Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«17» травня 2024 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

освітньо-наукова програма *Кібербезпека*
(назва освітньої програми)

на тему: «Моделі виявлення та ідентифікації інформаційних впливів»

Виконавець: студентка ІІ курсу, групи КБм-21

_____ **Наталія ЛЕБЄДЄВА**
(підпис) (Ім'я, ПРІЗВИЩЕ)

	Ім'я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Тетяна БАБЕНКО	
Нормоконтроль	Лариса МИРУТЕНКО	

Київ 2024

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«17» листопада 2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача(ки) КБм-21 (група) Лебєдєвої Наталії Володимирівни (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Моделі виявлення та ідентифікації інформаційних впливів

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 15.11.2023 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процеси виявлення та ідентифікації інформаційних впливів, які відбуваються в інформаційному середовищі
Предмет досліджень	Моделі виявлення та ідентифікації інформаційних впливів.
Мета	Аналіз, розробка та впровадження моделей виявлення та ідентифікації інформаційних впливів для підвищення ефективності захисту інформації та управління ризиками в інформаційному середовищі.

Вихідні дані для проведення роботи Моделі виявлення та ідентифікації інформаційних впливів

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна удосконалення моделі виявлення та ідентифікації інформаційних впливів на основі сучасних технологій та методик, а саме на основі соціально-мережевого аналізу

Практична цінність впровадження цих моделей дозволить забезпечити вчасне виявлення та реагування на інформаційні загрози та атаки, що підвищить рівень захищеності та безпеки інформаційних систем

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**
Уточнення постановки задачі	17.11.2023 – 29.01.2024
Аналіз літературних джерел	30.01.2024 – 12.02.2024
Ознайомлення з сучасними трактуваннями інформаційних впливів	13.02.2024 – 21.02.2024
Розгляд нормативно-правових актів, регулюючих функціонування та захист інформації в інформаційному просторі	22.02.2024 – 26.02.2024
Дослідження загроз, вразливостей та атак, що пов’язані з інформаційними впливами	27.02.2024 – 04.03.2024
Аналіз проблеми виявлення інформаційних впливів	05.03.2024 – 10.03.2024
Дослідження моделей та методів протидії інформаційним впливам	11.03.2024 – 17.03.2024
Розробка моделі виявлення інформаційних впливів	18.03.2024 – 17.04.2024
Розробка рекомендацій щодо захисту інформаційних ресурсів від інформаційних впливів	18.04.2024 – 25.04.2024
Оформлення пояснювальної записки згідно методичних рекомендацій	26.04.2024 – 12.05.2024

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Подача пакету документів на розгляд ЕК	13.05.2024 – 18.05.2024

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект Зниження фінансових збитків завдяки ефективному виявленню та ідентифікації інформаційних загроз, що включає скорочення витрат на відновлення, юридичні витрати та втрати від викрадення даних.

Соціальний ефект Підвищення рівня захисту інформації для користувачів та організацій, що сприяє зміцненню довіри до цифрових технологій і створенню більш безпечного інформаційного середовища.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Тетяна БАБЕНКО
(підпис) (Ім'я, ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ Наталія ЛЕБЄДЄВА
(підпис) (Ім'я, ПРІЗВИЩЕ)

Дата видачі завдання: 17.11.2023 р.
Термін подання кваліфікаційної роботи до ЕК 17.05.2024 р.

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Моделі виявлення та ідентифікації інформаційних впливів»: 79 сторінок, 5 рисунків та 3 таблиці. 48 літературних джерел.

Об’єкт дослідження – процеси виявлення та ідентифікації інформаційних впливів, які відбуваються в інформаційному середовищі..

Мета роботи – аналіз, розробка та впровадження моделей виявлення та ідентифікації інформаційних впливів для підвищення ефективності захисту інформації та управління ризиками в інформаційному середовищі.

Методи дослідження – методи аналізу даних, математичного моделювання, статистичних методів, а також методи імітації та комп'ютерного моделювання.

У роботі досліджено існуючі методи та підходи до виявлення та ідентифікації інформаційних впливів. Розроблено модель виявлення та ідентифікації інформаційних впливів на основі сучасних технологій та методик, проведено експериментальне порівняння та аналіз ефективності розроблених моделей.

Актуальність теми: у зв'язку зі зростанням кількості та складності інформаційних загроз, ризиків та атак, виявлення та ідентифікація інформаційних впливів стає надзвичайно актуальною задачею для бізнесу, урядових установ, організацій та індивідуальних користувачів.

Ключові слова: інформаційні впливи, моделі виявлення інформаційних впливів, соціально мережевий аналіз, ідентифікація загроз, аналіз поведінки користувачів, безпека мережі.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

APT	-	Advanced Persistent Threat
CGI	-	Common Gateway Interface
CNN	-	Convolutional Neural Network
CSS	-	Cascading Style Sheets
DDoS	-	Distributed denial-of-service
DNS	-	Domain Name System
DNS	-	Domain Name System
DoS	-	Denial of Service
HIDS	-	Host-based Intrusion Detection System
HTTP	-	HyperText Transfer Protocol
ICMP	-	Internet Control Message Protocol
IDS	-	Intrusion Detection System
IP	-	Internet Protocol
JS	-	JavaScript
LDA	-	Latent Dirichlet Allocation
LSTM	-	Long Short-Term Memory
ML	-	Machine Learning
NIC	-	Network Interface Card
NLP	-	Natural Language Processing
NTA	-	Network Traffic Analysis
OSI	-	Open Systems Interconnection
PCA	-	Principal Component Analysis
PCAP	-	Packet Capture
R2L	-	Remote to Local
R2U	-	Remote to User
RNN	-	Recurrent Neural Network
SIEM	-	Security Information and Event Management

SMTP	-	Simple Mail Transfer Protocol
SNA	-	Social Network Analysis
SVM	-	Support Vector Machine
TCP	-	Transmission Control Protocol
U2R	-	User to Root
UDP	-	User Datagram Protocol
UNIX	-	Uniplexed Information and Computing Service
БД	-	База даних
ІС	-	Інформаційна система
КПК	-	Кишеньковий персональний комп'ютер
ОВП	-	Об'єктно-орієнтоване програмування
ОС	-	Операційна система
СВВ	-	Система впливу на свідомість
СЕКК	-	Система електронного комерційного контенту
СЗВ	-	Система запобігання вторгнень
СМА	-	Соціальний мережевий аналіз
СОА	-	Система опису аномалій
СОВ	-	Системи виявлення вторгнень
СОР	-	Система обробки реальності
ССВВ	-	Система самозахисту від вторгнень
СУВ	-	Система управління версіями
ХСВВ	-	Хибна система впливу на свідомість
ХСЗВ	-	Хостова система захисту від вторгнень
ЦП	-	Центральный блок обрубки

ЗМІСТ

ВСТУП

У сучасному інформаційному суспільстві важливо вчасно виявляти та ідентифікувати інформаційні впливи для забезпечення безпеки, захисту даних та управління ризиками. Моделі виявлення та ідентифікації інформаційних впливів стають ключовими інструментами у розв'язанні цих завдань.

Актуальність. У зв'язку зі зростанням кількості та складності інформаційних загроз, ризиків та атак, виявлення та ідентифікація інформаційних впливів стає надзвичайно актуальною задачею для бізнесу, урядових установ, організацій та індивідуальних користувачів.

Метою даного дослідження є аналіз, розробка та впровадження моделей виявлення та ідентифікації інформаційних впливів для підвищення ефективності захисту інформації та управління ризиками в інформаційному середовищі.

Об'єктом дослідження є процеси виявлення та ідентифікації інформаційних впливів, які відбуваються в інформаційному середовищі.

Предметом дослідження є розробка та використання моделей для здійснення цих процесів.

Наукова новизна дослідження полягає в удосконаленні моделі виявлення та ідентифікації інформаційних впливів на основі сучасних технологій та методик.

Завдання:

- Провести аналіз існуючих методів та підходів до виявлення та ідентифікації інформаційних впливів.
- Розробити моделі виявлення та ідентифікації інформаційних впливів на основі сучасних технологій та методик.
- Провести експериментальне порівняння та аналіз ефективності розроблених моделей.
- Впровадити розроблені моделі в реальні інформаційні системи та забезпечити їхню належну підтримку та функціонування.

Методи аналізу. Для досягнення поставлених завдань будуть використані методи аналізу даних, математичного моделювання, статистичних методів, а також методи імітації та комп'ютерного моделювання.

Практична цінність. Результати дослідження та розроблені моделі виявлення та ідентифікації інформаційних впливів будуть корисними для організацій та підприємств у сферах інформаційної безпеки, захисту даних, управління ризиками та кібербезпеки. Впровадження цих моделей дозволить забезпечити вчасне виявлення та реагування на інформаційні загрози та атаки, що підвищить рівень захищеності та безпеки інформаційних систем.

Соціальний мережевий аналіз (СМА) може бути корисним інструментом для виявлення інформаційних впливів у різних сферах, включаючи політику, бізнес, академічні дослідження та громадські діяльності. Цей підхід дозволяє аналізувати взаємозв'язки та взаємодії між різними суб'єктами або об'єктами в мережі, що може розкрити ключові фактори, що визначають розподіл інформації та вплив у цій мережі.

Одним з потенційних застосувань СМА є виявлення впливових осіб або груп у соціальних мережах, які мають значний вплив на поширення інформації. Це може бути корисним, наприклад, для політичних кампаній, де ідентифікація ключових акторів у мережі може допомогти зрозуміти, які повідомлення або ідеї найефективніше поширюються.

Також за допомогою соціального мережевого аналізу можна виявити групи людей або організації, які мають схожі інтереси чи думки, і дослідити, як ці групи взаємодіють та як це впливає на поширення інформації в мережі. Це може бути корисним для розвитку маркетингових стратегій, аналізу громадської думки або вивчення питань громадського здоров'я.

Однак важливо враховувати, що соціальний мережевий аналіз також має свої обмеження. Наприклад, не завжди можна точно визначити всі зв'язки у мережі, особливо у великих та складних системах. Також важливо бути обережним у використанні отриманих даних, оскільки інформація з соціальних мереж може бути спотвореною або призвести до неточних висновків, якщо не враховувати контекст та особливості конкретної ситуації.

РОЗДІЛ 1
АНАЛІЗ ПРОБЛЕМИ ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ВПЛИВІВ

1.1 Концепція інформаційних впливів

Інформаційні впливи є складним феноменом, що набуває все більшої актуальності в умовах сучасного інформаційного суспільства. Інформаційні впливи можна визначити як сукупність дій, спрямованих на зміну поведінки, мислення або емоційної сфери суб'єктів шляхом цілеспрямованого використання інформаційних ресурсів. Ці впливи можуть здійснюватися через різноманітні канали, включаючи мас-медіа, соціальні мережі, офіційні заяви, рекламу та інші засоби комунікації.

У сучасних умовах ділового середовища стає очевидним, що будь-які системи безпеки повинні бути готові виявити та негайно реагувати на потенційні загрози. Раніше прагнення побудувати несуразне оборонне забезпечення схоже на мрію, оскільки більшість систем вже порушені або можуть бути легко вразливими до атак. Основне завдання сьогоднішньої системи безпеки полягає в швидкому виявленні атак та атакувальників, щоб мінімізувати шкоду.

Тому в останні роки спостерігається ріст попиту на високоінтелектуальні засоби захисту, які дозволяють ефективно виявляти атаки та події. Зокрема, такі технології, як системи управління подіями та безпекою (SIEM), аналіз мережевого трафіку (NTA) та складні рішення проти APT, набувають все більшого значення. Закінчивши рік, очікується майже тричі збільшення інтересу до цих технологій [1].

Зміни в економічних процесах національного рівня, що призвели до появи різних форм власності, вкладають нас усвідомлення, що безпека – це необхідна умова не лише для розвитку, але й для функціонування будь-якого бізнесу. Кожна компанія має розробити надійні засоби захисту, відповідальність за які лежить на її власнику. Можливості держави обмежені у забезпеченні безпеки, тому це завдання часто лежить на підприємствах.

Проте сьогодні спостерігаються ознаки переходу до наступного етапу наукового розвитку, який передбачає формування умов для економічного розвитку через корпоративну безпеку. Насправді, наукові дослідження показують, що питання корпоративної безпеки не отримує достатньої уваги в сучасному суспільстві.

У своїй роботі П. Кравчук визначає корпоративну безпеку як стан захисту життєво важливих інтересів підприємства від внутрішніх та зовнішніх загроз Вона гарантує найефективніше використання ресурсів для забезпечення стабільності та динамічного розвитку [2]. Другий автор, В. Франчук, розглядає корпоративну безпеку як здатність протистояти загрозам та реалізовувати власні інтереси в межах корпоративної системи [3, с. 167]. Важливим аспектом визначення О. Рудковського є підкреслення необхідності узгодження інтересів зовнішнього та внутрішнього середовища для забезпечення стабільної роботи підприємства [4, с. 147].

Думка полягає в тому, що основна мета корпоративної безпеки полягає в досягненні корпоративних цілей через ефективне використання наявних ресурсів та організацію захисту, що забезпечує стале зростання компанії. Враховуючи цільові орієнтири та визначену мету, можна визначити ключові завдання корпоративної безпеки, як показано на рисунку 1.1.

Рисунок 1.1 – Завдання корпоративної безпеки підприємства

Отже, можна зробити висновок, що корпоративна безпека охоплює ширший спектр завдань, ніж просто економічна безпека, оскільки вона включає в себе більш різноманітні функції та обов'язки.

Основні структурні компоненти корпоративної безпеки можуть бути наступними:

- Економічні (найефективніше використання ресурсів для досягнення цілей компанії).
- Фінансова (забезпечення фінансової стабільності та прибутковості).
- Персонал (організація роботи персоналу та ефективне управління).
- Технічно-технологічна (використання передових технологій та контроль їх стану).
- Інформаційна (захист інформаційних ресурсів та управління інформацією).
- Фізична (забезпечення фізичного захисту майна та персоналу) [5].

Узагальнюючи, як для "бізнес-безпеки", так і для майбутніх концепцій, важливо забезпечити ефективний захист від потенційних загроз, що створює основу для безпечного розвитку бізнесу.

Сучасні наукові дослідження у сфері корпоративної безпеки підкреслюють відсутність чіткого визначення поняття "загроза" та її впливу на безпеку підприємства. Вчені розрізняють два основних підходи до тлумачення цього поняття. Згідно з першим підходом, визначеним у роботах таких вчених як С. Покропивний, В. Пономаренко, В. Манілов, М. Дзлієв, О. Ареф'єва, та В. Кузьменко, загроза розглядається як сукупність умов, які негативно впливають на функціонування певної соціально-економічної системи.

Наприклад, у науковій праці О. Ареф'євої та В. Кузьменка загроза визначається як "сукупність умов, процесів, факторів, що заважають реалізації національних економічних інтересів або становлять загрозу для них та бізнесу". Інші вчені, такі як М. Єрмошенко, В. Білокур, В. Ярочкін, тлумачать загрозу як форму небезпеки, що може призвести до негативних наслідків.

Отже, загроза визначається як фактори, умови та процеси, які створюють небезпеку для функціонування підприємства або національних економічних

інтересів. Виявлені загрози, як зовнішні, так і внутрішні, визначаються як ключові елементи системи корпоративної безпеки та є основою для її подальшого розвитку і вдосконалення.

Отже, виокремлені зовнішні та внутрішні загрози стають важливими джерелами інформації для розробки та впровадження системи корпоративної безпеки. Вони є базою для аналізу ризиків та прийняття відповідних стратегій захисту підприємства від потенційних небезпек.

На основі зазначених загроз можна розробити план заходів зі зміцнення корпоративної безпеки, який включатиме в себе впровадження заходів з профілактики, моніторингу та реагування на потенційні небезпеки. Це може включати в себе застосування заходів інформаційної безпеки, вдосконалення систем управління, підвищення кваліфікації персоналу та впровадження сучасних технологій захисту.

Таким чином, аналіз загроз для корпоративної безпеки є важливим етапом у забезпеченні стійкості та безпеки підприємства в умовах сучасного бізнес-середовища. Це дозволяє підприємству адекватно реагувати на потенційні небезпеки та забезпечувати стабільність свого функціонування.

Концепція інформаційного впливу є комплексним підходом до вивчення та аналізу процесів передачі, сприйняття та обробки інформації в суспільстві [6]. Вона охоплює різноманітні аспекти, включаючи комунікаційні засоби, психологічні аспекти сприйняття, вплив технологій та соціокультурні чинники. Ця концепція допомагає розуміти, як інформація формує уявлення, переконання та поведінку людей, а також впливає на суспільні процеси, політику та економіку. Вона використовується в різних сферах, включаючи політичний маркетинг, медіа, психологію мас та кібербезпеку, для розробки стратегій комунікації, впливу та захисту від негативних впливів. Концепція інформаційного впливу базується на розумінні важливості інформації як інструменту формування світогляду, управління увагою та впливу на поведінку. Вона досліджує різні аспекти взаємодії між людьми та інформацією, включаючи комунікаційні канали, механізми переконання, психологічні механізми сприйняття, а також соціокультурні та технологічні фактори,

що впливають на цей процес. В контексті сучасного цифрового світу, де інформація легко поширюється та може впливати на масову аудиторію, концепція інформаційного впливу набуває особливого значення для розуміння та контролю над цими процесами.

Істотним є також розглядання етичних та правових аспектів інформаційного впливу, що допомагає зберегти баланс між свободою висловлювання та захистом від негативного впливу. Вторгнення в інформаційну систему – це дії, які порушують безпекову політику системи, а виявлення вторгнень – це процес, що використовується для ідентифікації вторгнень. Виявлення вторгнень вивчається близько 30 років. Загальний підхід базується на переконаннях, що поведінка зловмисника помітно відрізнятиметься від поведінки законного користувача і що багато несанкціонованих дій буде виявлено [7].

