, такими як файрволи та системи управління ідентифікацією. Завдяки цьому забезпечується комплексний підхід до захисту даних та координацію заходів безпеки[16].

Ці компоненти є перевагами використання систем запобігання витокам даних, але існують і певні недоліки, такі як:

1) Велика кількість ложнопозитивних спрацьовувань. Системи DLP можуть спрацьовувати на нормальні або нешкідливі дії, спричиняючи значну кількість ложнопозитивних тривог. Це призводить до витрат часу та ресурсів на перевірку та обробку.

2) Складність налаштування та підтримки. Налаштування та підтримка систем DLP можуть бути складними завданнями. Вимагається глибоке розуміння інфраструктури мережі, потоків даних та типів чутливої інформації для ефективного налаштування та використання системи[18].

3) Вплив на продуктивність мережі. Використання систем DLP може впливати на продуктивність мережі через потребу в моніторингу трафіку та аналізі даних. Це може спричинити затримки у передачі даних та вплинути на швидкість мережевих процесів[18].

4) Висока вартість. Реалізація та підтримка систем DLP можуть бути витратними завданнями. Вони вимагають інвестицій у апаратне та програмне забезпечення, навчання персоналу та регулярне оновлення системи[18].

5) Виклики управління політиками безпеки. Встановлення відповідних правил та політик безпеки, забезпечення відповідності регуляторним вимогам та вирішення конфліктів можуть бути викликами для організації.

При цьому, всі системи запобігання витокам даних можна умовно класифікувати за наступними категоріями:

1) За способом виявлення:

- Системи, що базуються на сигнатурах. Вони використовують базу шаблонів або сигнатур, які визначають відомі вектори атак.
- Системи, що базуються на поведінці. Ті системи, що аналізують активність користувачів, мережевий трафік та поведінку для виявлення підозрілих активностей, які можуть вказувати на витік даних.

2) За способом контролю та запобігання:

- Системи DLP, що базуються на правилах: Такі системи використовують заздалегідь визначені правила та політики для контролю доступу до конфіденційної інформації та запобігання її небажаній передачі.
- Системи DLP, що базуються на шифруванні. Застосовують методи шифрування для захисту конфіденційної інформації та запобігання її доступу незаконним особам.

3) За масштабом застосування:

- Корпоративні системи DLP. Встановлюються на рівні організації і застосовуються для захисту всієї корпоративної мережі та інфраструктури.
- Кінцеві системи DLP: Вони встановлюються на кінцевих пристроях, таких як комп’ютери або мобільні пристрої, і контролюють передачу даних з цих пристроїв.

Сучасні DLP-системи мають величезну кількість параметрів і характеристик, які необхідно враховувати при виборі рішення для захисту конфіденційної інформації від витоку. Класифікація систем DLP може варіюватися в залежності від виробника, архітектури та функціональних можливостей конкретної системи. Однак, ці категорії надають загальне уявлення про різноманітність систем DLP та їх характеристики.

Далі розглянемо декілька прикладів сучасних DLP-систем та визначимо їх переваги та недоліки.

Endpoint Protector від CoSoSys. Це система для запобігання витокам даних на рівні кінцевих точок. Вона надає захист і контроль над даними, що зберігаються і передаються через різноманітні кінцеві точки, такі як комп'ютери, ноутбуки, мобільні пристрої і USB-накопичувачі[18].

Endpoint Protector включає наступні можливості:

1) Контроль захоплення даних: Забезпечує контроль за копіюванням, вставленням, друком та пересиланням даних з кінцевих точок. Це включає контроль захоплення скріншотів, відеозаписів екрану, а також контроль захоплення зображень з камери.

2) Керування USB-пристроями: Дозволяє обмежувати або блокувати використання USB-пристроїв на кінцевих точках. Це може бути корисним для запобігання втрати даних через неправомірне копіювання на зовнішні носії.

3) Шифрування даних: Надає можливість шифрувати дані на рівні кінцевих точок для захисту від несанкціонованого доступу.

4) Контроль друку: Дозволяє керувати та обмежувати друк документів, забезпечуючи контроль над тим, що може бути надруковано та куди.

5) Виявлення загроз та атак: Забезпечує виявлення потенційних загроз та атак на кінцеві точки, такі як віруси, шкідливі програми, фішингові атаки тощо.

Переваги та недоліки використання Endpoint Protector наведені в таблиці 3.8.

Таблиця 3.8 – Переваги та недоліки Endpoint Protector

Переваги Endpoint Protector	Недоліки Endpoint Protector
• Комплексний захист даних на рівні кінцевих точок, що дозволяє контролювати, моніторити та захищати дані в різних контекстах використання;	• Потребує налаштування та підтримки, що вимагає додаткових ресурсів та експертизи;

Продовження таблиці 3.8

Переваги Endpoint Protector	Недоліки Endpoint Protector
• Гнучкість та налаштовуваність політик безпеки для керування даними в організації; • Інтуїтивний і простий у використанні інтерфейс для адміністрування та моніторингу системи; • Підтримує різноманітні типи платформ, включаючи Windows, macOS і Linux; Може бути інтегрована з іншими системами безпеки та інфраструктурою організації.	• Впливає на продуктивність кінцевих точок через моніторинг та контроль даних. • Потребує регулярного оновлення та моніторингу, щоб забезпечити ефективну роботу та захист від нових загроз. • Вимагає усвідомлення та співпраці користувачів для успішної реалізації політик безпеки та запобігання витокам даних.

