Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Поліно Івана Олександровича*

академічної групи *125-19-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Виявлення аномалій мережевого трафіку з використанням алгоритмів нечіткої кластеризації*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.т.н., доц. Герасіна О.В.			
розділів:				
спеціальний	к.т.н., доц. Герасіна О.В.			
економічний	к.е.н., доц. Романюк Н.М.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Поліно Івану Олександровичу* **академічної групи** *125-19-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Виявлення аномалій мережевого трафіку з використанням алгоритмів нечіткої кластеризації*

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз найбільших кібератак в Україні і світі у 2022 році, існуючих рішень запобігання вторгненням в інформаційно-комунікаційні мережі, а також основ нечіткої логіки і алгоритмів нечіткої кластеризації.	25.02.2023 – 31.03.2023
Розділ 2	Розробка підходу до виявлення аномалій трафіку в інформаційно-комунікаційних мережах за допомогою алгоритмів нечіткої кластеризації та оцінка його ефективності.	01.04.2022 – 12.05.2023
Розділ 3	Розрахунки капітальних витрат, економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень.	13.05.2022 – 09.06.2023

Завдання видано _____ Герасіна О.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Поліно І.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 76 с., 11 рис., 5 табл., 4 додатки, 46 джерел.

Об’єкт розробки – мережевий трафік.

Предмет розробки – підхід до виявлення аномалій мережевого трафіку за допомогою нечіткої кластеризації С-середніх та субтрактивної кластеризації.

Мета кваліфікаційної роботи – дослідження алгоритмів нечіткої кластеризації, що дозволяють виконувати виявлення аномалій трафіку в інформаційно-комунікаційних мережах.

Наукова новизна результатів полягає у тому, що використання алгоритмів нечіткої кластеризації С-середніх та субтрактивної кластеризації дозволяє виявляти аномалії мережевого трафіку в інформаційно-комунікаційних мережах.

У першому розділі проаналізовано найбільші кібератаки в Україні і світі у 2022 році, існуючі рішення запобігання вторгненням в інформаційно-комунікаційні мережі, а також основи нечіткої логіки і алгоритми нечіткої кластеризації.

У спеціальній частині роботи запропоновано підхід до виявлення аномалій трафіку в інформаційно-комунікаційних мережах за допомогою алгоритмів нечіткої кластеризації та оцінено його ефективність. За наслідками досліджень зроблено висновки щодо рішення поставленої задачі.

У економічному розділі виконані розрахунки капітальних витрат, економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень.

МЕРЕЖЕВІ АТАКИ, НЕЧІТКА ЛОГІКА, СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ, СУБТРАКТИВНА КЛАСТЕРИЗАЦІЯ, КІБЕРБЕЗПЕКА, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА МЕРЕЖА, АНОМАЛІЇ ТРАФІКУ, КЛАСТЕРИЗАЦІЯ С-СЕРЕДНІХ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

ABSTRACT

Explanatory note: p. 76, fig. 11, tab. 5, 4 additions, 46 sources.

The object of development is network traffic.

The subject of development is an approach to detecting network traffic anomalies using fuzzy C-means clustering and subtractive clustering.

The purpose of the qualification work is to study fuzzy clustering algorithms that allow detection of traffic anomalies in information and communication networks.

The scientific novelty of the results lies in the fact that the use of C-means fuzzy clustering and subtractive clustering algorithms make it possible to detect traffic anomalies in information and communication networks.

The first chapter analyzes the biggest cyber attacks in Ukraine and the world in 2022, existing solutions to prevent intrusions into information and communication networks, as well as the basics of fuzzy logic and fuzzy clustering algorithms.

In a special part of the work, an approach to the detection of traffic anomalies in information and communication networks using fuzzy clustering algorithms is proposed and its effectiveness is evaluated. Based on the results of the research, conclusions were made regarding the solution to the problem.

In the economic section, calculations of capital costs, economic effect and payback period of capital investments are performed using the proposed solutions.

NETWORK ATTACKS, FUZZY LOGIC, INTRUSION DETECTION SYSTEMS, SUBTRACTIVE CLUSTERING, CYBER SECURITY, INFORMATION AND COMMUNICATION NETWORK, TRAFFIC ANOMALIES, C-AVERAGE CLUSTERIZATION, SIMULATION MODELING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІКМ – Інформаційно-комунікаційна мережа;

ПЗ – Програмне забезпечення;

СВВ – Система виявлення вторгнень;

ШІ – Штучний інтелект;

ADS – Anomaly Detection System – Система виявлення аномалій;

IDS – Intrusion Detection System – Система виявлення вторгнень;

MDS – Misuse Detection System – Система виявлення зловживань.

ЗМІСТ

ВСТУП

Наразі задача виявлення мережевих атак є однією з найактуальніших у сфері інформаційної та кібербезпеки. Її значущість зростає з кожним днем завдяки постійному збільшенню обсягів передаваної інформації за допомогою інформаційно-комунікаційних систем і мереж (ІКМ), кількості користувачів, а також ускладненню методів атак зловмисників [1-20].

Останнім часом в світі переконались, що навіть найнадійніші системи захисту не здатні захистити від атак ІКМ державних і комерційних установ. Одна з причин – у тому, що в більшості систем безпеки застосовують стандартні механізми захисту: ідентифікацію та аутентифікацію, механізми обмеження доступу до інформації згідно з правами суб'єкта і криптографічні механізми. Такий традиційний підхід має певні недоліки, а саме: незахищеність від власних користувачів – зловмисників, розмитість розподілу суб'єктів системи на «своїх» і «чужих» через глобалізацію інформаційних ресурсів, порівняна легкість підбору паролів внаслідок використання їхнього змістового різновиду, зниження продуктивності й ускладнення інформаційних комунікацій внаслідок обмеження доступу до ресурсів організації [5].

Отже, виникла потреба в механізмах, які би доповнювали традиційні та давали можливість виявити спроби несанкціонованого доступу й інформували про це відповідальних за безпеку або реагували у відповідь. Важливим фактором є те, щоб такі системи могли протистояти атакам, навіть якщо зловмисник вже був автентифікований та авторизований і з формального погляду додержання прав доступу мав необхідні повноваження на свої дії. Такі функції і виконують системи виявлення вторгнень (IDS – Intrusion Detection Systems).

Оскільки передбачити всі сценарії розгортання подій в системі з активним «чужим» суб'єктом неможливо, потрібно або якомога детальніше описати можливі «зловмисні» сценарії або ж, навпаки, – «нормальні» і прийняти, що всяка активність, на яку не поширюється прийняте розуміння

«нормальності», є небезпечною. Системи виявлення вторгнень (СВВ) поділяються на системи, що реагують на відомі атаки, – системи виявлення зловживань (MDS – Misuse Detection Systems) і системи виявлення аномалій (ADS – Anomaly Detection Systems). Використання MDS може бути проблемним у разі, коли зустрічаються нові типи атак або якщо зловмисники намагаються замаскувати свою поведінку. ADS розроблені для протидії цьому виду виклику шляхом виявлення моделей нормальної поведінки з припущенням, що вторгнення зазвичай включає деяке відхилення від цієї нормальної поведінки [5].

Одним із способів забезпечення захисту від мережевих атак є використання мережевих СВВ, призначених для виявлення факту проведення мережевих атак на ресурси, що захищаються. Крім того, в залежності від конкретної реалізації, в функції системи виявлення вторгнень може входити застосування заходів щодо запобігання виявленої атаки. Наразі існує тенденція мати СВВ у будь-якій мережі, оскільки атаки та загрози створюють потенційний ризик для ІКМ [1-20].

Отже, враховуюче те, що збитки від кібератак постійно зростають, зокрема, збитки від кіберзлочинності у світі за 2020 р. склали 945 мільярдів доларів [10], засоби захисту від кібератак не можуть протидіяти існуючим загрозам. Тому актуальними є дослідження з синтезу моделей, що дозволяють вчасно виявити аномалії в роботі процесів, які в майбутньому можуть призвести до реалізації певного вектору атаки і компрометації ІКМ.

Слід зазначити, що взагалі ефективність будь-якої системи виявлення вторгнень залежить від методів аналізу наявної інформації про мережеві атаки. Одним із таких методів є використання для аналізу даних методів систем штучного інтелекту (ШІ). За допомогою таких інтелектуальних рішень стає можливим створити СВВ, яка буде здатна ефективно визначати як існуючі, так і невідомі раніше атаки, розпізнавати аномальний трафік, а також вдосконалюватись в процесі своєї роботи, не вимагаючи при цьому втручання людини [21-32].

Таким чином, дослідження, розробка та вдосконалення підходів до виявлення аномалій мережевого трафіку із використанням штучного інтелекту наразі є актуальною задачею.

Метою роботи є дослідження алгоритмів нечіткої кластеризації, що дозволяють виконувати виявлення аномалій трафіку в інформаційно-комунікаційних мережах.

Постановка задачі:

• провести аналіз найбільших кібератак в Україні і світі у 2022 році;

• провести аналіз існуючих рішень запобігання вторгненням в інформаційно-комунікаційні мережі;

• провести аналіз основ нечіткої логіки та алгоритмів нечіткої кластеризації;

• запропонувати підхід до виявлення аномалій трафіку в інформаційно-комунікаційних мережах за допомогою алгоритмів нечіткої кластеризації;

• оцінити ефективність запропонованого підходу.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Найбільші кібератаки в Україні і світі у 2022 році

Ряд потрясінь 2022 року, серед яких і війна в Україні, створили сприятливі умови для активності багатьох кіберзлочинців. Місяцями зловмисники атакували державні установи, лікарні, криптовалютні компанії та багато інших організацій. Вартість витоку даних зросла до 4,4 мільйона доларів США, а успіх підштовхуватиме кіберзлочинців до ще більшої активності у наступних роках [33-40].

За підсумками 2022 року спеціалісти ESET підготували список з 10 найбільших кіберінцидентів з урахуванням завданої ними шкоди, рівня складності чи геополітичних наслідків. І хоча порядок у списку не має значення, спочатку розглянемо атаки, що були спрямовані на Україну, і які більше вплинули на глобальні ризики цифрової безпеки [33].

1. Україна під прицілом кібератак. Критична інфраструктура України знову стала ціллю кіберзлочинців. На початку повномасштабного російського вторгнення дослідники ESET тісно співпрацювали з CERT-UA над усуненням атаки, націленої на систему енергопостачання країни з використанням шкідливої програми для знищення інформації. Цю загрозу група кіберзлочинців Sandworm намагалася розгорнути на високовольтних електричних підстанціях. Шкідливе програмне забезпечення отримало назву Industroyer2 на честь загрози, застосованої групою для відключення електроенергії в Україні у 2016 р. Однак цього разу програма використовувалась у поєднанні з новою версією загрози CaddyWiper для знищення інформації, ймовірно, щоб приховати сліди групи та уповільнити реагування та відновлення контролю для операторів енергетичної компанії.

Шкідлива програма Industroyer у 2016 р. стала першим відомим шкідливим програмним забезпеченням, яке було розроблено спеціально для атак на енергетичну інфраструктуру.

У квітні 2022 р. нова версія Industroyer спричинила відключення світла у тисячах будинків Києва, атакувавши місцеву електричну підстанцію. Атаці вдалося запобігти, перш ніж вона спричинила руйнівні наслідки. Дослідники ESET заявляють, що до нової атаки причетна група Sandworm.

Після встановлення Industroyer поширюється у мережі підстанції у пошуках конкретних пристроїв промислового управління, чиї протоколи зв'язку вона може використати (рис. 1.1). Потім загроза відключає усі автоматичні вимикачі, не зважаючи на будь-які спроби операторів підстанції відновити контроль. Якщо оператор намагався закрити вимикач, шкідливе програмне забезпечення відкривало його знову [34].

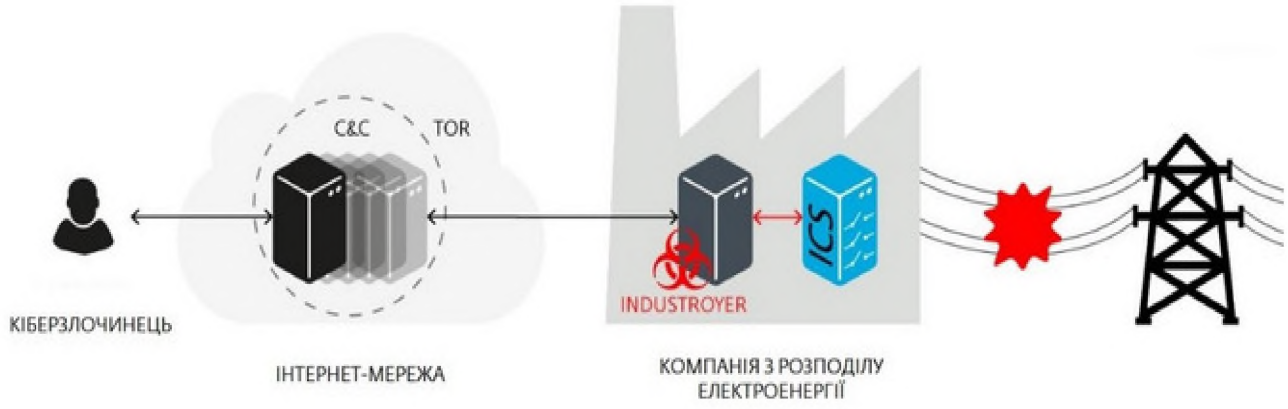


Рисунок 1.1 – Схема роботи шкідливої програми Industroyer

Щоб видалити всі ознаки зловмисної діяльності, загроза запускала інструмент для знищення даних, який був розроблений для виведення з ладу комп’ютерів підстанції та сповільнення відновлення їх роботи. Цей інструмент не працював належним чином, однак у іншому випадку наслідки могли б бути набагато гіршими – особливо взимку, коли відключення електроенергії може призвести до пошкодження труб з водою через замерзання.

Остання шкідлива дія була здійснена з метою відключення деяких захисних реле на підстанції, однак це здійснити не вдалося. Без функціонуючих

захисних реле обладнання підстанції могло б бути пошкоджене, коли оператори зрештою відновили електропостачання.

Від інших шкідливих програм, націлених на інфраструктуру, Industroyer відрізняє використання чотирьох компонентів, призначених для отримання прямого контролю над автоматичними вимикачами та перемикачами на підстанції розподілу електроенергії (рис. 1.2). Кожен з цих компонентів націлений на конкретні протоколи зв'язку, зазначені в наступних стандартах: IEC 60870-5-101, IEC 60870-5-104, IEC 61850 та OLE for Process Control Data Access (OPC DA) [35].

