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 магістра

студента *Старостенка Андрія Олександровича*

академічної групи *125м-21-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації*

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

Дніпро
2022

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

«_____»_____2022 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту *Старостенку Андрію Олександровичу* **академічної групи** *125м-21-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації*

затверджену наказом ректора НТУ «Дніпровська політехніка» від 31.10.2022 № 1200-с

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз сучасних систем виявлення вторгнень і атак, основ нечіткої логіки та алгоритмів нечіткої кластеризації, а також існуючих наборів даних для оцінки виявлення мережевих атак.	03.09.2022 – 10.10.2022
Розділ 2	Розробка підходу до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі та оцінка його ефективності.	11.10.2022 – 24.11.2022
Розділ 3	Розрахунки капітальних витрат, економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень.	25.11.2022 – 04.12.2022

Завдання видано _____ Мацюк С.М.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Старостенко А.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 88 с., 15 рис., 7 табл., 4 додатки, 53 джерела.

Об’єкт дослідження – мережевий трафік.

Предмет дослідження – підхід до виявлення мережевих атак з використанням алгоритмів нечіткої кластеризації.

Мета кваліфікаційної роботи – дослідження та обґрунтування алгоритмів нечіткої кластеризації, що дозволяють виконувати класифікацію вхідного трафіку мережі для ідентифікації різних інцидентів кібербезпеки.

Наукова новизна результатів полягає у тому, що було запропоновано виявляти атаки в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації; при цьому параметри цих інтелектуальних класифікаторів було налаштовано методом Фібоначчі.

У першому розділі проаналізовано сучасні системи виявлення вторгнень і атак в інформаційно-комунікаційних системах і мережах, основи нечіткої логіки та алгоритми нечіткої кластеризації, а також існуючі набори даних для оцінки виявлення мережевих атак.

У спеціальній частині роботи запропоновано підхід до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі 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.

СУБТРАКТИВНА КЛАСТЕРИЗАЦІЯ, МЕРЕЖЕВИЙ ТРАФІК, КЛАСТЕРИЗАЦІЯ С-СЕРЕДНІХ, СИСТЕМИ ВИЯВЛЕННЯ АТАК, НЕЧІТКА ЛОГІКА, ВИЯВЛЕННЯ МЕРЕЖЕВИХ АНОМАЛІЙ, МЕТОД ФІБОНАЧЧІ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

ABSTRACT

Explanatory note: p. 88, fig. 15, tab. 7, 4 additions, 53 sources.

The object of research is network traffic.

The subject of the study is an approach to detecting network attacks using fuzzy clustering algorithms.

The purpose of the qualification work is research and justification of fuzzy clustering algorithms, which allow classification of incoming network traffic to identify various cyber security incidents.

The scientific novelty of the results is that it was proposed to detect attacks in information and communication networks using fuzzy clustering algorithms; at the same time, the parameters of these intelligent classifiers were adjusted using the Fibonacci method.

The first chapter analyzes modern intrusion and attack detection systems in information and communication systems and networks, the basics of fuzzy logic and fuzzy clustering algorithms, as well as existing data sets for evaluating the detection of network attacks.

In a special part of the work, an approach to detecting attacks in information and communication networks using fuzzy clustering algorithms and the Fibonacci method 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.

SUBTRACTIVE CLUSTERIZATION, NETWORK TRAFFIC, C-AVERAGE CLUSTERIZATION, ATTACK DETECTION SYSTEMS, FUZZY LOGIC, NETWORK ANOMALIES DETECTION, FIBONACCI METHOD, SIMULATION MODELING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – Автоматизована система;

ІАД – Інтелектуальний аналіз даних;

ІКМ – Інформаційно-комунікаційна мережа;

ОС – Операційна система;

ПЗ – Програмне забезпечення;

СВА – Системи виявлення атак;

СВВ – Системи виявлення вторгнень;

DDoS attack – Distributed Denial of Service attack – Розподілена атака на відмову в обслуговуванні;

IDS – Intrusion Detection System – Система виявлення вторгнень;

IPS – Intrusion Prevention System – Система запобігання вторгненням.

ЗМІСТ

с.

ВСТУП ... 8

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ ... 11

1.1 Аналіз сучасних систем виявлення вторгнень і атак в інформаційно-комунікаційних системах і мережах ... 11

1.1.1 Історія розробок систем виявлення вторгнень і атак ... 11

1.1.2 Архітектура та основні характеристики систем виявлення вторгнень і атак ... 14

1.1.3 Класифікація систем виявлення вторгнень і атак ... 18

1.1.4 Недоліки сучасних систем виявлення вторгнень і атак ... 25

1.2 Нечітка кластеризація ... 27

1.2.1 Нечітка логіка ... 27

1.2.2 Кластерний аналіз ... 29

1.2.3 Нечітка кластеризація С-середніх ... 35

1.2.4 Субтрактивна кластеризація ... 39

1.2.5 Ефективність систем з нечіткою логікою ... 40

1.2.6 Реалізація алгоритмів нечіткої кластеризації в середовищі MATLAB/Simulink ... 42

1.3 Існуючі набори даних для оцінки виявлення мережевих атак ... 46

1.4 Висновок. Постановка задачі ... 51

2 СПЕЦІАЛЬНА ЧАСТИНА ... 55

2.1 Підхід до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі ... 55

2.2 Оцінка ефективності запропонованого підходу до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі ... 59

2.3 Висновок ... 64

3 ЕКОНОМІЧНИЙ РОЗДІЛ 66
3.1 Розрахунок капітальних (фіксованих) витрат 66
3.2 Розрахунок поточних витрат 69
3.3 Оцінка можливого збитку 71
3.4 Загальний ефект від впровадження системи інформаційної безпеки 73
3.5 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки 74
3.6 Висновок 75
ВИСНОВКИ 76
ПЕРЕЛІК ПОСИЛАНЬ 78
ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи 84
ДОДАТОК Б. Перелік документів на оптичному носії 85
ДОДАТОК В. Відгук керівника економічного розділу 86
ДОДАТОК Г. Відгук керівника кваліфікаційної роботи 87

ВСТУП

Для безпеки сучасних інформаційно-комунікаційних мереж (ІКМ) застосовуються так звані системи виявлення (Intrusion Detection System – IDS) та запобігання (Intrusion Prevention System – IPS) вторгнень (СВВ). В основі їх функціонування лежить збір, аналіз та обробка інформації про події, пов'язані з безпекою ІКМ, що захищається, накопичення отриманих даних, моніторинг мережевої активності окремих служб і сервісів, прийняття рішення про стан системи, що захищається з виявленням і можливою протидією несанкціонованого використання інфокомунікаційних ресурсів [1-10].

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.

Таким чином, важливим напрямом у вдосконаленні СВВ є дослідження аномалій (Anomaly-Based Intrusion Detection and Prevention Systems – AB IDPS) ІКМ, в основу якого може бути покладений статистичний аналіз мережевого трафіку. За такого підходу СВВ визначає «нормальну» мережну активність окремих служб та інформаційних сервісів ІКМ, після чого весь трафік, що не підпадає під визначення «нормального» позначається як «аномальний».

Головною перевагою статистичних методів СОПВ є можливість вивчати (моніторити) мережевий трафік і відрізняти «нормальну» мережеву активність від «аномальної». Крім того, існує можливість самонавчання, самоналаштовування, тобто первинний моніторинг мережевої активності ІКМ

може проводитися періодично (за відсутності вторгнень) із коригуванням порогових величин і критеріїв прийняття рішень про перехід системи в невстановлений («аномальний») режим функціонування. Все це в сукупності робить статистичну СВВ набагато гнучкішою за сигнатурну, дає їй можливість без відомих сигнатур вторгнень виявляти та запобігати новим, ще невідомим атакам та мережевим вірусам.

Наразі світ переживає інтенсивний розвиток штучного інтелекту, Інтернету речей (IoT) та великих даних (big data). Під час створення систем виявлення вторгнень і атак широко використовують штучний інтелект, машинне навчання, експертні системи тощо. Безліч параметрів для виявлення атак в ІКМ становить значний обсяг даних, що визначає можливість їх обробки саме методами штучного інтелекту [8-10].

Актуальність методів систем штучного інтелекту (нейронних мереж, систем нечіткого висновку, еволюційного моделювання, агентських алгоритмів оптимізації) при вирішенні питань в галузі кібербезпеки обумовлена здатністю інтелектуальних методів розв'язувати оптимізаційні задачі, які погано формалізуються, а також використанням для моделювання ефективних і універсальних апроксиматорів. Оскільки нейронні мережі та системи з нечіткою логікою є універсальними ефективними апроксиматорами, то побудовані на їх основі моделі ефективні для вирішення задач класифікації (до яких відноситься і виявлення мережевих атак) [11-13].

Таким чином, дослідження, розробка і вдосконалення підходів до виявлення мережевих атак з використанням методів систем штучного інтелекту наразі є актуальною задачею.

Метою роботи є дослідження та обґрунтування алгоритмів нечіткої кластеризації, що дозволяють виконувати класифікацію вхідного трафіку мережі для ідентифікації різних інцидентів кібербезпеки.

Постановка задачі:

• провести аналіз сучасних систем виявлення вторгнень і атак в інформаційно-комунікаційних системах і мережах;

• провести аналіз основ нечіткої логіки та алгоритмів нечіткої кластеризації;

• проаналізувати існуючі набори даних для оцінки виявлення мережевих атак;

• запропонувати підхід до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі;

• оцінити ефективність запропонованого підходу.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз сучасних систем виявлення вторгнень і атак в інформаційно-комунікаційних системах і мережах

1.1.1 Історія розробок систем виявлення вторгнень і атак

За всю свою історію системи виявлення вторгнень і атак (Intrusion Detection Systems – IDS) зазнали еволюційних змін, які відбивалися як на структурі, так і на їхньому функціональному призначенні. Уперше термін «виявлення атак» був запроваджений Джеймсом Андерсеном (James Anderson) у його роботі «Моніторинг та контроль загроз інформаційній безпеці», опублікованій у 1980 р. У цій роботі їм була висловлена гіпотеза про можливість виявлення погроз безпеки за допомогою збору та аналізу інформації, що міститься у журналах аудиту операційних систем [19].

Результати роботи Андерсена отримали розвиток у дослідженнях Дороті Денніг (Dorothy Denning), проведених у 1983 р. на замовлення уряду США в рамках компанії SRI International. Основне завдання цих досліджень полягало у розробці методів аналізу журналів аудиту мейнфреймів з метою створення профілів штатної роботи користувачів. Такі профілі призначались для виявлення штатних і несанкціонованих дії користувачів. У 1984 р. Д. Денніг було опубліковано відому роботу «Модель виявлення вторгнення», в якій описувались основні підходи до створення системи виявлення атак. У цьому ж році Дороті Денніг та Пітер Нойманн розробили так звану IDES (Intrusion Detection Expert System). Ця система використовувала статистичні методи, які дозволяли описати профіль штатних та несанкціонованих дій користувачів. Надалі вона була доопрацьована і названа як система NIDES (Next-Generation Intrusion Detection Expert System).

У 1988 р. у мережі Інтернет була зафіксована перша великомасштабна інформаційна атака, що отримала назву «Інтернет-хробак Морріса». Внаслідок

цього інциденту було інфіковано понад 2000 вузлів, що призвело до великих фінансових та матеріальних втрат. Ця подія, безумовно, сколихнула інтерес до проблеми захисту від атак і цього року співробітники лабораторії Lawrence Livermore Laboratories Каліфорнійського університету розробили на замовлення військово-повітряних сил США новий варіант СВА. Ця система дозволяла здійснювати пошук заданих шаблонів у вмісті журналів аудиту, що зберігаються на серверах автоматизованої системи (АС). У 1989 р. співробітники, які працювали над цією системою, утворили комерційну компанію «Haystack Labs», що випустила першу комерційну СВА, що отримала назву «Stalker».

У 1988 р. у Національному центрі комп'ютерної безпеки було розроблено ще одну версію СВА – MIDAS (Multics Intrusion Detection and Alerting System). Ця система призначалася для виявлення інформаційних атак у АС даного центру, яка була побудована на основі операційної системи (ОС) Multics та базувалася на апаратній платформі DPS 8/70. Для виявлення атак система MIDAS також використовувала статистичні методи аналізу.

У 1990 р. ще один дослідник з каліфорнійського університету Тод Геберляйн вперше розробив дослідний зразок СВА, який дозволяв виявляти інформаційні атаки на основі аналізу мережевих пакетів даних, а не журналів аудиту. Система отримала назву NSM (Network Security Monitor) та була встановлена у великій кількості урядових організацій. Поява цієї системи активізувала роботи у галузі виявлення атак.