Система виявлення вторгнень (IDS – Intrusion Detection System) – це програмне або програмно-апаратне рішення, призначене для виявлення аномальних впливів та певних типів шкідливої активності, які можуть загрожувати безпеці інформаційної системи [7]. Це можуть бути різні мережеві атаки, неавторизований доступ до системи або дії шкідливого програмного забезпечення. Сама система є пасивним засобом захисту. Усі інциденти інформаційної безпеки, що виникають, фіксуються і передаються у звітному вигляді кінцевому користувачеві або адміністратору комп'ютерної мережі. Сигнали про загрози надалі не обробляються у таких системах. Для їх обробки використовують системи запобігання вторгненням, які є активними засобами захисту. Система впливу на свідомість (СВВ) — це комплекс методів і технологій, спрямованих на зміну сприйняття, думок, почуттів або поведінки людей. Такі системи можуть використовуватися для різних цілей, включаючи маркетинг, політичну пропаганду, психотерапію та навіть кібербезпеку. Класифікацію СВВ (система впливу на свідомість) можна провести за декількома ознаками [8, с. 44]. Одним із них є розташування агента системи в даний момент. Існує сімейство інструментів СВВ, які використовують інформацію, отриману від одного хоста (системи), СВВ на основі хоста (Host-based IDS, ХСВВ) і ті СВВ, які використовують інформацію, отриману з цілого сегменту локальної мережі (Network-based IDS, СУВ)

та комбінована гібридна система виявлення вторгнень. Класифікація систем виявлення вторгнень наведена нижче:

- IDS з урахуванням хоста.
- Мережевий IDS.
- IDS на гібридній основі.

ХСВВ розміщується на одному пристрої, такому як сервер чи робоча станція, де обробляє дані, отримані зсередини системи, і практично не використовує зовнішні інтерфейси. ХСВВ виявляє порушення у внутрішній активності системи. Прикладом таких активностей може бути раптова спроба редактора тексту, клієнта завантаження даних змінити базу даних системних паролів. Також, дана система повинна стежити за станом використання оперативної пам'яті, процесорного часу, файлової системи та ін. ХСВВ можна представити в комп'ютерній системі як агента, який відстежує внутрішні спроби обходу прийнятої політики безпеки. ХСВВ можуть відслідковувати стани лише окремих робочих станцій, на яких встановлені агенти, і не можуть проводити моніторинг усієї мережі. Недоліки ХСВВ можна назвати:

- Складність аналізу спроб вторгнення кілька комп'ютерів.
- Складність підтримки єдиної системи ХСВВ у великій мережі, яка має різні набори операційних систем та конфігурацій.
- ХСВВ можуть бути відключені після злому системи.

Далі можна навести приклади ХСЗВ, тобто іншими словами така хостова система захисту від вторгнень або Host-based Intrusion Detection System (HIDS), що є типом системи виявлення вторгнень, яка встановлюється безпосередньо на окремих комп'ютерах або серверах. HIDS аналізує діяльність на цих хостах для виявлення підозрілих дій, таких як зміни в файловій системі, підозрілі процеси, незвичні дії користувачів та інші аномалії, що можуть вказувати на кібератаку або небажану активність. Системи, що відстежують спроби підключення (RealSecure Agent, PortSentry) [9]. Вони перевіряють вхідні та вихідні мережеві підключення хоста. Системи, особливо ефективні, виявлення неавторизованих спроб встановлення TCP і UDP з'єднань із системою, і навіть виявлення спроби сканування портів.

Наступні системи перевіряють мережевий вхідний трафік. Ці системи захищають хост, перехоплюючи підозрілі мережеві пакети та проводячи їх аналіз на наявність у них корисного навантаження (шкідливого коду).

Системи, що відстежують активність входу в систему на мережному рівні свого хоста (HostSentry). Їхня роль полягає у відслідковуванні спроб входу та виходу з системи, пошуку незвичайної активності в системі, що відбувається в несподіваний час, у певних місцях у мережі, або виявленні занадто частих спроб входу до системи (особливо невдалих).

ХСВВ, які дивляться лише на локальний трафік, можуть легко виявити local-to-local або local-to-root атаки, оскільки вони мають чітке уявлення про локально доступну інформацію, наприклад, вони можуть використовувати СВВ користувача. Крім того, інструменти виявлення аномалій краще охоплюють внутрішні проблеми, оскільки їхня здатність виявлення заснована на нормальних моделях поведінки користувача.

ХСВВ знаходиться на конкретному комп'ютері та забезпечує захист конкретної комп'ютерної системи. Вони не тільки оснащені засобами системного моніторингу, але й включають інші модулі типової СВВ. Продукти ХСВВ, такі як Snort, Dragon Squire, Emerald eXpert-BSM, NFR HID, Intruder Alert виконують цей тип моніторингу.

Мережеві системи виявлення вторгнень, система самозахисту від вторгнень (ССВВ) зазвичай складаються з мережного пристрою (або датчика) з картою мережного інтерфейсу (NIC), що працює в нерозбірливому режимі, і окремим інтерфейсом управління. СВВ розміщується вздовж сегмента чи межі мережі та відстежує весь трафік у цьому сегменті. СЗВ, така системм, яка не тільки виявляє, але й активно запобігає загрозам. розгортаються у стратегічній точці мережевої інфраструктури. ССВВ може збирати та аналізувати дані для виявлення відомих атак шляхом порівняння шаблонів або сигнатур у базі даних або виявлення незаконних дій шляхом сканування трафіку на наявність аномальної активності. ССВВ надає дані про використання всього сегмента мережі, якого вона підключена. ССВВ повторно збирає та аналізує всі мережеві пакети, що надходять на карту мережного інтерфейсу, що працює в нерозбірливому режимі. Вони мають справу не тільки з пакетами, що йдуть

до певного хосту, оскільки всі машини в сегменті мережі користуються захистом ССВВ [9]. Мережні ССВВ також можуть бути встановлені активних елементах мережі, наприклад, на маршрутизаторах. Оскільки при виявленні вторгнень (наприклад, атаки типу flood) використовуються статистичні дані навантаження на мережу, певний тип ССВВ може конфігуруватися на виявлення саме цього типу вторгнень (Novell Analyzer, Microsoft Network Monitor). Вони захоплюють усі пакети, які бачать у сегменті мережі, не аналізуючи їх, а просто зосереджуючись на створенні статистики мережного трафіку. Типовими мережевими системами виявлення вторгнень є: Cisco Secure IDS (раніше NetRanger), Hogwash, Dragon, E-Trust IDS [10].

Управління та оповіщення як від мережевих, так і від хостів пристроїв виявлення вторгнень, а також побудова їх правильної спільної конфігурації веде нас до єдиної системи - централізоване управління виявленням вторгнень. Як мережеві, так і хостові СВВ мають свої унікальні переваги та недоліки. СВВ на основі мережі простіше у розгортанні та дешевше у купівлі та обслуговуванні. Однак їх продуктивність залежить від відомих експлойтів безпеки та сигнатур. Якщо використовується новий експлойт, про який СВВ не знає, то система може легко не виявити атаку. СВВ на основі хоста в більшості залежить від рівня адміністратора безпеки в системі, який конфігурує та стежить за роботою даної системи. Придбання навичок роботи з цим програмним забезпеченням, його обслуговування та моніторинг можуть виявитися непростим завданням. Таким чином, найкращий підхід полягає у використанні комбінації кращих функцій СВВ на основі мережі та хоста для підвищення стійкості до атак та забезпечення більшої гнучкості. Цей підхід зазвичай називають гібридною СОР, що є технологічною системою, яка призначена для аналізу, інтерпретації та реагування на інформаційні впливи з навколишнього середовища з метою виявлення аномальної або загрозливої активності. Такі системи активно використовуються у сфері кібербезпеки для захисту інформаційних мереж та систем.

Методи, що використовуються в сучасних СОР, можна розділити на три групи:

- Сигнатурні. Базуються на використанні попередньо визначених шаблонів або сигнатур відомих атак. Система порівнює вхідні дані з цими шаблонами для

виявлення збігів. Наприклад, антивірусні програми, які використовують базу даних відомих вірусів для виявлення та блокування загроз.

- Аномально-орієнтовані. Використовують моделі нормальної поведінки системи. Аномалії визначаються як відхилення від цієї моделі. Наприклад, системи моніторингу мережевого трафіку, які виявляють аномальну активність, що може свідчити про потенційну атаку.

- Гібридні. Поєднують елементи сигнатурних та аномально-орієнтованих методів для досягнення більшої ефективності виявлення загроз. Прикладом можуть бути системи, які використовують базу даних сигнатур для виявлення відомих загроз і моделі аномалій для виявлення нових атак [11].

Система виявлення на основі сигнатур працює за рахунок пошуку за шаблонами вже відомих атак. Може легко, швидко та точно виявляти відомі атаки. Ця система залежить від отримання регулярних оновлень шаблонів і не зможе виявити невідомі старі загрози, яких немає в базі шаблонів, або нові атаки. Одна з великих проблем СВВ на основі сигнатур полягає в тому, що для кожної сигнатури потрібен запис у базі даних, тому повна база даних може містити сотні або навіть тисячі записів. Кожен пакет має порівнюватися з усіма записами у базі даних. Це може бути дуже ресурсномістким процесом, і це призведе до уповільнення пропускної спроможності та погіршення роботи СВВ. Написання шаблонів, які б описували всі можливі варіації атак певного типу, залишається невирішеним завданням. Також такі системи дуже вразливі для DoS-атак. Деякі інструменти обходу СВВ використовують цю вразливість і заповнюють системи СВВ на основі сигнатур занадто великою кількістю пакетів настільки, що СВВ не може впоратися з трафіком, що призводить до тайм-ауту СВВ і відкидання пакетів і, як наслідок, пропуск атаки або відмова в роботи мережі. Крім того, цей тип СВВ, як і раніше, уразливий для невідомих атак, оскільки для виявлення атак він використовує сигнатури, що знаходяться в даний час в базі даних.

Другий тип систем ґрунтується на твердженні того, що всі атаки відрізняються від нормальної поведінки. Цей тип виявлення залежить від класифікації мережі на нормальну та аномальну, оскільки ця класифікація заснована на правилах чи

евристиці, а не на шаблонах чи сигнатурах, і для реалізації цієї системи нам спочатку потрібно знати нормальну поведінку мережі. Для цього система на початку своєї роботи будує профілі нормальної поведінки. Система виявлення на основі аномалій на відміну від системи виявлення на основі сигнатур може виявляти раніше невідомі загрози, але ймовірність помилкового спрацьовування вище. Сигнатура нової атаки невідома доти, доки її не буде виявлено і ретельно проаналізовано. Тож складно робити висновки на підставі невеликої кількості пакетів. У цьому випадку системи на основі аномалій виявляють аномальну поведінку та генерують сигнали тривоги на основі відмінності мережного трафіку від нормального профілю трафіку або поведінки додатків. Типова аномальна поведінка, яка може бути зафіксована, включає:

- використання нестандартних портів;
- різке збільшення UDP, TCP пакетів;
- аномальне використання ресурсів системи.

Серйозними проблемами систем виявлення аномалій є визначення нормальної поведінки мережі, визначення порога спрацьовування тривоги та запобігання помилковим тривогам. Користувачі мережі, як правило, люди, а поведінка людей у деяких випадках передбачити дуже складно. Якщо нормальна модель не визначена ретельно, буде багато помилкових спрацьовувань, і система виявлення страждатиме від зниження продуктивності.

Гібридний тип систем використовує одночасно сигнатурний і аномально орієнтований.

1.2 Параметри інформаційних впливів

Параметри інформаційних впливів охоплюють широкий спектр факторів, які визначають характер та ефективність впливу інформації на суспільство, індивідів та організації. Основні параметри включають:

Зміст інформації: Це включає якість, достовірність, актуальність та спосіб подання інформації. Якісна інформація, що базується на фактах та дослідженнях, зазвичай має більший вплив.

Контекст: Сприйняття інформації залежить від контексту, в якому вона подається. Це може включати культурні, соціальні та політичні чинники.

Канали комунікації: Різні канали комунікації, такі як мас-медіа, соціальні мережі, особисті контакти та інтернет, мають різний вплив на сприйняття інформації.

Цільова аудиторія: Ефективність впливу інформації залежить від характеристик цільової аудиторії, таких як вік, соціальний статус, освіта та інші.

Стратегія впливу: Різні стратегії комунікації, такі як переконання, маніпуляція, пропаганда та освіта, мають різний вплив на сприйняття інформації.

Реакція аудиторії: Відповідь аудиторії на інформацію може варіюватися від прийняття до відмови та активного опору.

Спосіб представлення: Форма, стиль та манера представлення інформації впливають на сприйняття та реакцію аудиторії.

Час та частота: Відповідність інформації актуальним подіям та частота її появи впливають на увагу та запам'ятовування.

Емоційний вплив: Використання емоційних складових може підсилити ефект інформаційного впливу та забезпечити більш глибоке сприйняття.

Джерело інформації: Довіра до джерела інформації впливає на її прийняття та вірування.

Контекстуальність: Узгодженість інформації з контекстом оточення сприяє її ефективному сприйняттю.

Взаємодія з іншими повідомленнями: Вплив попередніх повідомлень та сприйняття подальших може модифікувати реакцію аудиторії.

Ці параметри визначають складну динаміку інформаційного впливу, врахування яких допомагає ефективно керувати комунікаційними процесами та досягати бажаних результатів [12].

Врахування цих параметрів допомагає аналізувати та розуміти процеси інформаційного впливу та розвивати стратегії для керування ними.

1.3 Механізми інформаційних впливів

Механізми інформаційних впливів становлять різноманітні шляхи та способи передачі і сприйняття інформації, які впливають на переконання, думки та поведінку людей. Вони включають у себе різні аспекти, такі як медіа, реклама, соціальні взаємодії, психологічні фактори, політичні та соціокультурні контексти. Ці механізми взаємодіють між собою, утворюючи складну систему, яка визначає сприйняття та реакцію на інформацію в суспільстві [13].

Механізми інформаційних впливів можуть включати:

Медіа: Засоби масової інформації, такі як телебачення, радіо, газети, інтернет-портали, соціальні мережі, які поширюють інформацію та формують погляди аудиторії.

Реклама: Використання рекламних кампаній та піару для впливу на сприйняття та поведінку споживачів.

Соціальні взаємодії: Вплив оточуючих людей, колег, друзів та родини на формування думок та переконань.

Психологічні фактори: Використання емоційного впливу, психологічних прийомів та маніпуляцій для зміни переконань та поведінки.

Політичні та соціокультурні контексти: Врахування політичних та культурних контекстів для впливу на громадську думку та управління сприйняттям інформації.

Ці механізми взаємодіють між собою та змінюються залежно від контексту, що визначає їх ефективність у впливі на індивідуумів та суспільство в цілому.

1.4 Методи виявлення та протидії інформаційним впливам

Інформаційна війна в сучасному світі набула надзвичайної актуальності через розвиток технологій та поширення інформаційних засобів масової комунікації. Вона стала одним із найефективніших інструментів впливу на суспільство, політику, економіку та культуру. Інформаційна війна передбачає цілеспрямоване використання

інформаційних ресурсів та технологій з метою досягнення певних політичних, економічних або військових цілей і може включати в себе:

Моніторинг медіа-контенту: аналіз контенту (використання текстового аналізу та розпізнавання образів для виявлення маніпулятивних або неправдивих повідомлень), відстеження тенденцій (моніторинг змін у темах та тоні повідомлень для виявлення координованих кампаній).

Соціально-мережевий аналіз: аналіз соціальних графів (дослідження структур взаємодії між користувачами для виявлення координації та організованих мереж), виявлення ботів (використання алгоритмів для ідентифікації автоматизованих облікових записів, що поширюють дезінформацію)

Аналіз поведінки користувачів: відстеження аномальної активності (виявлення різких змін у поведінці користувачів, що можуть свідчити про інформаційний вплив), психометричний аналіз (використання даних про поведінку користувачів для оцінки впливу на їхню свідомість та емоційний стан).

Технічний аналіз: аналіз трафіку (вивчення інтернет-трафіку для виявлення аномальних патернів, що можуть свідчити про інформаційні атаки), розпізнавання фейкових новин (використання машинного навчання для автоматичного виявлення неправдивої інформації).

У той час, як методами протидії інформаційним впливам можуть бути:

Освітні заходи: медіаграмотність (проведення тренінгів та освітніх програм для підвищення рівня медіаграмотності серед населення), інформаційна просвіта (розповсюдження інформації про методи виявлення та захисту від дезінформації).

Технічні заходи: фільтрація контенту (використання алгоритмів для автоматичного видалення або позначення неправдивої інформації), захист від ботів (впровадження систем захисту від автоматизованих облікових записів та фейкових новин).

Регуляторні заходи: законодавство (розробка та впровадження законодавчих актів, що передбачають відповідальність за поширення дезінформації), міжнародна співпраця (співпраця з іншими країнами та міжнародними організаціями для спільної протидії інформаційним загрозам).

Психологічні заходи: емоційний інтелект (розвиток навичок емоційного інтелекту для кращого розпізнавання маніпуляцій), підтримка психологічного здоров'я (надання психологічної допомоги для зниження вразливості до інформаційних атак).

Аналітичні заходи: інформаційний аудит (проведення регулярних аудитів інформаційної безпеки для виявлення та усунення слабких місць), прогнозування загроз (використання прогнозних моделей для передбачення та запобігання можливим інформаційним атакам) [14].

З одного боку, інформаційна війна може бути використана для захисту національних інтересів, впливу на геополітичну ситуацію, а також для боротьби з тероризмом та злочинністю. З іншого боку, вона може бути засобом маніпуляції громадською думкою, дестабілізації суспільства та викликати міжнаціональні конфлікти. Руйнівна потужність інформаційно-психологічного впливу може бути навіть більшою, ніж військова сила, оскільки вона працює безпосередньо на свідомість та емоції людей.

Тоді можна сказати, що застосування цих методів у комплексі дозволяє не лише ефективно виявляти інформаційні впливи, але й розробляти стратегії для їхньої нейтралізації, що є ключовим для забезпечення інформаційної безпеки в сучасному світі.

Механізми інформаційної війни включають розповсюдження дезінформації, провокаційні дії, кібератаки, вплив на соціальні мережі та масові засоби масової інформації. Ці методи дозволяють впливати на свідомість громадян, формувати певні уявлення та переконання, тим самим впливаючи на політичні процеси, економічну ситуацію та соціальну стабільність.

Захист від інформаційних атак вимагає комплексного підходу та впровадження різноманітних заходів. Серед них можуть бути створення сучасних систем кібербезпеки, вдосконалення законодавства щодо інформаційної безпеки, підвищення критичної грамотності серед населення та підтримка незалежних медіа.

У світлі сучасних викликів і загроз інформаційна війна стає дедалі більш складною та небезпечною. Тому важливо постійно аналізувати ситуацію, реагувати

на виклики та розробляти ефективні стратегії захисту. Тільки таким чином можна забезпечити стабільність та безпеку суспільства в умовах інформаційної епохи.