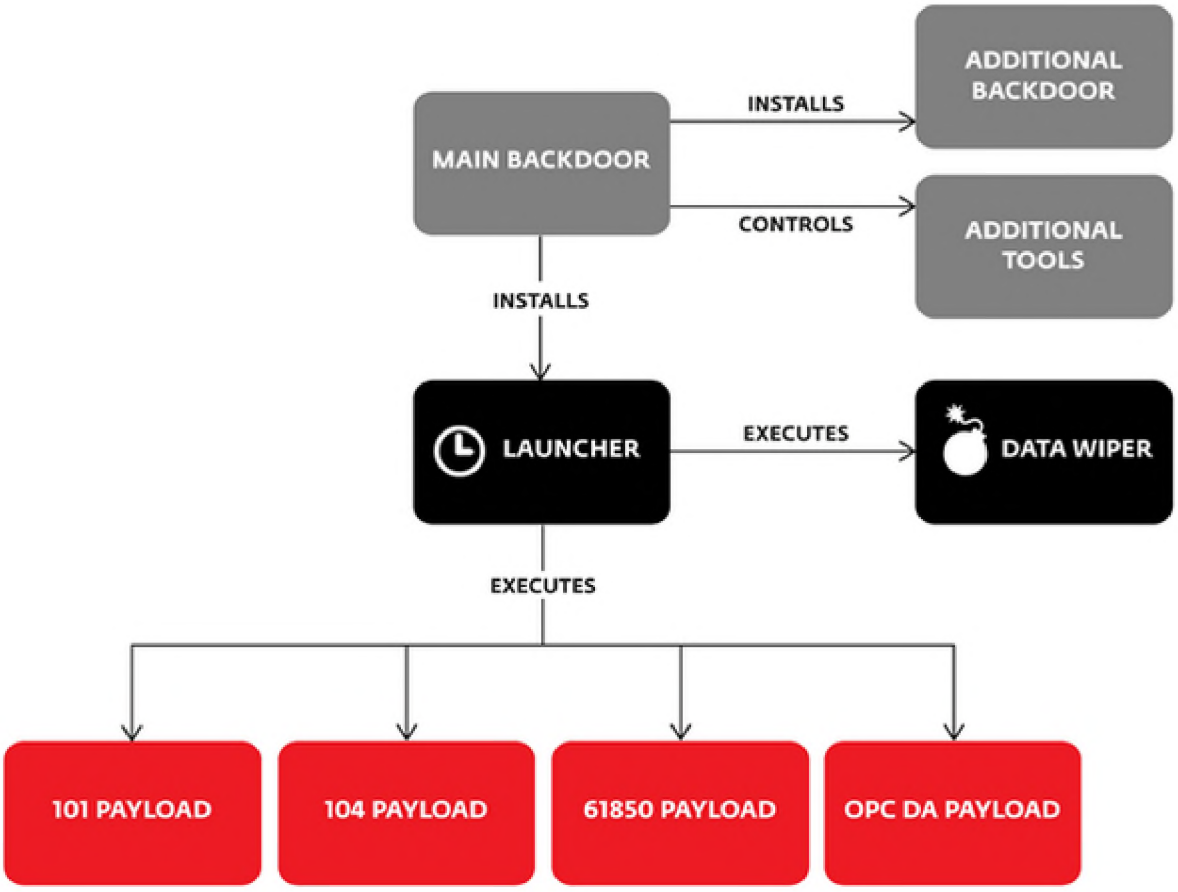


Рисунок 1.2 – Компоненти шкідливої програми Industroyer

Слід зазначити, що витонченість Industroyer дає змогу адаптувати шкідливе програмне забезпечення до будь-якого середовища. Загроза використовує протоколи промислового зв'язку, які застосовуються не тільки в

Україні, а й в інфраструктурі електропостачання, управлінні транспортом та інших критично важливих системах у всьому світі.

З іншого боку, попри складність загрози, вплив Industroyer був мінімальним. Можливо, це була лише перевірка для майбутніх атак або попередження про рівень можливостей кіберзлочинців.

2. Ще більше загроз для знищення інформації. CaddyWiper був далеко не єдиним інструментом для знищення даних, виявленим в Україні безпосередньо перед або в перші кілька тижнів повномасштабного вторгнення. 23 лютого 2022 року телеметрія ESET зафіксувала іншу загрозу такого ж функціоналу із назвою HermeticWiper на сотнях машин у кількох організаціях в Україні. Наступного дня почалася друга руйнівна атака на українську урядову мережу з метою знищення даних, цього разу з використанням IsaacWiper.

3. Перебої в роботі Інтернету. За годину до російського вторгнення масштабна кібератака на комерційного супутникового провайдера Viasat призвела до перебоїв у доступі до Інтернету для тисяч людей в Україні та навіть в інших країнах Європи. Взагалі вважається, що метою цієї атаки, під час якої був використаний неправильно налаштований VPN-пристрій для отримання доступу до розділу управління супутниковою мережею, було послабити комунікаційні можливості українського командування в перші години повномасштабного вторгнення. Проте її наслідки відчули далеко за межами України [37-38].

4. Надзвичайне положення в Коста-Ріці через програми-вимагачі. Однією з найактивніших у 2002 р. була група програм-вимагачів Conti, доступ до використання яких за плату зловмисники-розробники надають іншим хакерам. Одну з таких атак було спрямовано на невелику південноамериканську державу Коста-Ріка. Як результат, в країні було оголошено надзвичайний стан, а уряд назвав атаку актом «кібертероризму». Група з тих пір зникла, хоча її учасники, ймовірно, просто перейшли до іншої активності для уникнення уваги правоохоронних органів.

5. Атаки на державні органи в США. Інші програми-вимагачі також були активними у 2022 році. У вересні Агентство з кібербезпеки та захисту інфраструктури США повідомило, що пов'язані з Іраном кіберзлочинці атакували муніципальну установу США та аерокосмічну компанію, використовуючи уразливість Log4Shell для поширення програм-вимагачів. Також варта уваги атака на уряд США в листопаді 2022 р. Тоді організацію федеральної цивільної виконавчої влади було атаковано та розгорнуто в її мережі шкідливе програмне забезпечення для майнінгу криптовалют.

6. Крадіжка в розмірі 618 мільйонів доларів США з використанням Ronin Network. Цей сайдчейн Ethereum для гри Axie Infinity був створений в'єтнамським розробником блокчейн-ігор Sky Mavis. У березні 2022 р. з'ясувалось, що хакерам вдалося використати викрадені приватні ключі, щоб підробити зняття коштів на суму 173 600 Ethereum (592 мільйони доларів США) і 25,5 мільйонів доларів США через Ronin двома транзакціями. Крадіжка в розмірі 618 мільйонів доларів США за цінами березня 2022 р. стала найбільшою в історії криптокомпаній. Слід зазначити, що з атакою пов'язана північнокорейська група кібрезлочинців Lazarus [39].

7. Група програм-вимагачів Lapsus$, яка за допомогою резонансних крадіжок даних змушує своїх жертв платити, з'явилася протягом 2022 р. Серед її цілей – Microsoft, Samsung, Nvidia, Ubisoft, Okta і Vodafone. Одним з її методів є підкуп інсайдерів у компаніях та їхніх підрядників. Хоча деякий час група була відносно неактивною, вона знову повернулася наприкінці 2022 року, атакувавши розробника Grand Theft Auto Rockstar Games. Кілька ймовірних членів групи були заарештовані у Великобританії та Бразилії.

8. Витік даних Міжнародного комітету Червоного Хреста. У січні 2022 р. організація повідомила про серйозний інцидент, у результаті якого були скомпрометовані особисті дані понад 515 000 жертв. У швейцарського підрядника були викрадені дані про осіб, розлучених зі своїми родинами через конфлікти, міграцію та катастрофи, зниклих безвісти та їхніх сімей, а також

осіб, які перебувають під вартою. Під час атаки була використана уразливість у системі, на якій було не застосовано виправлення.

9. Новий витік даних в Uber. У 2016 році у компанії було викрадено дані про 57 мільйонів користувачів. У вересні 2022 року знову повідомлялося, що хакер, потенційно член групи Lapsus$, зламав електронну пошту та хмарні системи, сховища коду та внутрішній обліковий запис Slack. Кіберзлочинець націлився на зовнішнього підрядника Uber, найімовірніше, знайшовши їх корпоративний пароль у даркнеті.

10. Медичні дані у руках хакерів. Вперше про цю атаку стало відомо у жовтні 2022 р. Зловмисникам вдалося отримати доступ до даних 4 мільйонів клієнтів австралійського гіганта медичного страхування Medibank. Тоді було незрозуміло, скільки даних потрапило до рук хакерів і який викуп вони вимагають. Medibank не став грати за правилами злочинців і ті опублікували першу партію інформації клієнтів компанії у даркнеті. Зазначена атака може призвести до збитків компанії на близько 35 мільйонів доларів США. Вважається, що кіберзлочинці, пов'язані з програмою-вимагачем REvil (також відомою як Sodinokibi), отримали облікові дані адміністратора, і це стало початковим вектором атаки. Жертви цієї атаки тепер стикаються з хвилею подальших спроб шахрайства з особистими даними [39].

Отже, деякі висновки з наведених вище інцидентів можуть стати в нагоді користувачам під час посилення цифрового захисту своїх пристроїв та корпоративних мереж. Зокрема компаніям слід правильно налагодити свої процеси та операції, організувати тренінги з цифрової обізнаності для всіх співробітників та забезпечити багаторівневий захист корпоративної мережі за допомогою передових рішень з кібербезпеки.

Таким чином, за останні роки стало зрозуміло, що атаки кіберзлочинців можуть перешкоджати роботі критичної інфраструктури у всьому світі. Ряд інцидентів в Україні, а також в інших частинах світу, змушують багатьох замислитись про серйозні наслідки кібератак – відключення електроенергії,

перебої у подачі води, проблеми з паливом та втрата медичних даних, що може бути справді небезпечним для життя [34].

1.2 Аналіз існуючих рішень запобігання вторгненням в інформаційно-комунікаційні мережі

1.2.1 Структура систем виявлення вторгнень

Системи виявлення вторгнень – це системи, що збирають інформацію з різних точок ІКМ, що захищається, і аналізують цю інформацію для виявлення як спроб порушення, так і реальних порушень захисту (вторгнень) (рис. 1.3) [41-42].

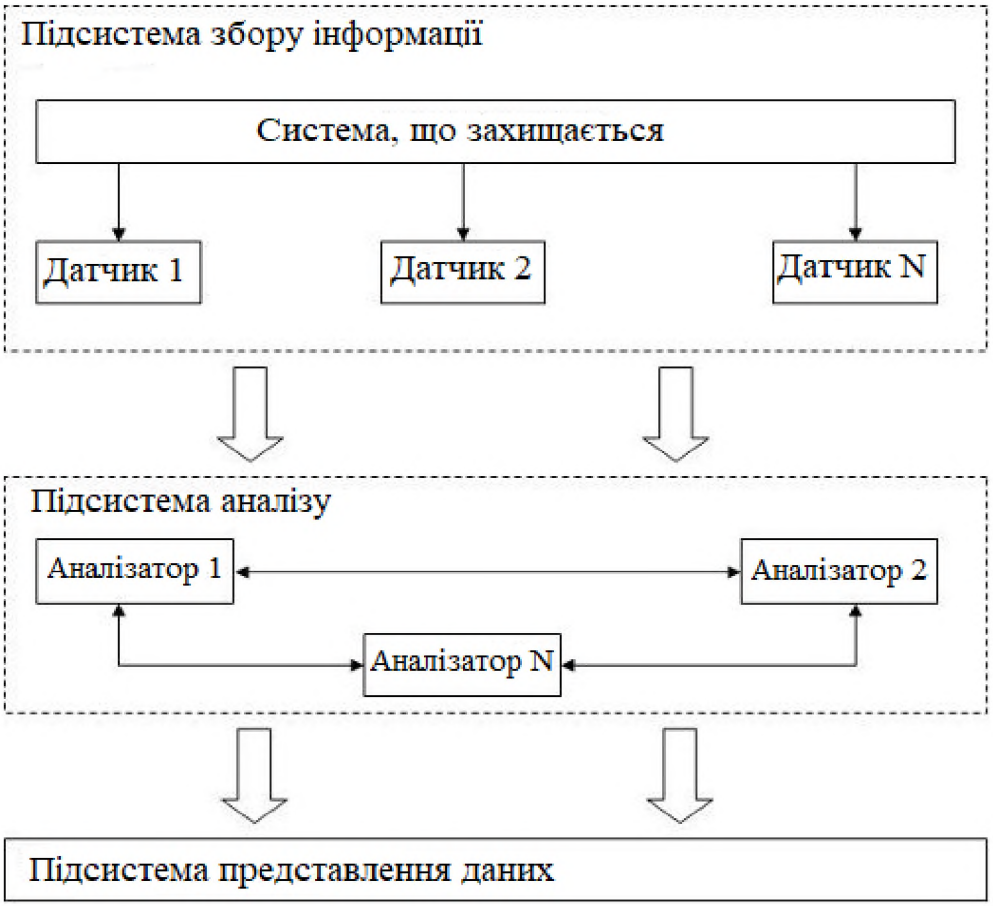


Рисунок 1.3 – Структура системи виявлення вторгнень

Сучасна СВВ, включає в себе такі підсистеми:

• підсистема збору інформації про систему, яка підлягає захисту;

• підсистема аналізу для пошуку атак та вторгнень у систему;

• підсистема представлення даних для контролю системи в режимі реального часу.

Підсистема збору інформації отримує дані від автономних модулів, датчиків програмного забезпечення (ПЗ) системи, датчиків хосту, міжмережевих та мережевих датчиків, скомпонованих у залежності від задач структури мережі та типу інформації, яка підлягає аналізу.

Ієрархічно підсистема аналізу як вхідні дані використовує інформацію із попередньої підсистеми і містить у собі набір аналізаторів, скомпонованих за задачами виявлення вторгнень заданого типу. Ефективність виявлення вторгнень залежить від параметрів аналізаторів та їх кількості.

Підсистема представлення даних орієнтована на різні групи користувачів, які контролюють певні підсистеми мережі. Тому в таких СВВ використовують розмежування доступу, групові політики, повноваження тощо.

У залежності від наборів параметрів оцінки стану системи сучасні СВВ використовують дві групи методів. У випадку фіксованого набору параметрів оцінки і фіксованого часу навчання використовуються методи контрольованого навчання («навчання з учителем»). У випадку, коли множина параметрів оцінки може змінюватися протягом заданого часу дослідження, а процес навчання відбувається весь час, використовуються методи неконтрольованого навчання («навчання без учителя»).

Основною ідеєю виявлення нестандартної поведінки ІКМ, яка підлягає захисту, є формування профілю чи образу мережі. Тому основними методами, на яких базується реалізація СВВ, є методи розпізнавання образів (класифікації). При цьому образ нормальної поведінки формується на основі аналізу параметрів оцінки мережі.

Висновки про аномальну поведінку формуються на основі відхилень значень оцінок параметрів від профілю мережі. Величина та характер

відхилень, як правило, в режимі реального часу, дають змогу проводити ідентифікацію аномалії – технічний збій, допустиме відхилення пов'язане із дією зовнішнього середовища, атака на мережу.

1.2.2 Існуючі програмні рішення запобігання вторгненням

З метою дослідження характеристик СВВ, які характеризують їх здібність до виявлення відповідних класів атак застосовують критерії, які представлені на рис. 1.4 [43].