У 1990 р. національна лабораторія Лос-Аламоса розробила СВА NADIR (Network Anomaly Detection and Intrusion Reporter) для захисту корпоративної обчислювальної мережі. Ця система забезпечувала можливість виявлення атак за допомогою аналізу вмісту журналів аудиту, які велися на серверах та робочих станціях АС.

У першій половині 1990-х технічний центр Cryptologic Support Center військово-повітряних сил США розробив систему автоматичного моніторингу безпеки ASIM (Automated Security Measurement System), яка призначалася для

аналізу мережевого трафіку, що циркулює у рамках військового відомства. Це була перша система, реалізована як програмно-апаратний комплекс. Крім того, система ASIM мала кращу масштабованість, порівняно з іншими аналогічними системами того часу. Система ASIM і досі використовується у декількох підрозділах військово-повітряних сил США для моніторингу мережевого трафіку. У 1995 р. дослідники, які працювали над проектом ASIM, організували власну комерційну компанію Wheel Group, яка випустила у світ СВА NetRanger.

У 1991 р. на замовлення низки урядових організацій США була створена розподілена СВА DIDS (Distributed Intrusion Detection System). Вона стала першою системою, яка дозволяла одночасно збирати та аналізувати інформацію про мережевий трафік, а також дані з журналів аудиту хостів АС. Для виявлення атак у системі використовувалася експертна система, написана мовою програмування Пролог.

У 1994 р. в одній з наукових лабораторій військово-морських сил США Стівеном Норткаттом було розроблено систему Shadow. Відмінною особливістю цієї системи було те, що вона базувалася на програмних утилітах, таких як tcpdump та OpenSSH. Згодом ця система була перетворена на загальнодоступний проект з відкритими вихідними текстами.

Незважаючи на те, що комерційні зразки СВА вже існували на початку 1990-х рр. ринок такого роду систем вийшов на рівень рентабельності тільки до 1997 р. Саме цього року була представлена перша версія системи «RealSecure» компанії ISS, що займала досить довго домінуюче положення у сегменті СВА. У 1998 р. компанія Cisco Systems купує Wheel Group і починає постачати СВА NetRanger від свого імені.

Ще однією знаковою подією в історії СВА стала розробка СВА «Snort» з відкритими вихідними текстами. Ця система була створена Марті Роеш у 1998 р. Система «Snort» набула великої популярності, коли у 2000 р. вона була портована на платформі Windows Міхаелем Девісом. Наразі ця СВА є найпоширенішою системою серед проектів Open-Source. Більш того, система

Snort послужила основою для створення багатьох комерційних програмних комплексів виявлення атак.

У 2000 р. кілька невеликих інноваційних компаній, таких як Okena та Entercept, розробили нові версії СВА, які дозволяли не тільки виявляти, а й запобігати інформаційним атакам. Цей тип засобів захисту був названий системами запобігання вторгненням (IPS – Intrusion Prevention Systems). Надалі компанія Okena була придбана Cisco Systems, а Entercept – Network Associates. Інші виробники СВА також почали поступово доопрацьовувати свої продукти шляхом оснащення їх функціями запобігання атакам. Цьому також сприяв звіт компанії Gartner, опублікований у 2003 р., в якому констатувалась неефективність існуючого покоління СВА та прогнозувався їх неминучий перехід до функціоналу систем запобігання вторгненням.

У 2000 р. було розпочато дослідження, спрямовані на розробку механізмів виявлення вторгнень і атак, пов'язаних з несанкціонованими діями внутрішніх користувачів інформаційно-комунікаційних мереж (ІКМ). Їх актуальність була обумовлена тим, що багато інформаційних атак реалізуються не зовнішніми, а внутрішніми порушниками. Наразі на ринку інформаційної безпеки вже представлено декілька таких комерційних продуктів, які дозволяють доповнити засоби розмежування доступу, що вже використовуються в АС.

Наразі на ринку інформаційної безпеки активно працює кілька десятків компаній та організацій, які займаються розробкою та постачанням СВА та СВВ. Серед основних гравців цього ринку можна назвати компанії Cisco Systems, ISS, eEye Digital Security, Jupiter Networks та інші.

1.1.2 Архітектура та основні характеристики систем виявлення вторгнень і атак

З урахуванням сучасного рівня розвитку технології виявлення вторгнень СВА можна визначити наступним чином. СВА – це спеціалізовані програмні

або програмно-апаратні комплекси, призначені для виявлення інформаційних атак на ресурси ІКМ за допомогою збору та аналізу даних про події, що реєструються в системі [20-22].

Узагальнена структура СВА представлена на рис. 1.1 і включає наступні компоненти:

• модулі-датчики, призначені для збору необхідної інформації про функціонування ІКМ; іноді датчики також називають сенсорами;

• модуль виявлення атак, що виконує аналіз даних, зібраних датчиками, з метою виявлення інформаційних атак;

• модуль реагування на виявлені атаки;

• модуль зберігання даних, в якому міститься вся конфігураційна інформація, а також результати роботи засобів виявлення атак;

• модуль управління компонентами засобів виявлення атак.

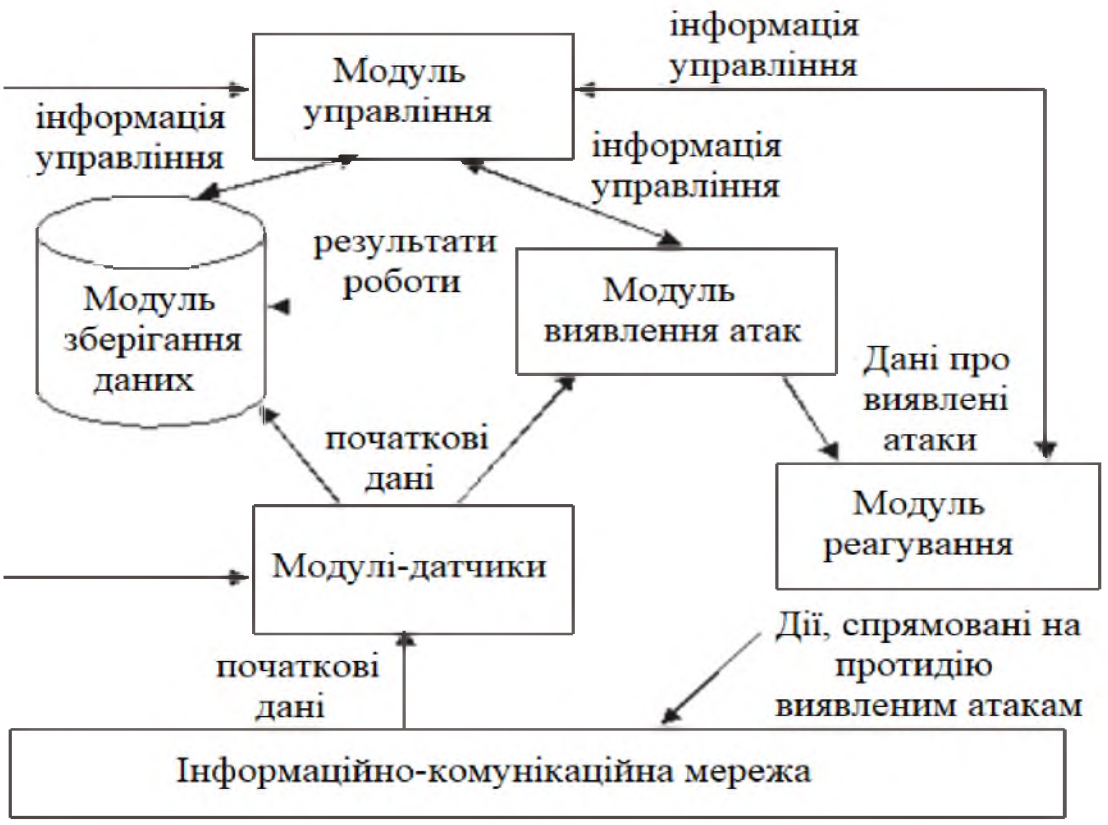


Рисунок 1.1 – Типова архітектура системи виявлення атак

СВА можуть включати два типи датчиків – мережеві і хостові. Мережеві датчики призначені для збору інформації про всі пакети даних, що передаються в рамках мережевого сегмента, де встановлений датчик. Мережеві датчики реалізуються у вигляді окремого програмно-апаратного блоку, що підключається до сегмента ІКМ. Хостові датчики встановлюються на робочі станції або сервери АС і збирають інформацію про всі події, що відбуваються на цих вузлах системи. Як правило, більшість існуючих СВА використовують обидва типи датчиків для того, щоб була можливість збору максимального обсягу даних, необхідного для виявлення атак.

Інформація, зібрана мережевими та хостовими датчиками, надходить у модуль виявлення атак СВА, в якому вона обробляється з метою виявлення подій, пов'язаних з порушенням інформаційної безпеки.

Після виявлення в ІКМ атаки СВА має можливість зробити певні дії у відповідь, за реалізацію яких відповідає модуль реагування СВА. При цьому модуль може використовувати як пасивні, так і активні методи реагування. До пасивних методів відноситься сповіщення адміністратора безпеки про виявлені атаки, а до активних – виконання дій, спрямованих на блокування виявленої атаки.

Результати роботи СВА записуються в сховище системи, якою може бути звичайний текстовий файл чи реляційна СУБД. Наразі, як правило, для зберігання інформації в СВА використовують СУБД, які добре зарекомендували себе, такі як Microsoft SQL Server, Oracle, Access та інші.

Управління компонентами СВА може виконуватися віддаленим чи локальним способом в залежності від використання тієї чи іншої системи. Локальне управління здійснюється безпосередньо з того вузла, на якому встановлено компонент СВА, а віддалене – за допомогою команд, що посилаються каналами зв'язку.

При цьому можна виділити два різні варіанти віддаленого управління. Перший варіант є більш простим і припускає, що модуль управління безпосередньо взаємодіє з іншими компонентами СВА. Перевагою такої схеми

управління є простота реалізації. Однак такий варіант взаємодії не має властивості масштабованості і може ефективно взаємодіяти тільки при невеликій кількості компонентів СВА, розміщених в АС. Це пов'язано з тим, що зі збільшенням числа компонентів СВА у комп'ютера з встановленим модулем управління може не вистачити обчислювальних ресурсів для виконання функцій модуля. Для вирішення цієї проблеми може використовуватись альтернативна схема, в якій модуль управління обмінюється службовою інформацією з іншими компонентами СВА через один або декілька проміжних серверів. Даний варіант є більш гнучким, оскільки дозволяє рівномірно розподілити навантаження між декількома серверами управління.