Інформаційна війна, залежно від її мети та спрямування, має різні складові, які включають захист власних соціальних і інформаційних систем від впливу противника, боротьбу з державними системами управління супротивника, ведення політичної та економічної інформаційної війни, психологічну війну, комп'ютерну та кібернетичну війну.

У сучасних умовах важливо враховувати методологічні принципи ведення інформаційної війни, а також аналізувати напрямки застосування інформаційних засобів та їх вплив на різні соціальні структури. Вивчення особливостей національної культури противника є важливим етапом при розробці стратегій захисту власних інформаційних та технічних систем.

При плануванні заходів захисту від інформаційних атак важливо враховувати високий рівень небезпеки, що вони несуть для державних та міжнародних структур. Розвиток нормативно-правової бази, підвищення здатності до використання технологій управління, підготовка кадрів у галузі інформаційно-телекомунікаційних технологій є важливими аспектами в боротьбі з інформаційними загрозами.

1.5 Аналіз методів та підходів до виявлення інформаційних впливів

Наразі впроваджені системи обміну даними використовують криптографічний підхід для захисту інформації. Для поліпшення ефективності системи захисту використовується комбінація методів ідентифікації, таких як динаміка підпису, аналіз мовного спектру та персональний код, який записаний в електронний ключ типу "Touch memory". Однак такий підхід не є досить надійним.

Аналіз показав, що існуючі методи ідентифікації доступу до автоматизованих систем не враховують напрямок, пов'язаний з біотехнологіями. Тому впровадження біометричних технологій як додаткового механізму дозволить підвищити рівень захищеності від несанкціонованого доступу та кібератак [15].

Серед важливих досліджень у галузі інформаційної безпеки слід відзначити роботи науковців, які досліджують різні аспекти генезису інформаційного суспільства та забезпечення інформаційної безпеки в загальному значенні. Розроблено і аналізовано різноманітні підходи та програмні рішення для оцінки та контролю інформаційних ризиків.

Актуальним є впровадження біометричних систем ідентифікації з використанням стеганографічного методу захисту інформації. Використання біометричних технологій, заснованих на досягненнях у різних галузях науки та техніки, дозволяє покращити захист інформації в комп'ютерних системах.

Зараз, у контексті розвитку інформаційних технологій, стає нагальною проблема забезпечення інформаційної безпеки та захисту технічних ресурсів в комп'ютеризованих системах. Забезпечення безпеки інформаційних ресурсів є системним завданням, що передбачає використання різноманітних засобів захисту, таких як апаратні, програмні, фізичні та організаційні.

На сьогодні існує велика кількість інструментів забезпечення інформаційної безпеки, які використовуються для захисту інформації в різних сферах діяльності. Серед них можна виділити засоби ідентифікації та автентифікації користувачів, системи шифрування інформації, міжмережні екрани, віртуальні приватні мережі, засоби контентної фільтрації, антивірусний захист та інші.

Криптографічні методи захисту інформації, такі як кодування та шифрування, залишаються одними з найпоширеніших. Поряд з ними застосовуються методи розділення та стиснення даних. Наприклад, у процесі захисту передачі усної інформації використовуються методи аналогового скемблірування та дискретизації мови з подальшим шифруванням.

Отже, забезпечення безпеки інформаційних систем є важливим завданням, яке вимагає комплексного підходу та постійного вдосконалення технологій захисту для запобігання потенційним загрозам та атакам на інформаційні ресурси.

Пропонується використовувати ідентифікаційну систему, яка базується на розпізнаванні особи за райдужною оболонкою та реакцією очного яблука на подразники. Цей метод забезпечує тривимірну аутентифікацію користувача. Метод

підвищення безпеки інформаційно-телекомунікаційної системи, який запропоновано, включає наступні етапи.

1.5.1 Аналіз методів машинного навчання для виявлення інформаційних впливів

В епоху цифрової інформації, коли інформаційні потоки впливають на суспільство швидше і глибше, ніж будь-коли раніше, важливо вміти розпізнавати та аналізувати ці впливи. Методи машинного навчання (ML) стають незамінними інструментами для виявлення та аналізу інформаційних впливів, забезпечуючи нові можливості для розуміння і контролю інформаційного простору.

Одним із основних підходів до виявлення інформаційних впливів є наглядове навчання, яке використовує мічені дані для тренування моделей. Класичні алгоритми, такі як логістична регресія та метод опорних векторів (SVM), дозволяють класифікувати повідомлення на основі певних характеристик, наприклад, визначення, чи є інформаційний вплив позитивним або негативним. Ансамблеві методи, такі як Random Forest та Gradient Boosting, забезпечують високу точність і стабільність в класифікації складних текстових даних, що особливо важливо для виявлення фейкових новин або пропагандистських матеріалів.

На противагу наглядовому навчанню, ненаглядове навчання використовує немічені дані для виявлення прихованих структур та патернів. Кластеризація, зокрема методи K-means і ієрархічна кластеризація, дозволяють групувати схожі повідомлення або статті, що допомагає виявити тематичні кластеризації у новинних стрічках або соціальних мережах. Аналіз головних компонент (PCA) і Latent Dirichlet Allocation (LDA) допомагають зрозуміти основні фактори та теми, які впливають на інформаційні потоки, що є ключовим для аналізу контенту та визначення джерел інформаційних кампаній.

Глибоке навчання, зокрема рекурентні нейронні мережі (RNN) та моделі довготривалої короткочасної пам'яті (LSTM), стають дедалі популярнішими завдяки їх здатності обробляти великі обсяги даних і виявляти складні патерни. Ці моделі

особливо ефективні для аналізу послідовних даних, таких як тексти, що дозволяє автоматично розпізнавати та класифікувати фейкові новини або аналізувати тональність тексту з високою точністю. Конволюційні нейронні мережі (CNN), зазвичай застосовувані для класифікації зображень, також показали ефективність у поєднанні з word embeddings для аналізу текстів [16].

Методи обробки природної мови (NLP) є невід'ємною частиною аналізу інформаційних впливів. Токенізація, лематизація та стемінг дозволяють перетворювати тексти у формати, зручні для аналізу, тоді як word embeddings (такі як Word2Vec та GloVe) перетворюють слова у векторні представлення, що дозволяє алгоритмам машинного навчання ефективніше працювати з текстовими даними. Ці методи застосовуються для аналізу тональності текстів, виявлення ключових слів і фраз, а також ідентифікації маніпулятивних та пропагандистських технік у текстах.

Загалом, застосування методів машинного навчання для виявлення інформаційних впливів має величезне значення для сучасного суспільства. Це сприяє підвищенню інформаційної безпеки, дозволяючи швидко і ефективно виявляти фейкові новини, пропаганду та інші форми маніпуляції. Використання різноманітних алгоритмів і технік машинного навчання допомагає не лише виявляти інформаційні впливи, але й розуміти їх природу, що є ключовим для забезпечення здорового інформаційного середовища.

З теоретичного погляду, машинне навчання розглядається як дисципліна, що об'єднує математичну статистику, чисельні методи оптимізації, теорію ймовірностей та дискретний аналіз. Його методи використовуються для отримання знань з даних. З практичної точки зору, машинне навчання спрямоване на створення систем, що можуть адаптуватися до вирішення різних завдань без явного програмування алгоритмів, тобто систем, що можуть навчатися. Це розділення засноване на тому, що машинне навчання здатне отримувати знання з даних та покращувати свою роботу через навчання. Таким чином, машинне навчання є складовою частиною науки про дані. Хоча воно перетинається з аналізом даних, воно також має свою власну специфіку, оскільки здатне вирішувати завдання без явного програмування алгоритмів.

З теоретичного погляду, машинне навчання представляє собою область, що зливає у собі різноманітні математичні дисципліни, такі як математична статистика, чисельні методи оптимізації, теорія ймовірностей і дискретний аналіз. Його методи використовуються для вивчення даних та отримання з них знань. З практичної точки зору, машинне навчання спрямоване на створення систем, які можуть адаптуватися до різних завдань без явного програмування алгоритмів. Це означає, що системи можуть навчатися на основі даних та покращувати свої результати з часом.

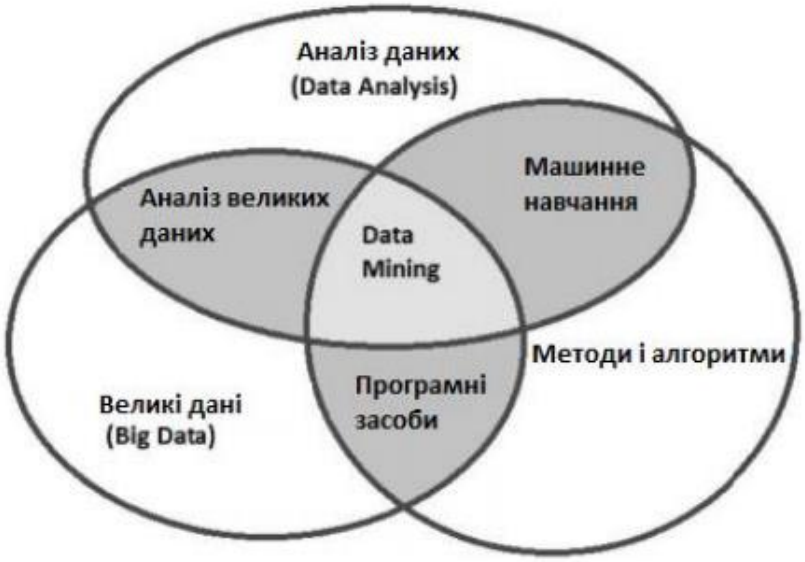


Рисунок 1.2 – Складові частини DataScience

Насправді, машинне навчання є складовою частиною науки про дані, але воно також має свої відмінності. Хоча воно перетинається з аналізом даних і використовує методи статистики, воно дозволяє вирішувати завдання без явного програмування алгоритмів [17]. Наприклад, у машинному навчанні алгоритми можуть самостійно визначати важливі закономірності та зв'язки в даних, що дозволяє їм автоматично вирішувати завдання без необхідності конкретного програмування для кожного випадку. На рисунку 1.2 зображені типові складові частини DataScience.

Задачі машинного навчання можна узагальнити на три основні категорії: регресію, класифікацію та кластеризацію.

Регресія полягає в наближенні невідомої функції або залежності на основі доступних даних. В даній задачі маємо набір даних, що складається з описів об'єктів та відповідних цільових значень. Мета полягає в тому, щоб побудувати алгоритм, який здатний наближати цю залежність для нових об'єктів.

Класифікація передбачає розподіл об'єктів на певні класи або категорії. Ми маємо набір даних, де кожен об'єкт має свою класову приналежність. Мета полягає в побудові алгоритму, який може визначати клас для нових об'єктів на основі їхніх ознак.

Кластеризація полягає в групуванні об'єктів на основі їхньої схожості без заздалегідь відомих класів. Ми шукаємо підмножини об'єктів, які схожі між собою, і групуємо їх у кластери. Мета полягає в тому, щоб кожен кластер мав об'єкти, які подібні між собою, але відрізняються від об'єктів інших кластерів.

Усі ці задачі мають свої варіації і можуть використовуватися в різних сферах, від прогнозування цін на акції до розпізнавання образів.

Задача регресії включає в себе наближення функції або залежності між вхідними та вихідними даними. Наприклад, це може бути прогнозування ціни на нерухомість на основі різноманітних характеристик будинку.

Класифікація передбачає розподіл об'єктів на певні категорії або класи на основі їхніх характеристик. Наприклад, класифікація електронних листів на "спам" та "не спам" на основі їхнього змісту та структури.

Кластеризація включає в себе групування схожих об'єктів у кластери без заздалегідь визначених категорій. Наприклад, це може бути групування клієнтів за їхнім споживацьким паттерном для подальшого аналізу ринку.

Усі ці задачі можуть використовуватися для різноманітних цілей, від прогнозування та рекомендацій до виявлення паттернів та аналізу даних. Вони є важливими інструментами в сучасному аналізі даних та машинному навчанні.

1.5.2 Аналіз можливості застосування соціального мережевого аналізу для виявлення інформаційних впливів

Соціальний мережевий аналіз (SNA) може бути потужним інструментом для виявлення інформаційних впливів і є методологією, яка використовується для дослідження соціальних структур за допомогою графічних моделей. В основі SNA лежить аналіз вузлів (користувачів) і зв'язків (взаємодій) між ними. Ключові поняття SNA включають центральність, кластери, та шляхи розповсюдження інформації.. Шляхом аналізу зв'язків та взаємодій між користувачами в соціальних мережах можна виявити ключових впливових осіб, групи та спільноти. Це дозволяє розуміти, як інформація поширюється в мережі, хто є її основними джерелами та які тенденції виникають у процесі цього поширення [18].

Застосування соціального мережевого аналізу для виявлення інформаційних впливів може мати широкий спектр застосувань, включаючи виявлення вірусних тем, аналіз впливу певних користувачів на популяризацію ідей чи продуктів, та виявлення групових динамік в розповсюдженні інформації. Крім того, цей аналіз може допомогти виявити ключові вузли в мережі, які можуть бути важливими для стратегій розповсюдження інформації або впливу на групи користувачів. Такий аналіз може бути корисним для маркетингових досліджень, політичних кампаній, аналізу громадської думки та багатьох інших галузей, де важливо розуміти та впливати на сприйняття та поведінку користувачів у соціальних мережах і може допомогти виявляти та аналізувати впливові теми, патерни поведінки та стратегії поширення інформації. Шляхом ідентифікації ключових користувачів, які мають найбільший вплив у мережі, можна визначити, які повідомлення або контент найефективніше поширюються та які групи аудиторії на них реагують.

Крім того, аналіз мережевих структур може допомогти виявити вразливості у поширенні дезінформації або негативного впливу. Розуміння того, які групи користувачів мають найбільший потенціал впливу та як вони взаємодіють один з одним, дозволяє розробляти стратегії протидії поширенню шкідливої інформації та підтримувати позитивний вплив у мережі.

Загалом, соціальний мережевий аналіз може стати потужним інструментом для розуміння та управління інформаційними впливами у соціальних мережах, що в свою чергу може мати велике значення для різних сфер діяльності, від маркетингу та політики до науки та громадської діяльності.

1.5.3 Лексичний аналіз

Лексичний аналіз - це процес обробки тексту для виділення та аналізування окремих лексичних одиниць, таких як слова, символи, фрази тощо. Основна мета лексичного аналізу полягає в розпізнаванні та класифікації цих лексичних одиниць з метою подальшого розуміння тексту або виконання певних дій з ним. Є важливим інструментом для виявлення інформаційних впливів, особливо в контексті аналізу текстових даних. Цей підхід дозволяє досліджувати структуру і зміст текстів, визначаючи ключові слова, фрази, тональність і семантичні зв'язки. Використання методів лексичного аналізу допомагає розуміти, як інформація передається через мову, та виявляти приховані патерни впливу.

Основними методами лексичного аналізу є те, що даний аналіз охоплює різні методи та техніки, які дозволяють аналізувати текстові дані на різних рівнях, таких як наприклад, токенізація (процес розбиття тексту на окремі слова або токени, цей крок є базовим для будь-якого текстового аналізу, оскільки дозволяє перетворити неструктурований текст у набір елементів, які можна досліджувати окремо); лематизація і стемінг – це процес зведення слів до їх базової форми (леми), наприклад, слова "біг", "біжить" і "бігали" зводяться до леми "біг", у той час як стемінг – це більш простий метод, який обрізає закінчення слів, зводячи їх до основи та ці обидва методи допомагають зменшити варіативність слів і покращити точність аналізу; виявлення ключових слів і фраз (методи виявлення ключових слів і фраз дозволяють ідентифікувати найважливіші елементи тексту, це можуть бути прості підрахунки частоти вживання слів або більш складні підходи, такі як TF-IDF (Term Frequency-Inverse Document Frequency), який враховує частоту слова в документі та його рідкість у корпусі текстів); аналіз тональності дозволяє визначити емоційне

забарвлення тексту – позитивне, негативне або нейтральне (цей метод широко використовується для оцінки громадської думки, аналізу відгуків та виявлення маніпулятивних впливів у текстах) та семантичний аналіз включає дослідження значень слів і їх зв'язків у тексті (це може бути досягнуто за допомогою таких методів, як word embeddings (наприклад, Word2Vec, GloVe), які представляють слова у вигляді векторів у багатовимірному просторі, це дозволяє виявляти семантичні схожості між словами та контекстуальні зв'язки).

У сфері обробки природної мови (Natural Language Processing, NLP) лексичний аналіз часто включає в себе такі завдання, як токенізація (розділення тексту на окремі слова або символи), нормалізація (перетворення слів у стандартну форму, наприклад, перетворення дієслів у їх базову форму), виявлення частин мови (Part-of-Speech tagging), виявлення іменованих сутностей (Named Entity Recognition) та інші [19].

Лексичний аналіз є важливим етапом у багатьох аспектах обробки тексту, включаючи машинне навчання, аналіз тексту для пошуку інформації, автоматичне розпізнавання мови, створення пошукових систем та інші області. Він допомагає перетворити текст у структурований формат, з яким можна працювати для подальшого аналізу та обробки.

Лексичний аналіз також може використовуватись для виявлення певних лінгвістичних характеристик тексту, таких як частота вживання певних слів або фраз, аналіз синтаксичних зв'язків між словами, виявлення тематичних аспектів тексту та багато іншого. Важливим аспектом лексичного аналізу є також розрізнення між істотною і неістотною інформацією, що допомагає покращити якість аналізу та розуміння тексту.

У сучасних системах обробки природної мови лексичний аналіз часто використовується разом з іншими видами аналізу, такими як синтаксичний аналіз (розбір тексту на складові синтаксичні одиниці), семантичний аналіз (розуміння значення тексту) та прагматичний аналіз (врахування контексту та мети спілкування). Ці різноманітні методи аналізу разом сприяють більш глибокому розумінню тексту та його контексту, що дозволяє створювати більш ефективні та інтелектуальні системи обробки мови.

Лексичний аналіз може бути ефективно використаний для виявлення інформаційних впливів у різних контекстах: аналіз пропаганди та дезінформації (виявлення характерних лексичних патернів, які використовуються у пропагандистських або дезінформаційних матеріалах); моніторинг громадської думки (аналіз тональності соціальних медіа постів, коментарів та інших текстових даних для оцінки громадської думки щодо певних подій або тем); виявлення тем і тенденцій (ідентифікація ключових тем і трендів у великих обсягах текстових даних за допомогою тематичного моделювання (наприклад, Latent Dirichlet Allocation)); оцінка впливу (визначення основних джерел і каналів інформаційних впливів на основі лексичного аналізу текстів, що поширюються у медіа та соціальних мережах).