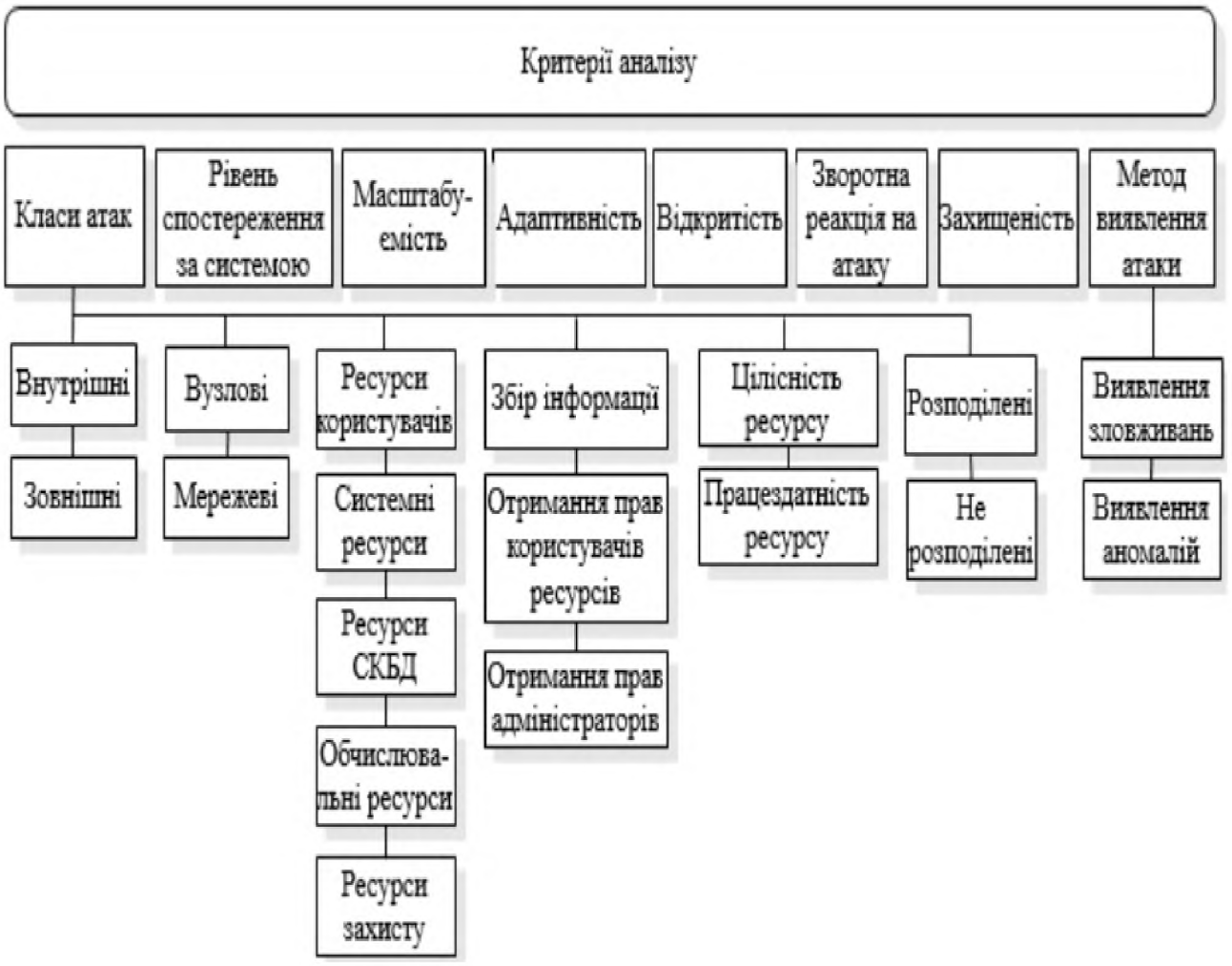


Рисунок 1.4 – Критерії порівняльного аналізу СВВ

Аналіз наведених критеріїв показує, що найбільш ефективною можна вважати СВВ, яка: є повною (покриває всі класи атак); дозволяє аналізувати поведінку ІТМ, яка захищається, на всіх рівнях (мережевому, вузловому, окремих додатків тощо); є адаптивною до раніше невідомих типів атак; масштабується для різних класів ІТМ (від локальних до корпоративних); є відкритою; має вбудовані механізми реагування на атаки; є захищеною від атак на свої компоненти.

В табл. 1.1 приведено коротку інформативну довідку про найбільш розповсюджені СВВ.

Таблиця 1.1 – Сучасні програмні рішення запобігання вторгненням

Найменування системи	Операційна система	Виробник	Офіційний веб-сайт
Bro	Linux	Vern Paxson	https://www.bro.org/
OSSEC	FreeBSD, Linux, UNIX, Mac OS X, Microsoft Windows	Daniel B. Sid , OSSEC.net	http://ossec.github.io/
Prelude	Linux, BSD, Windows	CS Group C-S	http://www.prelude-siem.com/
Suricata	FreeBSD, Linux, UNIX, Mac OS X, Microsoft Windows	Open Information Security Foundation	https://suricata-ids.org/

Наведений аналіз за вказаними критеріями показує, що наразі жодна з СВВ з відкритим кодом не відповідає у повній мірі сформульованим критеріям, зокрема завдяки відсутньої адаптації до невідомих типів атак та неможливості аналізувати поведінку ІКМ на всіх рівнях одночасно (табл. 1.2).

1.2.3 Аналіз методів запобігання вторгненням

Наразі методи виявлення атак у сучасних СВВ недостатньо повно опрацьовані з точки зору стійкості, адаптованості та верифікації, а також достатньо складно оцінити їх властивості такі, як обчислювальна складність та коректність [43].

Таблиця 1.2 – Результати аналізу СВВ

	Bro	OSSEC	Prelude	Suricata
Класи атак:				
Внутрішні	+	+	+	+
Зовнішні	+	-	+	+
Вузлові	-	+	+	+
Мережеві	+	-	+	+
Ресурси користувачів	+	+	+	+
Системні ресурси	+	-	+	+
Ресурси СКБД	-	-	-	-
Обчислювальні ресурси	-	-	-	-
Ресурси захисту	-	-	+	-
Отримання прав доступу	+	+	+	+
Цілісність ресурсу	-	-	-	-
Порушення працездатності	+	+	+	+
Розподілені	+	+	-	+
Нерозподілені	+	+	+	+
Рівень спостереження за системою	Системний	Системний	Системний, мережевий	Системний, мережевий
Метод виявлення	Сигнатурний	Сигнатурний	Сигнатурний	Сигнатурний
Адаптивність	-	+/-	-	-
Масштабованість	-	+	+	+
Відкритість (API)	+	+	+	+
Реакція	-	-	-	+

Класифікація відомих методів виявлення атак і вторгнень наведена на рис. 1.5.

Наразі одним з популярних напрямків досліджень є застосування різних методів інтелектуального аналізу даних (ІАД) в СВВ [20].

ІАД (інтелектуальний або глибинний аналіз даних) – сукупність методів виявлення в даних раніше невідомих, нетривіальних, практично корисних і доступних інтерпретації знань, необхідних для прийняття рішень в різних сферах людської діяльності. В основі даних методів лежить припущення, що вся легітимна активність в системі може бути представлена у вигляді математичної моделі.

Застосовувані для виявлення мережевих атак методи ІАД переслідують одну з наступних цілей: виявлення порушень; виявлення аномалій. Перші

моделюють атаки і застосовують засоби класифікації, другі моделюють нормальну поведінку і виконують пошук винятків.

Рисунок 1.5 – Методи виявлення атак/вторгнень

При використанні методів ІАД для виявлення мережевих атак можна виділити наступні проблеми: дані, аналізовані системами виявлення, мають високу розмірність і обсяг; вимога обробки даних в режимі реального часу; велика кількість шумів і невідповідностей в даних, що обробляються що викликають неадекватну реакцію методів інтелектуального аналізу даних.

Практика застосування СВВ сформувала два напрямки протидії кібернетичним вторгненням [20]:

• виявлення зловживань (Misuse detection);

• виявлення аномалій (Anomaly detection).

Перший підхід орієнтований на виявлення лише класифікованих (відомих) вторгнень на основі підходів синтаксичного порівняння відповідності структурних (сигнатур), інваріантних та кореляційних ознак виконуваного процесу (системи) з існуючою базою відомих шаблонів (рис. 1.6).

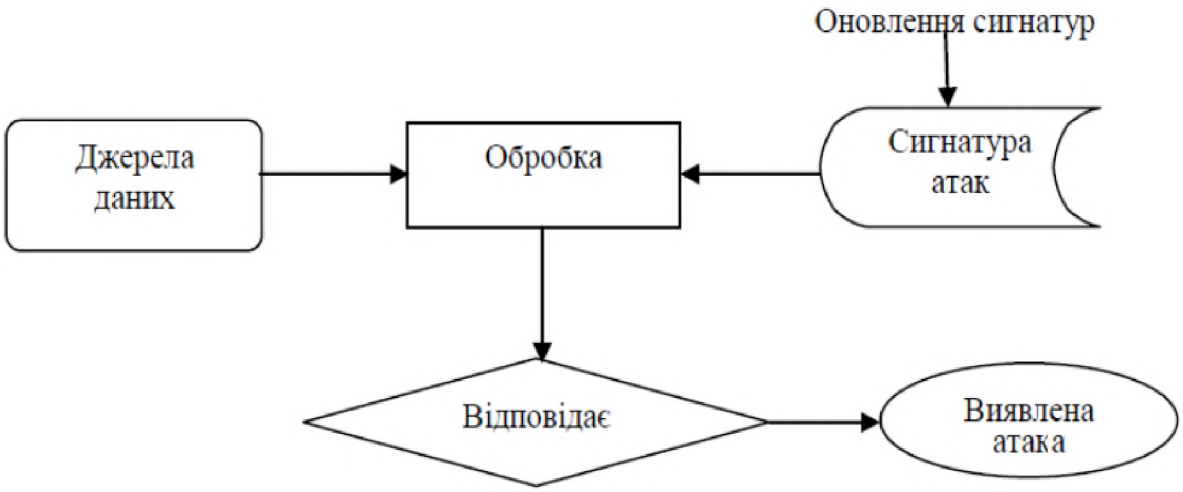


Рисунок 1.6 – Схема виявлення вторгнень на основі сигнатур

Головними недоліками виявлення вторгнень на основі сигнатур є неможливість виявлення нових модифікацій кібернетичних вторгнень і атак нульового дня (0-day) та неможливість автоматичного вводу нових шаблонів, що свідчить про їх достатньо малу ефективність.

Підхід до виявлення аномалій зводиться до задачі виявлення невідомих кібернетичних вторгнень на основі знаходження набору ознак, який не відповідає очікуваній поведінці об’єкта (користувача/системи) – шаблони характеристик, які не задовольняють визначеному поняттю нормальної поведінки фіксуються як аномалії (рис. 1.7).

Прикладами аномальної поведінки є велика кількість з’єднань за короткий проміжок часу, високі завантаження центрального процесора і коефіцієнт мережевого навантаження або використання периферійних пристроїв, які зазвичай не використовуються.

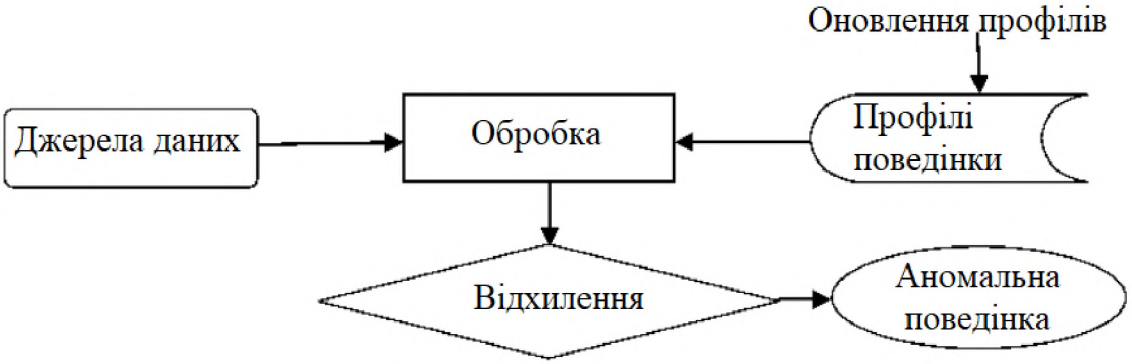


Рисунок 1.7 – Схема системи виявлення аномальної поведінки

Результати порівняльного аналізу методів виявлення атак наведено в табл. 1.3, де H – спостереження на рівні вузла, N – спостереження на рівні мережевої взаємодії, HG – спостереження на різних рівнях [43].

Результати порівняльного аналізу методів виявлення атак показують, що для більшості поведінкових методів характерним недоліком є слабка верифікованість та стійкість. З іншого боку, основною їх перевагою є адаптивність та здатність виявляти раніше невідомі атаки. Основним недоліком методів на основі знань є слабка їх адаптивність до виявлення ще не класифікованих атак, а більшість методів ІАД є слабко верифікованими. Проте, серед них можна виділити методи, які показали найбільш повну відповідність заданим критеріям аналізу, є одночасно верифікованими, адаптивними та стійкими: експертні системи та методи на основі нечіткої логіки [43].

Проведений аналіз методів і СВВ дозволяє зробити висновок про відсутність СВВ, яка мала б адаптивність до невідомих мережевих атак. Дані програмні рішення використовують на базовому рівні ту чи іншу реалізацію сигнатурного методу виявлення (запобігання) вторгненням. Реалізації відрізняються рівнем розгляду системи, алфавітом сигнатур, структурою, архітектурою і способом побудови сигнатур – від простого пошуку до повноцінної реалізації регулярних виразів над заданим алфавітом. Незважаючи на те, що існує велика кількість методів виявлення аномалій, їхня слабка стійкість, відсутність верифікації, велика кількість хибних спрацьовувань,

вузька спеціалізація та дослідницький характер, не дозволяють широко їх використовувати.

Таблиця 1.3 – Результати порівняльного аналізу методів виявлення атак

	Рівень спостереження	Аномалії/ зловживання	Верифікованість	Адаптивність	Стійкість	Обчислювальна складність
Сигнатурний аналіз	*HG*	-/+	+	-	+	*ln(n)*
Аналіз систем станів	*HG*	-/+	+	-	+	*> O(n)*
Графи сценаріїв атак	*HG*	-/+	+	+	+	*NP*
Методи на специфікаціях	*N*	-/+	+	-	-	*ln(n)*
Методи на сплайнах	*N,H*	-/+	-	+	-	*> O(n)*
Експертні системи	*N,H*	+/+	+	+	+	*NP*
Мережі Петрі	*HG*	-/+	+	-	+	*NP*
Генетичні алгоритми	*HG*	+/+	-	+	+	*ln(n)*
Нейронні мережі	*N,H*	+/+	-	+	-	*> O(n)*
Імунні мережі	*N,H*	+/+	-	+	-	*> O(n)*
Нечітка логіка	*N,H*	+/+	+	+	+	*> O(n)*
Метод опорних векторів	*N,H*	+/+	-	+	-	*ln(n)*
Дерева рішень	*N,H*	+/+	+	-	-	*NP*
Мережі Баєса	*N*	+/+	-	+	+	*> O(n)*
Роєві алгоритми	*N,H*	+/+	+	+	-	*P*
Регресійний аналіз	*HG*	+/+	-	+	-	*P*
Статичний аналіз	*N,H*	+/-	-	+	-	*> O(n)*
Вейвлет-аналіз	*N*	+/-	-	+	-	*NP*
Кластерний аналіз	*HG*	+/+	-	+	-	*> O(n)*
Спектральний аналіз	*N*	+/-	-	+	-	*NP*
Фрактальний аналіз	*N*	+/-	-	+	-	*> O(n)*
Аналіз ентропії	*N,H*	+/-	+	+	-	*> O(n)*
Біометрія	*H*	+/-	-	+	-	*> O(n)*

Отже, основними недоліками існуючих рішень запобігання вторгненням є наступні:

• існуючі методи виявлення атак не є одночасно адаптивними, стійкими та верифікованими;

• досить високий рівень помилкових спрацьовувань та пропусків атак;

• слабкий механізм виявлення нових атак;

• більшість вторгнень неможливо визначити на початкових етапах;

• практична відсутність змоги ідентифікації атакуючого та визначення цілі атаки;

• слабкий механізм виявлення відомих атак, що використовують нові стратегії;

• складність виявлення вторгнень у реальному часі з необхідною повнотою у високошвидкісних мережах;

• значне завантаження систем при роботі в реальному часі;

• слабка можливість інтерпретації адміністратором безпеки результатів поточної ситуації;

• видача результату, точність ідентифікації якого не завжди відома та ін.

Для усунення вищевказаних недоліків є доцільним проведення низки наукових досліджень щодо розробки адаптивних СВВ, в основу функціонування яких необхідно покласти методи, які б при низькій обчислювальній складності та високій стійкості та верифікації мали б низькій рівень хибних спрацьовувань.

Проведений порівняльний аналіз методів виявлення атак демонструє перевагу експертних систем серед методів на основі знань, а методи на основі нечіткої логіки – серед методів ІАД. Важливою особливістю експертних систем є практично повна відсутність помилкових тривог. Проте, повний перебір великого числа альтернатив залишає за ним досить велику обчислювальну складність. До того ж, щоб залишатися актуальними, експертні системи вимагають постійного оновлення бази правил, оскільки навіть невелика модифікація вже відомої атаки може стати серйозною перешкодою для коректного функціонування СВВ [43].

У зв’язку з цим перспективним підходом є створення гібридних інтелектуальних СВВ, в основу функціонування яких необхідно покласти методи інженерії знань, а також методи та технології інтелектуального аналізу даних.

1.3 Нечітка кластеризація

1.3.1 Нечітка логіка

Наразі для побудови інтелектуальних систем використовують різні підходи. Одним з них є логічний підхід [20-32].