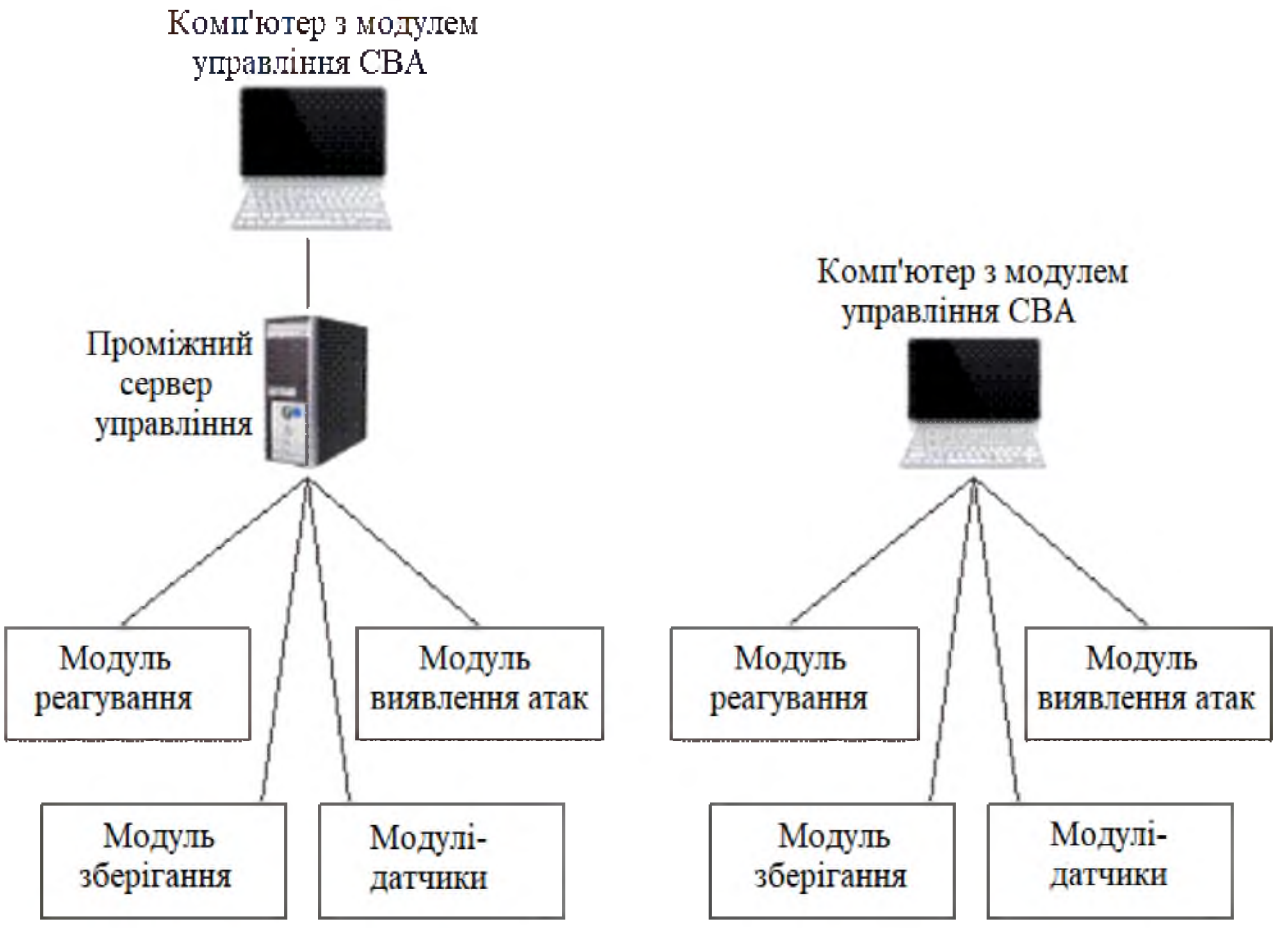


Рисунок 1.2 – Можливі варіанти віддаленого управління компонентами

Функціональні модулі, з яких складається СВА, можуть реалізовуватися як окремі програмні компоненти чи об'єднуватись у єдиний комплекс. Крім того, СВА може включати декілька модулів одного і того ж типу. Так, наприклад, до складу СВА може бути включено декілька різних модулів-датчиків, кожен з яких відповідає за збирання інформації певного типу.

1.1.3 Класифікація систем виявлення вторгнень і атак

Системи виявлення вторгнень та атак прийнято класифікувати за сферою застосування. Виділяють такі типи IDS:

• Network Intrusion Detection System (NIDS) – системи, що аналізують мережевий трафік з метою виявлення шкідливої активності. На відміну від міжмережевих екранів, NIDS виконують моніторинг як вхідного, так і внутрішнього мережевого трафіку.

• Host Intrusion Detection System (HIDS) – інструменти, що контролюють роботу окремих пристроїв. Зазвичай HIDS фіксує стан усіх файлів, розміщених на кінцевій точці, та інформує адміністратора про видалення або зміну системних об'єктів. Крім того, цей вид IDS перевіряє всі пакети даних, що передаються на пристрій або з нього.

• Protocol-based Intrusion Detection System (PIDS) – система перевірки даних, що передаються за протоколом HTTP / HTTPS. Зазвичай PIDS застосовується для захисту веб-серверів та контролює трафік, що передається між пристроєм користувача та інтернет-ресурсом.

• Application Protocol-based Intrusion Detection System (APIDS) – система виявлення вторгнень, що контролює пакети, які передаються за певним протоколом прикладного рівня – наприклад, заданим для звернення до бази даних SQL.

• Hybrid Intrusion Detection System – гібридна система для комплексного виявлення шкідливої активності, що поєднує властивості двох або більше з перелічених вище типів, наприклад NIDS і HIDS.

Класифікація систем виявлення атак за принципом реалізації наведена на рис. 1.3.

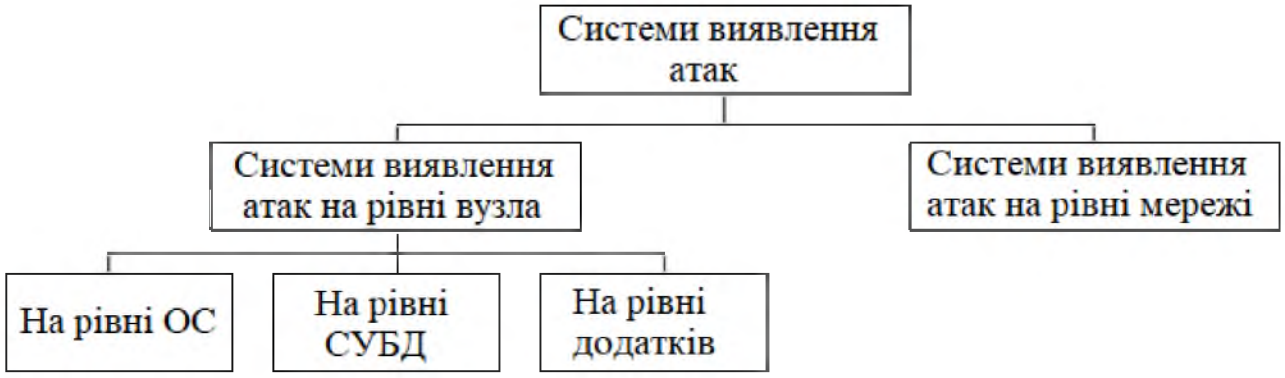


Рисунок 1.3 – Класифікація СВА за принципом реалізації

Класифікація систем виявлення атак за методом виявлення загроз наведена на рис. 1.4 [23].

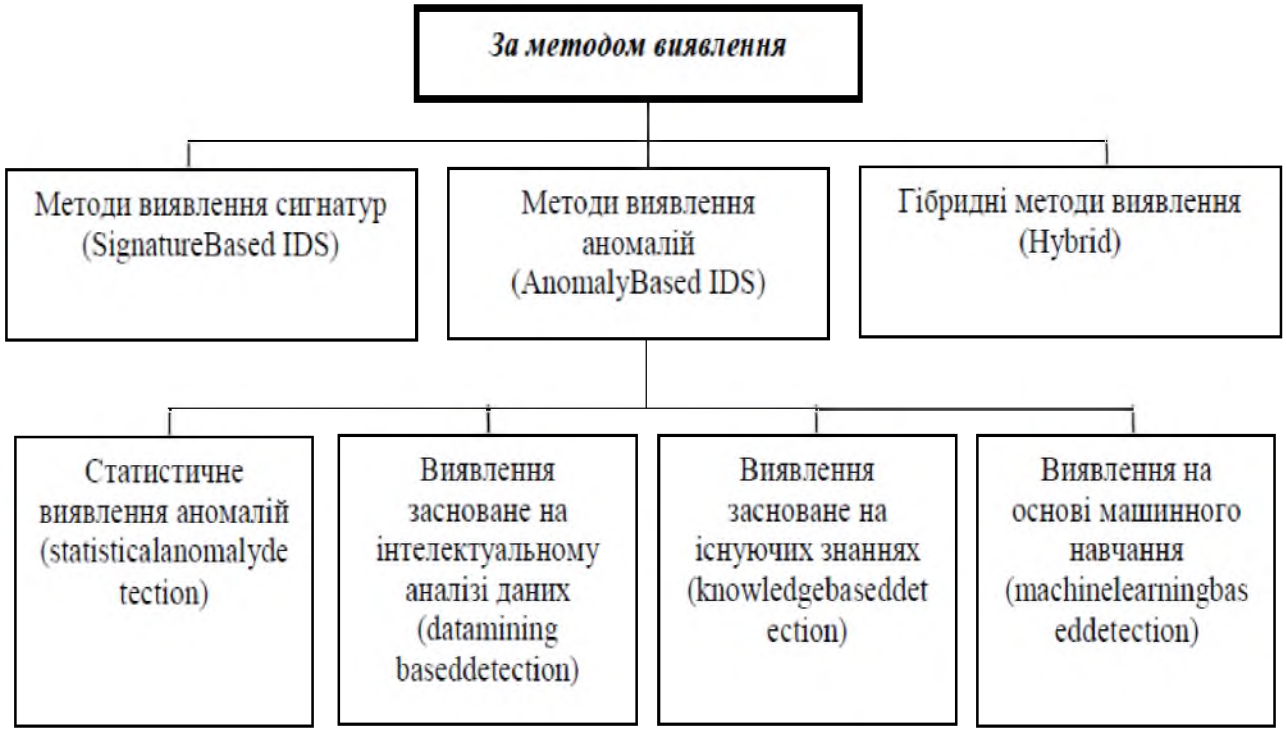


Рисунок 1.4 – Класифікація СВА за методом виявлення загроз

Історично прийнято розділяти системи виявлення атак на ті, що засновані на використанні методу виявлення сигнатур, і ті, що базуються на використанні методу виявлення аномалій. У цьому сходяться думки майже всіх науковців, що працюють над класифікацією СВА. Проте розбіжності спостерігаються далі, коли принципи, що належать конкретно до методів виявлення аномалій ставлять в один ряд з іншими, що є некоректним. У свою чергу найточнішу класифікацію СВА заснованих на методах виявлення аномалій було представлено у роботах [24-25].

Особливістю технології виявлення вторгнень на основі сигнатур є процес опису вторгнень у вигляді шаблону або сигнатури і пошуку даного шаблону в контрольованому просторі (наприклад, мережевому трафіку або журналі реєстрації). Така СВА може виявити всі відомі вторгнення (атаки), але вона мало пристосована для виявлення нових, ще невідомих, атак [1-10, 19-31].

При розробці СВА, заснованих на цьому підході, виникають дві основні проблеми. Перша полягає у створенні механізму опису сигнатур, тобто мови опису атак, а друга проблема виражається в наступному: як записати атаку, щоб зафіксувати всі можливі її модифікації? Схема технології виявлення атак на основі сигнатур показана на рис. 1.5.

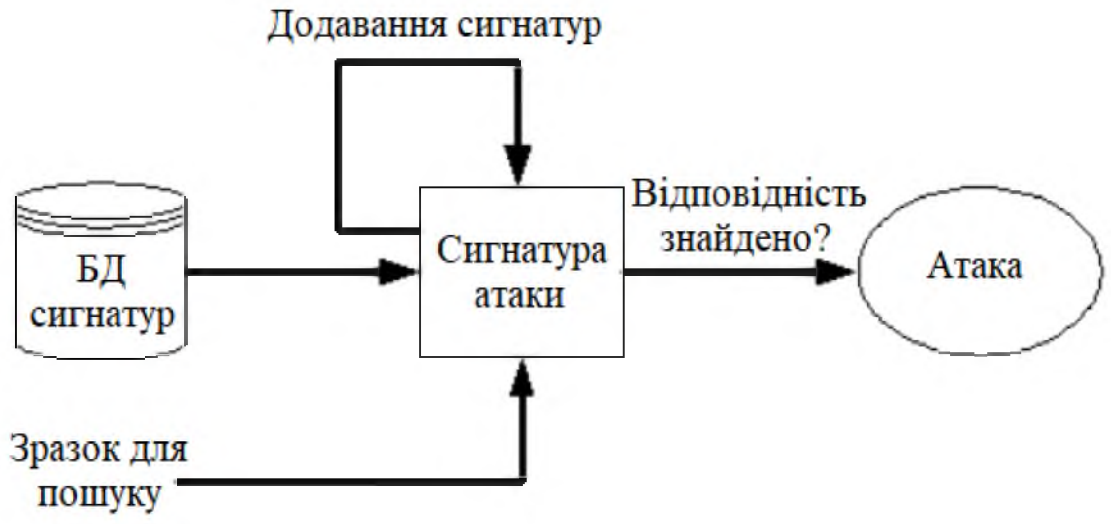


Рисунок 1.5 – Схема виявлення вторгнень на основі сигнатур

Виявлення вторгнень на основі аномалій побудоване на припущенні, що аномальна поведінка суб'єкта інформаційної системи (ІС), тобто, як правило, атака або яка-небудь ворожа дія часто проявляється як відхилення від нормальної поведінки. Зазвичай системи виявлення аномальної активності використовують як джерело даних журнали реєстрації і поточну діяльність користувача.