1.5.4 Семантичний аналіз

Семантичний аналіз - це процес розуміння значення тексту на основі його змісту та контексту. Він визначається як аналіз смислових відношень між словами, фразами, реченнями та текстами. Основна мета семантичного аналізу - відтворення смислової структури тексту або виразу, щоб зрозуміти його значення та інтенції.

Семантичний аналіз може включати різноманітні завдання:

Словниковий аналіз: Визначення значень окремих слів та їх контекстуальних відтінків.

Розпізнавання іменованих сутностей: Виявлення та класифікація іменованих об'єктів у тексті, таких як імена людей, місця, організації тощо.

Аналіз семантичних відносин: Визначення взаємозв'язків між словами або фразами у тексті, таких як синоніми, антоніми, гіпероніми тощо.

Семантична розрізненість: Встановлення різниці в значенні між словами або фразами, які здавалося б схожими або синонімічними.

Семантична класифікація та категоризація: Групування слів або фраз за семантичними ознаками або категоріями.

Аналіз структури тексту: Розуміння семантичної організації та логічної послідовності в тексті.

Семантичний пошук: Пошук інформації на основі її семантичного змісту та відношень.

Семантичний аналіз є ключовим етапом у багатьох задачах обробки природної мови, таких як машинний переклад, аналіз настроїв відгуків користувачів, виявлення суттєвої інформації в тексті, автоматичне розуміння запитів користувачів та багато інших. Він сприяє покращенню автоматизованої обробки мовленнєвої інформації та розробці розумних систем, які здатні адаптуватися до контексту та інтенцій користувача.

Семантичний аналіз також використовується в соціальних мережах для розуміння інформаційних впливів. Він допомагає виявляти не лише самі повідомлення, але й їхній контекст, настрій, аспекти, що можуть бути ключовими для розуміння впливу. Наприклад, за допомогою семантичного аналізу можна визначити, які теми або продукти найбільше обговорюються в соціальних мережах, яка їхня тональність (позитивна, негативна, нейтральна), а також які користувачі мають найбільший вплив або авторитет у певній галузі. Це дозволяє компаніям, політикам та іншим учасникам визначити стратегії впливу, а також виявити тенденції та зміни в громадській думці.

1.5.5 Аналіз поведінки користувачів

Аналіз поведінки користувачів у соціальних мережах – це процес вивчення та розуміння того, як користувачі взаємодіють з платформою, її контентом та іншими користувачами і є ключовим інструментом для виявлення інформаційних впливів у цифровому середовищі. Зі зростанням популярності соціальних мереж, форумів і платформ для обміну повідомленнями, розуміння того, як користувачі взаємодіють з контентом і один з одним, стає надзвичайно важливим. Цей підхід дозволяє не лише виявляти потенційні загрози у вигляді дезінформації або пропаганди, але й оцінювати ефективність інформаційних кампаній.

Методами аналізу поведінки користувачів можуть бути:

Логування та аналіз дій – збір і аналіз логів дій користувачів дозволяє зрозуміти, як вони взаємодіють з платформою. Ці дані можуть включати кліки, перегляди сторінок, лайки, поширення контенту, коментарі та інші форми взаємодії. Аналізуючи ці дані, можна виявити патерни поведінки, які свідчать про сприйнятливість до певних видів інформаційних впливів.

Виявлення аномалій – методи виявлення аномалій дозволяють ідентифікувати нестандартну поведінку користувачів, яка може свідчити про маніпуляції або координовані дії. Алгоритми машинного навчання, такі як кластеризація та методи підвищення чутливості до аномалій (Anomaly Detection), дозволяють виявляти відхилення від норми у великих обсягах даних.

Соціальна взаємодія та мережевий аналіз – аналіз соціальної взаємодії користувачів в межах соціальних мереж допомагає виявляти впливові вузли та групи. Важливими показниками є кількість та якість взаємодій між користувачами, а також структура їхніх зв'язків. Соціальний мережевий аналіз (SNA) дозволяє визначити, як інформація поширюється в мережі, та виявити ключові вузли, через які проходять інформаційні потоки.

Аналіз контенту – аналіз контенту, з яким взаємодіють користувачі, дозволяє зрозуміти їхні інтереси та уподобання. Методи обробки природної мови (NLP) можуть бути використані для виявлення тем, тональності та емоційного забарвлення контенту. Це допомагає визначити, які теми викликають найбільший резонанс серед аудиторії та як інформаційні впливи формують громадську думку [20].

Цей аналіз може включати в себе:

Статистичний аналіз: Вивчення кількості лайків, коментарів, репостів та інших метрик взаємодії з контентом.

Сегментація аудиторії: Розподіл користувачів на різні групи за демографічними ознаками, інтересами, поведінковими звичками тощо.

Аналіз впливу: Визначення впливових користувачів, які мають значний вплив на інших учасників мережі через свої публікації та дії.

Аналіз заходів користувачів: Вивчення того, як користувачі взаємодіють з контентом, наприклад, скільки часу вони проводять на певних сторінках, які пости вони переглядають або лайкають.

Прогнозування поведінки: Використання аналітичних методів для передбачення майбутніх дій користувачів, наприклад, ймовірності реакції на певний контент.

Виявлення аномалій: Виявлення незвичайних або відхилень в поведінці користувачів, що можуть свідчити про шахрайство, або інші проблеми.

Персоналізація: Використання даних про поведінку користувачів для індивідуального підходу до них, наприклад, підбору персоналізованого контенту або рекомендацій.

Аналіз поведінки користувачів у соціальних мережах є важливим інструментом для розуміння та взаємодії з аудиторією, покращення стратегій маркетингу та залучення цільової аудиторії.

Висновки до розділу 1

Аналіз проблеми виявлення інформаційних впливів виявив, що це важка та складна задача, особливо у сучасному цифровому середовищі. Спричинено це різноманітністю джерел інформації, швидким поширенням контенту через соціальні мережі та інші канали зв'язку, а також складністю алгоритмів визначення впливу.

Щоб ефективно виявляти інформаційні впливи, необхідно використовувати широкий спектр інструментів аналізу, включаючи соціальний мережевий аналіз, аналіз тексту та зображень, статистичні методи та машинне навчання. При цьому важливо брати до уваги контекст і специфіку кожної ситуації.

Також виявлено, що необхідно постійно вдосконалювати методи аналізу та враховувати нові тенденції у цифрових комунікаціях, оскільки сфера впливу постійно розвивається. Враховуючи ці фактори, можна зробити аналіз інформаційних впливів більш ефективним та точним, що допоможе приймати обґрунтовані рішення у сфері медіа, маркетингу та громадської діяльності.

РОЗДІЛ 2
РОЗРОБКА МОДЕЛІ ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ВПЛИВІВ

2.1 Збір та підготовка даних для моделювання

Атакою на інформаційну систему називаються навмисні дії зловмисника, які використовують уразливості інформаційної системи та призводять до порушення доступності, цілісності та конфіденційності оброблюваної інформації [21].

Усунення вразливості інформаційної системи призводить до усунення та самої можливості реалізації атак.

Атаки можна поділити на такі типи [22]:

Розвідка. Ці атаки включають ping sweeps, передачу DNS-зони, розвідку за допомогою e-mail, сканування TCP або UDP портів та аналіз публічно доступних серверів з метою знаходження cgi-дір. Розвідувальні атаки - це досить поширені способи збору інформації про апаратне забезпечення, програмне забезпечення машин, підключених до мережі, а також дізнатися кількість самих машин, а при атаці на хост може відбуватися перевірка можливості реалізації конкретних типів уразливостей, отриманих при зборі інформації. Ця атака використовується для отримання корисної інформації про хости, дійсні IP-адреси, використовувані операційні системи і т. д. шляхом сканування мережі у відповідному режимі. Атакуючий використовує цю інформацію для пошуку потенційних уразливостей системи з метою їх подальшого використання при запуску атак проти машин та сервісів. Типовими прикладами такої атаки є:

- сканування мережі, наприклад, утилітою nmap, де ми зможемо перевірити чи відкрити порт, що цікавить;
- сканування всіх доступних портів для отримання інформації про тип хоста жертви та які сервіси на ньому запущені та доступні;
- повне сканування мережі.

Подібні варіанти сканування є попередниками інших мережевих атак.

Експлойт – це комп'ютерна програма, фрагмент програмного коду або послідовність команд, які використовують уразливості у програмному забезпеченні та застосовуються для проведення атаки на обчислювальну систему. Безпосередньо не реалізовується, оскільки у зловмисника вже має бути хоч якийсь доступ до системи. Може використовуватися в подальшому при реалізації DDoS-атак як вузл ботнет мережі.

Атака User to Root (U2R) – атака, за якої зловмисник намагається отримати незаконний доступ до адміністративного облікового запису, щоб маніпулювати чи зловживати важливими ресурсами [23]. Такий тип атак непросто відрізнити від нормального трафіку внаслідок того, що вони намагаються отримати привілейовані права в системі, що можуть робити авторизовані користувачі. Спочатку при виконанні цієї атаки зловмиснику необхідно отримати дані для автентифікації будь-якого користувача або сервісу, що працює в системі. Це можна зробити різними способами: брутфорс, фішинг, соціальна інженерія, тобто не завжди використовуючи комп'ютерну мережу, в якій запущено систему. Як тільки зловмисник отримує дані для аутентифікації, відбувається більш детальний аналіз програмного забезпечення, що використовується, і далі пошук шляхів реалізації вразливостей для підвищення свого рівня доступу до адміністратора. Ці атаки можуть належати до різних типів: переповнення буфера, при якому програма атакуючого відправляє в буфер великі обсяги даних без перевірки його ємності, використання руткітів, завантажувачів та інші.

Атака Remote to User (R2U), також відома як Remote to Local (R2L), запускається, коли зловмисник хоче отримати локальний доступ як користувача цільової машини, щоб мати привілей відправляти пакети по мережі. Цей тип атак схожий на атаки на перевищення прав доступу. Вона включає відправлення віддаленій машині або хосту пакетів через мережу, легітимним користувачем якої система не є. Далі так само, як і адміністратор чи користувач, атакуючий намагається отримати доступ до системи та виконати шкідливі дії. Двома найбільш часто зустрічаються варіантами даної атаки є переповнення буфера і атака з неперевіреними

вхідними даними. Вони також робляться проти громадських сервісів чи через з'єднання із захищеними сервісами [23].

Відмова в обслуговуванні (Denial of Service, DoS) [24]. За такої атаки порушник намагається зруйнувати сервіс (або комп'ютер), перевантажити мережу, перевантажити центральний процесор або переповнити диск. Атаки на відмову в обслуговуванні часто трапляються і мають безліч варіацій. Такі атаки вживаються для блокування доступу до певних ресурсів, для чого робляться недоступними відповідні мережеві сервіси або тимчасово скидаються всі мережеві з'єднання. Навіть у нинішніх реаліях при покупці сервісу захисту від DDoS-атак ваш сервіс може стати недоступним через те, що провайдер захисту (cloudflare, amazon shield) переведе ваші сервіси в недоступний пул для захисту власних ресурсів. В основному атаки на відмову в обслуговуванні перевантажують ресурси цільової системи таким числом запитів, що відповідна послуга не може бути їй надана. Однак перевантажуються не тільки ресурси системи, а й сам канал доступу до системи та відповідних сервісів, що може призвести до ще гірших наслідків. У деяких випадках атаки на відмову в обслуговуванні здатні тимчасово припинити доступ до ресурсів мільйонів його легальних користувачів. Такі атаки при успішному проведенні здатні швидко розходитися по гілках мережі та можуть призводити до серйозних проблем у роботі мережі. Наприклад, при перевантаженні каналу може припинитися нормальний доступ не тільки до системи, що атакується, але і до всієї підмережі. Типовими прикладами таких атак є переповнення буфера, перевантаження пінгом, TCP SYN (перевантаження запитами на синхронізацію за протоколом TCP) та інші. Також не варто забувати, що даний тип атак може застосовуватись для «замітання слідів» інших типів атак [25].

2.2 Синтез моделі виявлення інформаційних впливів

У процесі інформатизації суспільства починають бурхливо розвиватися мережеві послуги і відбувається процес впровадження їх у майже всі верстви суспільства. Перед адміністраторами інформаційно-обчислювальних систем стоїть

завдання забезпечити керованість цих систем, а також цілісність, доступність та конфіденційність даних. Зрештою забезпечити штатне функціонування системи за максимального виключення нестандартного поведінки системи (мережеві аномалії).

Аномалія – це відхилення від норми, загальної закономірності, яке характеризує неправильність поведінки. Стандартним видом аномалії трафіку є вихід інформативного параметра сигналу за його діапазон допустимих значень як за величиною, так і за швидкістю зміни часу [26].

У контексті мережної безпеки аномалії можна розділити на точкові, контекстні та колективні аномалії [27].

Точкові аномалії характеризуються появою окремого об'єкта, який не узгоджується з рештою набору даних. Прикладом може бути ізольований екземпляр мережного трафіку, який відрізняється від нормальних екземплярів, на певному часовому відрізку.

Контекстні аномалії характеризуються появою екземпляра даних, що є аномалією у цьому контексті. Контекст формується з урахуванням структур у наборах даних. Для його опису використовуються два основні набори змінних: контекстні та поведінкові. Перші використовуються визначення оточення кожному за екземпляра. Другі – визначають всі характеристики, що відносяться до конкретного примірника даних.

Колективні аномалії характеризуються наявністю пов'язаних екземплярів даних, визнаних аномальними порівняно з іншими даними. Окремий екземпляр може і не бути відхиленням, однак спільна поява таких екземплярів є колективною аномалією. Прикладом може бути поява подій «переповнення буфера» і копіювання файлів за протоколом ftp, які є звичайними подіями в деякій системі, однак їх спільна поява може служити про віддалену атаку на комп'ютерну систему.

Також має місце виявлення аномалій на основі продуктивності системи та зміни станів окремих додатків [22].

Аномалія у продуктивності. По аномалії в продуктивності можна судити про те, що поведінка програми, що спостерігається (наприклад, поточне використання центрального процесора ЦП) не може бути поясненою та спостерігається робочим

навантаженням програми (наприклад, тип і обсяг транзакцій, оброблюваних додатком, передбачає різний рівень використання ЦП).

Зміна у продуктивності транзакцій програми. Під зміною продуктивності транзакцій, як правило, мають на увазі істотну зміну (збільшення або зменшення) під час обробки транзакцій, наприклад, в результаті останнього оновлення програми.

Також важливо розрізняти аномалію продуктивності та зміну робочого навантаження. Аномалія продуктивності вказує на ненормальну ситуацію, яку необхідно досліджувати та вирішувати. Навпаки, зміна робочого навантаження (тобто зміни змішування транзакцій і навантаження) типова для веб-додатків. Тому вкрай бажано уникати помилкових тривог, викликаних алгоритмом через зміни робочого навантаження, хоча інформація про зміни робочого навантаження, що спостерігаються, може бути надана постачальнику послуг. За допомогою методів обчислювального інтелекту можна вирішити проблему точної ідентифікації атаки при її розподілі в часі або при проведенні кількома зловмисниками. До переваг даних методів можна віднести можливість розв'язання задачі при невідомих закономірностях, стійкість до шумів у вхідних даних, адаптація до змін у середовищі, потенційна надвисока швидкодія, відмовостійкість при апаратній реалізації нейронної мережі.

Штучні нейронні мережі . Більшість сучасних методів виявлення атак використовують деяку форму аналізу контрольованого простору з урахуванням правил чи статистичного підходу. Як контрольований простір можуть виступати журнали реєстрації або мережевий трафік. Аналіз спирається на набір заздалегідь визначених правил, які створюються адміністратором чи системою виявлення атак.

Будь-які розподілені атаки в часі або атаки, в яких бере участь велика кількість зловмисників, важкі для детектування експертними системами. Через велику різноманітність атак і хакерів навіть спеціальні постійні оновлення бази даних (БД) правил експертної системи ніколи не дадуть гарантії точної ідентифікації всього діапазону атак.

Використання нейронних мереж одна із способів усунення цього недоліку експертних систем. На відміну від експертних систем, які можуть дати користувачеві

певну відповідь про відповідність цих характеристик закладеним у БД правилам, нейронна мережа проводить аналіз інформації та надає можливість оцінити, чи узгоджуються дані з характеристиками, які вона навчена розпізнавати. Ступінь відповідності нейромережевого подання може досягати 100% достовірності вибору. Важливою перевагою нейронних мереж при виявленні зловживань є їхня здатність «вивчати» характеристики навмисних атак та ідентифікувати елементи, які не схожі на ті, що спостерігалися в мережі раніше.

Метод виявлення аномалій на основі нейронних мереж включає два етапи. На першому етапі нейронна мережа навчається розпізнаванню класів нормальної поведінки на тренувальній вибірці. На другому етапі кожен екземпляр надходить як вхідний сигнал нейронної мережі. Система, заснована на ІНС, може розпізнавати як один, і кілька класів нормальної поведінки. Для знаходження аномалій за допомогою розпізнавання лише одного класу використовують реплікативні нейронні мережі. Також можуть використовуватися технології глибокого навчання для ефективного виявлення аномалій у цих системах.

Дія нейронних мереж зумовлена безліччю функцій наближення, що залежать від вхідної інформації та спочатку невідомих. Головна перевага нейронних мереж полягає в тому, що вони менш чутливі до неточних вхідних даних, а також можливість створення рішення за відсутності інформації про залежність, закономірності у вхідних даних.

Деякі переваги нейронних мереж перед традиційними обчислювальними системами:

- вирішення завдань за невідомих закономірностей;
- стійкість до шумів у вхідних даних;
- адаптація до змін довкілля;
- потенційна надвисока швидкодія;
- відмовостійкість при апаратній реалізації нейронної мережі.

Еволюційне моделювання. Термін «еволюційне моделювання» включає в себе:

- генетичні алгоритми;
- генетичне програмування;

- еволюційні стратегії;

- штучні імунні системи [28].