Основою для логічного підходу служить булева алгебра, яка має свій подальший розвиток у вигляді числення предикатів, в якому вона розширена за рахунок введення предметних символів, відносин між ними, кванторів існування та загальності. Домогтися більшої виразності логічного підходу дозволяє такий напрям, як нечітка логіка.

Теорія нечітких множин (fuzzy sets theory) веде свій початок з 1965 р., коли професор Лотфі Заде (Lotfi Zadeh) з університету Берклі опублікував свою основну роботу «Fuzzy Sets» в журналі «Information and Control». Ця робота заклала основи моделювання інтелектуальної діяльності людини і стала початковим поштовхом у розвитку нової математичної теорії.

Прикметник «fuzzy», який можна перекласти як «нечіткий», «розмитий», «пухнастий», введено в назву нової теорії з метою дистанціювання від традиційної чіткої математики і аристотелевої логіки, що оперують з чіткими поняттями: «належить – не належить», «істина – неправда». Концепція нечіткої множини зародилася у Заде як «незадоволеність математичними методами класичної теорії систем, яка змушувала домагатися штучної точності, недоречної в багатьох системах реального світу, особливо в так званих гуманістичних системах, що включають людей».

Л. Заде розширив класичне поняття множини (по Г. Кантору), допустивши, що характеристична функція (функція належності елемента множині) може приймати будь-які значення в інтервалі [0; 1], а не тільки значення 0 або 1. Такі множини були названі їм нечіткими (fuzzy). Він визначив також ряд операцій над нечіткими множинами і запропонував узагальнення відомих методів логічного висновку modus ponens і modus tollens. Ввівши

поняття лінгвістичної змінної, і допустивши, що в якості її значень (термів) виступають нечіткі множини, Л. Заде створив апарат для опису процесів інтелектуальної діяльності, включаючи нечіткість і невизначеність виразів.

Подальші роботи професора Л. Заде і його послідовників заклали міцний фундамент нової теорії і створили передумови для впровадження методів нечіткого керування в інженерну практику.

Прийнято виділяти три періоди в розвитку теорії нечіткої логіки і нечітких систем. Перший період (кінець 60-х – початок 70 рр. XX ст.) Характеризується розвитком теоретичного апарату нечітких множин (Заде, Мамдані, Беллман). У другому періоді (70-80-ті рр. XX ст.) з'являються перші практичні результати в області нечіткого керування технічними системами (поршневий двигун). Одночасно вчені колективи стали приділяти увагу питанням побудови експертних систем на основі нечіткої логіки, розробці нечітких контролерів. Нарешті, в третьому періоді, який триває з кінця 80-х років XX ст. по теперішній час, з'являються пакети програм для побудови нечітких експертних систем, а області застосування нечіткої логіки помітно розширюються. До початку 90-х рр. XX ст. більша частина досліджень велась на Сході (Японія, Китай).

Наразі, системи з нечіткою логікою успішно впроваджені в таких областях, як керування технологічними процесами, керування транспортом, медична діагностика, технічна діагностика, фінансовий менеджмент, біржове прогнозування, розпізнавання образів, тощо. Спектр додатків дуже широкий – від відеокамер і побутових пральних машин до засобів наведення ракет протиповітряної оборони і керування бойовими вертольотами. Практичний досвід розробки систем нечіткого логічного висновку свідчить про те, що терміни і вартість їх проектування значно менше, ніж при використанні традиційного математичного апарату; при цьому забезпечується необхідний рівень робастності і прозорості моделей.

Поняття нечіткої множини – це спроба математичної формалізації нечіткої інформації для побудови математичних моделей. В основі цього

поняття лежить уявлення про те, що елементи, які складають дану множину та володіють загальною властивістю, можуть володіти цією властивістю у різній мірі й, отже, належати до даної множини із різною мірою. У разі такого підходу вислови про те, що «елемент належить даній множині» втрачають сенс, оскільки необхідно вказати «наскільки сильно» цей елемент задовольняє властивостям даної множини.

Для більшості логічних методів характерна велика трудомісткість, оскільки під час пошуку доказу можливий повний перебір варіантів. Тому даний підхід вимагає ефективної реалізації обчислювального процесу, і його працездатність, зазвичай, гарантується при порівняно невеликому розмірі бази даних.

1.3.2 Кластерний аналіз

Кластеризація – це об'єднання об'єктів в групи (кластери) на основі схожості ознак для об'єктів однієї групи і відмінностей між об'єктами з різних груп, що відповідає навчанню без учителя [21, 24].

Кластеризація включає в себе наступні етапи:

- виділення ознак;
- визначення метрики;
- розбиття об'єктів на групи;
- представлення результатів.

Для початку необхідно вибрати ознаки, які характеризують об'єкти. Ними можуть бути кількісні ознаки – координати, висота, довжина тощо або якісні ознаки – колір, статус, військове звання, тощо. Далі варто спробувати зменшити розмірність простору ознак, тобто виділити найбільш важливі атрибути об'єктів. Зменшення розмірності прискорює процес кластеризації і в ряді випадків дозволяє візуально оцінювати її результати.

Вихідною інформацією для кластеризації є матриця спостережень:

$$\mathbf{X} = \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \dots & & & \\ x_{M1} & x_{M2} & \dots & x_{Mn} \end{bmatrix}, \quad (1.1)$$

в кожному рядку якої записано значення n атрибутів одного із M об'єктів. Кластеризація полягає в розбитті об'єктів з X на кілька підмножин (кластерів), в яких об'єкти між собою більш схожі, ніж з об'єктами з інших кластерів. У метричному просторі «схожість» зазвичай визначають через відстань. Відстань може розраховуватися як між об'єктами – рядками матриці X, так і від цих об'єктів до прототипів кластерів. Найчастіше координати прототипів заздалегідь невідомі, їх знаходять одночасно з розбивкою даних на кластера.

Отже, кластерний аналіз призначений для розбиття множини об'єктів на задане або невідоме число кластерів на підставі деякого математичного критерію якості класифікації (від англ. «cluster» – пучок, скупчення, група елементів, що характеризуються будь-якою загальною властивістю).

Критерій якості кластеризації в тій чи іншій мірі відображає наступні неформальні вимоги:

а) в середині кластера об'єкти повинні бути тісно пов'язані між собою;

б) об'єкти різних кластерів повинні бути далекі один від одного;

в) за інших рівних умов розподілу об'єктів по кластерам повинні бути рівномірними.

Вимоги а) і б) відображають стандартну концепцію компактності класів розбиття; вимога в) полягає у тому, щоб критерій не нав'язував об'єднання окремих груп об'єктів.

Вузловим моментом в кластерному аналізі вважається вибір метрики (або міри близькості об'єктів), від якого залежить остаточний варіант розбиття об'єктів на групи (кластери) при заданому алгоритмі розбиття. У кожній конкретній задачі цей вибір проводиться по різному, з урахуванням головних цілей дослідження, фізичної та статистичної природи використовуваної інформації тощо.

Іншою важливою величиною в кластерному аналізі є відстань між цілими групами об'єктів, що характеризують взаємне розташування окремих груп об'єктів. Нехай w_i – i-а група (клас, кластер) об'єктів, N_i – число об'єктів, що утворюють групу w_i, вектор μ_i – середнє арифметичне об'єктів, що входять в w_i (або μ_i – «центр ваги» i-ї групи) , $q(w_l, w_m)$ – відстань між групами w_l і w_m.

Найбільш поширеними відстанями між групами об'єктів є наступні (рис. 1.8):

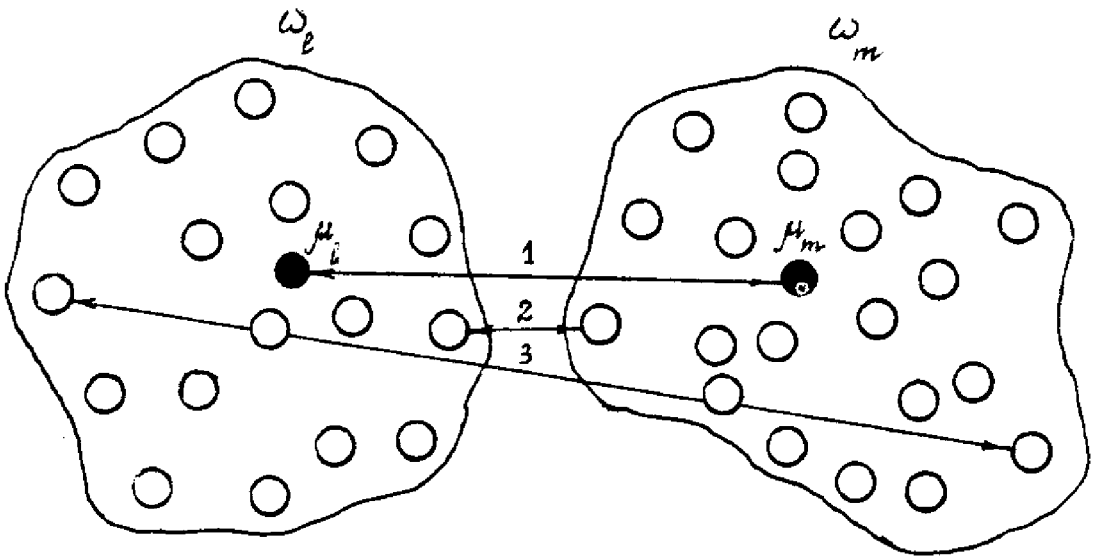


Рисунок 1.8 – Ілюстрація способів визначення відстані
між кластерами w_l і w_m: 1 – по центрам тяжіння,
2 – по найближчим об'єктам, 3 – по далеким об'єктам

• відстань центрів тяжіння – відстань між центральними точками кластерів:

$$q(w_l, w_m) = d(\mu_l, \mu_m); \tag{1.2}$$

• відстань найближчого сусіда – відстань між найближчими об'єктами кластерів:

$$q_{\min}(w_l, w_m) = \min_{x_i * w_l, x_j * w_m} d(x_i, x_j); \tag{1.3}$$

• відстань дальнього сусіда – відстань між найбільш далекими об'єктами кластерів:

$$q_{\max}(w_l, w_m) = \max_{x_i * w_l, x_j * w_m} d(x_i, x_j). \tag{1.4}$$

Узагальнена (за Колмогоровим) відстань між класами, або узагальнена K-відстань, обчислюється наступним чином:

$$q_{\tau}^{(K)}(w_l, w_m) = \left[\frac{1}{N_l N_m} \sum_{x_i * w_l} \sum_{x_j * w_m} d^{\tau}(x_i, x_j) \right]^{\frac{1}{\tau}}. \tag{1.5}$$

Зокрема, при $\tau \to \infty$ і при $\tau \to -\infty$ маємо:

$$q_{\infty}^{(K)}(w_l, w_m) = q_{\max}(w_l, w_m); \tag{1.6}$$

$$q_{-\infty}^{(K)}(w_l, w_m) = q_{\min}(w_l, w_m). \tag{1.7}$$

Вибір тієї чи іншої міри відстані між кластерами впливає, головним чином, на вигляд геометричних угруповань об'єктів в просторі ознак, які виділяються алгоритмами кластерного аналізу. Так, алгоритми, засновані на відстані найближчого сусіда, добре працюють в разі угруповань, що мають складну, зокрема, ланцюгову структуру. Відстань далекого сусіда застосовується, коли шукані угруповання утворюють в просторі ознак кулясті хмари. Щодо алгоритмів, які використовують відстані центрів тяжіння і середнього зв'язку, вони найкраще працюють у разі угруповань еліпсоїдної форми.

Кластеризація може бути ієрархічною або планарною. Планарна кластеризації здійснюється на одному рівні – «об’єкти – кластера», тобто кожний об’єкт приписують до якогось кластера. За ієрархічної кластеризації рівнів може бути кілька. На найнижчому рівні об’єкти розподілять за кластерами першого рівня. На другому рівні об’єднуються деякі кластера. На третьому рівні об’єднуються між собою кластера другого рівня, або кластера першого та другого рівнів. На будь-якому рівні об’єднуватися можуть не лише кластера, але і до кластерів додаватися окремі об’єкти.

Найбільш відомим методом ієрархічної кластеризації є метод дендрограм. Приклад ієрархічної кластеризації 30 документів за цим методом наведено на рис. 1.9 [24].

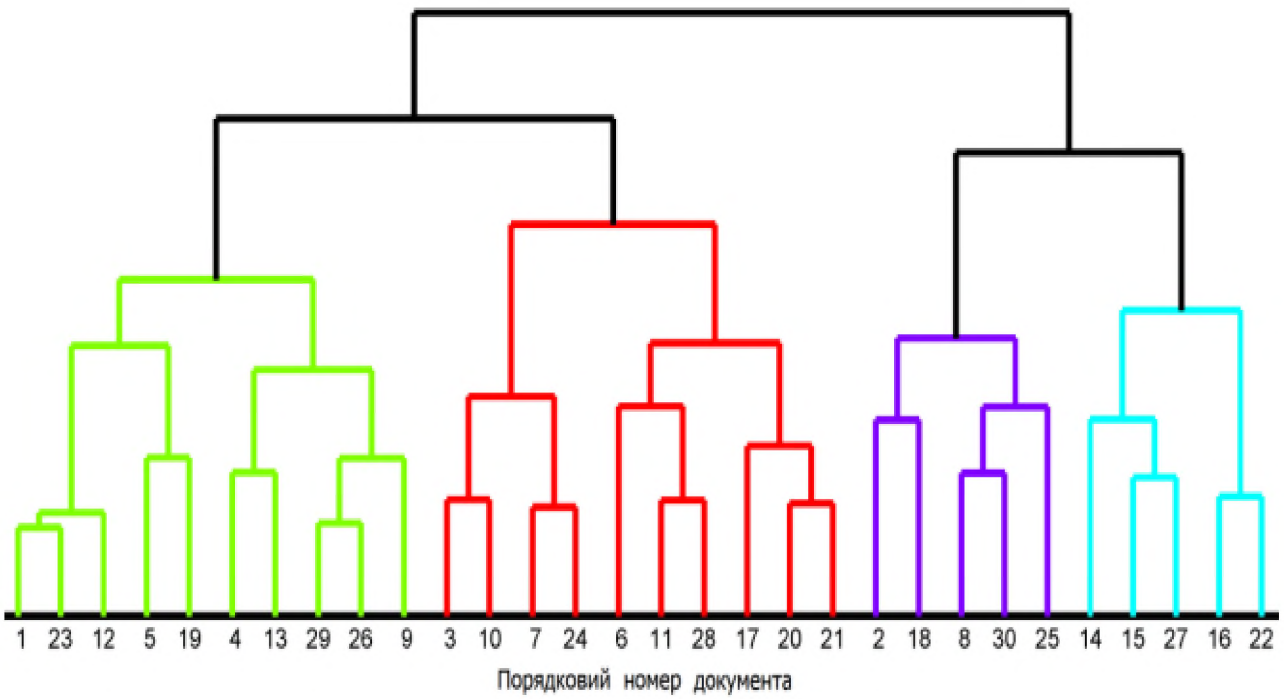


Рисунок 1.9 – Приклад ієрархічної кластеризації

Наразі існує багато методів кластеризації, які можна класифікувати на чіткі та нечіткі.

Чіткі методи кластеризації розбивають початкову множину об'єктів X на кілька підмножин, що не перетинаються. При цьому будь-який об'єкт з X належить тільки одному кластеру.

Нечіткі методи кластеризації дозволяють одному й тому ж об'єкту належати одночасно декільком (або навіть усім) кластерам, але з різним ступенем зв'язку. Таким чином, нечітка кластеризація в багатьох ситуаціях більш «природна», ніж чітка, наприклад, для об'єктів, розташованих на кордоні кластерів.

Можна проілюструвати вищеназвану тезу на «метелику» – добре відомому в теорії кластеризації прикладі. «Метелик» складається із 15 об'єктів, двовимірне зображення яких нагадує однойменну комаху (рис. 1.10).