Традиційне використання цієї технології полягає не в чіткому виявленні атак, а у визначенні підозрілої активності, що відрізняється від нормальної. Основна проблема методу полягає в тому, щоб визначити критерій нормальної активності. Необхідно також встановити допустимі відхилення від нормального трафіку, які ще не вважатимуться атакою.

При використанні технології виявлення вторгнень на основі аномалій можливі два варіанти неправильного виявлення атаки:

• виявлення дії, яка не є атакою, і віднесення його до класу атак;

• пропуск атаки, яка не підпадає під сигнатури атак (цей випадок більш небезпечний, ніж помилкове віднесення дозволеного дії до класу атак).

Іноді елементи такого аналізу зустрічаються і в інших методах, скажімо, в розшифровці протоколу, коли виявлений елемент, що не належить наперед визначеному протоколу або порушує правила використання протоколів. Схема типової системи виявлення аномалій показана на рис. 1.6.

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.

Отже, наразі методи виявлення аномалій є пріоритетними у побудові СВА. Найпопулярнішими серед них можна виділити чотири підгрупи, а саме (див. рис. 1.4):

• статичне виявлення аномалій,

• виявлення засноване на інтелектуальному аналізі даних,

• виявлення засноване на існуючих знаннях,

• виявлення на основі машинного навчання.

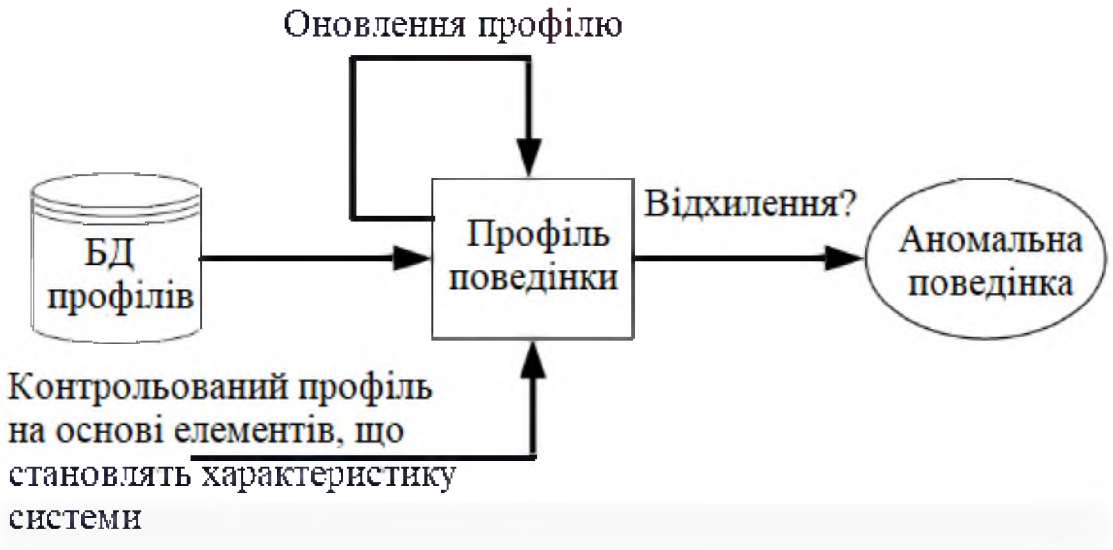


Рисунок 1.6 – Схема виявлення вторгнень на основі аномалій

Також у більшості класифікацій відсутні гібридні методи (див. рис. 1.4), які наразі стрімко досліджуються і являють собою синтез сигнатурного методу і методу виявлення аномалій.

Розвиток СВВ і СВА на основі аномалій складається з двох етапів: навчання та тестування.

На етапі навчання використовується звичайний профіль дорожнього руху для вивчення моделі нормальної поведінки, а потім на етапі тестування використовується новий набір даних для встановлення здатності системи узагальнювати до раніше невидимих вторгнень. СВВ і СВА на основі аномалій можна класифікувати на ряд категорій на основі методу, що використовується для навчання, наприклад, на статистичній основі, на основі знань та на основі машинного навчання.

Головною перевагою СВВ на основі аномалій є можливість ідентифікувати атаки нульового дня через те, що розпізнавання ненормальної активності користувачів не покладається на базу даних підписів. Така СВВ

викликає сигнал небезпеки, коли досліджувана поведінка відрізняється від звичайної поведінки.

Також СВВ на основі аномалій мають різні переваги. По-перше, вони мають можливість виявляти внутрішні шкідливі дії. Якщо зловмисник починає робити транзакції в викраденому обліковому записі, які не ідентифіковані під час типової діяльності користувача, це створює сигнал тривоги. По-друге, кіберзлочинцю дуже важко розпізнати, що є нормальною поведінкою користувача, не видаючи попередження, оскільки система побудована з індивідуальних профілів.

У табл. 1.1 представлені відмінності між СВВ і СВА на основі сигнатур та на основі аномалій. Як вже зазначалось вище, СВВ і СВА на основі сигнатур можуть ідентифікувати лише добре відомі вторгнення, тоді як СВВ і СВА на основі аномалій можуть виявити напади нульового дня.

Таблиця 1.1 – Відмінності між СВВ на основі сигнатур та аномалій

	Переваги	**Недоліки**
СВВ на основі сигнатур	• Дуже ефективні при виявленні вторгнень з мінімальним числом помилкових тривог. • Оперативно виявляють вторгнення. • Покращені для виявлення відомих атак. • Простий дизайн.	• Потрібно часто оновлювати новий підпис. • Призначені для виявлення атак на відомі підписи. Коли попереднє вторгнення було трохи змінено на новий варіант, такі системи не зможуть визначити це нове відхилення подібної атаки. • Не вдається виявити атаку нульового дня. • Не підходять для виявлення багатоетапних атак. • Мало розуміння нападів.

	Переваги	Недоліки
СВВ на основі аномалій	• Можуть використовуватись для виявлення нових атак. • Можуть використовуватись для створення підпису про вторгнення.	• Не можуть обробляти зашифровані пакети, тому атака може залишатися не виявленою та представляти загрозу. • Високі помилкові позитивні тривоги. • Важко створити нормальний профіль для дуже динамічної ІКМ. • Некласифіковані оповіщення. • Потрібне початкове навчання.

Однак слід зауважити, що іноді СВВ і СВА на основі аномалій можуть призвести до високого показника хибнопозитивних результатів, оскільки аномалії можуть бути просто новою звичайною діяльністю, а не справжніми вторгненнями.

Слід також зазначити, що з розвитком інформаційних технологій особливо актуальною стала проблема обробки великих даних. Безліч параметрів для виявлення атак в інформаційно-комунікаційних системах та мережах становить значний обсяг даних, що визначає можливість їх обробки за допомогою інтелектуального аналізу даних, тобто за допомогою методів систем штучного інтелекту (ШІ) – нейронних мереж та систем з нечіткою логікою, які є універсальними ефективними апроксиматорами.

Встановлено, що наразі протидіяти вторгненням і атакам основуючись тільки на одному з методів штучного інтелекту є малоефективним, тому рекомендовано підходити до цього питання комплексно і будувати інтелектуальну систему протидії вторгненням і атакам, засновану одночасно на декількох методах ШІ.

1.1.4 Недоліки сучасних систем виявлення вторгнень і атак

До недоліків сучасних СВВ і СВА можна віднести наступні дві групи проблем [32]:

• недоліки, пов’язані зі структурою СВВ і СВА;

• недоліки реалізованих методів виявлення.

Характеристика недоліків структур сучасних СВВ і СВА представлена в табл. 1.2.

Таблиця 1.2 – Недоліки структур СВВ і СВА

Проблема	Причина
Відсутність загальної методології побудови	Новий напрям дослідження. Недостатність загальних правил та понять формування термінології
Ефективність	Орієнтованість на виявлення всіх видів атак; суттєве споживання ресурсів; орієнтованість командних інтерпретаторів на власний набір правил; множина правил дозволяє тільки непрямі залежності послідовності зв'язків між подіями
Портативність	Орієнтованість СВВ і СВА для використання на конкретному обладнанні, для конкретних задач. Складність переорієнтації СВВ і СВА для роботи в інших системах і задачах
Установка СВВ	Необхідність додаткових навичок, знань нових експертних систем
Продуктивність і допоміжні тести	Складність оцінки продуктивності СВВ і СВА у реальних умовах. Відсутній набір правил для тестування СВВ і СВА, на основі яких оцінюється доцільність використання системи в заданих умов
Тестування	Відсутність ефективних способів тестування СВВ і СВА

Проблема	Причина
Можливості оновлення	Складність оновлення існуючих систем новими технологіями. Труднощі забезпечення взаємодії нових підсистем із всією системою

У роботах [32-33] приведені наступні недоліки систем виявлення вторгнень і атак:

• неприпустимо високий рівень похибок першого та другого роду;

• слабкі можливості щодо виявлення нових видів атак;

• неможливість виявлення більшості вторгнень на початкових етапах;

• надзвичайні складнощі з ідентифікацією мети атаки та атакуючого;

• відсутність оцінок точності та адекватності результатів роботи;

• неможливість виявлення відомих атак з новими стратегіями;

• складність виявлення вторгнень у режимі реального часу з необхідною повнотою в високошвидкісних мережах.

Крім вказаних недоліків, проблемою є також значне перевантаження систем, які використовують СВВ, в режимі реального часу та автоматизація процесу виявлення складних атак.

До недоліків сучасних СВВ і СВА можна віднести також наступні [34-37]:

• відсутня універсальна методологія проектування,

• обмежена гнучкість (включає універсальність і динамічне налаштування);

• недолік ефективності;

• недостатня мобільність в контрольованому просторі;

• обмежена можливість оновлення методів виявлення;

• відсутність тестів продуктивності і покриття мережі;

• труднощі з підтримкою наборів правил функціонування;

• немає прийнятного способу перевіряти ефективність СВВ і СВА.

Багато хто продовжує вирішувати деякі з зазначених вище недоліків через удосконалення існуючих методів, але деякі недоліки властиві основам, на яких створені СВВ і СВА.

1.2 Нечітка кластеризація

1.2.1 Нечітка логіка

Наразі для побудови інтелектуальних систем використовують різні підходи. Одним з них є логічний підхід [11-18, 38-43].

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.

1.2.2 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 [11, 12].

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. 1.7):

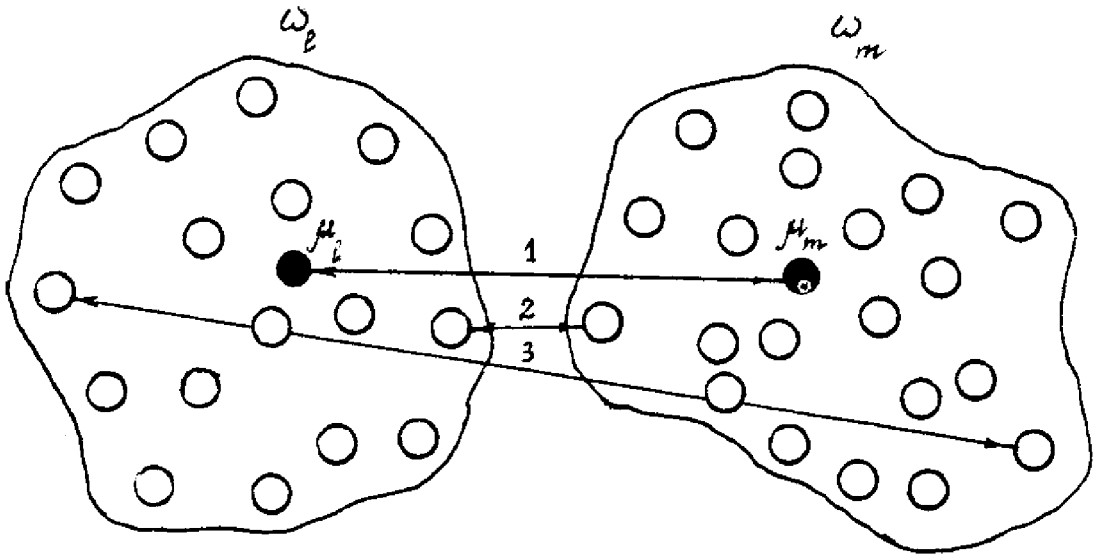


Рисунок 1.7 – Ілюстрація способів визначення відстані
між кластерами w_l і w_m: 1 – по центрам тяжіння,
2 – по найближчим об'єктам, 3 – по далеким об'єктам

• відстань центрів тяжіння – відстань між центральними точками кластерів:

$$q(w_l, w_m) = d(\mu_l, \mu_m); \qquad (1.2)$$

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

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

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

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

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

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

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

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

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

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. 1.8 [12].