Найбільш поширеними серед методів еволюційного моделювання є генетичні алгоритми та генетичне програмування. Вони обидва засновані на принципі «виживає найсильніший» і оперують населенням особин (хромосомами), використовуючи певні оператори. Основними операторами є відбір, кросинговер (кросовер) та мутація. Працювати алгоритми починають із випадково згенерованою популяцією (не обов'язково життєздатною). Для кожної особини обчислюється параметр пристосованості, який описує, як конкретний фенотип може вирішувати поставлене завдання. Особи з найвищими показниками пристосованості отримують більший шанс стати батьками. Два батьки можуть виконувати кросинговер і також кожен з них має шанс піддатися мутації. Особи з найкращими значеннями пристосованості копіюються в наступне покоління.

Головна різниця між генетичними алгоритмами та генетичним програмуванням є у поданні особин. По-перше, вони представлені у вигляді наборів бітових рядків і всі операції дуже прості. У генетичному програмуванні особини є програми і тому представляються у вигляді дерев, де внутрішніми вузлами є такі оператори, як плюс, мінус, множення, поділ, або, І, НЕ, а також різні програмні блоки такі, як умовний оператор, цикли та інші . У генетичному програмуванні всі операції видаються набагато складнішими, ніж у генетичних алгоритмах.

Головними перевагами генетичних алгоритмів виявлення аномалій є їх гнучкість та стійкість до випадкових шумових змін послідовності вхідних даних. На додаток до цього особливістю даних алгоритмів є прагнення оптимального вирішення проблеми з урахуванням ймовірнісних правил відбору кращих шляхів рішення. На відміну від більшості методів пошуку аномалій, генетичні алгоритми математично спрощені та легко сприймаються. Існує й низка недоліків генетичних алгоритмів виявлення викидів. До них відносяться складність підбору правил відбору найкращих рішень, а також варіація часу обчислення від ситуації до ситуації. Більше того, немає гарантії, що генетичний алгоритм дозволить знайти глобальний оптимум рішення.

Гібридні методи. Останні досягнення у галузі виявлення аномалій пов'язані саме з гібридними методами. Такі методи включають як мінімум два алгоритми, що відносяться до різних класів пошуку аномалій. Гібридизація використовується для того, щоб подолати недоліки одного методу шляхом використання переваг іншого, узгодивши їх функції.

Гібридні методи розпізнавання аномалій дозволяють поєднувати переваги різних підходів. При цьому досягнення середніх результатів можуть застосовуватися різні технології як послідовно, і паралельно. Прикладами гібридних систем розпізнавання аномалій можуть бути такі типи [29]:

- поєднання кластеризації та алгоритму найближчого сусіда;

- паралельне використання поєднаних алгоритмів, наприклад, баєсових мереж та вирішальних дерев, а також алгоритму найближчого сусіда з класифікацією на основі правил;

- поєднання методу опорних векторів та нейронної мережі.

До методів на основі знань відносять такі методи, які в контексті заданих фактів, правил виведення та зіставлень, що відображають ознаки заданих атак, виявляють аномалії (атаки) на основі закладеного механізму пошуку. У цьому випадку як процедура пошуку можуть застосовуватися зіставлення за зразком, апарат регулярних виразів, аналіз переходу станів і т. д. Своєю назвою ці методи зобов'язані тим, що системи, засновані на їх застосуванні, працюють з базою знань, до якої включені описи вже відомих атак [30].

Своєю назвою ці методи завдячують тим, що системи, засновані на їх застосуванні, працюють з базою знань, до якої включені описи вже відомих атак. Тут база знань представлена сховищем, що містить записи експертів за допомогою логіки їх обробки та інтерпретації (тобто характеризується наявністю підсистеми логічного висновку).

Сигнатурні методи (методи контекстного пошуку) полягають у виявленні у вихідній інформації певної множини символів. Так, наприклад, для виявлення атаки на Web-сервер під керуванням операційної системи сімейства Unix, спрямованої на отримання несанкціонованого доступу до файлу паролів, проводиться пошук

послідовності символів GET*/etc/passwd» у заголовку HTTP-запиту, або ж «GET */.htaccess». Для розширення функціональних можливостей контекстного пошуку в деяких випадках використовують спеціалізовані мови, що описують сигнатуру атаки. Також може відбуватися запис станів системи, де відбуватиметься формування сигнатури атак у вигляді послідовності переходів ІС з одного стану до іншого. По суті, кожен такий перехід визначається наступом в ІС певної події, а набір цих подій задається параметрами сигнатури атаки.

Сигнатурне виявлення включає пошук мережного трафіку з рядом шкідливих байтів або послідовністю пакетів. Основною перевагою даного методу є те, що сигнатури дуже легко розробляти та розуміти, якщо відомо, яку мережеву поведінку потрібно ідентифікувати. Наприклад, можна використовувати сигнатуру, яка шукає певні рядки в межах або перевіряє, чи використовують певну вразливість переповнення буфера. СОВ, побудовані на цих методах, можуть з високою точністю повідомити про причину тривоги. Так як зіставлення відбувається за конкретними типами сигнатур. Також варто зауважити, якщо система використовує лише певний вид комунікації в мережі (DNS, SMTP, ICMP, HTTP), інші сигнатури можна відключити для більш гнучкого і ефективного використання даної системи.

Існує кілька способів зіставлення сигнатур із реальними даними [31]:

- збіг із шаблоном;
- збіг із шаблоном стану;
- аналіз на основі шаблону протоколу, що використовується;
- контроль частоти подій чи перевищення порогової величин.

Збіг з шаблоном передбачає виявлення, що базується на пошуку певної послідовності байтів у оброблюваних даних. В результаті ми отримуємо простоту завдання правил і можемо створити прямий зв'язок із аномалією. Також цей спосіб буде застосований майже всім типів протоколів. Але також з'являються і недоліки: можливість помилкового спрацьовування, необхідність створення великої кількості шаблонів, обмеженість у застосуванні, а також велика кількість умов, за яких аномалії не будуть виявлені.

Збіг з шаблоном стану по одним пакетам встановлює поточний стан потоку даних, а з появою інших пакетів формує повідомлення про наявність аномалії. По суті має всі переваги попереднього способу, але демонструє більш високу надійність. Але також має ті ж недоліки: необхідність наявності великої бази шаблонів і при зміні аномалії може призвести до пропуску її виявлення.

Аналіз на основі шаблону використовуваного протоколу використовується для оцінки стану конкретного типу протоколу або його різних станів. Перевагами даного способу можна назвати прямий зв'язок з аномаліями та можливість виявлення великих, розподілених аномалій. До недоліків – велика кількість перепусток, а також складність формування сигнатур для конкретних систем.

Контроль частоти подій чи перевищення порогової величини передбачає, що у проміжок часу сигнатури описують ситуації, у яких частота певних подій перевищує заданий поріг.

До переваг можна віднести можливість опису складних взаємозв'язків, і навіть виявлення нових типів аномалій. До недоліків – складність у реалізації та пристосуванні сигнатур до певного виду трафіку.

2.3 Аналіз адекватності синтезованої моделі

Для оцінки фрактальних властивостей різних процесів широкого розповсюдження набув показник Херста H, який однозначно пов'язаний з розмірністю Хаусдорфа Df [32]:

$$D_f = 2 - H, \tag{2.1}$$

Показник ступеня Херста визначається термінах асимптотичного поведінки масштабованого діапазону як функції відрізка часу часового ряду так:

$$E\left[\frac{R(n)}{S(n)}\right] = CnH, \tag{2.2}$$

де $R(n)$ – розмах накопичених відхилень перших n значень від середнього значення ряду,

$S(n)$ – стандартне відхилення,

E – математичне очікування,

n – кількість точок у відрізку часового ряду,

C – константа.

Мандельброт показав [33], що з параметра Херста можна визначати розмірність простору ймовірностей. З цього отримуємо такі варіації:

- якщо $0 \leq H < 0.5$, то ряд схильний до змін. У нас виникає зворотна залежність поточного стану від часу. Стійкість системи залежить від того, наскільки близько показник Херста розташований до 0;

- якщо $H = 0.5$, то маємо випадковий ряд. Поточні значення не впливають на майбутні;

- якщо $0.5 < H \leq 1$, ряд є трендостійким. У ряду зберігається пряма залежність.

Показник Херста визначено на відрізку значень [0; 1].

Показник Херста може оцінюватися кількома способами: R/S, метод періодограм та методами вейвлет-аналізу. Однак у деяких випадках використовують інші методи [34].

Перевагою використання параметра Херста можна назвати швидкість обробки даних навіть при великих розмірах рядів, проте це є його недоліком: для отримання достовірних результатів необхідні великі розміри рядів; при малих значеннях можемо одержати помилку.

За основу було взято метод, який використовувався у цій роботі [27]. Алгоритм складається з двох етапів: розрахунок еталонів та виявлення аномалій у реальному часі. Для оцінки аномальності використовується інформація із заголовків пакетів транспортного та мережевого рівня моделі OSI за одну секунду:

- порт джерела/призначення;

- IP-адреса джерела/призначення;

- кількість пакетів IPv4;

- розмір корисного навантаження.

Дані, розрахунок яких проводитися на етапі розрахунку еталонних значень, порівнюватимуться з даними, які розраховуються в реальному часі на етапі виявлення. Для оцінки аномальності методом використовується параметр Херста. Етап розрахунку еталонів є кінцевою процедурою, що показано рисунку 2.2, та її тривалість становить звичайному режимі 4 хвилини. В результаті ми отримуємо два масиви з 4 значеннями: значення параметрів Херста для різних часових інтервалів та їхнє середньоквадратичне відхилення. Для оцінки параметра Херста використовується метод R/S, в основі якого використовується формула 2.3.

Як відомо, основною формулою RS-аналізу є відношення:

$$R/S = (a \cdot N)H, \tag{2.3}$$

де H – показник Херста;

S – стандартне відхилення низки спостережень;

R – розмах накопиченого відхилення;

N – дискретний час (обсяг вибірки); a – задана позитивна константа.

Розмах накопиченого відхилення R є найважливішим елементом формули розрахунку показника Херста. У загальному вигляді R обчислюють наступним способом:

$$R = \max_{1 \le U \le N} (Z_U) - \min_{1 \le U \le N} (Z_U), \tag{2.4}$$

де ZU – накопичене відхилення від середнього Xср.

Херс темпірично розрахував константу, для порівняльно короткострокових тимчасових рядів у природних явищ. Таким чином, формула набуде вигляду:

$$R/S = (N/2)H. \tag{2.5}$$

Знаходження значення параметра H можна розбити на такі етапи:

1) вихідний часовий ряд розбиваємо на блоки однакової довжини;

2) для кожного блоку обчислюємо розмах R;

3) для кожного блоку обчислюємо середньоквадратичне відхилення:

$$S = \sqrt{N-1} \sum_{i=1}^{N} (X - X)2; \quad (2.6)$$

4) приймаємо за N обсяг вибірки (дискретний час);

5) логарифмуємо отриманий вираз;

6) отримуємо шуканий параметр:

$$H = \log(R/S)/\log(N/2). \quad (2.7)$$

Відомо знаючи тривалість етапу розрахунку еталонів – 4 хвилини, можна для розрахунку використовувати наступну схему розбиття на інтервали:

• разів на 5 с;

• разів на 15 з;

• разів на 60 з;

• разів на 120 с.

Схема «разів у n» секунд означає, що весь часовий відрізок, рівний чотирма хвилинами (240 з), розбивається на інтервали по n секунд, й у кожному інтервалі виробляється розрахунок параметрів Херста.

У цьому розділі буде розглянуто побудову базової архітектури системи виявлення аномалій [35]. Схема даної архітектури показано рисунку 2.1.

Розглянемо основні компоненти цієї моделі:

• підсистема захоплення трафіку – відповідає за моніторинг і захоплення мережевого трафіку та забезпечує отримання даних для подальшого аналізу;

• ядро СОА – основний аналітичний модуль системи, виконує обробку та аналіз захоплених даних, може використовувати різні методи аналізу, включаючи сигнатурний аналіз, поведінковий аналіз і машинне навчання;

• довідкові дані – база даних з інформацією про відомі загрози та вразливості, містить сигнатури, правила і інші дані, необхідні для ідентифікації загроз;

• менеджер безпеки - інструмент управління та налаштування політик безпеки, дозволяє адміністраторам налаштовувати правила виявлення, реагування на інциденти і звітність;

• веб-інтерфейс – графічний інтерфейс для доступу до системи, забезпечує зручний доступ до інформації про поточний стан безпеки, налаштування системи та звіти про інциденти.

Підсистема захоплення трафіку є необхідним модулем у системі такого типу. Необроблені дані записуються як на рівні пакетів, так і на рівні потоків. Пакет дані можуть бути перехоплені будь-яким інструментом (наприклад Wireshark) і після і перед обробки відправлені в ядро системи. Поточні дані у разі систем високошвидкісної передачі даних можуть містити узагальнену інформацію про декілька пакетів. До часто використовуваних інструментів для захоплення даних потокового рівня можна віднести Nfpdump, Nfsen, Cisco Netflow [36]. Основні компоненти підсистеми захоплення трафіку зображені рисунку 2.1 Необроблені дані мережного трафіку захоплюються та буферизуються через мережевий адаптер у файлі формату tcpdump. Для отримання та обробки фільтрованого трафіку у форматі tcpdump можна використовувати бібліотеку libpcap.

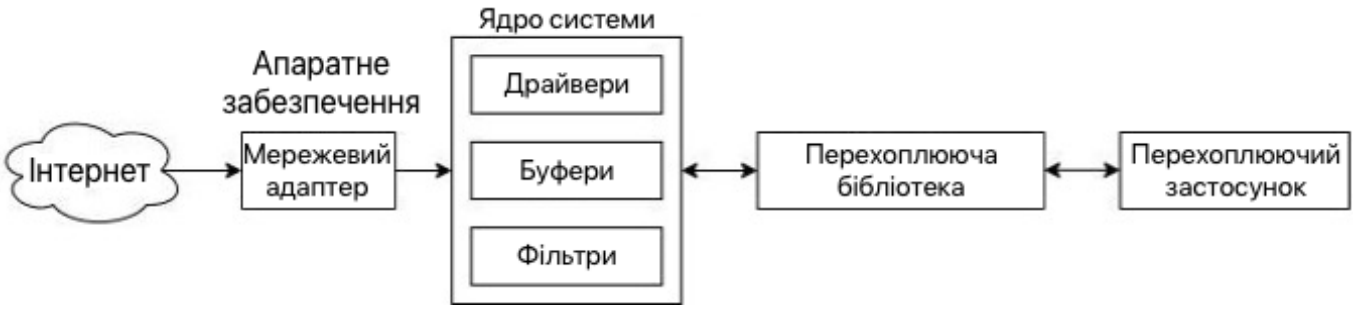


Рисунок 2.1 – Підсистема захоплення мережевого трафіку

Ядро системи виявлення аномалій покликане виявляти наявність аномалій у мережевому трафіку. Однак перед відправкою мережного трафіку на ядро необхідно провести його переробку. Якщо така атака вже відома, то її можна виявити щодо

залучення відповідних ресурсів. З іншого боку, невідомі атаки може бути виявлено шляхом зіставлення поточного стану з еталонним (нормальним прогнозованим).

Порівняння з талоном має на увазі під собою пошук патерна або профілю в мережевому графіку, які можуть бути побудовані на основі тривалого моніторингу поведінки мережі з відомими вразливістю або експлойтами. При побудові механізму порівняння з еталоном необхідно враховувати такі аспекти:

- кожен новий, не зустрічався раніше, кадр багатовимірного профілю роботи мережі оцінюється щодо того, належить він до відомого класу чи ні. порівняння має бути незалежним;
- порівняння з талоном має бути швидким;
- ефективна організація профілів здатна підвищити швидкість пошуку при порівнянні.

Довідкові дані (еталон та конфігурація) містять такі дані, як інформація про розміри даних, профілі відомих вторгнень або нормальну поведінку. Такі дані повинні зберігатися таким чином, щоб мінімізувати обчислювальні витрати на доступ до них та їхню обробку.

У разі СОА в основному це будуть профілі та сигнатури. Елементи обробки оновлюють профілі в міру появи нових знань про спостережуване поведінці. Ці оновлення виконуються пакетно-орієнтованим способом шляхом вирішення конфліктів, якщо вони виникають.

Еталонні дані є інформацією про відомі сигнатури атак або профілі нормальної поведінки мережі. Еталонні дані вимагають ефективної організації їхнього зберігання. Що стосується СОА частіше застосовуються профілі. Робочі елементи системи оновлюють профілі з надходженням нової інформації про функціонування мережі. Ці оновлення готуються в регулярні проміжки часу в пакетно-орієнтованому режимі.

Ці конфігурації можна віднести до проміжних результатів, наприклад, частково сформовані сигнатури вторгнень. Сховище, необхідне таких даних, може трохи більше. Проміжні дані повинні поєднуватися з існуючими знаннями для забезпечення стійкості та актуалізації результатів роботи системи.

Модуль сигналізація призначений для генерації сигнальних повідомлень на основі даних, отриманих від ядра СОА [37].

Основні цілі модуля аналізу – інтерпретація даних про аномалії, отримані від ядра СОА, та вжиття відповідних захисних заходів. До завдань цього модуля можна також віднести оновлення профілів і шаблонів за допомогою менеджера безпеки.

Компонент постобробки покликаний проводити постобробку згенерованих повідомлень про аномалії для діагностики актуальних атак.

Адміністратор безпеки. Цей модуль оновлює сигнатури, що зберігаються при виявленні нових вторгнень [38].

Також для ефективної роботи системи має бути представлений веб-інтерфейс. Він призначений для візуалізації даних та простої системи адміністрування СОА. За допомогою нього можна переглянути всі події по загрозах, весь трафік, що входить за певний період, за певними протоколами в режимі реального часу. Для адміністратора доступне часткове редагування даних конфігурації, налаштування способів візуалізації відображених протоколів, подій.

Висновки до розділу 2

У висновку можна зазначити, що розробка моделі виявлення інформаційних впливів є складним і багатогранним завданням, яке вимагає інтеграції різноманітних методів та підходів. Ця модель може включати в себе аналіз текстової інформації, аудіо- та відеоматеріалів, виявлення патернів та трендів у соціальних мережах, а також використання машинного навчання та штучного інтелекту для автоматизації процесу.

Важливою складовою такої моделі є розробка надійних алгоритмів та інструментів для виявлення негативних впливів, таких як дезінформація, маніпуляція громадською думкою та інші форми цифрової маніпуляції. Також важливою є здатність моделі оперативно реагувати на нові та еволюючі загрози, шляхом постійного вдосконалення та адаптації.