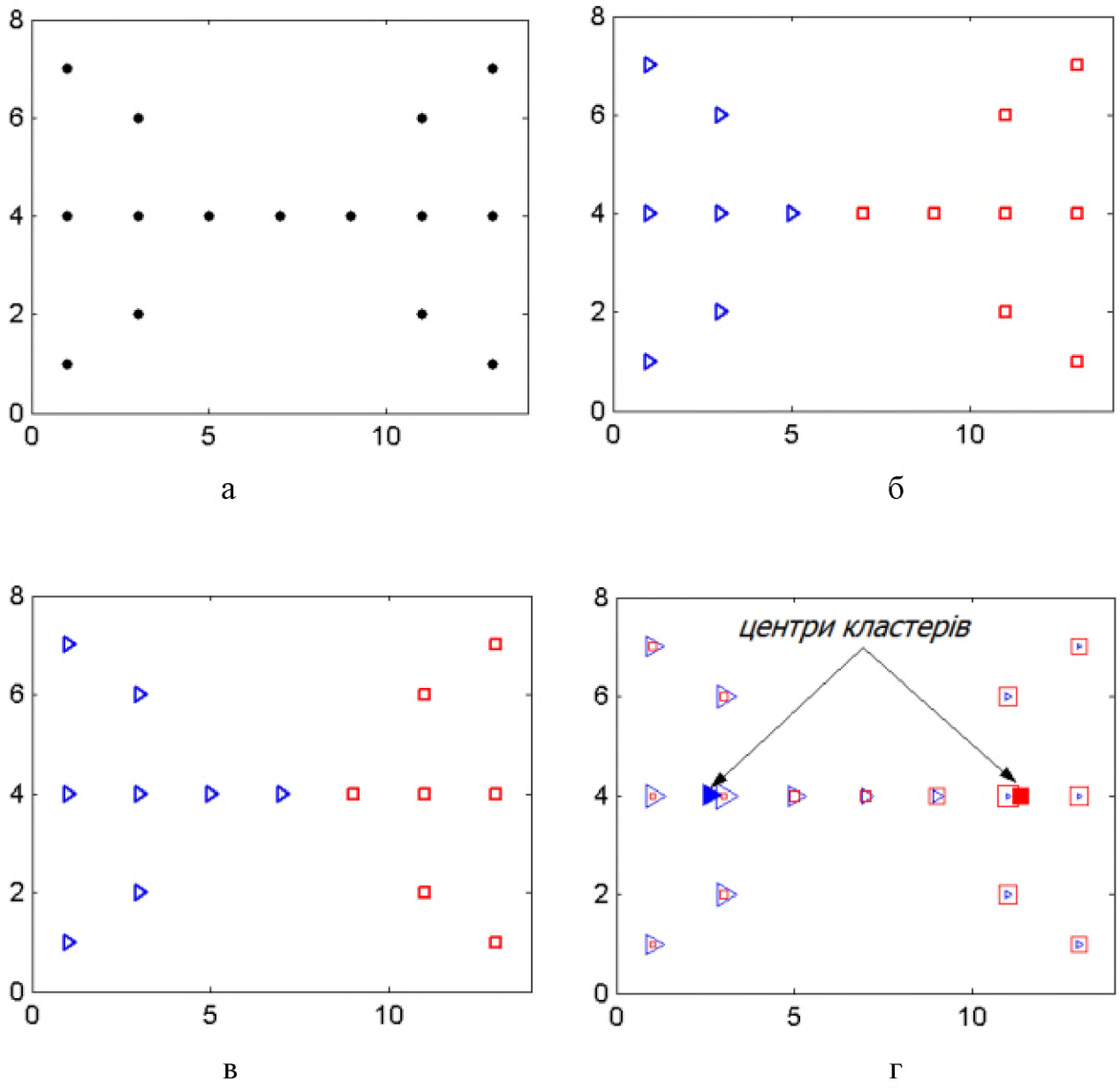


Рисунок 1.10 – Кластеризація «метелика»: а – початкові дані;
б – чітка кластеризація I; в – чітка кластеризація II;
г – нечітка кластеризація

За чіткої кластеризації (рис. 1.10,б і в) виходять два кластери із 7 і 8 об'єктів.

На рис. 1.10 об'єкти першого кластера позначені трикутниками, а другого – квадратами. Симетричний «метелик» за чіткої кластеризації розбивається на два несиметричних кластера.

За нечіткої кластеризації (рис. 1.10,г) проблемний восьмий об'єкт, розташований в центрі «метелика», одночасно належить двом симетричним кластерам з одним і тим же ступенем. На цьому рисунку розмір маркерів пропорційний ступеню належності об'єкта кластеру.

Методи кластеризації також класифікуються за тим, чи визначено кількість кластерів заздалегідь чи ні. В останньому випадку кількість кластерів визначається в ході виконання алгоритму на основі розподілу початкових даних.

Найбільш відомими методами нечіткої кластеризації є:

• субтрактивна кластеризація (Subtractive Clustering) – поліпшена версія методу гірської кластеризації та

• нечітка кластеризація C-середніх (Fuzzy C-means).

1.3.3 Нечітка кластеризація C-середніх

В основі алгоритму нечіткої кластеризації C-середніх лежить метод невизначених множників Лагранжа, який дозволяє задачі знаходження умовного екстремуму цільової функції на множині допустимих значень перетворитись на задачу безумовної оптимізації функції [21, 24].

Алгоритм нечіткої кластеризації C-середніх – це ітеративна процедура, в якій виконуються наступні кроки:

1. Завдання нечітких кластерів матрицею розбиття:

$$M_D = [\mu_{\theta i}],\ \mu_{\theta i} \in [0,1],\ \theta = \overline{1,\Theta},\ i = \overline{1,k_c};\tag{1.8}$$

при цьому

$$\sum_{i=1}^{k_c} \mu_{\theta i} = 1,\ \ 0 < \sum_{\theta=1}^{\Theta} \mu_{\theta i} < \Theta;\tag{1.9}$$

де $\mu_{\theta i}$ – ступінь належності об'єкта θ до кластеру i, k_c – кількість кластерів, Θ – кількість елементів.

2. Установка параметрів алгоритму: k_c – кількість кластерів, ϖ – експоненційна вага, яка визначає нечіткість, розмазаність кластерів ($\varpi \in [1,\infty]$), ε – параметр зупинки алгоритму.

3. Генерація випадковим чином матриці нечіткого розбиття з урахуванням умов (1.9).

4. Розрахунок центрів кластерів Ω_i:

$$\Omega_i = \frac{\sum_{\theta=1}^{\Theta} \mu_{\theta i}^{\varpi} * |X_\theta|}{\sum_{\theta=1}^{\Theta} \mu_{\theta i}^{\varpi}}, \; i = \overline{1, k_c}. \tag{1.10}$$

5. Розрахунок відстані між об'єктами з матриці спостережень і центрами кластерів:

$$D_{\theta i} = \sqrt{\|X_\theta - \Omega_i\|^2}. \tag{1.11}$$

6. Перерахунок елементів матриці розбиття.

- якщо $D_{\theta i} > 0$, то $\mu_{\theta i} = 1 \Big/ \left(D_{j\theta}^2 * \sum_{j=1}^{k_c} \frac{1}{D_{j\theta}^2} \right)^{1/(\varpi-1)}$. (1.12)

- якщо $D_{\theta i} = 0$, то $\mu_{\theta i} = \begin{cases} 1, j = i \\ 0, j \neq i \end{cases}, \; j = \overline{1, k_c}$. (1.13)

6. Перевірка умови (якщо вона виконується, то кінець алгоритму, інакше – перехід до пункту 4):

$$\|M_D - M_D^*\| < \varepsilon, \tag{1.14}$$

де M_D^* – матриця нечіткого розбиття на попередній ітерації алгоритму.

У наведеному алгоритмі найважливішим параметром, який може сильно вплинути на результат, є число кластерів k_c. Правильно вибрати кількість кластерів для реальних завдань без будь-якої апріорної інформації про структури даних досить складно, й наразі існують два підходи до цього.

Перший підхід заснований на критерії компактності і віддаленості отриманих кластерів. Логічно припустити, що за вірного вибору кількості кластерів дані будуть розбиті на компактні і добре віддалені один від одного групи. Існує кілька критеріїв оцінювання компактності кластерів, однак питання про те, як формально і достовірно визначити правильність вибору кількості кластерів для довільного набору даних все ще залишається відкритим. Для алгоритму нечітких с-середніх як критерій компактності кластерів можна використовувати коефіцієнт Ксі-Бені (Xie-Beni):

$$\chi = \frac{\sum\limits_{i=\overline{1,c}} \sum\limits_{k=\overline{1,M}} (\mu_{ik})^m \cdot \|X_k - V_i\|^2}{M \cdot \min\limits_{i \neq j} \left(\|X_k - V_i\|^2 \right)}. \tag{1.15}$$

За другим підходом розпочинають за великої кількості кластерів, а потім послідовно об'єднують схожі суміжні кластера. При цьому застосовують різні формальні критерії схожості кластерів.

Важливим чинником успішної кластеризації є вибір релевантної метрики. Кожен тип метрики продукує кластера певної форми. За евклідової метрики форма кластерів близька до сферичної.

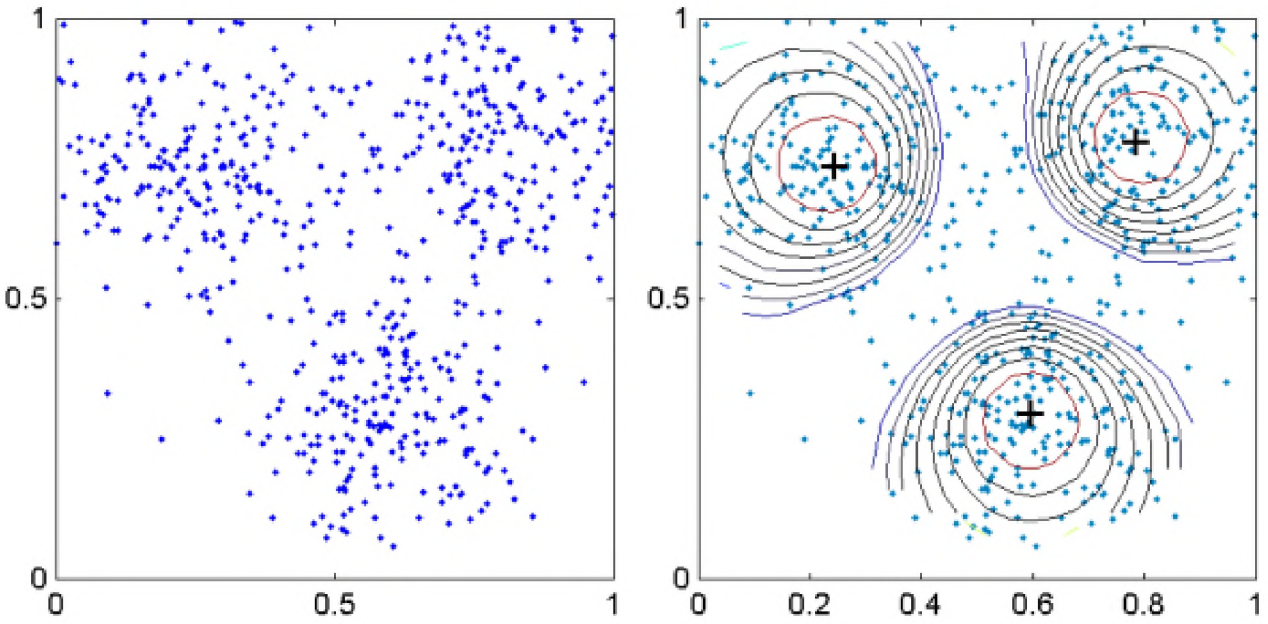
На рис. 1.11 наведено приклад нечіткої кластеризації за методом С-середніх з використанням евклідової метрики:

На рис. 1.11,а зображені початкові об'єкти; на рис. 1.11,б показані результати нечіткої кластеризації. Центри нечітких кластерів позначені символами '+'. Вісім ізоліній функцій належності нечітких кластерів побудовані для наступних значень: 0.67, 0.71, 0.75, 0.79, 0.83, 0.87, 0.91 та 0.95.

Для деяких наборів даних можна на око виділити скупчення об'єктів у вигляді різних геометричних фігур: сфер, еліпсоїдів різної орієнтації, ланцюжків тощо. В результаті кластеризації за алгоритмом з фіксованою метрикою форма усіх кластерів виходить однаковою.

Алгоритми кластеризації ніби нав'язують даними невластиву їм структуру, що призводить не тільки до неоптимальних, але іноді і до принципово неправильних результатів. Для усунення цього недоліку

запропоновано кілька методів, серед яких виділимо алгоритм Густавсона-Кеселя (Gustafson-Kessel).



а б

Рисунок 1.10 – Нечітка кластеризація з використанням евклідової метрики: а –початкові об'єкти; б – результати нечіткої кластеризації

Алгоритм Густавсона-Кеселя використовує адаптивну норму для кожного кластера, тобто для кожного і-го кластера існує своя норм-породжуюча матриця B_i. За цим алгоритмом виділяються кластера різної геометричної форми, так як оптимізуються не тільки координати центрів кластерів і матриця нечіткого розбиття, але також метрики. Критерій оптимальності лінійний відносно B_i, тому для отримання ненульових рішень, вводяться деякі обмеження на норм-породжуючі матриці. Таким чином, в алгоритмі Густавсона–Кеселя це таке обмеження на значення визначника норм-породжуючих матриць:

$$|\mathbf{B}_i| = \beta_i, \ \beta_i > 0, \ i = \overline{1, c} \ . \tag{1.16}$$

Оптимальне рішення знаходять за допомогою методу невизначених множників Лагранжа. Алгоритм Густавсона-Кеселя має значно більшу обчислювальну трудомісткість е порівнянні з алгоритмом нечітких С-середніх.

Також слід зазначити, що на результат алгоритму нечіткої кластеризації С-середніх може вплинути такий параметр, як експоненційна вага (ϖ), яка задає рівень нечіткості отриманих кластерів. Наразі не існує обґрунтованого правила вибору значення експоненціального ваги, і зазвичай її встановлюють рівною 2.

1.3.4 Субтрактивна кластеризація

В основі методу субтрактивної кластеризації лежить припущення, що кожна експериментальна точка може бути центром кластеру [21, 24].

При субтрактивній кластеризації генерується система нечіткого логічного висновку типу Сугено. Екстракція правил з даних відбувається в два етапи. Спочатку визначається кількість правил і потужностей терм-множин вихідних змінних. Далі за допомогою методу найменших квадратів визначається «то-» частина кожного правила. Результатом є система нечіткого логічного висновку з базою правил, що охоплюють всю предметну область.

Алгоритм субтрактивної кластеризації може бути представлений наступним чином:

1. Розрахувати потенціалу кожної точки x_k (як міри просторової близькості між нею та іншими):

$$\mathrm{E}(x_k) = \frac{1}{K}\sum_{i=1}^{K} e^{-\frac{\|x_k - x_i\|}{(R_c/2)^2}}, \qquad (1.17)$$

де R_c – позитивне число, яке представляє собою радіус центру кластера, K – число точок даних в навчальній послідовності.

2. Встановити кількість кластерів k_c=0.

3. Виявити точку даних з найвищим потенціалом $E(x_p)$, x_p:

$$p = \arg\max_{i=1}^{K} \mathrm{E}(x_i). \quad (1.18)$$

4. Встановити j-й центр кластера:

$$k_{c_j} = x_p, \quad (1.19)$$

при цьому $E(j_1)$ – його потенціал, $j=j+1$ – приріст.

5. Знизити потенціал всіх точок:

$$\mathrm{E}(\mathrm{x_i}) = \mathrm{E}(\mathrm{x_i}) - \mathrm{E}(\mathrm{k_{cj}})\mathrm{e}^{-\frac{\|\mathrm{k_{cj}}-\mathrm{x_i}\|}{(\mathrm{r}/2)^2}}, \quad (1.20)$$

де r=[1,1.5] R_c – позитивна постійна, що визначає діапазон впливу одного кластера; i=1, …K.