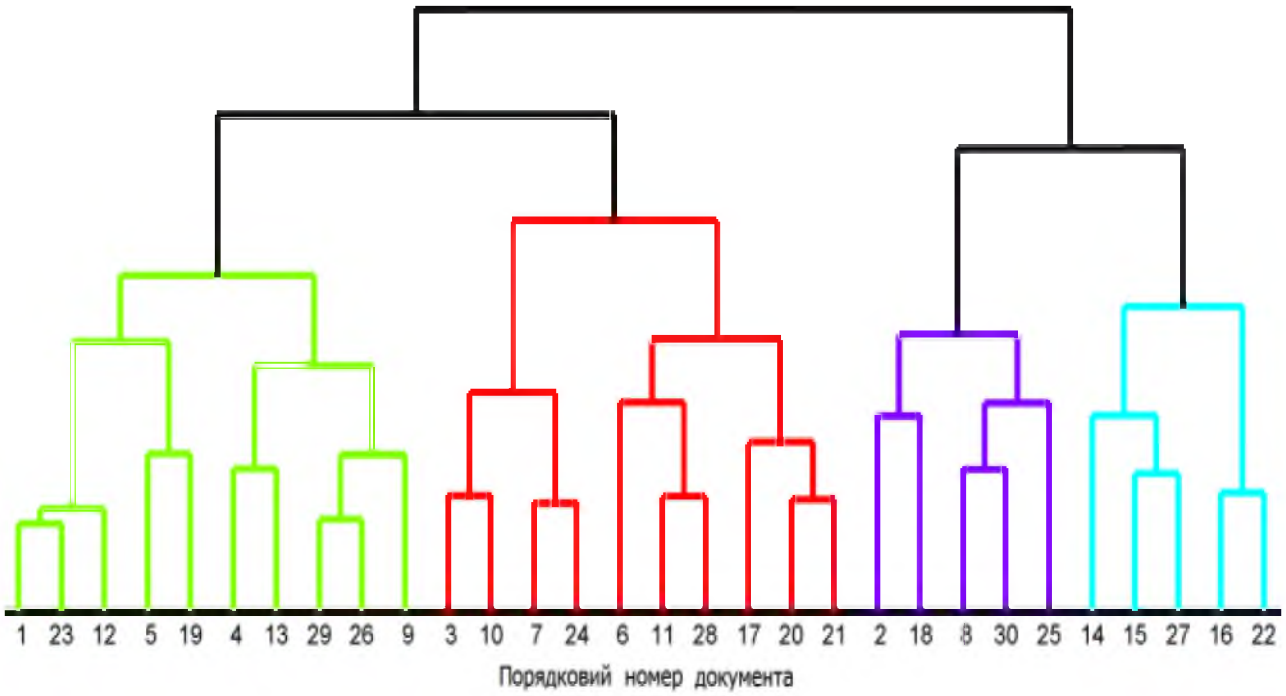


Рисунок 1.8 – Приклад ієрархічної кластеризації

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. 1.9).

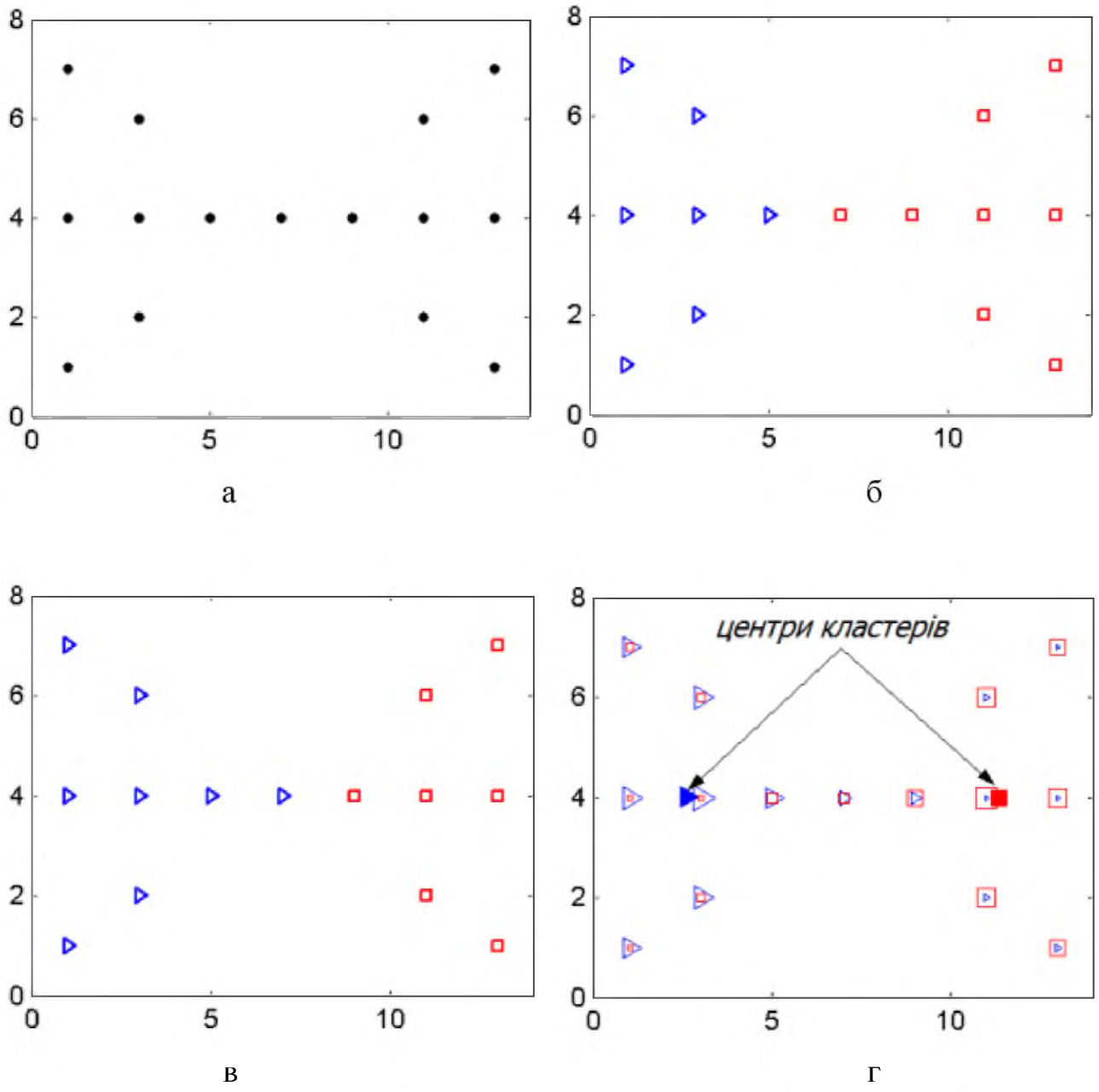


Рисунок 1.9 – Кластеризація «метелика»: а – початкові дані;
б – чітка кластеризація I; в – чітка кластеризація II;
г – нечітка кластеризація

За чіткої кластеризації (рис. 1.9,б і в) виходять два кластери із 7 і 8 об'єктів. На рис. 1.9 об'єкти першого кластера позначені трикутниками, а другого – квадратами. Симетричний «метелик» за чіткої кластеризації розбивається на два несиметричних кластера.

За нечіткої кластеризації (рис. 1.9,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).

1.2.3 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 [11, 12, 41-43].

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

1. Завдання нечітких кластерів матрицею розбиття:

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

при цьому

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

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:

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

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):

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

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):

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

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.

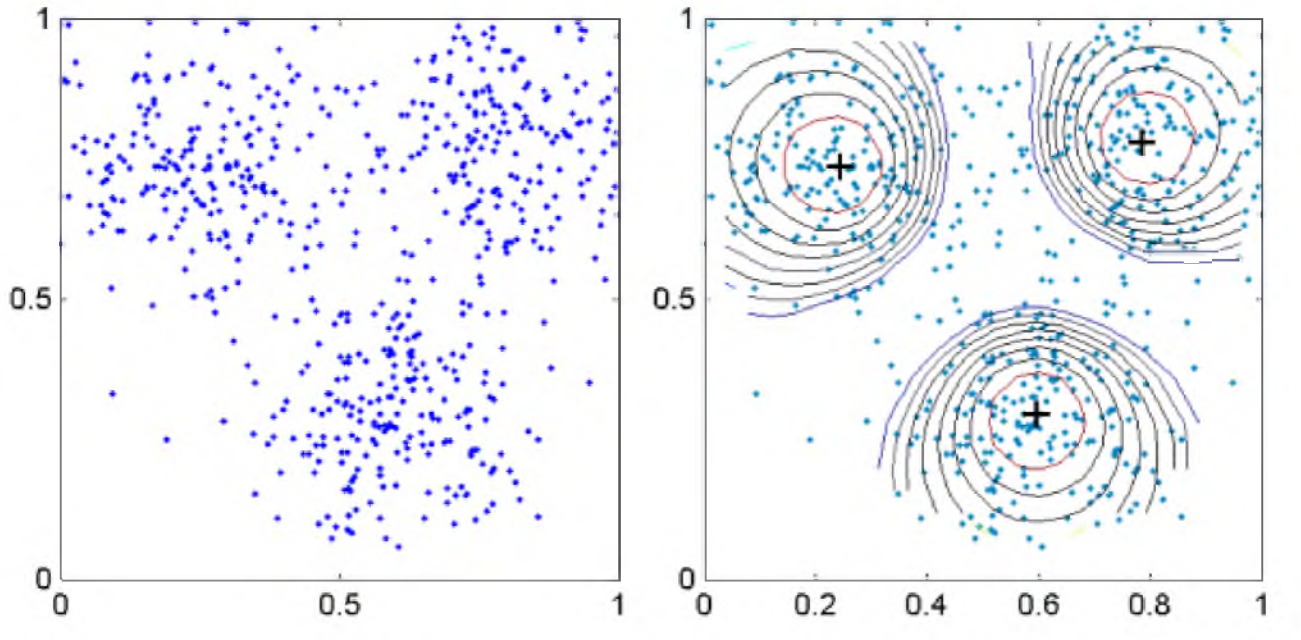
На рис. 1.10 наведено приклад нечіткої кластеризації за методом С-середніх з використанням евклідової метрики:

На рис. 1.10,а зображені початкові об'єкти; на рис. 1.10,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.

1.2.4 Субтрактивна кластеризація

В основі методу субтрактивної кластеризації лежить припущення, що кожна експериментальна точка може бути центром кластеру [11, 12, 41-43].

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.

1.2.5 Ефективність систем з нечіткою логікою

Ефективність використання апарату нечіткої логіки базується на наступних результатах [11].

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 ||·|| – 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.

1.2.6 Реалізація алгоритмів нечіткої кластеризації в середовищі MATLAB/Simulink

В середовищі MATLAB/Simulink нечітка кластеризація за методом С-середніх реалізована функцією fcm. Обов'язковими аргументами функції є матриця спостережень X та кількість кластерів. Функція повертає матрицю належностей кожного об'єкта до кластерів, а також центри нечітких кластерів.

Проілюструємо роботу зазначеної вище функції fcm на прикладі кластеризації метелика. Початкові дані для даної кластеризації задано в табл. 1.3. Графічне зображення цих даних наведено на рис. 1.9,а. Кластеризуємо ці дані за таких параметрах алгоритму нечіткої кластеризації С-середніх: c=2 та m=2.

Таблиця 1.3 – Початкові дані для прикладу кластеризації метелика

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
x_1	1	1	1	3	3	3	5	7	9	11	11	11	13	13	13
x_2	1	4	7	2	4	6	4	4	4	2	4	6	1	4	7

В результаті кластеризації, після 8-ми ітерацій одержимо нечітке розбиття згідно табл. 1.4. Значення критерію (1.11) для цього нечіткого розбиття дорівнює 82.94.

Таблиця 1.4 – Результати роботи функції fcm для прикладу кластеризації метелика

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
μ_{k1}	0.91	0.98	0.91	0.95	1	0.95	0.86	0.5	0.12	0.05	0	0.05	0.09	0.02	0.09
μ_{k2}	0.09	0.02	0.09	0.05	0	0.05	0.12	0.5	0.88	0.95	1	0.95	0.91	0.98	0.91

Результати нечіткої кластеризації показані на рис. 1.9,г (розмір маркерів пропорційний ступеню належності об'єкта кластеру).