Нарешті, ефективність моделі виявлення інформаційних впливів залежить від співпраці між різними зацікавленими сторонами, включаючи урядові органи, дослідницькі установи, технологічні компанії та цивільне суспільство. Тільки шляхом спільної роботи та обміну інформацією можна досягти значних результатів у боротьбі з інформаційними загрозами.

РОЗДІЛ 3
МОДЕЛІ ТА МЕТОДИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ВПЛИВАМ

3.1 Синтез моделі оцінки ризику пов'язаного з інформаційним впливом

Для реалізації багатьох основних компонентів системи було обрано мову програмування Go [39]. Для реалізації інтерфейсу користувача був обраний стек технологій HTML/CSS/JS. Вихідний код розташований за цим посиланням: https://github.com/hiuon/network-analyzer/tree/master.

HTML або мова гіпертекстової розмітки дозволяє веб-розробникам створювати та структурувати розділи, абзаци та посилання з використанням елементів, тегів та атрибутів. Однак варто відзначити, що HTML не вважається мовою програмування, оскільки вона не може створювати динамічні функції [40].

HTML має безліч варіантів використання, а саме:

• Веб розробка. Розробники використовують код HTML для проектування того, як браузер відображає елементи веб-сторінки, такі як текст, гіперпосилання та мультимедійні файли.

• Інтернет-навігація. Користувачі можуть легко переміщатися та вставляти посилання між пов'язаними сторінками та веб-сайтами, оскільки HTML активно використовується для вбудовування гіперпосилань.

• Веб-документація. HTML дозволяє організовувати та форматувати документи аналогічно Microsoft Word.

Також варто відзначити, що HTML тепер вважається офіційним веб-стандартом. Консорціум World Wide Web (WWW) підтримує та розробляє специфікації HTML, а також надає регулярні оновлення.

Каскадні таблиці стилів, ласкаво звані CSS, є простою мовою дизайну, призначеною для спрощення процесу створення презентабельних веб-сторінок.

CSS обробляє зовнішній вигляд веб-сторінки. Використовуючи CSS, можна керувати кольором тексту, стилем шрифтів, відстанню між абзацами, розміром та

розташуванням стовпців, використовуваними фоновими зображеннями або кольорами, дизайном макета, варіантами відображення для різних пристроїв та розмірів екрану, а також безліч інших ефектів.

CSS легко вивчити і зрозуміти, але забезпечує потужний контроль над поданням HTML-документа. Найчастіше CSS узгоджується з мовами розмітки HTML чи XHTML.

Переваги CSS [40]:

• CSS заощаджує час – ви можете написати CSS один раз, а потім повторно використовувати один і той самий аркуш на кількох HTML-сторінках. Ви можете визначити стиль для кожного елемента HTML та застосувати його до будь-якої кількості веб-сторінок.

• Сторінки завантажуються швидше. Якщо ви використовуєте CSS, вам не потрібно щоразу писати атрибути HTML-тегів. Просто напишіть одне правило CSS для тега і застосуйте його до всіх входів цього тегу. Таким чином, менше коду означає швидший час завантаження.

• Просте обслуговування. Щоб змінити глобальну зміну, просто змініть стиль, і всі елементи на всіх веб-сторінках будуть оновлені автоматично.

• Покращені стилі в порівнянні з HTML - CSS має набагато ширший набір атрибутів, ніж HTML, тому ви можете набагато краще поглянути на свою сторінку HTML в порівнянні з атрибутами HTML.

• Сумісність із кількома пристроями – таблиці стилів дозволяють оптимізувати вміст для більш ніж одного типу пристроїв. Використовуючи один і той же HTML-документ, різні версії веб-сайту можуть бути представлені для портативних пристроїв, таких як КПК та мобільні телефони, або для друку.

• Глобальні веб-стандарти – тепер атрибути HTML застаріли і рекомендується використовувати CSS. Тому було б непогано почати використовувати CSS у всіх HTML-сторінках, щоб зробити їх сумісними з майбутніми браузерами.

JavaScript – це динамічна мова програмування. Він легкий та найчастіше використовується як частина веб-сторінок, реалізація яких дозволяє скрипту на

стороні клієнта взаємодіяти з користувачем та створювати динамічні сторінки. Це інтерпретована мова програмування з об'єктно-орієнтованими можливостями.

Спочатку JavaScript був відомий як LiveScript, але Netscape змінила свою назву на JavaScript, можливо через хвилювання, викликаного Java. JavaScript вперше з'явився у Netscape 2.0 у 1995 році під назвою LiveScript. Універсальне ядро мови було вбудоване у Netscape, Internet Explorer та інші веб-браузери.

Клієнтський JavaScript – найпоширеніша форма мови. Сценарій повинен бути включений до HTML-документа або на нього має бути посилання, щоб код міг бути інтерпретований браузером.

Це означає, що веб-сторінка не обов'язково має бути статичним HTML, але може включати програми, які взаємодіють із користувачем, керують браузером та динамічно створюють HTML-контент.

Клієнтський механізм JavaScript забезпечує безліч переваг, порівняно з традиційними серверними сценаріями CGI. Наприклад, ви можете використовувати JavaScript, щоб перевірити, чи введено користувач дійсну адресу електронної пошти в полі форми.

Код JavaScript виконується, коли користувач надсилає форму, і тільки якщо всі записи дійсні, вони будуть надіслані на веб-сервер.

JavaScript можна використовувати для перехоплення ініційованих користувачем подій, таких як натискання кнопок, навігація за посиланнями та інші дії, які користувач ініціює явно чи неявно.

Переваги використання JavaScript:

• Менш взаємодії із сервером – ви можете перевірити введення користувача перед відправкою сторінки на сервер. Це заощаджує трафік сервера, що означає менше навантаження на ваш сервер.

• Негайний зворотний зв'язок з відвідувачами – їм не потрібно чекати на перезавантаження сторінки, щоб побачити, чи не забули вони щось ввести.

• Підвищена інтерактивність - Ви можете створювати інтерфейси, які реагують, коли користувач наводить на них курсор миші або активує їх за допомогою клавіатури.

• Більш багаті інтерфейси. Ви можете використовувати JavaScript для включення таких елементів, як компоненти перетягування та повзунки, щоб надати відвідувачам вашого сайту багатий інтерфейс.

GoLang – це мова програмування з відкритим вихідним кодом, яка покликана вирішувати спільні завдання розробників. Деякі з проблем, які вирішує Go – це повільний час складання, неконтрольовані залежності, дублювання коду, складність написання автоматичних інструментів та крос-мовна розробка. Go працює з використанням «горутин» чи полегшених потоків, що дозволяє підвищити ефективність. Go також використовує набір пакетів для ефективного керування залежностями. Так як Go є кросплатформною мовою, ця програма може використовуватися на всіх поширених ОС.

Деякі приклади організацій, які використовують Go, включають Google, Cloudflare, Dropbox, MongoDB, Netflix, SoundCloud, Twitch та Uber.

Go включає ряд функцій, таких як стандартна бібліотека, управління пакетами, статична типізація, підтримка тестування, а також кросплатформеність. Стандартна бібліотека Go ґрунтується на використанні розподілених пакетів. Пакети можна опублікувати за допомогою невеликого набору команд. Go також підтримує модульні тести для запуску паралельно з написаним кодом. Крім того, завдяки модульній конструкції Go-код можна скомпілювати практично на будь-якій платформі.

Зокрема, Go використовує полегшені процеси, які забезпечують паралельну обробку і поводяться як потоки. Синтаксис імітуватиме шаблони, які зазвичай зустрічаються в динамічних мовах. Golang віддає перевагу складовим інтерфейсам успадкування. Деякі з інструментів Go, на які варто звернути увагу, – це функція Go fmt, яка автоматично форматує код і робить відступи для зручності читання, Go run, яка одночасно компілює та запускає код, «Go get», яка легко інтегрується з GitHub, та «Go doc», яка генерує HTML-код – документація відповідно до структури коду та коментарів розробників.

Використання Go у порівнянні з іншими мовами програмування має низку переваг, таких як [41]:

• швидка компіляція та швидкість виконання;

• відсутність віртуальної машини;

• портативність;

• горутини, що підтримують паралелізм;

• автоматичне збирання сміття;

• незалежна обробка помилок;

• великі вбудовані бібліотеки.

Деякі потенційні недоліки включають:

• не підтримує дженерики чи можливість писати абстрактний неявний код;

• суворі правила синтаксису;

• відсутність можливості навантаження функцій;

• відсутність повної підтримки ОВП.

3.2 Метод маркування контенту як попередження

Метод маркування контенту як попередження є важливим інструментом у боротьбі з дезінформацією та захистом користувачів від небажаного або шкідливого контенту в Інтернеті. Він передбачає використання різних технічних і соціальних підходів для ідентифікації, позначення і попередження користувачів про потенційно небезпечний або неправдивий контент. Існують певні принципи та механізми до відповідного методу, з них можна виокремити: автоматичні системи ідентифікації: аналіз тексту (використання алгоритмів машинного навчання та обробки природної мови для аналізу текстового контенту з метою виявлення фейкових новин, пропаганди або інших форм шкідливої інформації, наприклад, системи можуть аналізувати лексичні особливості тексту, структуру речень та інші маркери, які часто зустрічаються в дезінформації), зображення і відео (технології комп'ютерного зору можуть аналізувати зображення та відео для виявлення маніпуляцій або фальсифікацій, таких як дипфейки (deepfakes)); соціальні сигнали: фактчекінг (важливу роль у маркуванні контенту відіграють незалежні організації та платформи для перевірки фактів, які можуть надати експертний висновок щодо правдивості інформації. Результати їхньої роботи можуть бути інтегровані в алгоритми

соціальних мереж та пошукових систем для автоматичного маркування контенту), повідомлення користувачів (користувачі також можуть брати участь у процесі маркування контенту, повідомляючи про підозрілий або шкідливий матеріал. Це дозволяє створювати динамічну систему контролю контенту, яка враховує колективну думку спільноти); маркування та попередження: візуальні індикатори (контент, який було визначено як потенційно небезпечний або неправдивий, може бути помічений спеціальними значками, попереджувальними повідомленнями або ярликами, наприклад, соціальні мережі можуть додавати попередження перед переглядом відео або статті, що містить неправдиву інформацію), зниження видимості (окрім маркування, такий контент може бути знижений у видачі пошукових систем та соціальних мереж, щоб обмежити його поширення та вплив на користувачів) [42].

Щодо практичного застосування, tcpdump утиліта UNIX (є клон для Windows), що дозволяє захоплювати та аналізувати мережевий трафік, що проходить через комп'ютер, на якому запущена дана програма [43].

Програма складається з двох основних блоків: захоплення пакетів (зі зверненням до бібліотеки libpcap (Unix) або Pcap (Windows)) та відображення захоплених пакетів (яка на рівні вихідного коду є модульною і для підтримки нового протоколу достатньо додати новий модуль).

tcpdump дані [44]. Класифікатори, що породжуються, використовують дані tcpdump, щоб відрізнити мережеві атаки від нормального трафіку. TCPdump (або Windump для Windows) є популярним і широко застосовуваним програмним засобом, що дозволяє детально дослідити процес передачі інформації в мережі. Висновок tcpdump містить дані пакетів мережевих з'єднань у порядку появи пакета мережі. Перед збиранням інформації ці пакети повинні попередньо оброблятися. Конвертори tcpdump даних перетворюють записи з'єднання на безліч особливостей (тобто атрибутів), наприклад, time (час початку з'єднання тобто, позначка часу першого пакета), dur (тривалість з'єднання), src і dst (хост-джерело і хост -адресат), bytes (кількість байтів даних, відправлених із джерела адресату), srv (сервіс, тобто порт

адресата), flag (як з'єднання відповідає мережному протоколу) і т.д. Ці суттєві особливості по суті підсумовують інформацію пакетного рівня в межах з'єднання.

Сніффер tcpdump був використаний у численних роботах у сфері комп'ютерних мереж та фактично є стандартною утилітою для захоплення трафіку. За допомогою нього встановлено вихідний формат файлів PCAP, який є файловим форматом, що найбільш використовується для захоплення і зберігання пакетів. Сніффер tcpdump пропонує механізм фільтрації, який дозволяє захоплювати тільки пакети, що відповідають певному критерію, наприклад, TCP-пакети з фіксованим номером порту призначення, рівним 80. На жаль, даний механізм не дозволяє вибрати пакети тільки однієї програми, особливо якщо процес, що спостерігається, є peer- to-peer програмою, що призначає нові порти динамічно кожні кілька секунд. Однак це можна реалізувати з використанням мов програмування, які підтримують роботу з даним сніффером, за допомогою аналізу заголовків пакетів вищого рівня.

Блок захоплення пакетів (при запуску) передає вислів про логіку захоплення (що йде після всіх параметрів командного рядка) безпосередньо бібліотеці захоплення пакетів, яка перевіряє вираз синтаксису, компілює його (у внутрішній формат даних), а потім копіює у внутрішній буфер програми мережні пакети, проходять через вибраний інтерфейс і задовольняють умовам у ньому.

Блок відображення пакетів вибирає захоплені пакети по одному з буфера, що заповнюється бібліотекою, і виводить їх (у легкочитабельному вигляді) на стандартний висновок рядково відповідно до заданого (у командному рядку) рівня деталізації. Якщо встановлено докладний висновок пакетів, програма перевіряє для кожного пакета мережі, чи є у неї модуль розшифровки даних, і, у разі наявності, відповідною підпрограмою витягує (і відображає) тип пакета в протоколі або параметри, що передаються в пакеті.

В основному tcpdump використовується для налагодження мережевих додатків, мережі та мережевої конфігурації в цілому.

Реалізація сніфера трафіку відбувається з використанням мови Go та утиліти tcpdump з відповідним драйвером libpcap. Для взаємодії з tcpdump використається відповідний модуль gopacket [45]. Модуль gopacket надає оболонку Go для libpcap,

написану на C. Однак це більше ніж просто оболонка. Він надає додаткову функціональність та використовує такі переваги Go, як інтерфейси, що робить його неймовірно потужним.

У ядрі системи відбувається обробка мережного трафіку, отриманого від сніфера. У реалізації використовується два методи на основі параметра Херста, описані вище. Як метрики, що використовуються для підрахунку, використовується кількість IP-пакетів, отриманих за 5 с. Однак також можуть використовуватися дані про протоколи, порти призначення та прийому, що використовуються, а також IP-адрес призначення та прийому.

Модуль розрахунку еталонних даних та їх захоплення схожий на підхід, який використовується для розрахунку параметра Херста в реальному часі. Головна відмінність полягає у завданні кінцевого інтервалу часу, для отримання великої кількості відліків у послідовності. У межах навчання відбувається обчислення необхідних параметрів використовуваних методів і далі запис еталонних даних. Повинен хоча б один раз запущено для правильної роботи системи.

Модуль оповіщення описується окремою функцією, яка веде загальний підрахунок кількості виходів за межі допустимих інтервалів. Оскільки описувалося вище, у статистичних методах одними з основних проблем є вибір меж допустимих значень і, отже, досить багато хибних спрацьовувань.

Для реалізації серверної частини використовувався стандартний модуль мови Go net/http і виведення логів сервера модуль log. HTTP-сервер запущено на 5000 порту інтерфейсу localhost і вимагає запуску від імені адміністратора або з привілеями користувача root (залежно від використовуваної ОС), для можливості прослуховування всіх інтерфейсів та портів у системі. Взаємодія між клієнтами та сервером відбувається за допомогою GET запитів.

Для обробки запитів можливі наступні маршрути:

/devices. Призначений для отримання поточного списку доступних мережних інтерфейсів у системі.

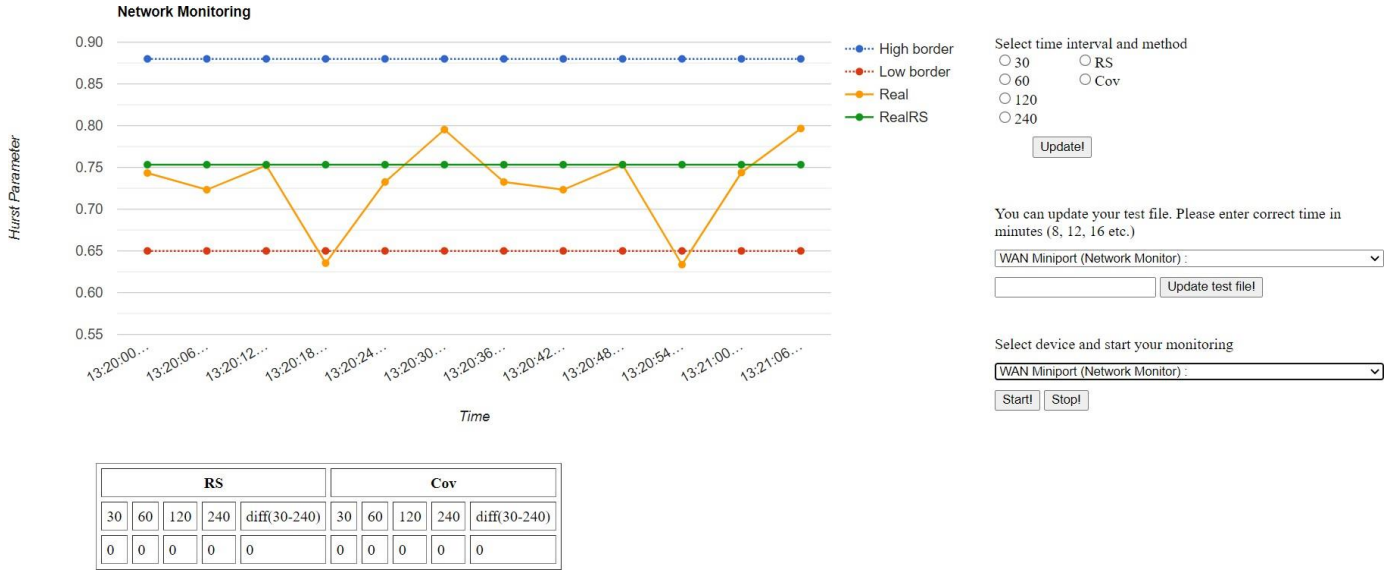
/start. Призначений для запуску моніторингу мережного трафіку. Відбувається запуск ядра системи в асинхронному режимі за допомогою горутину. Використовує один параметр deviceName для вибору пристрою прослуховування трафіку.

/get-data. Призначений для отримання поточної статистики вимірювання параметра Херста. Використовує параметри type – інформація про та використовується метод розрахунку, interval – інформація про що цікавить тимчасовому інтервалі.