Symantec DLP. Це система, призначена для виявлення та запобігання витокам даних в організаціях. Вона надає засоби для ідентифікації, моніторингу та контролю руху даних, а також застосування політик безпеки для їх захисту[18].

Symantec DLP включає наступні можливості:

1) Виявлення чутливої інформації: Здатність ідентифікувати і класифікувати чутливі дані, такі як фінансова інформація, персональні дані, інтелектуальна власність тощо.

2) Моніторинг руху даних: Система може відстежувати рух даних в мережі, на кінцевих точках, в електронній пошті, на файлових серверах та інших місцях зберігання, що дозволяє виявляти потенційні витоки даних.

3) Контроль доступу та застосування політик: Забезпечує можливість налаштування політик безпеки, включаючи блокування, шифрування, реєстрацію подій та інші дії для запобігання витокам даних.

4) Інтеграція з іншими системами безпеки: Може бути інтегрована з іншими системами безпеки, такими як фаєрволи, системи керування ідентифікацією та авторизацією, для забезпечення комплексного захисту даних.

Переваги та недоліки використання Symantec DLP наведені в таблиці 3.9

Таблиця 3.9 – Переваги та недоліки Symantec DLP

Переваги Symantec DLP	Недоліки Symantec DLP
• Високий рівень точності виявлення і класифікації чутливих даних; • Гнучкість у налаштуванні політик безпеки та контролю руху даних; • Широкий спектр інтеграцій з іншими системами безпеки для забезпечення комплексного захисту даних	• Високі вимоги до ресурсів, таких як обчислювальна потужність та зберігання, для ефективної роботи системи; • Складність в управлінні та конфігуруванні системи, що потребує спеціалістів з безпеки для належного налаштування та підтримки; • Вартість впровадження та підтримки системи може бути високою, особливо для невеликих організацій

Враховуючи переваги та недоліки, використання Symantec DLP може бути ефективним рішенням для організацій, які мають високі вимоги до захисту своїх чутливих даних та потребують розширеного контролю та моніторингу їх руху. Проте, варто враховувати складність налаштування та витрати на впровадження та підтримку системи.

McAfee DLP. Це система, яка призначена для виявлення та запобігання витокам даних в організаціях. Вона надає рішення для ідентифікації, контролю та

захисту чутливої інформації, а також забезпечує моніторинг та аудит активності даних[18].

McAfee DLP включає наступні можливості:

1) Виявлення чутливих даних: Система здатна ідентифікувати та класифікувати чутливу інформацію, включаючи фінансові дані, персональну інформацію, інтелектуальну власність та інші типи конфіденційних даних.

2) Моніторинг та контроль руху даних: Забезпечує постійний моніторинг руху даних на мережевому рівні, на кінцевих точках, в електронній пошті, в системах зберігання та інших місцях зберігання даних.

3) Застосування політик безпеки: Дозволяє встановлювати та застосовувати політики безпеки для контролю доступу до даних, блокування небажаних дій, шифрування даних та інших заходів захисту.

4) Аналіз та аудит активності даних: Забезпечує можливість аналізувати та аудитувати дії з даними, виявляти підозрілі активності та спостерігати за змінами в поведінці користувачів.

Переваги та недоліки використання McAfee DPL наведені в таблиці 3.10.

Таблиця 3.10 – Переваги та недоліки McAfee DPL

Переваги McAfee DPL	Недоліки McAfee DPL
• Висока точність виявлення чутливих даних та потенційних витоків; • Широкий спектр інтеграцій з іншими системами безпеки та розширена функціональність для комплексного захисту даних; • Легка інтеграція з існуючими інфраструктурними рішеннями.	• Вимагає належного налаштування та конфігурування для досягнення оптимальної продуктивності та точності; • Вартість впровадження та підтримки може бути високою; • Потребує певних ресурсів для ефективної роботи, таких як

Продовження таблиці 3.10

Переваги McAfee DPL	Недоліки McAfee DPL
	обчислювальна потужність та зберігання.

McAfee DLP є потужним рішенням для захисту чутливої інформації та запобігання витокам даних. Його переваги полягають у високій точності виявлення, широких можливостях інтеграції та простоті використання.

Зрештою ми маємо те, що практично всі згадані системи схожі між собою за своїм функціоналом і недоліками. Деякі підходять для великих, а деякі навпаки для середніх і маленьких компаній.

У виборі системи запобігання витоку даних завжди потрібно звертати увагу на зазначений функціонал, складність налаштування та його ціну, також на ціну підтримки системи.