Тривимірні зображення нечітких кластерів згідно алгоритму нечіткої кластеризації С-середніх наведені на рис. 1.11.

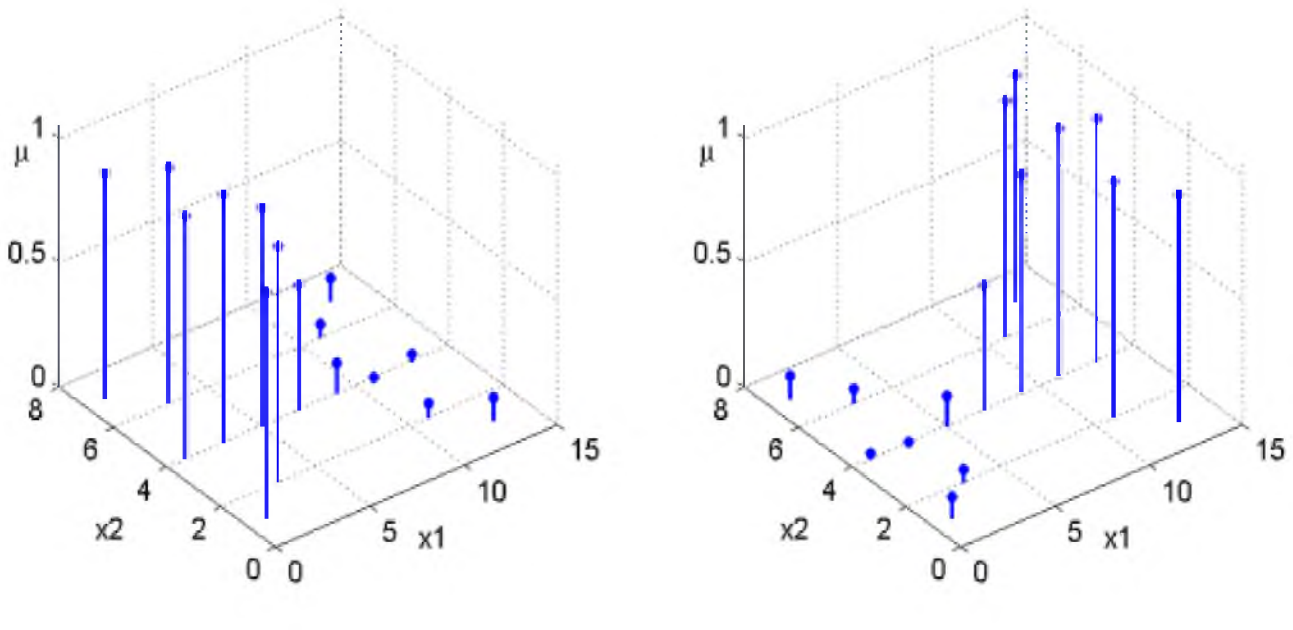


Рисунок 1.11 – Тривимірне зображення нечітких кластерів згідно алгоритму нечіткої кластеризації С-середніх

В середовищі MATLAB субтрактивна кластеризація (як поліпшена версія методу гірської кластеризації) реалізована функцією subclust. Обов’язковими аргументами функції є матриця спостережень X. Додатковими аргументами є параметри алгоритму кластеризації.

Функція subclust викликається у такому форматі:

[centers, sigmas] = subclust (X, radii, xBounds, options),

де centers – центри знайдених кластерів;

sigmas – радіуси знайдених кластерів;

X – матриця спостережень X;

radii – вектор радіусів кластерів за кожною ознакою; за малих значень radii функція виокремлює багато дрібних кластерів;

xBounds – діапазони атрибутів, які необхідні для масштабування даних на одиничний гіперкуб;

options – параметри кластеризації;

options(1) – коефіцієнт липкості, значення за замовченням – 1.25. Значення options(1)*radii використовується для визначення близьких до центру кластера об'єктів. Ці об'єкти вважаються такими, що належать кластеру і вилучаються із подальшого аналізу;

options(2) – коефіцієнт прийняття, значення за замовченням – 0.5. Якщо відношення потенціалів вузлової точки та центру першого кластера більше за цей коефіцієнт, тоді вузлова точка включається до списку можливих центрів кластерів;

options(3) – коефіцієнт відторгнення, значення за замовченням – 0.15. Якщо вузлова точка відхилена за коефіцієнтом прийняття, тоді вона може потрапити у список потенціальних центрів кластерів за двох умов: 1) точка розташована далеко від вже знайдених кластерів; 2) відношення її потенціалу до потенціалу центра першого кластера більше за коефіцієнт відторгнення;

options(4) – управління виводом на екран проміжних даних. За замовченням дані не виводяться.

Процедуру субтрактивної кластеризації в середовищі MATLAB/Simulink також можна виконати в модулі Findcluster. Основне графічне вікно модуля Findcluster з прикладом субтрактивної кластеризації ірисів зображено на рис. 1.12.

На рис. 1.12 призначення специфічних полів модуля Findcluster є наступним:

- Influence Range – важливість ознак (radii);
- Squash – коефіцієнт липкості;
- Accept Ratio – коефіцієнт прийняття;
- Reject Ratio – коефіцієнт відторгнення.

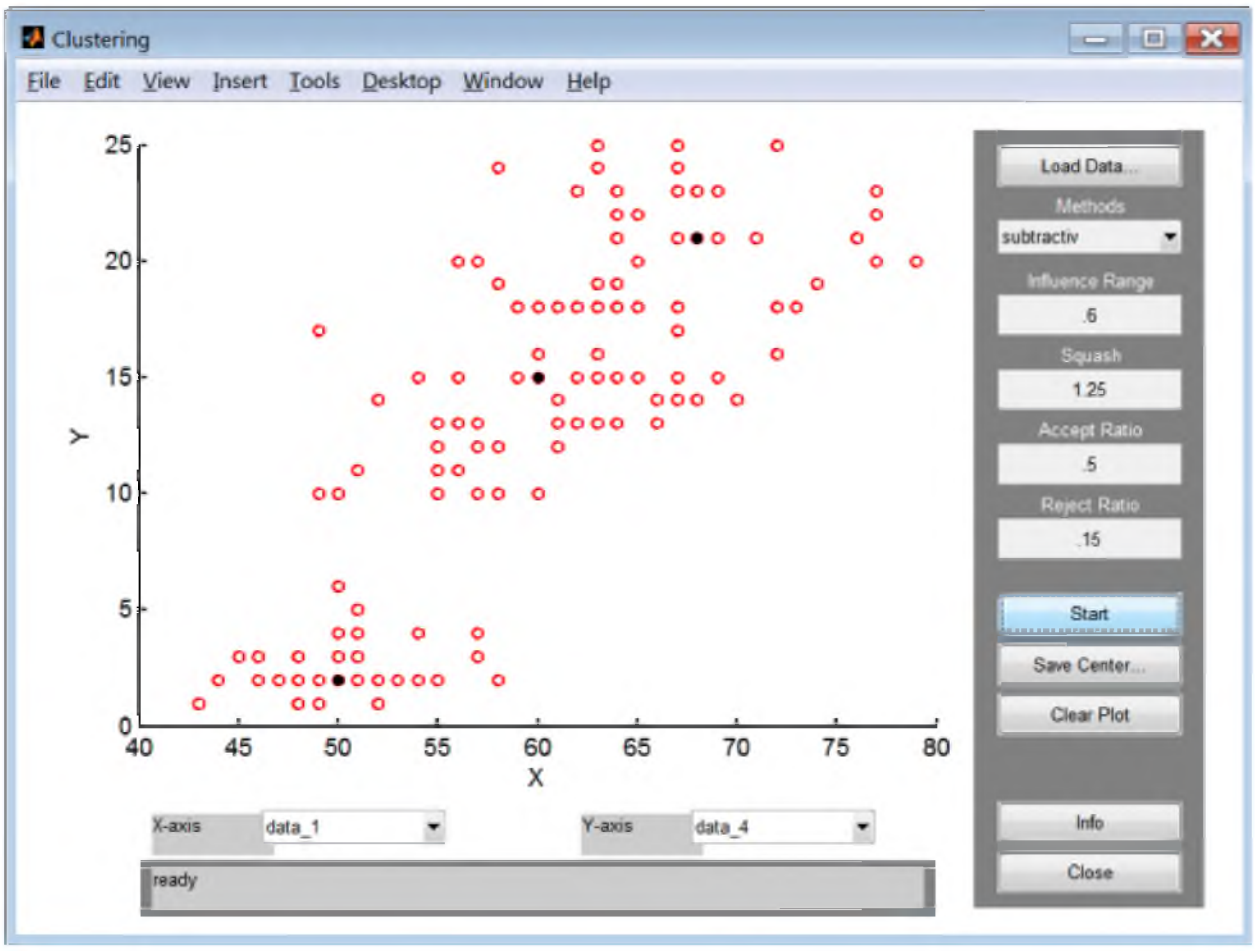


Рисунок 1.12 – Субтрактивна кластеризація в модулі Findcluster (в середовищі MATLAB/Simulink)

Таким чином, узагальнюючи все вищенаведене слід зазначити, що нечітка логіка 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 систем виявлення вторгнень і атак, 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 систем виявлення вторгнень і атак 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.

За допомогою нечіткої логіки (у тому числі алгоритмів нечіткої кластеризації) частоту помилкових тривог при визначенні нав'язливих дій можна зменшити. Слід тільки коректно окреслити групу нечітких правил для опису нормальної та ненормальної діяльності в ІКМ та механізм нечітких умовиводів для визначення вторгнень.

1.3 Існуючі набори даних для оцінки виявлення мережевих атак

Для навчання систем виявлення атак рівня мережі застосовуються спеціалізовані загальнодоступні набори розмічених даних. До найбільш відомих та опублікованих у відкритих джерелах наборів даних можна віднести наступні: DARPA1998, KDD Cup 1999, Kyoto 2006, NSL-KDD 2009, ISCX 2012, CTU-13, UNSW-NB15, CIDDS-001, UGR-16, CICIDS 2017, CICIDS 2018 та інші [48].

Зазначені набори використовуються переважною більшістю дослідників для апробації досліджуваних та запропонованих підходів до виявлення атак. Для опису наборів даних зазвичай використовуються наступні характеристики набору даних.

1. Число ознак у наборі даних.

До ознак входять:

- ознаки, що характеризують загальну інформацію про з'єднання / потік (наприклад, час початку з'єднання; IP адреса джерела атаки; порт джерела атаки тощо);

- інформативні ознаки (наприклад, тривалість з'єднання, число переданих / прийнятих байт і т.п.);

- ознаки, які використовуються для опису атаки або нормального мережевого з'єднання (наприклад, мітка класу трафіку, опис атаки, реакція антивірусної програми на з'єднання).

2. Інструмент, який був використаний для виділення ознак із мережевого трафіку.

3. Типи мережевих атак у наборі даних.

4. Природа інформативних ознак.

У табл. 1.5 наведено опис існуючих загальнодоступні наборів даних, які можуть бути використані для навчання систем виявлення комп'ютерних атак рівня мережі.