/stop. Призначений для зупинення моніторингу мережі та оновлення даних, отриманих у реальному часі.

/get-test-data. Призначений для оновлення тестового файлу, який використовується для розрахунку початкових еталонів. Використовує параметр deviceName для вибору пристрою прослуховування трафіку.

/get-anomaly-count. Призначений для отримання та оновлення статистики за ситуаціями, що вийшли за межі допустимих значень.



RS					Cov				
30	60	120	240	diff(30-240)	30	60	120	240	diff(30-240)
0	0	0	0	0	0	0	0	0	0

Рисунок 3.1 – Зовнішній вигляд інтерфейсу користувача

На рисунку 3.1 представлений зовнішній вигляд користувальницького інтерфейсу системи. Як зазначалося вище, для його відображення використовується стек JavaScript/HTML/CSS.

Складається з 3 ключових блоків:

• графік залежності показника Херста від часу;

• таблиця, що відображає кількість попереджень, що виникли;

• блок керування.

Для відображення графіка використовувалася бібліотека Google Charts.

У таблиці відображається кількість виявлених попереджень за кожен інтервал часу для кожного методу. В останньому стовпці вказується кількість виявлених попереджень за останні 4 хвилини моніторингу системи. Висновок про проблеми вторгнення в мережі робиться на основі останніх стовпців для кожного методу. Максимальне значення даного поля 8 + 4 + 2 + 1 = 15. При перевищенні певного порога в обох методах можна формувати повідомлення та передати цю інформацію наступним пристроям у периметрі захисту системи.

У блоці управління (конфігурації) задаються різні параметри виведення і роботи ядра системи. У верхньому блоці задається конфігурація про те, яка інформація відображатиметься на графіку моніторингу. У наступному блоці можемо оновити існуючий PCAP файл, на основі якого обчислюються межі допустимих значень. І в останньому блоці відбувається запуск чи зупинка моніторингу мережі системи.

У цьому розділі було побудовано базову архітектуру системи виявлення аномалій. Розглянуто її основні модулі: підсистема захоплення трафіку, ядро СОА, довідкові дані, менеджер безпеки, веб-інтерфейс. Також представлено діаграму використання СОА. Актору буде доступно чотири основні варіанти використання: зміна конфігурації, запуск навчання, перегляд статистики трафіку, що передається, і запуск моніторингу трафіку. Також були описані іструменти, які використовувалися для побудови кожного модуля системи. І було дано описи реалізованих модулів та його базовий функціонал.

3.3 Метод блокування контенту чи джерел його поширення

Метод блокування контенту чи джерел його поширення є важливим інструментом у сфері інформаційної безпеки та боротьби з дезінформацією. Цей

підхід спрямований на обмеження доступу до шкідливих або небажаних матеріалів через технічні та адміністративні заходи. Розглянемо основні аспекти цього методу, його реалізацію та ефективність. Для такого методу існують наступні принципи та механізми:

Технічні заходи: IP-блокування: Включає блокування доступу до певних IP-адрес або діапазонів адрес, які асоціюються з шкідливими сайтами або серверами. Цей метод ефективний для запобігання доступу до конкретних джерел дезінформації або кіберзагроз. DNS-блокування: Зміна або видалення записів DNS для шкідливих доменів, що ускладнює або робить неможливим доступ до цих ресурсів. DNS-фільтри можуть бути налаштовані на рівні інтернет-провайдерів або організацій для забезпечення безпеки користувачів. URL-фільтрація: Блокування доступу до конкретних URL-адрес, які ідентифіковані як небезпечні або шкідливі. Це дозволяє більш гнучко контролювати доступ до конкретних сторінок веб-сайтів.

Адміністративні заходи: Чорні списки (blacklists): Створення та підтримка списків веб-сайтів, доменів або IP-адрес, доступ до яких заборонений через їхню шкідливу діяльність. Ці списки можуть бути централізованими або розповсюдженими серед різних організацій. Блокування на рівні платформ: Соціальні мережі та інші платформи можуть блокувати облікові записи або сторінки, які поширюють шкідливий контент. Це включає видалення фейкових акаунтів, ботів та груп, які займаються дезінформацією. Законодавчі та нормативні заходи: Прийняття законів та регуляцій, що вимагають від інтернет-провайдерів і платформ блокувати доступ до певних типів контенту або джерел його поширення [46].

Перевагами чого є:

Ефективне стримування: Блокування джерел дезінформації та шкідливого контенту може суттєво зменшити їхній вплив і поширення.

Захист користувачів: Забезпечує безпеку користувачів шляхом обмеження доступу до потенційно небезпечних ресурсів.

Зниження навантаження на мережу: Зменшення обсягу шкідливого трафіку може покращити загальну продуктивність мережі.

Для тестування роботи СОВ було збудовано базову мережа, зображена рисунку 3.2. Це два пристрої з запущеним агентом на різних операційних системах, а також один атакуючий пристрій з операційною системою Kali Linux на базі Ubuntu. На атакуючому пристрої реалізовувалися два типи атак: DoS та розвідка. Перша запускалася з використанням утиліти hping3, за допомогою якої генерувався трафік: hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.0.106(105). Це звичайна атака SYN-flood, в якій відправляється 15000 пакетів розміром 120 байт кожен. Для реалізації другої використовувалася утиліта nmap: nmap 192.168.0.106 (105).

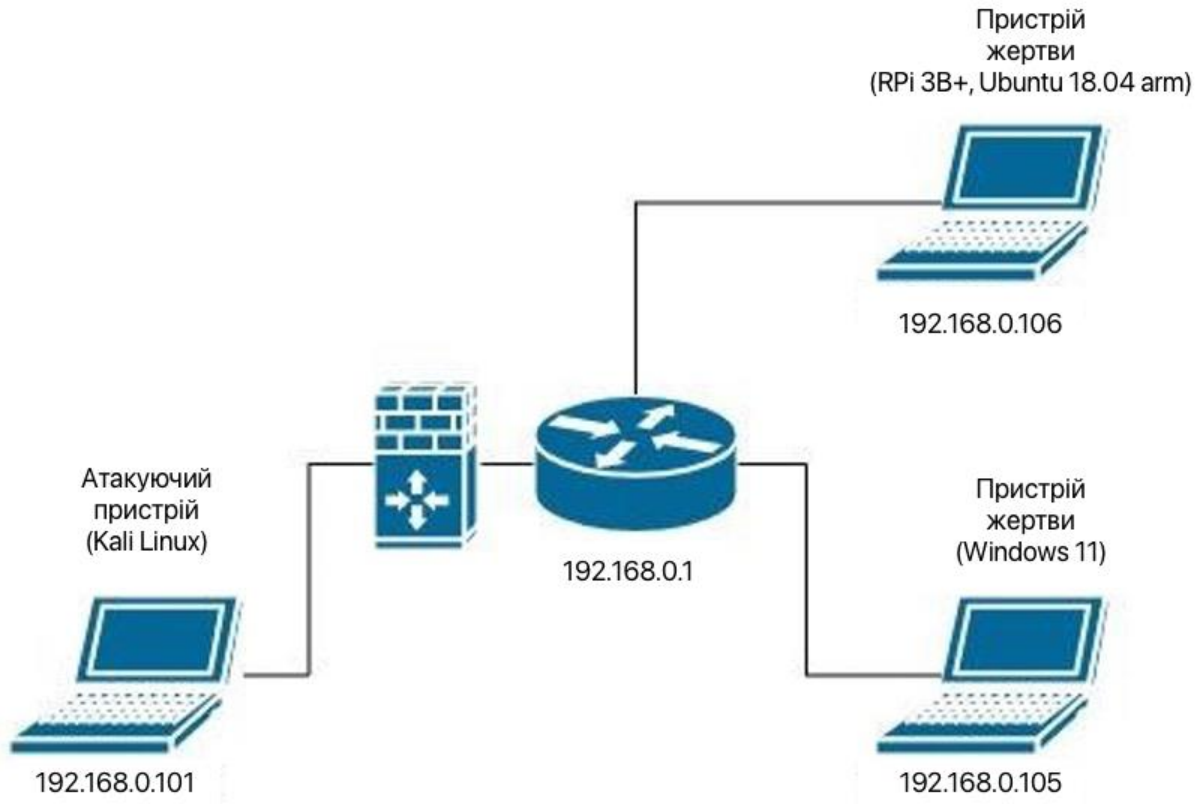


Рисунок 3.2 – Схема мережі

При роботі у звичайному режимі за 45 хв. у середньому одержуємо дані значення про кількість попереджень (середнє значення за 5 проходів) відображені у таблиці 3.1. Однак варто зауважити, що при розрахунку значень з дуже розрядженим трафіком у часі самі алгоритми відпрацьовують не зовсім коректно і дуже часто отримуємо значення параметра Херста, які виходять за межі 0 та 1.

Таблиця 3.1 – Результати роботи у нормальному режимі

	Інтервали часу (с)							
	30		60		120		240	
	RS	Cov	RS	Cov	RS	Cov	RS	Cov
Кількість попереджень	40	35	23	22	2	3	3	2

Як видно з отриманих значень, кількість попереджень наближається до половини від максимально можливих у 30-ти та 60-ти секундних інтервалах. В інтервалах 120-ти та 240 секунд отримуємо більш прийнятні значення. Що стосується загального числа попереджень за 4 хвилини, то в середньому виходить 5-6 мінімум до 0 і максимум до 8-9.

При реалізації DoS-атаки протягом 45 хв. отримуємо такі дані (середнє значення за 5 проходів), які відображені у таблиці 3.2. Значення в малих інтервалах змінилися не дуже сильно, але переступили 50% бар'єр від максимальної кількості можливих попереджень. У великих інтервалах часу кількість попереджень значно змінилася (аж до 4-х разів).

Таблиця 3.2 – Результати роботи в умовах DoS-атаки

	Інтервали часу (с)							
	30		60		120		240	
	RS	Cov	RS	Cov	RS	Cov	RS	Cov
Кількість попереджень	52	45	22	22	8	11	6	5

Щодо загальної кількості попереджень за кожні 4 хвилини, то в середньому отримували від 8 до 12, у піку – 13, у мінімумі – 6. Дані результати показують ефективність методів виявлення колективних і розподілених атак.

Так як у нормальному режимі роботи виникає досить чимало помилкових попереджень, виявлення будь-яких точкових аномалій виглядає практично

неможливим. Результати показали схожий результат із нормальною роботою, таблиця 3.3, за 45 хв.

Таблиця 3.3 – Результати роботи в умовах розвідки

	Інтервали часу (с)							
	30		60		120		240	
	RS	Cov	RS	Cov	RS	Cov	RS	Cov
Кількість попереджень	42	34	20	23	3	1	2	1

Однак не виключений варіант про можливість виявлення даної атаки, якщо вона буде більше розподілена в часі.

Використання як метрик не кількості всіх пакетів, а кількості запитів на різні порти вирішить цю проблему, але з цим можуть впоратися звичайні сигнатурні методи.

За отриманими результатами можна сказати, що використання 30-ти та 60-ти секундних інтервалів не має великого сенсу. Система отримує велику кількість помилкових спрацьовувань, що не дає ефективно виявляти точкові атаки. Як можна помітити, зі збільшенням інтервалу часу зменшується кількість помилкових спрацьовувань у системі. Даний інтервал, можливо, можна збільшувати до одного дня або одного тижня (залежно від навантаження в мережі). Також збільшення інтервалу часу зменшить проблему обчислення параметра Херста у розрядженому трафіку у часі. Для виявлення точкових аномалій більш ефективно буде використовувати інші методи (наприклад, штучні імунні системи або генетичні алгоритми). І для більш ефективного виявлення колективних аномалій можна використовувати комбінацію деяких методів.

У цьому розділі побудовано мережу, де тестувалася СОВ. Як показали результати у роботі даних методів, є проблема вибору правильного допустимого інтервалу значень параметра Херста. Виникає досить висока кількість помилкових спрацьовувань, що свідчить про непридатність до виявлення точкових атак. Однак

дана система може дуже ефективно виявляти колективні та розподілені в часі атаки, такі як DoS-атаки. Запропоновано способи щодо можливого поліпшення роботи даної системи.

3.4 Метод видалення контенту

Метод видалення контенту - це процес видалення або приховання вмісту або інформації з певної платформи, сервісу або простору в Інтернеті. Цей метод може бути застосований з різних причин, таких як виправлення помилок, забезпечення конфіденційності даних, дотримання законодавства або політик використання, а також для контролю над вмістом.

Існують різні способи видалення контенту, включаючи фізичне видалення файлів з серверів, приховання вмісту шляхом зміни налаштувань приватності, блокування доступу до контенту за допомогою фільтрів або модерації вмісту. Вибір конкретного методу залежить від конкретної ситуації та потреб користувачів або адміністраторів платформи.

Метод видалення контенту важливий для забезпечення безпеки, конфіденційності та ефективного управління інформацією в цифровому середовищі. Цей процес може бути складним, оскільки вимагає уважного підходу до забезпечення повної та безпечної елімінації вмісту, не викликаючи при цьому непередбачених наслідків [47].

Зокрема, методи видалення контенту повинні бути ефективними, швидкими та надійними, щоб забезпечити вчасне втручання та виконання вимог щодо заборони або видалення певного вмісту. Крім того, важливо дотримуватися відповідних правових норм та політик, які регулюють видалення контенту, зокрема стосовно прав користувачів та авторських прав.

Успішне використання методів видалення контенту може сприяти збереженню довіри користувачів до платформи чи сервісу, а також захисту їхньої особистої інформації. Однак важливо також уникати зловживання цими методами, щоб не обмежувати свободу вираження та доступ до інформації без обґрунтованих підстав.

Розробка функціональних вимог для підсистем формування, управління та супроводу контенту в системах електронної комерції та культурного контенту сприяє створенню типової архітектури для таких систем. Ці системи полегшують роботу модераторів, авторів, аналітиків та адміністраторів, а також збільшують функціональність для їхніх користувачів.

Використання СЕКК дозволяє підбирати актуальні питання у вигляді контенту з різних джерел для модераторів та авторів з урахуванням їхнього рейтингу через підсистему формування комерційного контенту. Автори створюють власний комерційний контент на основі аналізу вибраного контенту з різних джерел. Модератори можуть створювати нові правила для фільтрації контенту та оновлювати адреси джерел у підсистемі формування комерційного контенту. Аналітики вивчають діяльність аудиторії та функціонування СЕКК для розроблення нових правил аналізу статистики і динаміки етапів життєвого циклу комерційного контенту через підсистему супроводу комерційного контенту [48].

Ці функціональні вимоги до підсистем опрацювання інформаційних ресурсів у СЕКК, таких як формування, управління та супровід комерційного контенту, спрямовані на полегшення роботи для різних користувачів та забезпечення їхніх потреб. Архітектура СЕКК має рівні ієрархії, що забезпечує незалежність збережених даних від програм, що їх використовують, та можливість розвитку системи без руйнування існуючих застосувань. СЕКК працюють на основі зв’язків між контентом, менеджером, базою даних та користувачем, що забезпечує ефективну роботу з інформаційним ресурсом через зручний і зрозумілий інтерфейс.

Таким чином, можна запропонувати модель роботи методу:

Крок 1: Введення тексту. На початку ми маємо вхідний текст, який ми хочемо проаналізувати на предмет наявності впливових слів та фраз.

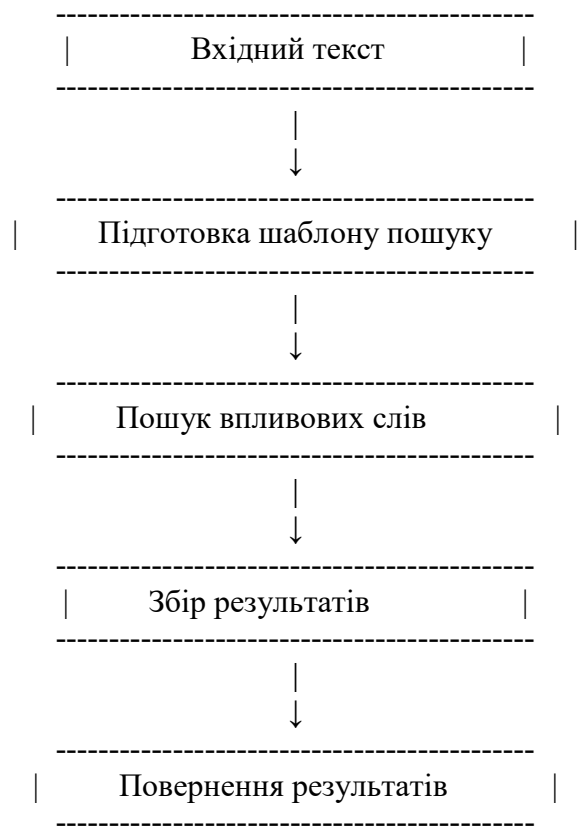
Крок 2: Підготовка шаблону пошуку. Ми використовуємо регулярний вираз, який визначає шаблон для пошуку ключового слова "вплив" у тексті. Цей шаблон включає границі слова та нечутливість до регістру.

Крок 3: Пошук впливових слів. Ми застосовуємо шаблон до введеного тексту за допомогою об'єкта Matcher. Пошук впливових слів проводиться за допомогою методу matcher.find(), який знаходить всі появи ключового слова "вплив" у тексті.

Крок 4: Збір результатів. Після знаходження кожного входження ключового слова ми додаємо його до карты influenceMap або збільшуємо лічильник, якщо слово вже є в карті.

Крок 5: Повернення результатів. Після завершення пошуку ми повертаємо карту influenceMap, яка містить кількість появ кожного ключового слова "вплив" у тексті.

Візуалізація моделі:



Ця модель показує послідовний процес роботи методу detectInfluence в аналізі тексту та виявленні впливових слів. Вона допомагає нам краще зрозуміти, як взаємодіють компоненти методу та як він функціонує для виконання своєї задачі.

Висновки до розділу 3

У висновку можна зазначити, що існує різноманітність моделей та методів протидії інформаційним впливам, які використовуються для виявлення, аналізу та запобігання негативним впливам на користувачів, споживачів інформації та суспільство в цілому. Вони включають в себе технічні методи фільтрації та блокування контенту, аналітичні інструменти для виявлення підроблених або недостовірних даних, а також розробку політик і законодавчих заходів для регулювання інформаційного простору.

Ці моделі та методи використовуються для захисту від різноманітних загроз, включаючи дезінформацію, кібератаки, онлайн-шахрайство та інші форми цифрового злочину. Правильне застосування цих інструментів може сприяти підвищенню рівня кібербезпеки, зміцненню довіри до інформаційного середовища та забезпеченню свободи слова та доступу до інформації.