ВИСНОВКИ

У ході дослідження методів і систем запобігання витоку даних аналізуються та порівнюються різні методи та техніки в цій галузі. Отримані результати показують, що системи запобігання витокам даних є ефективним і необхідним засобом захисту інформації. Загальносвітова тенденція у вирішенні цієї проблеми свідчить про постійний розвиток і вдосконалення існуючих систем, впровадження нових технологій і алгоритмів, забезпечення інтеграції з іншими системами безпеки.

Результати досліджень можуть бути використані в різних сферах, де цінується безпека даних і конфіденційність інформації. Установи у фінансовій сфері, медичній промисловості, державні установи, банки, телекомунікаційні компанії тощо, які залучають великі обсяги конфіденційних даних, можуть використовувати методи та системи, які були розроблені для запобігання витоку даних, щоб забезпечити безпеку своїх інформаційних ресурсів.

Дослідження методів і систем запобігання витоку даних має велике значення для національних економік, оскільки забезпечення безпеки даних стає все більш важливим у сучасному цифровому світі. Науково-технічне значення полягає в розробці нових алгоритмів, методів і систем для ефективного виявлення, блокування та запобігання витоку даних. Соціальна значущість цієї роботи полягає в забезпеченні конфіденційності інформації, захисту персональних даних користувачів та забезпеченні довіри до цифрових сервісів та Інтернет-комунікацій.

На основі отриманих результатів організаціям рекомендується ретельно проаналізувати свої потреби у захисті даних і вибрати найкращі методи та системи для запобігання витокам. Під час впровадження систем для запобігання витоку даних слід враховувати організаційні особливості, а також слід приділяти увагу

встановленню процесів моніторингу, аналізу та реагування на інциденти. Крім того, для забезпечення ефективності та безпеки даних рекомендується постійне оновлення системи та підтримка виробника.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Шифрування даних: все, про що ви повинні знати, щоб захистити дані. *SIM-Networks – Your Goals, our Tech. IT Infrastructure from German Provider*. URL: https://www.sim-networks.com/ukr/blog/data-encryption-best-practices (дата звернення: 07.05.2023).
2. Русин Б. П., Варецький Я. Ю. Біометрична аутентифікація та криптографічний захист : монографія. Львів : Коло, 2007. 287 с.
3. Social network for programmers and developers. Morioh. URL: https://morioh.com/p/86c882866c6c (дата звернення: 07.05.2023).
4. Symmetric Key Encryption - why, where and how it's used in banking. Cryptomathic - Security Solutions. URL: https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking (дата звернення: 07.05.2023).
5. Хеш функція – Wiki ТНТУ. *Wiki ТНТУ*. URL: https://wiki.tntu.edu.ua/Хеш_функція (дата звернення: 07.05.2023).
6. Контроль доступу (Access control) до інформації як один із ключових елементів інформаційної безпеки | BSO Privacy Group. BSO Privacy Group. URL: https://bsoprivacygroup.com/gdpr-personal-data-access-control/ (дата звернення: 08.05.2023).
7. Lowekamp B. Using passive traces of application traffic in a network monitoring systems. / B.B. Lowekamp, M. Zangrilli. – IEEE Computer Society, 2004. – P. 73 – 75
8. Fry C. Security Monitoring / C. Fry, M. Nystrom – Sebastopol : O'Reily Media, 2009. – P.40 – 56, 163 – 170.

9. Benantar M. Access control systems: security, identity, management, and trust models. New York : Springer, 2005.
10. Access management system - user access rights guide | solarwinds. *Observability and IT Management Platform | SolarWinds*. URL: https://www.solarwinds.com/access-rights-manager/access-management-system (дата звернення: 24.05.2023).
11. 12 best access management software & tools. *Comparitech*. URL: https://www.comparitech.com/net-admin/best-access-management-software-tools/#What_is_access_rights_management (date of access: 25.05.2023).
12. Active Directory – Сервис каталогов AWS – AWS. *Amazon Web Services, Inc.* URL: https://aws.amazon.com/ru/directoryservice/ (дата звернення: 25.05.2023).
13. What is intrusion prevention system? | vmware glossary. *VMware*. URL: https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html (date of access: 25.05.2023).
14. Intrusion Prevention System (IPS) - GeeksforGeeks. *GeeksforGeeks*. URL: https://www.geeksforgeeks.org/intrusion-prevention-system-ips/ (date of access: 26.05.2023).
15. Top 10 Intrusion Detection and Prevention Systems. *ClearNetwork, Inc*. URL: https://www.clearnetwork.com/top-intrusion-detection-and-prevention-systems/ (date of access: 26.05.2023).
16. What is Data Loss Prevention (DLP)? Definition, Types & Tips. *Digital Guardian*. URL: https://www.digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention (date of access: 28.05.2023).
17. Alneyadi S., Sithirasenan E., Muthukkumarasamy V. A survey on data leakage prevention systems. Journal of network and computer applications.

2016. Vol. 62. P. 137–152. URL: https://doi.org/10.1016/j.jnca.2016.01.008 (date of access: 28.05.2023).

18. 11 BEST Data Loss Prevention Software DLP Solutions In 2023. *Software Testing Help*. URL: https://www.softwaretestinghelp.com/data-loss-prevention-software/ (date of access: 29.05.2023).