Таблиця 1.5 – Опис існуючих наборів даних, призначених для навчання СВА рівня мережі

Набір даних	**Число ознак у наборі даних**	**Природа інформативних ознак**	**Інструмент для виділення ознак**	**Типи мережевих атак у наборі даних**
DARPA 1998	10	ОМЗ	Немає відомостей	DoS, Remote to User, User-to-Root, Surveillance/probing attacks
KDD Cup 1999	42	ОМЗ, ОПР	MADAM ID	DoS, Remote to User, User-to-Root, Surveillance/probing attacks

Набір даних	**Число ознак у наборі даних**	**Природа інформативних ознак**	**Інструмент для виділення ознак**	**Типи мережевих атак у наборі даних**
Kyoto 2006+	24	ОМЗ	Немає відомостей	Різні атаки на honeypots (backscatter, DoS, exploits, malware, port scans, shellcode)
NSL-KDD 2009 (створений на основі KDD Cup 1999)	42	ОМЗ, ОПР	MADAM ID	DoS, Remote to User, User-to-Root, Surveillance/probing attacks
ISCX 2012	19	ОМЗ, ОНП	Немає відомостей	Brute Force SSH, HTTP DoS, DDoS using an IRC Botnet, Infiltrating the network from inside
CTU-13	33	ОМЗ, ОНП	Argus	botnets (Menti, Murlo, Neris, NSIS, Rbot, Sogou, Virut)
UNSW-NB15	45	ОМЗ, ОНП, ОПР	Argus, Bro-IDS	Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconaissance, Shellcode, Worms

Набір даних	**Число ознак у наборі даних**	**Природа інформативних ознак**	**Інструмент для виділення ознак**	**Типи мережевих атак у наборі даних**
CIDDS-001	14	ОМЗ, ОНП	NetFlow	Port scanning, DoS, BruteForce, Ping Scan
UGR-16	132 (Feature as Counter), 13 (у CSV файлі)	ОМЗ, ОНП	FCParser	low- and high-rate DoS, Port scanning, UDP port scanning, SSH scanning, Botnet, Spam
CICIDS 2017	85	ОМЗ, ОНП, ОПР	CICFlowMeter	DoS Hulk, PortScan, DDoS, DoS GoldenEye, FTP-Patator, SSH-Patator, DoS slowloris, DoS Slowhttptest, Bot, Infiltration, Heartbleed, Web Attack – Brute Force, Web Attack – XSS, Web Attack – SQL Injection
CICIDS 2018 та інші набори	80	ОМЗ, ОНП, ОПР	CICFlowMeter -v3	Brute Force, Heartbleed, Botnet, DoS, DDoS, Web

Набір даних	Число ознак у наборі даних	Природа інформативних ознак	Інструмент для виділення ознак	Типи мережевих атак у наборі даних
даних, створені в Canadian Institute for Cybersecurity				attacks, Infiltration of the network from inside

У табл. 1.5 використовуються наступні позначення: ОМЗ – ознаки, що характеризують мережеве з'єднання (наприклад, тривалість мережевої сесії); ОНП – ознаки, що характеризують напрям передачі даних (наприклад, число байт переданих у напрямку сервера; середній час між мережними пакетами в напрямі клієнта); ОПР – ознаки, що характеризують операції, які виконуються на прикладному рівні (наприклад, успіх операції віддаленої автентифікації користувача, кількість операцій з файлами в даному з'єднанні тощо).

Аналіз публікацій з результатами оцінки якості різних класифікаторів мережевого трафіку, навчання яких здійснювалося на представлених вище наборах даних, показав наступні висновки [48-51]:

• для побудови систем виявлення комп'ютерних атак рівня мережі використання ознак, що характеризують операції, що виконуються на прикладному рівні, неможливо через те, що в даний час практично весь мережевий трафік є зашифрованим (використовуються протоколи TLS/SSL та IPSEC);

• у більшості наведених вище наборів даних використовуються ознаки, що характеризують лише мережне з'єднання в цілому (адресна інформація, тривалість з'єднання, число переданих байт), а також додаткові ознаки, отримані під час аналізу даних прикладного рівня;

• для поліпшення якості класифікаторів мережного трафіку необхідне використання ознакового простору, що включає безліч ознак, що характеризують мережне з'єднання в цілому, кожен напрямок окремо, а також особливості конкретного з'єднання (потоку) на транспортному рівні.

Більшість публічних наборів даних для навчання систем виявлення комп'ютерних атак було розроблено з головною метою – надати дослідникам можливість порівняти різні методи виявлення в однакових умовах. При порівнянні параметрів різних наборів даних важливим є питання формалізації єдиних вимог до них.

Основними вимогами до наборів даних, що публікуються, є наступні:

• можливість однозначної ідентифікації – набір даних має бути унікальним, містити докладний опис, бути проіндексованим у відповідних пошукових системах;

• доступність – повинен бути наданий вільний доступ до набору даних по його ідентифікатору;

• можливість порівняння метаданих – набори даних мають використовувати єдині словники метаданих;

• багаторазове використання – дані мають бути точно описані сукупністю релевантних атрибутів та відповідати галузевим стандартам, мають бути зазначено походження даних та ліцензійні умови їх використання.

1.4 Висновок. Постановка задачі

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. Системи виявлення вторгнень і атак 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 елементів комп'ютера або мережі 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 [44-47].

Встановлено, що з розвитком інформаційних технологій особливо актуальною стала проблема обробки великих даних. Безліч параметрів для виявлення атак в інформаційно-комунікаційних системах та мережах становить значний обсяг даних, що визначає можливість їх обробки саме методами штучного інтелекту.

Встановлено, що протидіяти вторгненням і атакам основуючись тільки на одному з методів штучного інтелекту є малоефективним, тому рекомендовано підходити до цього питання комплексно і будувати інтелектуальну систему протидії вторгненням, засновану на декількох методах штучного інтелекту [11-12, 41-43].

Слід зазначити, що актуальність методів систем штучного інтелекту (нейронних мереж, систем нечіткого висновку, еволюційного моделювання, агентських алгоритмів оптимізації) при вирішенні питань в галузі кібербезпеки обумовлена здатністю інтелектуальних методів розв'язувати оптимізаційні

задачі, які погано формалізуються, а також використанням для моделювання ефективних і універсальних апроксиматорів.

В розділі проаналізовано системи штучного інтелекту, а саме алгоритми нечіткої кластеризації – субтрактивна кластеризація та нечітка кластеризація С-середніх. Встановлено, що традиційні методи виявлення вторгнень і атак не здатні забезпечити надійний захист ІКМ. Методи штучного інтелекту дозволяють створити принципово нові алгоритми виявлення вторгнень і атак, дозволяють значно підвищити рівень захищеності ІКМ.

Встановлено, що уся 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 систем виявлення вторгнень і атак, 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 систем виявлення вторгнень і атак 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, за допомогою нечіткої логіки (у тому числі алгоритмів нечіткої кластеризації - субтрактивної кластеризації та нечіткої кластеризації С-середніх) частоту помилкових тривог при визначенні нав'язливих дій можна

зменшити. Слід тільки коректно окреслити групу нечітких правил для опису нормальної та ненормальної діяльності в ІКМ та механізм нечітких умовиводів для визначення вторгнень.

В розділі було проаналізовано найбільш відомі спеціалізовані загальнодоступні набори розмічених даних (DARPA1998, KDD Cup 1999, Kyoto 2006, NSL-KDD 2009, ISCX 2012, CTU-13, UNSW-NB15, CIDDS-001, UGR-16, CICIDS 2017, CICIDS 2018), що використовуються для оцінки виявлення мережевих атак. Встановлено, що більшість публічних наборів даних для навчання СВА було розроблено з головною метою – надати дослідникам можливість порівняти різні методи виявлення в однакових умовах. Встановлено основні вимоги до цих наборів даних.

Отже, висновки, які отримані в цьому розділі, визначають подальші цілі і завдання, та підтверджують актуальність кваліфікаційної роботи.

Таким чином, для виконання мети кваліфікаційної роботи необхідно:

• запропонувати підхід до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі;

• оцінити ефективність запропонованого підходу.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Підхід до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі

Метод Фібоначчі є методом однопараметричної оптимізації.

Методи однопараметричної оптимізації використовуються: при дослідженні впливу окремих параметрів на показник оптимальності; а також для визначення довжини кроку вздовж обраного напряму пошуку у багатопараметричних задачах оптимізації.

Методи однопараметричної оптимізації за обсягом інформації, що використовується в кожній точці пошуку, можна розділити на два класи алгоритмів.

Алгоритми першого класу враховують при визначенні довжини кроку лише ознаку зростання (зменшення) показника оптимальності у декількох послідовно вибираних точках пошуку. До цього класу належать методи: загального пошуку, розподілу інтервалу навпіл, дихотомії, золотого перетину, Фібоначчі та інші.

Алгоритми другого класу враховують при визначенні довжини кроку зміни числових значень цільової функції в одній або декількох ітераціях. Сюди відноситься метод квадратичної апроксимації та інші.

При вирішенні задачі оптимізації передбачається, що досліджувана цільова функція $y=F(x)$ є «унімодальною», тобто в інтервалі зміни значень x ($a \le x \le b$) існує лише один екстремум. Інших відомостей про цільову функцію немає.

Вводиться поняття «інтервал невизначеності» – це інтервал значень x, в якому укладено оптимум. На початку процесу оптимізації цей інтервал має довжину L або (b-a) – початковий інтервал невизначеності. Задача оптимізації полягає в систематичному звуженні інтервалу невизначеності до такої

величини, в якій знаходиться екстремум із заданою точністю. Оцінка положення екстремуму виходить інтервальною, а не точковою.

Таким чином, метод Фібоначчі – це метод пошуку відсортованого масиву за допомогою алгоритму «розділяй та владарюй», який звужує можливі місця за допомогою чисел Фібоначчі. Метод пошуку Фібоначчі походить від методу пошуку золотого перетину, алгоритму Джека Кіфера для пошуку максимуму або мінімуму унімодальної функції в інтервалі. Цей метод є найкращим (в сенсі максимального зменшення довжини відрізка локалізації) серед активних методів пошуку.

Метод Фібоначчі є більш ефективним за збіжністю, ніж метод дихотомії, і має найбільшу швидкість збіжності для класу безперервних функцій. У ньому, як і методі золотого перетину, на кожному кроці виробляється лише одне визначення цільової функції, а в методі дихотомії два. Але в цьому методі потрібно заздалегідь обрати число випробувань N.

Метод ґрунтується на використанні чисел Фібоначчі для знаходження точок, в яких визначається цільова функція F(x).

Числа Фібоначчі утворюють послідовність цілих чисел таким чином, що $Ф_N=Ф_{N-1}+Ф_{N-2}$, при N≥2. $Ф_0=Ф_1=1$.

Перші 15 чисел Фібоначчі наведені в табл. 2.1

Таблиця 2.1 – Перші 15 чисел Фібоначчі

N	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$Ф_N$	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610

В основу схеми пошуку екстремуму покладено два вихідні співвідношення:

$$L_{N-2}=L_{N-1}+L_N, \tag{2.1}$$

при $N\geq 3$, та

$$L_N=\frac{1}{2}\left(L_{N-1}+\varepsilon\right). \tag{2.2}$$

Перше з них (2.1) пов'язує довжини трьох сусідніх (за номерами) інтервалів невизначеності. Друге (2.2) вимагає, щоб пошук екстремуму завжди завершувався однаково: симетричним розміщенням двох останніх точок (x_{N-1} і x_N) на інтервалі L_{N-1}.

Координати точок, в яких визначаються цільові функції, знаходяться за формулами:

$$x_1^{r+1} = a_r + l_r \cdot \frac{\Phi_{N-1-r}}{\Phi_{N+1-r}}, \tag{2.3}$$

$$x_2^{r+1} = a_r + l_r \cdot \frac{\Phi_{N-r}}{\Phi_{N+1-r}}, \tag{2.4}$$

де r – номер кроку (r=0, 1, 2, 3,…,N –3);

l_r=(b_r–a_r) – довжина інтервалу невизначеності на r-му кроці;

a_r, b_r – початок і кінець r-го інтервалу невизначеності.

Алгоритм методу Фібоначчі є ітераційною процедурою, яка включає наступні етапи.

На першому етапі, який відповідає першому кроку пошуку (r=0) симетрично від кінців початкового інтервалу невизначеності (a і b) проводиться пара випробувань у точках x_1^1 і x_2^1, що визначаються N-м та (N–1) числами Фібоначчі.

Отримуємо:

$$x_1^1 = a + (b-a) \cdot \frac{\Phi_{N-1}}{\Phi_{N+1}}, \tag{2.5}$$

$$x_2^1 = a + (b-a) \cdot \frac{\Phi_N}{\Phi_{N+1}}. \tag{2.6}$$

У цих точках визначається цільова функція та в залежності від її значень обирається новий (звужений) інтервал невизначеності.

Другий етап включає (N-3) ітераційних кроків. На кожному r-му кроці в інтервалі невизначеності l_r, отриманому на попередньому кроці, розглядається нова пара випробувань $\left(x_1^{r+1}, x_2^{r+1}\right)$.

Особливістю даного алгоритму пошукової оптимізації є те, що з двох точок x_1^{r+1} і x_2^{r+1}, що розглядаються на (r+1)-му кроці, одна завжди співпадатиме з однією з точок попереднього кроку (x_1^r або x_2^r), в якій вже було проведено випробування.

Третій етап характеризується тим, що після проведення (N-1)-го випробування необхідно вирішити, по який бік від точки x, яка знаходиться в інтервалі невизначеності l_{N-1}, лежить точка істинного екстремуму. Для цього останнє N випробування проводиться поблизу точки попереднього випробування в точці (x–ε) або (x+ε), що дозволяє визначити апостеріорний інтервал невизначеності l_N.

На рис. 2.1 наведена схема пошуку екстремуму за методом Фібоначчі (другий та третій етапи).