6. Перевірити значення потенціалу точок відносно встановленого порогу *thr*:

$$\max_{i=1}^{K} \mathrm{E}(x_i) < thr. \quad (1.21)$$

Якщо умова (1.21) виконується, то кінець алгоритму, інакше – перехід до пункту 3.

В алгоритмі субтрактивної кластеризації радіуси кластерів визначають наскільки далеко від центру кластера можуть бути його елементи. Слід зазначити, що вибір радіусу може сильно вплинути на результат. Якщо задати невелике значення радіусу, то база буде повнішою, але чутливою до викидів і неточностей вимірів. Якщо задати радіус занадто великим, то можна втратити деякі правила при синтезі моделі.

1.3.5 Ефективність систем з нечіткою логікою

Ефективність використання апарату нечіткої логіки базується на наступних результатах [21].

1. У 1992 р. Ванг (Wang) показав, що нечітка система, яка використовує набір правил виду:

Правило i: якщо $x_i \in A_i$ *і* $y_i \in B_i$, *то* $z_i \in C_i$, $i=1,2,\ldots,n$ (1.22)

при гаусівських функціях належності, композиції у вигляді добутку, імплікації у формі Ларсена, а також центроїдного методу приведення до чіткості є універсальним апроксиматором, тобто може апроксимувати будь-яку безперервну функцію з довільною точністю (звісно, при n→∞).

Інакше кажучи, Ванг довів теорему:

Для кожної речової безперервної функції g, заданої на компакті U і для довільного $\varepsilon>0$ існує нечітка експертна система, що формує вихідну функцію $f(x)$ таку, що

$$\sup_{x\in U}\|g(x)-f(x)\|\le\varepsilon, \tag{1.23}$$

де $\|\cdot\|$ – символ прийнятої відстані між функціями.

2. У 1995 р. Кастро (Castro) показав, що логічний контролер Мамдані при симетричних трикутних функціях належності, композиції з використанням операції min, імплікації у формі Мамдані, а також центроїдного методу приведення до чіткості також є універсальним апроксиматором.

Взагалі, системи з нечіткою логікою доцільно застосовувати для складних процесів, коли немає простої математичної моделі, а також якщо експертні знання про об'єкт або про процес можна сформулювати тільки в лінгвістичній формі.

Системи з нечіткою логікою застосовувати недоцільно у випадках, коли необхідний результат може бути достатньо просто отриманий будь-яким іншим (стандартним) шляхом, а також коли для об'єкта або процесу вже знайдена адекватна й легко досліджувана математична модель.

Основні недоліки систем з нечіткою логікою:

1. Вихідний набір нечітких правил-постулатів формулюється експертом-людиною і може виявитися неповним або суперечливим.

2. Вид і параметри функцій належності, що описують вхідні і вихідні змінні системи, обираються суб'єктивно і можуть виявитися такими, що не цілком відображають реальну дійсність.

1.4 Висновок. Постановка задачі

Наразі задача виявлення мережевих атак є однією з найактуальніших у сфері інформаційної та кібербезпеки. Її значущість зростає з кожним днем завдяки постійному збільшенню обсягів передаваної інформації за допомогою ІКМ, кількості користувачів, а також ускладненню методів атак зловмисників. За останні роки стало зрозуміло, що атаки кіберзлочинців можуть перешкоджати роботі критичної інфраструктури у всьому світі. Ряд інцидентів в Україні, а також в інших частинах світу, змушують багатьох замислитись про серйозні наслідки кібератак, які можуть бути небезпечними для життя.

СВВ відповідають за моніторинг мережевого трафіку на будь-які підозрілі події і піднімають тривогу, щоб вжити належних дій проти вторгнення. СВВ збирають та аналізують інформацію з різних ІКМ для виявлення можливих загроз безпеки, які включають у себе загрози як ззовні, так і зсередини. Вони допомагають автоматично сформувати з даних корисний шаблон, який буде еталоном нормальної поведінки для подальшої класифікації.

Наразі існує два типи виявлення вторгнень: виявлення зловживань та виявлення аномалій. Виявлення зловживань може застосовуватися до атак, які слідують певному фіксованому шаблону і зазвичай створюються для дослідження шаблонів вторгнення, які були розпізнані та повідомлені експертами. Використання цього підходу може бути проблемним у разі, коли зустрічаються нові типи атак або якщо зловмисники намагаються замаскувати свою поведінку. Методи виявлення аномалій розроблені для протидії цьому виду виклику шляхом виявлення моделей нормальної поведінки з припущенням, що вторгнення зазвичай включає деяке відхилення від цієї нормальної поведінки.

Традиційні методи виявлення аномалій мережевого трафіку не здатні забезпечити надійний захист ІКМ. Методи штучного інтелекту дозволяють створити принципово нові алгоритми виявлення вторгнень і атак, дозволяють значно підвищити рівень захищеності ІКМ.

Нечітка логіка (у тому числі алгоритми нечіткої кластеризації) базується на ступенях невизначеності, а не на типовій істинній або хибній булевій логіці, на якій створені сучасні персональні комп'ютери. Отже, вона представляє прямий спосіб дійти до остаточного висновку на основі неясних, неоднозначних, галасливих, неточних або відсутніх вхідних даних. З нечітким доменом нечітка логіка дозволяє екземпляру належати, можливо частково, одночасно до декількох класів.

Тому нечітка логіка є хорошим класифікатором для вирішення проблем СВВ, оскільки сама безпека включає нечіткість, а межа між нормальним та аномальним станами недостатньо чітко визначена. Крім того, проблема виявлення вторгнень містить різні числові особливості у зібраних даних та кілька похідних статистичних показників. Побудова СВВ на основі числових даних з жорсткими порогами виробляє високі помилкові тривоги.

Діяльність, яка лише незначно відхиляється від моделі, не може бути розпізнана або незначна зміна нормальної активності може спричинити помилкові тривоги. За допомогою нечіткої логіки (у тому числі алгоритмів нечіткої кластеризації) можна змоделювати цю незначну аномалію, щоб зберегти низькі показники хибних ставок.

Таким чином, для виконання мети кваліфікаційної роботи необхідно:

• запропонувати підхід до виявлення аномалій трафіку в інформаційно-комунікаційних мережах за допомогою алгоритмів нечіткої кластеризації;

• оцінити ефективність запропонованого підходу.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Підхід до виявлення аномалій трафіку в інформаційно-комунікаційних мережах за допомогою алгоритмів нечіткої кластеризації

Як вже зазначалось у розділі 1.2.1 та на рис. 1.1, сучасні СВВ включають в себе наступні підсистеми: підсистема збору інформації про систему, яка підлягає захисту; підсистема аналізу для пошуку атак та вторгнень у систему; підсистема представлення даних для контролю системи в режимі реального часу.

Підсистема аналізу мережевого трафіку містить у собі набір аналізаторів, скомпонованих за задачами виявлення вторгнень заданого типу. Вона виконує аналіз кожного запису про потік за допомогою різних алгоритмів, найчастіше таких, які використовують методи систем штучного інтелекту. В результаті для кожного запису визначається вид з'єднання: нормальне або атака, а також вид атаки у разі її виявлення.

Запропоновано будувати інтелектуальну підсистему аналізу мережевого трафіку на основі різних алгоритмів нечіткої кластеризації: субтрактивної кластеризації та нечіткої кластеризації C-середніх. Також необхідно більш докладно дослідити переваги та недоліки зазначених алгоритмів нечіткої кластеризації при виявленні аномалій на реальному мережевому трафіку.

Оскільки основними методами, на яких базується реалізація СВВ, є методи розпізнавання образів (класифікації), було розглянуто постановку задачі класифікації.

Завдання класифікації полягає у розбитті об'єктів на декілька класів. Об'єкти в межах одного класу вважаються еквівалентними з погляду критерію розбиття.

Взагалі, у задачі класифікації та регресії потрібно визначити значення залежної змінної об'єкта на підставі значень інших змінних, що характеризують цей об'єкт.

Формально завдання класифікації та регресії можна описати наступним чином. Є безліч об'єктів:

$$I = \{i_1, i_2, ..., i_j, ..., i_n\}, \tag{2.1}$$

де i_j – досліджуваний об'єкт.

Кожен об'єкт характеризується набором змінних:

$$I_j = \{x_1, x_2, ..., x_h, ..., x_m, y\}, \tag{2.2}$$

де x_h – незалежні змінні, значення яких відомі і на підставі яких визначається значення залежної змінної y.

В Data Mining часто набір незалежних змінних позначають у вигляді вектору:

$$X = \{x_1, x_2, ..., x_h, ..., x_m\}. \tag{2.3}$$

Кожна змінна x_h може набувати значень з деякої множини:

$$C_h = \{c_{h1}, c_{h2}, ...\}. \tag{2.4}$$

Якщо значення змінної є елементи кінцевої множини, то кажуть, що вона має категоріальний тип.

Якщо безліч значень $C = \{c_1, c_2, ..., c_r, ..., c_k\}$ змінної y кінцева, то задача називається задачею класифікації. Якщо змінна y набуває значення на множині дійсних чисел R, то завдання називається завданням регресії.

Отже, класифікатор – це система, яка вводить (як правило) вектор дискретних і/або неперервних функцій і виводить одне дискретне значення класу [44-45].

Для всіх класифікаторів найважливішими є 3 компоненти:

1. Представлення.

2. Оцінювання.

3. Оптимізація.

Класифікатор повинен бути представлений за допомогою формальної мови, яку комп'ютер може обробляти. І, навпаки, вибір представлення для учня рівносильний вибору набору класифікаторів, яких він може навчитися. Цей

набір називається гіпотезою простору учня. Якщо класифікатор не знаходиться в гіпотезі простору, то він не можу бути вивчений.

Функція оцінювання (так звана цільова функція) потрібна для виділення «гарних» класифікаторів від «поганих».

Також потрібен метод пошуку серед всіх класифікаторів такого, який буде класифікувати найбільш швидко й правильно. Вибір методу оптимізації є ключовим елементом ефективності учня, а також допомагає визначити вибраний класифікатор, якщо функція оцінки має більше ніж один оптимум. Для нових учнів найкраще почати використовувати загальноприйняті оптимізатори, які пізніше замінюються спеціально розробленими [45].

Для оцінки якості класифікації зазвичай використовують наступні показники (метрики): матриця помилок або неточностей (Confusion Matrix); акуратність (Accuracy); точність (Precision); повнота (Recall); F-міра (F-score); ROC-крива або крива робочих характеристик (Receiver Operating Characteristics curve); Precision-Recall (PR) крива.

Взагалі будь який класифікатор робить помилки. Таких помилок може бути дві:

• нормальна ситуація у мережі за даними трафіка розпізнається моделлю як аномальна (даний випадок можна трактувати як «помилкову тривогу»);

• аномальна ситуація розпізнається як нормальна і ніяких дій по захисту від атаки не відбувається (даний випадок можна розглядати як «пропуск цілі»).

Зазначені помилки нерівноцінні по зв'язаними з ними наслідками. У разі «помилкової тривоги» втрати складуть тільки марно потрачений час та ресурси на протидію неіснуючій загрозі. У разі ж «пропуску цілі» можна втратити набагато більше (інформацію, роботу мережі та інше, в залежності від виду атаки). Тому системі захисту важливіше не допустити «пропуску цілі», ніж «помилкової тривоги».

Виходячи з вищевказаного можливі наступні результати класифікації:

• True Positive (TP) – наявність атаки класифікована як наявна атака;

• True Negative (TN) – нормальна робота мережі класифікована як нормальна робота без аномалій;

• False Positive (FP) – нормальна робота мережі класифікована як аномальна;

• False Negative (FN) – атака чи аномальна робота мережі розпізнана як нормальна.

Як метрика оцінки якості розглянутих класифікаторів на основі алгоритмів нечіткої кластеризації використовувалась Accuracy (акуратність, точність) – частка від навчальної та перевірочної вибірки щодо якої класифікатор прийняв правильне рішення:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}. \quad (2.5)$$

Тобто, Accuracy – частка правильних відповідей класифікатору на основі алгоритмів нечіткої кластеризації. Взагалі це швидкий та інформативний індикатор продуктивності моделі.

2.2 Оцінка ефективності підходу до виявлення аномалій трафіку в інформаційно-комунікаційних мережах за допомогою алгоритмів нечіткої кластеризації

Оцінка ефективності запропонованого підходу до виявлення аномалій мережевого трафіку за допомогою алгоритмів нечіткої кластеризації виконувалась в середовищі Matlab/Simulink за допомогою стандартних і розроблених програм.

Як експериментальні дані було обрано набір даних Intrusion Detection Evaluation Dataset (CICIDS 2017), створений співробітниками Канадського Інституту Кібербезпеки (Canadian Institute for Cybersecurity (CIC)) [46].

Канадський Інститут Кібербезпеки – це міждисциплінарний навчальний, науково-дослідний і підприємницький підрозділ, який спирається на досвід дослідників у соціальних науках, бізнесі, інформатиці, інженерії, праві та науці.

CIC базується в Університеті Нью-Брансвіка (University of New Brunswick), об’єднує дослідників і практиків з усього академічного спектру для обміну інноваційними ідеями, створення проривних технологій і проведення новаторських досліджень найактуальніших проблем у галузі кібербезпеки.

Набір даних CICIDS 2017 містить приклади аномального та нормального трафіку. Автори створили систему з 25 профілів легальних користувачів, а також шкідливі дії порушників, що передають дані за протоколами http, https, ftp, ssh та email. Дані збиралися протягом п'яти днів. В результаті вихідний набір даних містить 80 ознак мережевого трафіку, та інформацію про те, до якого з 15 класів відноситься з'єднання: нормальні з'єднання (Benign) або один із 14 різних видів атак.

Набір даних CICIDS 2017 має наступні характеристики:

• повна конфігурація мережі: включає шлюзи, брандмауери, комутатори, маршрутизатори та наявність багатьох операційних систем, таких як Windows, Ubuntu та Mac OS X;

• повний трафік: наявність агента профілювання користувачів, 12 різних машин у мережі (об'єкті атаки) та реальні атаки з мережі (джерела атаки);

• позначений набір даних: показані ярлики для нормального трафіку і атак для кожного дня, а також подробиці часу атаки, що опубліковані в документі набору даних;

• повна взаємодія: показані атаки як усередині, так і між внутрішніми LAN; були дві різні мережі та зв'язок через Інтернет;

• повне захоплення: використовувався дзеркальний порт і весь трафік був захоплений та записаний на сервері зберігання;

• доступні протоколи: наявність усіх доступних протоколів, таких як http, https, ftp, ssh та протоколи електронної пошти;

• різноманітність атак: у наборі представлені різноманітні атаки;

• неоднорідність: захоплення мережевого трафіку з головного комутатора, дампа пам'яті та системних викликів з усіх машин-жертв під час виконання атак;

• набір функцій: вилучено понад 80 функцій мережевого потоку із згенерованого мережевого трафіку за допомогою CICFlowMeter та надано набір даних мережевого потоку у вигляді файлу csv;

• метадані: повністю пояснений набір даних, який включає час, атаки, потоки та мітки.

Таким чином, можна зробити висновок про придатність набору даних CICIDS 2017 для проведення експериментальних досліджень. Однак для цього набору властивий дисбаланс класів, як видно з табл. 2.1.

Таблиця 2.1 – Співвідношення класів атак у наборі даних CICIDS 2017

№	**Вид атаки**	**Кількість записів**	**Відсоток від загальної кількості записів**
1.	Benign	2273097	80.3004
2.	DoS Hulk	231073	8.163
3.	PortScan	158930	5.6144
4.	DDoS	128027	4.5227
5.	DoS Goldeneye	10293	0.3636
6.	FTP Patator	7938	0.2804
7.	SSH Patator	5897	0.2083
8.	DoS Slowloris	5796	0.2048
9.	DoS Slowhttptest	5499	0.1943
10.	Bot	1966	0.0695
11.	Web-Brute force	1507	0.0532
12.	Web attack XSS	652	0.023
13.	Infiltration	36	0.0013
14.	Web attack-SQL injection	21	0.0007
15.	Heartbleed	11	0.0004
	Усього	2830743	100

Експериментальні дані (набір даних CICIDS 2017) було розділено на навчальну вибірку, яка склала 70 % даних і перевірочну – 30 % даних.