Однак важливо пам'ятати, що ефективність цих моделей і методів може залежати від їхньої спроможності адаптуватися до швидкозмінюючого цифрового ландшафту та нових методів атаки. Тому постійне вдосконалення та актуалізація цих інструментів є ключовим аспектом боротьби з інформаційними загрозами.

ВИСНОВКИ

У результаті виконання дипломної роботи було отримано такі результати:

1) Розглянуто існуючі системи виявлення вторгнень, їх класифікацію та сферу застосування. Це класифікація з урахуванням методів, які у алгоритмах виявлення вторгнень, і основі топології одержуваної інформації.

2) Проведено класифікацію мережевих атак, приклади їх експлуатації та описано процедуру реалізації атаки. Основними типами атак є розвідка, U2R, R2U, експлоїт та DoS-атаки.

3) Вивчено методи виявлення аномалій, представлено їх класифікацію, переваги та недоліки. Можна виділити кілька груп аномалій: точкові, контекстні та колективні. Методи виявлення можна розділити такі великі групи: поведінкові методи, методи машинного навчання, методи обчислювального інтелекту і методи з урахуванням знань.

4) Більш детально було розглянуто та реалізовано методи виявлення аномалій на основі фрактального аналізу. Як міра оцінки аномальності трафіку використовується показник Херста.

5) Було представлено та реалізовано базову архітектуру СВВ.

6) Здійснено тестування роботи системи з використанням різних типів атак.

Результати виконаної роботи показують, що для виявлення колективних і розподілених у часі атак використання методів на основі фрактального аналізу з використанням показника Херста можуть ефективно виявляти дані впливу. Для виявлення точкових та контекстних атак необхідно використовувати інші методи, оскільки складність вибору правильного інтервалу допустимих значень призводить до великої кількості помилкових спрацьовувань. Що, зрештою, не дозволяє ефективно виявити даний тип впливу на систему.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Network Traffic Analysis | NTA Software and Tools. *ManageEngine NetFlow Analyzer*. URL: https://www.manageengine.com/products/netflow/network-traffic-analysis.html?network=g&device=c&keyword=network%20traffic%20analyzer&campaignid=11495718157&creative=614382195247&matchtype=e&adposition=&placement=&adgroup=109478600342&targetid=kwd-10171971&location=9061014&gad_source=1&gclid=Cj0KCQjwgJyyBhCGARIsAK8LVLO467y9ZBF2LcshBhQAR8AJ0UZlet_Y4okS9mLQF_g6VFI7W5QUqxIaAuRUEALw_wcB (accessed 20.05.2024).

2. Кравчук П. Я. Сутність та передумови виникнення поняття корпоративної безпеки підприємства. *Науковий вісник Волинського держ. ун-ту ім. Лесі Українки*. 2005. Вип. 1. С. 165–170.

3. Франчук В. І. Теоретичні засади корпоративної безпеки. *Актуальні проблеми економіки*. 2009. Issue 7. P. 161–167.

4. Рудковський О. В. Формування функцій управління корпоративної безпеки. *Соціально-економічний розвиток регіонів в контексті міжнародної інтеграції*. 2013. Вип. 12. С. 1.

5. [PDF] Corporate Security Management by Marko Cabric eBook | Perlego. URL: https://www.perlego.com/book/1813654/corporate-security-management-challenges-risks-and-strategies-pdf?utm_source=google&utm_medium=cpc&campaignid=20933451054&adgroupid=162926082892&gad_source=1&gclid=Cj0KCQjw6auyBhDzARIsALIo6v_AaALlowysHFxmLzNX65KBXnt_587AnU06rvk_uNXEM2S9CoYd8hwaAvzjEALw_wcB (accessed 21.05.2024).

6. McQuail′s Mass Communication Theory - Denis McQuail. URL: https://books.google.com.ua/books/about/McQuail_s_Mass_Communication_Theory.html?id=CvcvLsDxhvEC&redir_esc=y (accessed 21.05.2024).

7. Northcutt S., Novak J. Network intrusion detection. Sams Publishing, 2002. ISBN 0-7357-1265-4.

8. Rajasekaran K. Classification and Importance of Intrusion Detection System. *International Journal of Computer Science and Information Security,*. 2020. Vol. 10, 15.04.2020. P. 44.

9. Bace R. G., Mell P. Intrusion detection systems. 2001. 2001.

10. Snort S. The Open Source Network Intrusion Detection System. *http://www. snort. org*. 2003. 2003.

11. Axelsson S. Intrusion detection systems: A taxonomy and survey. Technical Report 99-15. 2000. 2000.

12. Hepp A. Katz/Lazarsfeld (1955): Personal Influence. 2019. P. 293–296. DOI:10.1007/978-3-658-21742-6_67.

13. Cialdini R. Influence: Science and Practice. 1993.

14. Grinberg N., Joseph K., Friedland L. та ін. Fake news on Twitter during the 2016 U.S. presidential election. *Science (New York, N.Y.)*. 2019. Вип. 363, Вип. 6425. С. 374–378. DOI:10.1126/science.aau2706.

15. Rajaraman A., Ullman J. D. Mining of massive datasets. Autoedicion, 2011.

16. Sabharwal A., Selman B. S. Russell, P. Norvig, Artificial Intelligence: A Modern Approach, Third Edition. *Artif. Intell.* 2011. Vol. 175, 30.04.2011. P. 935–937. DOI:10.1016/j.artint.2011.01.005.

17. Yu P., Tsai J. Machine Learning in Cyber Trust. 2009. DOI:10.1007/978-0-387-88735-7.

18. (PDF) Social Network Analysis: Methods and Applications | Pantha Biswas - Academia.edu. URL: https://www.academia.edu/2612257/Social_Network_Analysis_Methods_and_Applications (accessed 21.05.2024).

19. Manning C. D. Introduction to information retrieval. Syngress Publishing,, 2008.

20. Sharp H., Rogers Y., Preece J. Interaction Design. Beyond Human-Computer Interaction. 2007. ISBN 978-0-470-01866-8.

21. Northcutt S., Novak J. Network Intrusion Detection: An Analyst’s Handbook. *Edpacs*. 2000. Vol. 27, 01.01.2000. DOI:10.1201/1079/43253.27.7.20000101/30304.4.

22. Шелухін, О.І. Виявлення вторгнень у комп’ютерні мережі/О.І.Шелухін - Київ.: Гаряча лінія - С.5-16.

23. Rehman R. U. Intrusion detection systems with Snort: advanced IDS techniques using Snort, Apache, MySQL, PHP, and ACID. Prentice Hall Professional, 2003. ISBN 0-13-140733-3.

24. Chen Y., Hwang K., Kwok Y.-K. Collaborative defense against periodic shrew DDoS attacks in frequency domain. *ACM transactions on information and system security*. 2005. Vol. 30, 2005.

25. Lau F., Rubin S., Smith M. H. et al. Distributed denial of service attacks. P. 2275–2280 вип.3. DOI:10.1109/ICSMC.2000.886455.

26. Marchenko R., Kovalenko A., Znaidiuk V. Аналіз методів виявлення аномального трафіку в мережах IOT. *Системи управління, навігації та зв’язку. Збірник наукових праць*. 2024. Вип. 1, 09.02.2024. С. 133–136. DOI:10.26906/SUNZ.2024.1.133.

27. Гасанов, В.І. Виявлення аномалій у мережевому трафіку на основі нейромережевого моделювання динаміки зміни обсягів IP-пакетів / В.І. Гасанов // Математичні Машини та Системи. - 2018. - №2. - С.40-45.

28. У. Л. Токарев – Виявлення Мережевих Атак На Основі Штучних Імунних Систем / В.Л.Токарєв, Сичугов А.А., А.П. Анчишкін // Системний аналіз,управління та обробка інформації. - 2018. - №10. - С.117-124.

29. Genetic Algorithms and Machine Learning | Machine Learning. URL: https://link.springer.com/article/10.1023/A:1022602019183 (accessed 21.05.2024).

30. Ning P., Jajodia S. Intrusion Detection Techniques. 2004. DOI:10.1002/047148296X.tie097.

31. Cheboli D. Anomaly Detection of Time Series / Cheboli D. - Minesota. - Tcpdump&libpcap // The tcpdump group - 2022. – Mode of access: – Date of access: 15.03.2022. URL: https://www.tcpdump.org/

32. Hurst, H. E. (1951). Long-term storage capacity of reservoirs. Transactions of the American Society of Civil Engineers, 116, 770-799. - References - Scientific Research Publishing. URL: https://www.scirp.org/reference/ReferencesPapers?ReferenceID=946282 (accessed 21.05.2024).

33. Mandelbrot, B.B. (1982) The Fractal Geometry of Nature. Freeman Press, New York. - References - Scientific Research Publishing. URL: https://www.scirp.org/reference/referencespapers?referenceid=1221294 (accessed 21.05.2024).

34. Карачанська, Є.В. Метод виявлення аномалій мережевого трафіку, що ґрунтується на його самоподібній структурі / О.В. Карачанська, Н.І. Сосєдова, //Безпека інформаційних технологій - 2019. - Том 26, №1. - С. 98-110.

35. Mane D., Sangve S., Upadhye G. et al. Detection of Anomaly using Machine Learning: A Comprehensive Survey. *International Journal of Emerging Technology and Advanced Engineering*. 2022. Vol. 12, 01.11.2022. P. 134–152. DOI:10.46338/ijetae1122_15.

36. Naidu Ms. N., Dharaskar R. Intrusion Detection Based on Genetic Algorithm and Bayesian Networks.

37. Lunt T., Tamaru A., Gilham F. et al. A Real-Time Intrusion-Detection Expert System. 1992. 01.01.1992.

38. RFC 1034: Domain names - concepts and facilities. URL: https://www.rfc-editor.org/rfc/rfc1034 (accessed 21.05.2024).

39. Go Programming Blueprints - Second Edition: Build real-world, production-ready solutions in Go using cutting-edge technology and techniques: Ryer, Mat: 9781786468949. URL: https://www.amazon.com/Programming-Blueprints-real-world-production-ready-cutting-edge/dp/1786468948 (accessed 21.05.2024).

40. HTML and CSS: Design and Build Websites | Wiley. URL: https://www.wiley.com/en-us/HTML+and+CSS%3A+Design+and+Build+Websites-p-9781118206911 (accessed 21.05.2024).

41. Golang Pros and Cons- The Pros And Cons Of Programming In Go. URL: https://blog.mobcoder.com/golang-pros-and-cons/ (accessed 21.05.2024).

42. Pennycook G. Fighting misinformation on social media using crowdsourced judgments of news source quality. *Proceedings of the National Academy of Sciences*. 2019. Vol. 116, 28.01.2019. P. 201806781. DOI:10.1073/pnas.1806781116.

43. GO gopacket // Google [Електронний ресурс]. – 2022. – Mode of access: https://pkg.go.dev/github.com/google/gopacket/. – Date of access: 15.03.2022.

44. Mahfouz A., Abuhussein A., Venugopal D. та ін. Ensemble Classifiers for Network Intrusion Detection Using a Novel Network Attack Dataset. *Future Internet*. 2020. Вип. 12, Вип. 11. С. 180. DOI:10.3390/fi12110180.

45. Leland, W. Ha Self-Similar Nature of Ethernet traffic / W. Leland, Taqqu M., Willinger W., Wilson D. // Protocols and Applications. - 1993. - September. - P.13-17.

46. (PDF) Classification of security threats in information systems. URL: https://www.researchgate.net/publication/315714820_Classification_of_security_threats_in_information_systems (accessed 21.05.2024).

47. Gorwa R., Binns R., Katzenbach C. Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*. 2020. Vol. 7, 01.02.2020. P. 205395171989794. DOI:10.1177/2053951719897945.

48. Mauthe A., Thomas P. System and Data Integration in CMS. 2005. P. 225–244. DOI:10.1002/0470855444.ch8.

ДОДАТОК А
СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Тези наукових доповідей:

Панченко М., Лебєдєва Н.В., Бабенко Т. Оцінка та прогнозування ризиків для атак cryptojacking. Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS) : Тези науково-практ. конф., м. Київ, 26 квіт. 2024 р. Київ, 2024. С. 153–155.

ДАДАТОК Б
ЛІСТИНГ ПРОГРАМНОГО КОДУ

```
import java.util.HashMap;
import java.util.Map;

public class InfluenceDetection {

    // Метод для аналізу тексту та виявлення впливу
    public static Map<String, Integer> detectInfluence(String text) {
        // Здійснюємо обробку тексту та аналіз
        Map<String, Integer> influenceMap = new HashMap<>();
        // Приклад аналізу: лічильник певних слів або фраз
        String[] words = text.split(" ");
        for (String word : words) {
            // Перевірка на наявність певних ключових слів
            if (word.equalsIgnoreCase("вплив")) {
                influenceMap.put(word, influenceMap.getOrDefault(word, 0) + 1);
            }
        }
        return influenceMap;
    }

    // Тестування роботи методу
    public static void main(String[] args) {
        String text = "Цей текст містить впливові слова та фрази. Вплив важливий
для аналізу.";
        Map<String, Integer> result = detectInfluence(text);
        System.out.println("Результат виявлення впливу:");
        for (Map.Entry<String, Integer> entry : result.entrySet()) {
            System.out.println(entry.getKey() + ": " + entry.getValue());
        }
    }
}
```

```
import java.util.HashMap;
import java.util.Map;
import java.util.regex.Matcher;
import java.util.regex.Pattern;

public class InfluenceDetection {

    // Метод для аналізу тексту та виявлення впливу
    public static Map<String, Integer> detectInfluence(String text) {
        // Здійснюємо обробку тексту та аналіз
        Map<String, Integer> influenceMap = new HashMap<>();
        // Приклад аналізу: використання регулярних виразів для знаходження
певних фраз
        Pattern pattern = Pattern.compile("\\bвплив\\b", Pattern.CASE_INSENSITIVE);
        Matcher matcher = pattern.matcher(text);
        while (matcher.find()) {
            String word = matcher.group();
            influenceMap.put(word, influenceMap.getOrDefault(word, 0) + 1);
        }
        return influenceMap;
    }

    // Метод для видалення контенту, що не містить інформаційний вплив
    public static String removeNonInfluenceContent(String text) {
        // Приклад: видаляємо всі речення, в яких відсутній вплив
        String[] sentences = text.split("\\.\\s+");
        StringBuilder result = new StringBuilder();
        for (String sentence : sentences) {
            if (sentence.toLowerCase().contains("вплив")) {
                result.append(sentence).append(". ");
            }
        }
        return result.toString().trim();
    }

    // Тестування роботи методів
    public static void main(String[] args) {
        String text = "Цей текст містить впливові слова та фрази. Вплив важливий
для аналізу. " +
                      "Але деякі речення можуть бути не пов'язані з впливом.";
```

```
        // Виявлення впливу
        Map<String, Integer> result = detectInfluence(text);
        System.out.println("Результат виявлення впливу:");
        for (Map.Entry<String, Integer> entry : result.entrySet()) {
            System.out.println(entry.getKey() + ": " + entry.getValue());
        }

        // Видалення контенту без впливу
        String filteredText = removeNonInfluenceContent(text);
        System.out.println("\nТекст після видалення контенту без впливу:");
        System.out.println(filteredText);
    }
}

//-----------
import java.util.ArrayList;
import java.util.List;

public class InfluenceDetection {

    // Метод для аналізу тексту та виявлення впливу
    public static List<String> identifyInfluentialEntities(String text) {
        // Припустимо, що впливові сутності в тексті містяться виключно у вигляді назв
        // Здійснюємо обробку тексту та аналіз
        List<String> influentialEntities = new ArrayList<>();
        // Приклад аналізу: використання простого розбиття тексту на слова та подальшого виявлення назв
        String[] words = text.split("\\s+");
        for (String word : words) {
            // Перевірка на впливовість слова (наприклад, враховуємо, що назви мають першу велику літеру)
            if (Character.isUpperCase(word.charAt(0))) {
                influentialEntities.add(word);
            }
        }
        return influentialEntities;
    }

    // Метод для виявлення тематичного спрямування тексту
    public static String identifyTextTheme(String text) {
        // Припустимо, що тематичне спрямування тексту можна визначити за наявністю ключових термінів
```

```
        // Здійснюємо аналіз тексту та визначення теми
        String theme = "";
        // Приклад аналізу: перевірка наявності ключових слів
        if (text.contains("політика")) {
            theme = "політична";
        } else if (text.contains("економіка")) {
            theme = "економічна";
        } else if (text.contains("технології")) {
            theme = "технологічна";
        } else {
            theme = "інше";
        }
        return theme;
    }

    // Тестування роботи методів
    public static void main(String[] args) {
        String text = "Цей текст містить впливові слова та фрази. " +
                      "Вплив важливий для аналізу. " +
                      "Але деякі речення можуть бути не пов'язані з впливом. " +
                      "Текст також має зв'язок з політикою та економікою.";

        // Виявлення впливових сутностей
        List<String> influentialEntities = identifyInfluentialEntities(text);
        System.out.println("Виявлені впливові сутності:");
        for (String entity : influentialEntities) {
            System.out.println(entity);
        }

        // Визначення тематичного спрямування тексту
        String theme = identifyTextTheme(text);
        System.out.println("\nТематичне спрямування тексту: " + theme);
    }
}
```

```
import java.util.List;

public class Main {
    public static void main(String[] args) {
        String text = "Тут ваш текст"; // Замість "Тут ваш текст" вкажіть власний текст

        // Виявлення впливових сутностей
        List<String> influentialEntities = identifyInfluentialEntities(text);
        System.out.println("Виявлені впливові сутності:");
        for (String entity : influentialEntities) {
            System.out.println(entity);
        }

        // Визначення тематичного спрямування тексту
        String theme = identifyTextTheme(text);
        System.out.println("\nТематичне спрямування тексту: " + theme);
    }

    // Метод для ідентифікації впливових сутностей у тексті
    public static List<String> identifyInfluentialEntities(String text) {
        // Ваш код для ідентифікації впливових сутностей
        return null; // Змініть цей рядок на результат ідентифікації впливових
сутностей
    }

    // Метод для ідентифікації тематичного спрямування тексту
    public static String identifyTextTheme(String text) {
        // код для ідентифікації тематичного спрямування тексту
        return null; // Змініть цей рядок на результат ідентифікації тематичного
спрямування
    }
}
```