Як класифікатори на основі алгоритмів нечіткої кластеризації використовувались: субтрактивна кластеризація та нечітка кластеризація C-середніх. При цьому для алгоритму субтрактивної кластеризації діапазон впливу кластерного центру R_c дорівнював 0,5 (R_c=0,5). Для нечіткої кластеризації C-середніх використовувалась структура алгоритму Сугено та 15 кластерів (k_c=15).

Результати імітаційного моделювання – результати роботи класифікаторів на основі алгоритмів нечіткої кластеризації (значення Accuracy) за видами атак представлені в табл. 2.2 та на рис. 2.1.

Таблиця 2.2 – Значення Accuracy для обраних класифікаторів за видами атак

	Вид атаки														
Класифікатор на основі алгоритму нечіткої кластеризації	Benign	DoS Hulk	PortScan	DDoS	DoS Goldeneye	FTP Patator	SSH Patator	DoS Slowloris	DoS Slowhttptest	Bot	Web-Brute force	Web attack XSS	Infiltration	Web attack-SQL injection	Heartbleed
Субтрактивна кластеризація	0,98	0,962	0.958	0,805	0,802	0,917	0,858	0,909	0,899	0,905	0,855	0,762	0,412	0,306	0,274
Кластеризація C-середніх	0,986	0,97	0.964	0,849	0,824	0,933	0,872	0,924	0,883	0,931	0,871	0,779	0,456	0,332	0,299

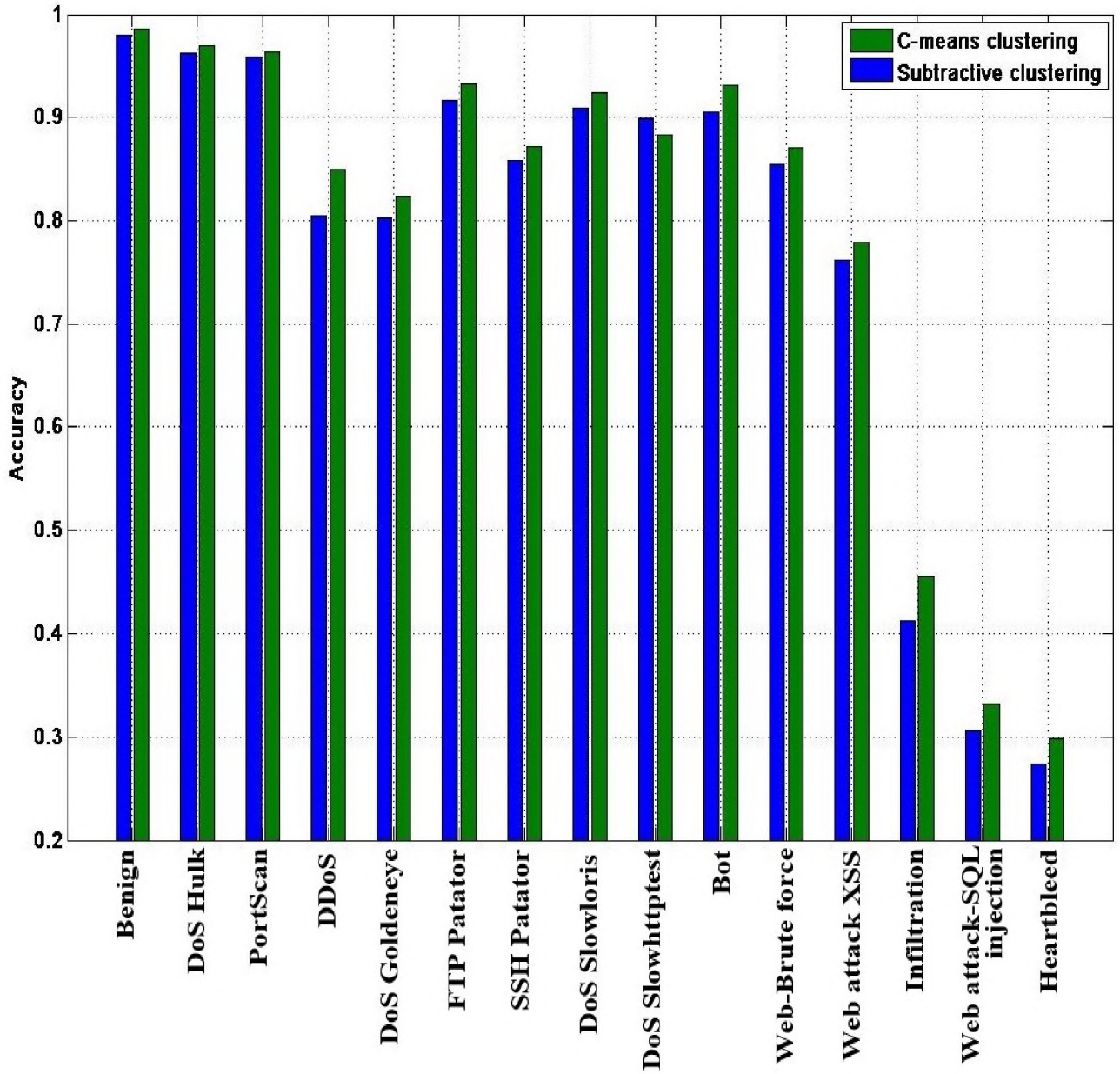


Рисунок 2.1 – Результати роботи класифікаторів на основі субтрактивної кластеризації та нечіткої кластеризації *C*-середніх за видами атак з набору даних CICIDS 2017

Встановлено (див. табл. 2.2 та рис. 2.1), що розпізнавання нормального трафіку (Benign) обраними класифікаторами відбувається вірно у переважній більшості випадків (98-98,6 %).

Як видно з табл. 2.2 та рис. 2.1 , класифікатори на основі алгоритмів нечіткої кластеризації з високою точністю визначають з'єднання, що не містять

атаку (тип Benign), і розпізнають 10 з 14 представлених видів атак (з ймовірністю понад 80%).

Існує високий відсоток похибок при розпізнаванні наступних видів атак: Web attack XSS, Infiltration, Web attack-SQL injection, Heartbleed. Це пов'язано, у першу чергу, з недостатністю даних (малою кількістю записів) про ці атаки у обраному наборі CICIDS 2017 для навчання та тестування розглянутих класифікаторів.

Встановлено (див. табл. 2.2 та рис. 2.1), що в цілому розглянуті класифікатори показали приблизно однакові результати, але найкращим виявився класифікатор на основі алгоритму нечіткої кластеризації C-середніх.

Таким чином, наукова новизна отриманих результатів полягає у тому, що використання класифікаторів на основі алгоритмів нечіткої кластеризації C-середніх та субтрактивної кластеризації дозволяє виявляти аномалії трафіку в інформаційно-комунікаційних мережах.

Практична цінність роботи полягає в тому, що розглянуті у цьому розділі класифікатори на основі алгоритмів субтрактивної кластеризації та нечіткої кластеризації C-середніх можуть бути використані в засобах моніторингу, здатних аналізувати трафік в інформаційно-комунікаційних мережах в режимі реального часу.

Подальші дослідження мають бути спрямовані на налаштування параметрів класифікаторів на основі алгоритмів субтрактивної кластеризації та нечіткої кластеризації C-середніх та оцінки їх ефективності на інших експериментальних даних (DARPA 1998, KDD CUP 99, NSL KDD, ISCX 2012, ADFA 2013, UNSW-NB15, CSE-CIC-IDS 2018 тощо).

2.3 Висновки

Сучасні СВВ включають в себе наступні підсистеми: підсистема збору інформації про систему, яка підлягає захисту; підсистема аналізу для пошуку

атак та вторгнень у систему; підсистема представлення даних для контролю системи в режимі реального часу.

Підсистема аналізу мережевого трафіку містить у собі набір аналізаторів, скомпонованих за задачами виявлення вторгнень заданого типу. Вона виконує аналіз кожного запису про потік за допомогою різних алгоритмів, найчастіше таких, які використовують методи систем штучного інтелекту. В результаті для кожного запису визначається вид з'єднання: нормальне або атака, а також вид атаки у разі її виявлення.

Запропоновано будувати інтелектуальну підсистему аналізу мережевого трафіку на основі різних алгоритмів нечіткої кластеризації: субтрактивної кластеризації та нечіткої кластеризації C-середніх. Оскільки основними методами, на яких базується реалізація СВВ, є методи розпізнавання образів (класифікації), було розглянуто постановку задачі класифікації.

Оцінка ефективності запропонованого підходу до виявлення аномалій мережевого трафіку за допомогою алгоритмів нечіткої кластеризації виконувалась в середовищі Matlab/Simulink за допомогою стандартних і розроблених програм.

Як експериментальні дані було обрано набір даних Intrusion Detection Evaluation Dataset (CICIDS 2017), створений співробітниками Канадського Інституту Кібербезпеки та який містить приклади аномального та нормального трафіку.

Як класифікатори на основі алгоритмів нечіткої кластеризації використовувались: субтрактивна кластеризація та нечітка кластеризація C-середніх. При цьому для алгоритму субтрактивної кластеризації діапазон впливу кластерного центру R_c дорівнював 0,5 (R_c=0,5). Для нечіткої кластеризації C-середніх використовувалась структура алгоритму Сугено та 15 кластерів (k_c=15).

Як метрика оцінки якості розглянутих класифікаторів використовувалась Accuracy. Встановлено, що розпізнавання нормального трафіку (Benign) обраними класифікаторами відбувається вірно у переважній більшості випадків

(98-98,6 %). Також було встановлено, що класифікатори на основі алгоритмів нечіткої кластеризації розпізнають 10 з 14 представлених видів атак (з ймовірністю понад 80%).

Існує високий відсоток похибок при розпізнаванні наступних видів атак: Web attack XSS, Infiltration, Web attack-SQL injection, Heartbleed. Це пов'язано, у першу чергу, з недостатністю даних (малою кількістю записів) про ці атаки у обраному наборі CICIDS 2017 для навчання та тестування розглянутих класифікаторів.

Встановлено, що в цілому розглянуті класифікатори показали приблизно однакові результати, але найкращим виявився класифікатор на основі алгоритму нечіткої кластеризації C-середніх.

3 ЕКОНОМІЧНА ЧАСТИНА

Метою розділу є обґрунтування економічної доцільності розробки підходу до виявлення аномалій мережевого трафіку за допомогою алгоритмів нечіткої кластеризації. Досягнення цієї мети потребує виконання таких розрахунків, як:

– капітальні витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення;

– річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування;

– річний економічний ефект від впровадження запропонованих заходів;

– показники економічної ефективності впровадження системи захисту на підприємстві.

3.1 Розрахунок капітальних (фіксованих) витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Витрати на впровадження системи захисту інформації на підприємстві визначаються, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

Визначення трудомісткості розробки підходу до виявлення аномалій мережевого трафіку за допомогою алгоритмів нечіткої кластеризації

Взагалі трудомісткість розробки системи захисту інформації на підприємстві визначається тривалістю кожної робочої операції, до яких належать наступні:

де $t_{тз}$ – тривалість складання технічного завдання на розробку підходу щодо виявлення аномалій мережевого трафіку за допомогою алгоритмів нечіткої кластеризації, $t_{тз}$=19;

$t_в$ – тривалість вивчення технічного завдання, літературних джерел за темою тощо, $t_в=40$;

$t_{ім}$ – тривалість імітаційного моделювання для дослідження алгоритмів нечіткої кластеризації С-середніх та субтрактивної кластеризації, що дозволяють виявляти аномалії трафіку в інформаційно-комунікаційних мережах, $t_а=65$;

$t_р$ – тривалість розробки підходу щодо виявлення аномалій мережевого трафіку за допомогою алгоритмів нечіткої кластеризації, $t_{ап}=55$;

$t_д$ – тривалість підготовки технічної документації, $t_д=22$.

Отже,

$$t = t_{тз}+ t_в+ t_{ім}+ t_р + t_д = 19+40+65+55+22= 201 \text{ година.}$$

Розрахунок витрат на розробку підходу щодо виявлення аномалій мережевого трафіку за допомогою алгоритмів нечіткої кластеризації

Витрати на розробку системи захисту інформації на підприємстві $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч}\ .$$

$$К_{рп} = З_{зп} + З_{мч} = 37185 +1573,83 = 38758,83 \text{ грн.}$$

$$З_{зп} = t\ З_{пр} = 208*185 = 37185 \text{ грн.}$$

де t – загальна тривалість розробки підходу щодо виявлення аномалій мережевого трафіку за допомогою алгоритмів нечіткої кластеризації, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч}= t*С_{мч}=201*7,83=1573,83 \text{ грн.}$$

де t – загальна тривалість розробки підходу щодо виявлення аномалій мережевого трафіку за допомогою алгоритмів нечіткої кластеризації, годин;

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = 1{,}1 \cdot 3 \cdot 1{,}68 + \frac{6400 \cdot 0{,}4}{1920} + \frac{9100 \cdot 0{,}2}{1920} = 7{,}83 \text{ грн.}$$

Оцінка ефективності запропонованого підходу щодо виявлення аномалій мережевого трафіку за допомогою алгоритмів нечіткої кластеризації виконувалась за допомогою стандартних та розроблених програм в середовищі Matlab/Simulink із використанням експериментальних даних – про мережеві вторгнення CSE-CIC-IDS2018. Зазначений пакет прикладних програм вже використовується (або можливий варіант використання безкоштовної навчальної версії з офіційного сайту розробника), тому в цьому випадку капітальні витрати не виникають.

Таким чином, додаткові витрати щодо придбання апаратного та програмного забезпечення не виникають.

Витрати на залучення зовнішніх консультантів складають 7000 грн.

Витрати на налагодження системи інформаційної безпеки становитимуть 4000 грн.

Таким чином, капітальні (фіксовані) витрати на розробку засобів підвищення рівня інформаційної безпеки складуть:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} =$$
$$= 38758{,}83 + 7000 + 4000 = 49758{,}83 \text{ грн.}$$

де $К_{рп}$ – вартість розробки політики інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

$К_н$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \text{ грн.}$$

де $С_в$ – вартість відновлення й модернізації системи ($С_в = 0$);

$С_к$ – витрати на керування системою в цілому;

$С_{ак}$ – витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн.).

Оскільки оцінку ефективності запропонованого підходу до виявлення аномалій мережевого трафіку за допомогою алгоритмів нечіткої кластеризації здійснено за допомогою стандартних та розроблених програм в середовищі Matlab/Simulink, то витрати щодо відновлення й модернізації системи не виникають.

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються сукупною величиною витрат на організаційні заходи, яка складає 4000 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 18000 грн. Додаткова заробітна плата – 8% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,1 ставки. Отже,

$$С_з = (18000*12 + 18000*12*0,08)*0,1= 23328 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2021 р. складає 22%.

$$С_{єв} = 23328*0,22 = 5132,16 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.,}$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=1,1 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,68 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 1,1*3*1920*1,68 = 10644,8 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 1%:

$$С_{тос} = 49758,83*0,01=497,59 \text{ грн.}$$

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 4000+23328+5132,16 +10644,8 +497,59 = 43602,55 \text{ грн.}$$

Витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) можна орієнтовно визначити, виходячи з величини капітальних витрат та середньостатистичних даних щодо активності користувачів. За статистичними даними активність користувачів складає 10%.

Тому:

$$С_{ак} = 49758,83*0,1=4975,88 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = 43602,55+4975,88 = 48578,43 \text{ грн.}$$

3.3 Оцінка можливого збитку від атаки на вузол або сегмент мережі

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 2 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 3 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 2 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 20100 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 18400 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 4 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 250 тис. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, 5200 грн.;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 76.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_п = \frac{18400 \cdot 4}{176} \cdot 2 = 836{,}36 \text{ грн.},$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{18400 \cdot 4}{176} \cdot 2 = 836{,}36 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в = \frac{20100 \cdot 1}{176} \cdot 3 = 342{,}61 \text{ грн.}$$

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$П_в = 836,36+342,61+5200 = 6378,97 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із средньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви})$$

$$V = \frac{250000}{2080} \cdot (2 + 3 + 2) = 841,35 \text{ грн.}$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$U = 836,36+6378,97+841,35 = 8056,68 \text{ грн.}$$

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n U = \sum_1 \sum_{76} 8056,68 = 612307,68 \text{ грн.}$$

3.4 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної:

$$E = B \cdot R - C \text{ грн.,}$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (22%);

C – щорічні витрати на експлуатацію системи інформаційної безпеки.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 612307,68*0,22 – 48578,43 = 86129,26 \text{ грн.}$$

3.5 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Для встановлення економічної ефективності визначають такі показники як: коефіцієнт повернення інвестицій (ROSI) та термін окупності капітальних інвестицій (T_o).

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI=86129,26 /49758,83 =1,73, \quad \text{частки одиниці.}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} – N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (7%);

$N_{інф}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$1,73 > (7 – 5)/100 = 1,73 > 0,02.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_o = \frac{К}{Е} = \frac{1}{ROSI}$$

$$T_0= 1 / 1,73 = 0,58 \text{ років.}$$

3.6 Висновок

Отже, згідно з наведеними розрахунками можна зробити висновок, що розробка підходу до виявлення аномалій мережевого трафіку за допомогою алгоритмів нечіткої кластеризації є економічно доцільною.

Капітальні витрати, які складають 49758,83 грн., дозволяють отримати ефект величиною 86129,26 грн. Відповідно до отриманих значень показників економічної ефективності можна зазначити, що запропонований підхід дозволить отримувати 1,73 економічного ефекту на 1 грн. капітальних витрат (коефіцієнт повернення інвестицій ROSI складає 1,73 грн.). Термін окупності при цьому складатиме 0,58 років.

ВИСНОВКИ

1. Наразі у зв'язку зі швидким розвитком глобальної мережі Інтернет у повсякденному житті, безпека інформаційно-комунікаційних систем і мереж стала однією з важливих проблем захисту даних та інформації від зловмисників. Одним із рішень актуальної задачі захисту ІКМ від кібератак є розробка та вдосконалення СВВ, які збирають інформацію з різних точок ІКМ, що захищається, і аналізують цю інформацію для виявлення як спроб порушення, так і реальних порушень захисту (вторгнень).

Наразі СВВ є невід'ємною частиною будь-якої сучасної системи безпеки. Особливо необхідні СВВ, які орієнтовані на виявлення аномальних станів. Вони, як правило, формують (містять) профіль нормальної (ненормальної) активності в ІКМ та детектують відхилення від нього.

2. Ефективність будь-якої СВВ залежить від методів аналізу наявної інформації про мережеві атаки, одним з яких є методи систем штучного інтелекту.

Сучасні СВВ не дозволяють враховувати всі актуальні типи атак, а також залишають місце для модифікації та покращення точності результатів ідентифікації, оскільки залежать від експертної оцінки та алгоритмів оптимізації. Застосування нечіткої логіки для виявлення мережевих атак різного типу підтверджує ефективність дослідження алгоритмів нечіткої кластеризації та більш докладного вивчення їх переваг та недоліків при виявленні аномалій на реальному мережевому трафіку.

3. Сучасні СВВ включають в себе підсистему аналізу мережевого трафіку, яка містить у собі набір аналізаторів, скомпонованих за задачами виявлення вторгнень заданого типу. Вона виконує аналіз кожного запису про потік за допомогою різних алгоритмів, найчастіше таких, які використовують методи систем штучного інтелекту. В результаті для кожного запису визначається вид з'єднання: нормальне або атака, а також вид атаки у разі її виявлення.

Запропоновано будувати інтелектуальну підсистему аналізу мережевого трафіку на основі різних алгоритмів нечіткої кластеризації: субтрактивної кластеризації та нечіткої кластеризації C-середніх.

4. Оцінка ефективності запропонованого підходу виконувалась в середовищі Matlab/Simulink. Як експериментальні дані було обрано набір даних Intrusion Detection Evaluation Dataset (CICIDS 2017).

Як метрика оцінки якості розглянутих класифікаторів використовувалась Accuracy. Встановлено, що розпізнавання нормального трафіку (Benign) відбувалось вірно у переважній більшості випадків (98-98,6 %), також з ймовірністю понад 80% відбувалось розпізнавання 10 з 14 представлених видів атак. Існує високий відсоток похибок при розпізнаванні наступних видів атак: Web attack XSS, Infiltration, Web attack-SQL injection, Heartbleed.

Встановлено, що в цілому розглянуті класифікатори показали приблизно однакові результати, але найкращим виявився класифікатор на основі алгоритму нечіткої кластеризації C-середніх.

ПЕРЕЛІК ПОСИЛАНЬ

1. Dhangar K. A Proposed Intrusion Detection System. / K. Dhangar, D. Kulhare, A. Khan. // International Journal of Computer Applications. – 2013. – Vol. 65, N 23. – P. 46-50.

2. Vijayarani S. Intrusion Detection System – A Study. / S. Vijayarani, M. Sylviaa // International Journal of Security, Privacy and Trust Management. – 2015. – Vol. 4, N 1. – P. 31-44.

3. Shaker A. Intrusion Detection System (IDS): Case Study. / A. Shaker, S. Gore // International Conference on Advanced Materials Engineering IPCSIT. – 2011. – Vol. 15. – P. 6-9.

4. Рубан І.В. Класифікація методів виявлення аномалій в інформаційних системах / І.В. Рубан, В.О. Мартовицький, С.О. Партика // Системи озброєння і військова техніка. – 2016. – № 3. – С. 100-105.

5. Колодчак О.М. Сучасні методи виявлення аномалій в системах виявлення вторгнень. / О.М. Колодчак // Вісник Національного ун-ту «Львівська політехніка». Комп'ютерні системи та мережі. – 2012. – № 745. – С. 98-104.

6. Хорошко, В.А. Методы и средства защиты информации : научное издание / В.А. Хорошко, А.А. Чекатков; Ред. Ю.С. Ковтанюк. – К. : ЮНИОР, 2003. – 505 с.

7. Кобозєва, А.А. Аналіз захищеності інформаційних систем / А.А. Кобозєва, І.О. Мачалін, В.О. Хорошко. – К. : Вид. ДУІКТ, 2010. – 316 с.

8. Жилін А.В. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А.В. Жилін, О.М. Шаповал, О.А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

9. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков. – К.: Видавнича група BHV, 2009 – 608 с.

10. Smith Z.M. The hidden costs of cybercrime. / Z.M. Smith, E. Lostri, J.A. Lewis // McAfee. – 2020. [Електронний ресурс]. – Режим доступу: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

11. Юдін О.К. Захист інформації в мережах передачі даних / О.К. Юдін, Г.Ф. Конахович, О.Г. Корченко / Підручник МОН України. – К.: Видавництво DIRECTLINE, 2009. – 714 с.

12. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. / Л.Л. Гончарова, А.Д. Возненко, О.І. Стасюк, Ю.О. Коваль. – К., 2013. – 435 с.

13. Проблеми захисту критично важливих об'єктів інфраструктури / Н. Лукова-Чуйко, В. Наконечний, С. Толюпа, Р. Зюбіна // Безпека інформаційних систем і технологій. – 2020. – № 1 (2). – С. 31-39.

14. Носенко К.М. Огляд систем виявлення атак в мережевому трафіку / К.М. Носенко, О.І. Півторак, Т.А. Ліхоузова // Міжвідомчий науково-технічний збірник «Адаптивні системи автоматичного управління». – 2014. – № 1(24). – С. 67-75.

15. Лазаренко С.В. Особливості функціонування систем виявлення атак на автоматизовані системи / С.В. Лазаренко // Сучасний захист інформації. – 2015. – №1. – С. 33-40.

16. Гулак Г.М. Модель системи виявлення вторгнень з використанням двоступеневого критерію виявлення мережевих аномалій / Г.М. Гулак, В.В. Семко, П.М. Складанний // Сучасний захист інформації. – 2015. – №4. – С. 81-85.

17. Казмірчук С. Аналіз систем виявлення вторгнень. / С. Казмірчук, А. Корченко, Т. Паращук // Захист інформації: науковий журнал. – 2018. – Т. 20, № 4. – С. 259-276.

18. Ghorbani A.A. Network Intrusion Detection and Prevention: Concepts and Techniques / A.A. Ghorbani, W. Lu, M. Tavallaee. // Springer Science & Business Media. – 2009. – 212 p.

19. Смирнов А. Имитационная модель NIPDS для обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях / А. Смирнов, Ю. Дрейс, Д. Даниленко // Ukrainian Scientific Journal of Information Security. – 2014. – Vol. 20, issue 1. – P. 29-35.

20. Довбешко С.В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак / С.В. Довбешко, С.В. Толюпа, Я.В. Шестак // Сучасний захист інформації. – 2019. – №1(37). – С. 6-15.

21. Корнієнко В.І. Інтелектуальне моделювання нелінійних динамічних процесів в системах керування, кібербезпеки, телекомунікацій: підручник / В.І. Корнієнко, О.Ю. Гусєв, О.В. Герасіна; за заг. ред. В.І. Корнієнка ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2020. – 536 с. – ISBN 978-966-350-735-4.

22. Bonabeau Eric. Swarm Intelligence: From Natural to Artificial Systems / Eric Bonabeau, Marco Dorigo, Guy Therauaz. – NY: Oxford University Press Inc. – 1999. – 306 p.

23. Haykin S. Neural Networks and Learning Machines / S. Haykin. – Prentice Hall. – 2009. – 906 с.

24. Штовба С.Д. Machine learning: стартовий курс : електронний навчальний посібник / С.Д. Штовба, О.М. Козачко. – Вінниця : ВНТУ, 2020. – 81 с.

25. Bache K. UCI Machine Learning Repository / Bache K. Lichman M.. Irvine: University of California, School of Information and Computer Science. 2014. [Електронний ресурс]. – Режим доступу: http://archive.ics.uci.edu/ml.

26. Frank J. Artificial intelligence and intrusion detection: Current and future directions / J. Frank // Proceedings of the 17 th National Computer Security Conference, October, 1994.

27. Yang H. Clustering and classification based anomaly detection / H. Yang, F. Xie, Y. Lu // Fuzzy Systems and Knowledge Discovery – 2006. – Vol. 4223. – P. 1082–1091.

28. Tajbakhsh A. Intrusion detection using fuzzy association rules / A. Tajbakhsh, M. Rahmati, A. Mirzaei // Applied Soft Computing – 2009 – Vol. 9. – No. 2. – P. 462.

29. Tsai C.F., Hsub Y.F., Linc C.Y., Lin W.Y. Intrusion detection by machine learning: A review // Expert Systems with Applications. – 2009. – Vol. 36. Issue 10. – P. 11994-12000.

30. Нейрокомпьютеры и интеллектуальные роботы / Под ред. Н. М. Амосова. – Киев.: Наукова думка, 1991. – 412 с.

31. Ротштейн А. П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети / А. П. Ротштейн. – Винница: «УНІВЕРСУМ-Вінниця», 1999. – 320 с.

32. Nelles O. Nonlinear System Identification: From Classical Approaches to Neural and Fuzzy Models / O. Nelles. – Berlin: Springer, 2001. – 785 pp.

33. Найбільші кібератаки 2022: під прицілом — енергетика, держустанови та корпорації. [Електронний ресурс]. – Режим доступу: https://www.eset.com/ua/about/newsroom/press-releases/malware/krupneyshie-kiberataki-2022-pod-pricelom-energetika-gosuchrezhdeniya-i-korporacii/.

34. Загроза Industroyer: кіберзброя для атак на електромережу. [Електронний ресурс]. – Режим доступу: https://www.eset.com/ua/about/newsroom/press-releases/malware/ugroza-industroyer-kiberoruzhiye-dlya-atak-na-elektroset/.

35. Industroyer: нова загроза для систем управління виробничими процесами. [Електронний ресурс]. – Режим доступу: https://www.eset.com/ua/about/newsroom/press-releases/malware/industroyer-novaya-ugroza/

36. Поширені APT-загрози 2022: Україна залишається головною ціллю кібершпигунів. [Електронний ресурс]. – Режим доступу: https://www.eset.com/ua/about/newsroom/press-releases/malware/rasprostranennyye-apt-ugrozy-2022-ukraina-ostaetsya-glavnoy-celyu-kibershpionov/.

37. AcidRain | A Modem Wiper Rains Down on Europe. [Електронний ресурс]. – Режим доступу: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/.

38. A Mysterious Satellite Hack Has Victims Far Beyond Ukraine. [Електронний ресурс]. – Режим доступу: https://www.wired.co.uk/article/viasat-internet-hack-ukraine-russia.

39. U.S. officials link North Korean hackers to $615 million cryptocurrency heist. [Електронний ресурс]. – Режим доступу: https://www.cnbc.com/2022/04/15/ronin-hack-north-korea-linked-to-615-million-crypto-heist-us-says.html.

40. Ransomware gang threatens to release stolen Medibank data. [Електронний ресурс]. – Режим доступу: https://www.bleepingcomputer.com/news/security/ransomware-gang-threatens-to-release-stolen-medibank-data/.

41. Аналіз систем та методів виявлення несанкціонованих вторгнень у комп'ютерні мережі / Литвинов В.В., Стоянов Н., Скітер І.С., Трунова О.В., Гребенник А.Г. // Інформаційні і телекомунікаційні технології: Математичні машини і системи. – 2018. – №1. – С. 31-40.

42. Denning D.E. Requirements and model for IDES-A real-time intrusion detection system : Technical Report / D.E. Denning, P.G. Neumann // Computer Science Laboratory, SRI International, Menlo Park, CA. – 1985. – 157 p.

43. Субач І.Ю. Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі / І.Ю. Субач І., В.В. Фесьоха, Н.О. Фесьоха // Information Technology and Security. – January-June 2017. – Vol. 5. – Iss. 1 (8). – P. 29-41.

44. Rao C. Handbook of Statistics: Machine Learning: Theory and Applications, // C. Rao, V. Govindaraju. – Oxford: North Holland & IFIP, 2013. – 552 с.

45. Кравченко С.М. Методи класифікації машинного навчання з використанням бібліотеки Scikit-Learn / С.М. Кравченко, Є.О. Гришкун, О.В.

Власенко // Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки. – 2020. – № 31 (70). – С. 121-125.

46. Intrusion Detection Evaluation Dataset (CIC-IDS 2017) // Canadian Cybersecurity Institute. [Електронний ресурс]. – Режим доступу: https://unb.ca/cic/datasets/ids-2017.html.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	**Формат**	**Найменування**	**Кількість листів**	**Примітки**
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	3	
5	А4	Стан питання. Постановка задачі	33	
6	А4	Спеціальна частина	11	
7	А4	Економічний розділ	10	
8	А4	Висновки	2	
9	А4	Перелік посилань	6	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація Поліно.ppt

2 Диплом Поліно.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-19-2 Поліно І.О.

на тему: «Виявлення аномалій мережевого трафіку з використанням алгоритмів нечіткої кластеризації»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 76 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на дослідження алгоритмів нечіткої кластеризації, що дозволяють виконувати виявлення аномалій трафіку в інформаційно-комунікаційних мережах.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу найбільших кібератак в Україні і світі у 2022 році, існуючих рішень запобігання вторгненням в інформаційно-комунікаційні мережі, а також основ нечіткої логіки і нечіткої кластеризації в ній сформульовано задачі, вирішенню яких присвячений спеціальний розділ. У ньому було запропоновано підхід до виявлення аномалій трафіку в інформаційно-комунікаційних мережах за допомогою алгоритмів нечіткої кластеризації та оцінено його ефективність.

Практична цінність роботи полягає у тому, що запропоновані рішення можуть бути використані в засобах моніторингу, здатних аналізувати трафік мережі в режимі реального часу.

До недоліків роботи слід віднести недостатню проробку окремих питань.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Поліно І.О. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доцент **О.В. Герасіна**