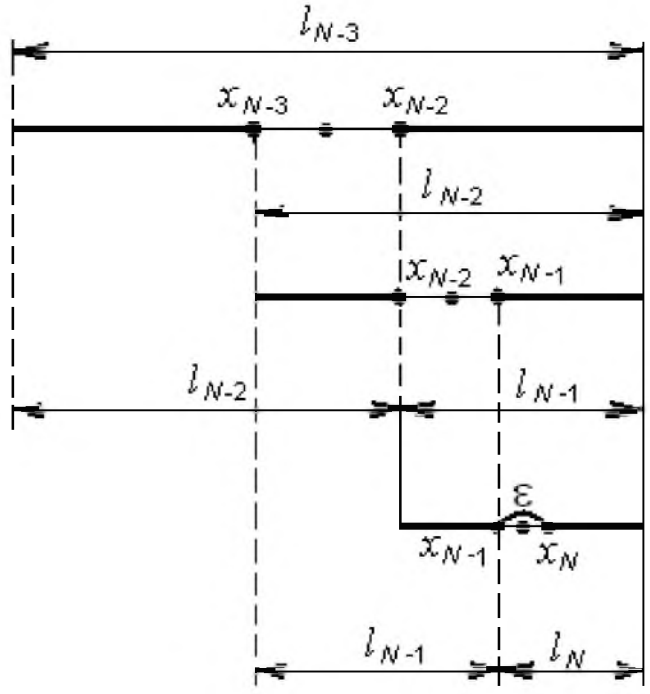


Рисунок 2.1 – Схема пошуку екстремуму за методом Фібоначчі: другий та третій етапи

До недоліків методу Фібоначчі слід віднести наступні.

1. Заздалегідь задане число випробувань, яке не можна змінювати в процесі звуження інтервалу невизначеності, і якщо після N випробувань не отримана потрібна точність визначення оптимуму, то доводиться починати спочатку, задавшись більшим N.

2. При застосуванні ЕОМ необхідно запам'ятовувати (чи щоразу обчислювати) числа Фібоначчі.

Слід зазначити, що метод Фібоначчі ефективніший за збіжністю у порівнянні з методами дихотомії та золотого перетину, тобто для досягнення необхідного звуження інтервалу невизначеності при однаковій кількості визначень цільової функції.

Таким чином, запропонований підхід до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі полягає у використанні однопараметричної оптимізації (методу Фібоначчі) для вибору параметрів інтелектуальних класифікаторів (на основі алгоритмів субтрактивної кластеризації та нечіткої кластеризації C-середніх).

2.2 Оцінка ефективності запропонованого підходу до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі

Оцінка ефективності запропонованого підходу до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі виконувалась в середовищі Matlab/Simulink за допомогою стандартних і розроблених програм.

Як експериментальні дані було обрано базу UNSW-NB15, яка достатньо нова (була створена у 2015 р.), у ній були виправлені недоліки попередніх баз – KDD CUP 99 та NSL KDD, а також додано нові сучасні види атак [52].

В базі даних UNSW-NB15 кожен запис містить 47 ознак мережевого трафіку п'яти типів: номінальні, цілочисельні, числові, часові, бінарні. Для

кожного запису міститься інформація про те, до якого з десяти класів відноситься з'єднання: нормальні з'єднання (Normal) або один із 9 різних видів атак:

• Normal – нормальні транзакції даних;

• Exploits – зловмисник знає про проблеми безпеки в системі та використовує дані вразливості у своїх цілях;

• Fuzzers – спроба викликати зупинення програми або мережі шляхом подання на її вхід великого обсягу випадково згенерованих даних;

• Reconnaissance – містить всі типи атак, які збирають інформацію про мережу (з метою розвідки);

• Generic – техніка працює проти всіх блокових шифрів (із заданим блоком та розміром ключа), незалежно від структури блокового шифру;

• DoS – шкідлива спроба зробити сервер або мережевий ресурс недоступним для користувачів, зазвичай це тимчасове переривання або припинення послуг хоста, підключеного до Інтернету;

• Analysis – містить різні атаки шляхом сканування портів, відправки спаму та проникнення html-файлів;

• Backdoors – техніка, в якій механізм безпеки системи обходиться непомітно для доступу до комп'ютера або його даних;

• Shellcode – невеликий фрагмент коду, що використовується як корисне навантаження під час експлуатації вразливостей програмного забезпечення;

• Worms – атакуючий реплікує себе, щоб поширитися на інші комп'ютери (часто він використовує комп'ютерну мережу для поширення, покладаючись на збої безпеки на цільовому комп'ютері для доступу до нього).

Для налаштування параметрів класифікаторів на основі алгоритмів нечіткої кластеризації експериментальні дані (база UNSW-NB15) було розділено на навчальну вибірку, яка склала 70 % даних і тестову – 30 % даних.

Як класифікатори на основі алгоритмів нечіткої кластеризації використовувались: субтрактивна кластеризація та нечітка кластеризація *C*-

середніх. При цьому алгоритмом нечіткої логіки в кластеризації C-середніх було обрано алгоритм Сугено.

Як метод параметричної оптимізації використовувався метод Фібоначчі, який налаштовував наступні параметри алгоритмів нечіткої кластеризації:

- для субтрактивної кластеризації – діапазон впливу кластерного центру R_c;

- для нечіткої кластеризації C-середніх – число кластерів k_c.

Як критерій параметричної оптимізації використовувався критерій регулярності, який заснований на розподілі даних на навчальну А і перевірочну В вибірки [53]:

$$C_{рег} = \frac{\left\| Y_B^*[m+n] - \hat{Y}_B[m+n] \right\|}{\left\| Y_B^*[m+n] \right\|}, \qquad (2.7)$$

де m – глибина пам'яті, n – глибина прогнозу.

Встановлено, що мінімуму критерію (2.7) ($C_{рег}$=0,034) відповідає алгоритм субтрактивної кластеризації з діапазоном впливу кластерного центру, що дорівнює 0,63 (R_c=0,63).

Встановлено, що мінімуму критерію (2.7) ($C_{рег}$=0,038) відповідає алгоритм нечіткої кластеризації C-середніх з використанням структури алгоритму Сугено і 9 кластерами (k_c=9).

Для досліджень класифікаторів на основі алгоритмів нечіткої кластеризації для виявлення атак експериментальні дані було розділено на навчальну вибірку, яка склала 70 % даних, тестову та перевірочну вибірки (по 15 % даних).

На рис. 2.2 і в табл. 2.2 представлені результати роботи класифікаторів на основі алгоритмів нечіткої кластеризації з попередньо налаштованими параметрами методом Фібоначчі.

Як метрика оцінки якості отриманих інтелектуальних класифікаторів використовувалась Accuracy (акуратність, точність) – частка від навчальної, тестової, перевірочної вибірки щодо якої класифікатор на основі алгоритмів

нечіткої кластеризації прийняв правильне рішення. Тобто, Accuracy – частка правильних відповідей алгоритму:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}. \quad (2.8)$$

де True Positive (TP) – наявність атаки класифіковано як 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.

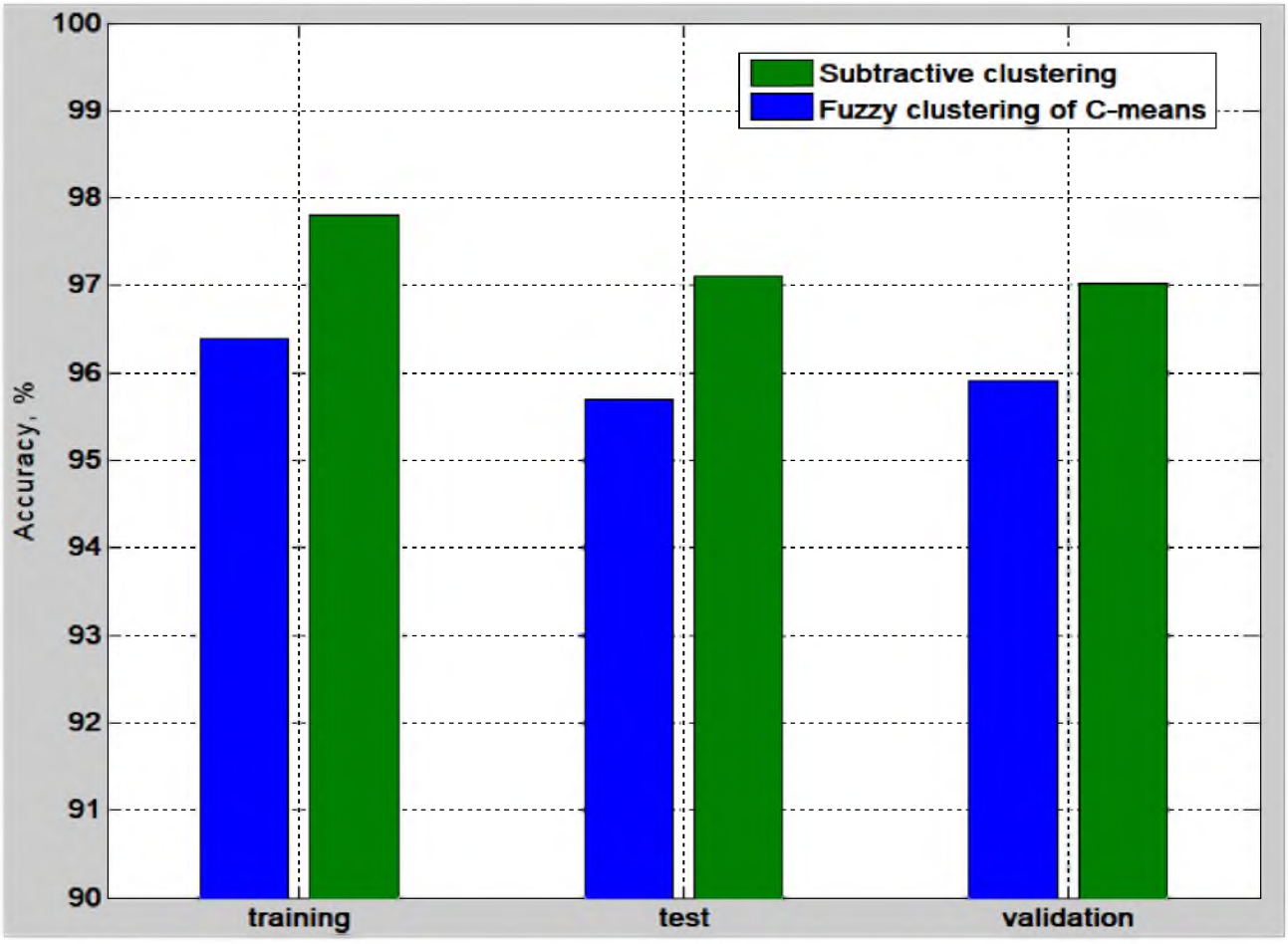


Рисунок 2.2 – Результати роботи класифікаторів на основі алгоритмів нечіткої кластеризації для виявлення мережевих атак

Встановлено, що найкращі результати – найменша похибка перевірки Accuracy (рис. 2.2 і табл. 2.2) показав класифікатор на основі алгоритму субтрактивної кластеризації з діапазоном впливу кластерного центру, що дорівнює 0,63.

Таблиця 2.2 – Результати роботи класифікаторів на основі алгоритмів нечіткої кластеризації для виявлення мережевих атак

Тип класифікатору	Accuracy (точність), %		
	навчання	тестування	перевірки
Субтрактивна кластеризація (діапазон впливу кластерного центру R_c=0,63)	97,81	97,11	97,02
Нечітка кластеризація C-середніх (число кластерів k_c=9)	96,40	95,70	95,91

Для цього класифікатору на рис. 2.3 представлені результати класифікації за видами атак.

Встановлено (див. рис. 2.3), що, незважаючи на високу точність перевірки, для отриманого класифікатору на основі алгоритму субтрактивної кластеризації з діапазоном впливу кластерного центру R_c=0,63, визначення окремих видів атак відбувається важко (DoS, Worms, Analysis, Backdoors). Лише 6 із 10 видів з'єднань (Normal, Generic, Reconnaissance, Shellcode, Exploits, Fuzzers) вдається визначити з точністю понад 65%. При цьому розпізнавання нормального трафіку відбувається вірно в переважній більшості випадків (98,34%).

Практична цінність роботи полягає в тому, що отримані в цьому розділі класифікатори на основі алгоритмів нечіткої кластеризації можуть бути використані в засобах моніторингу, здатних аналізувати трафік мережі в режимі реального часу

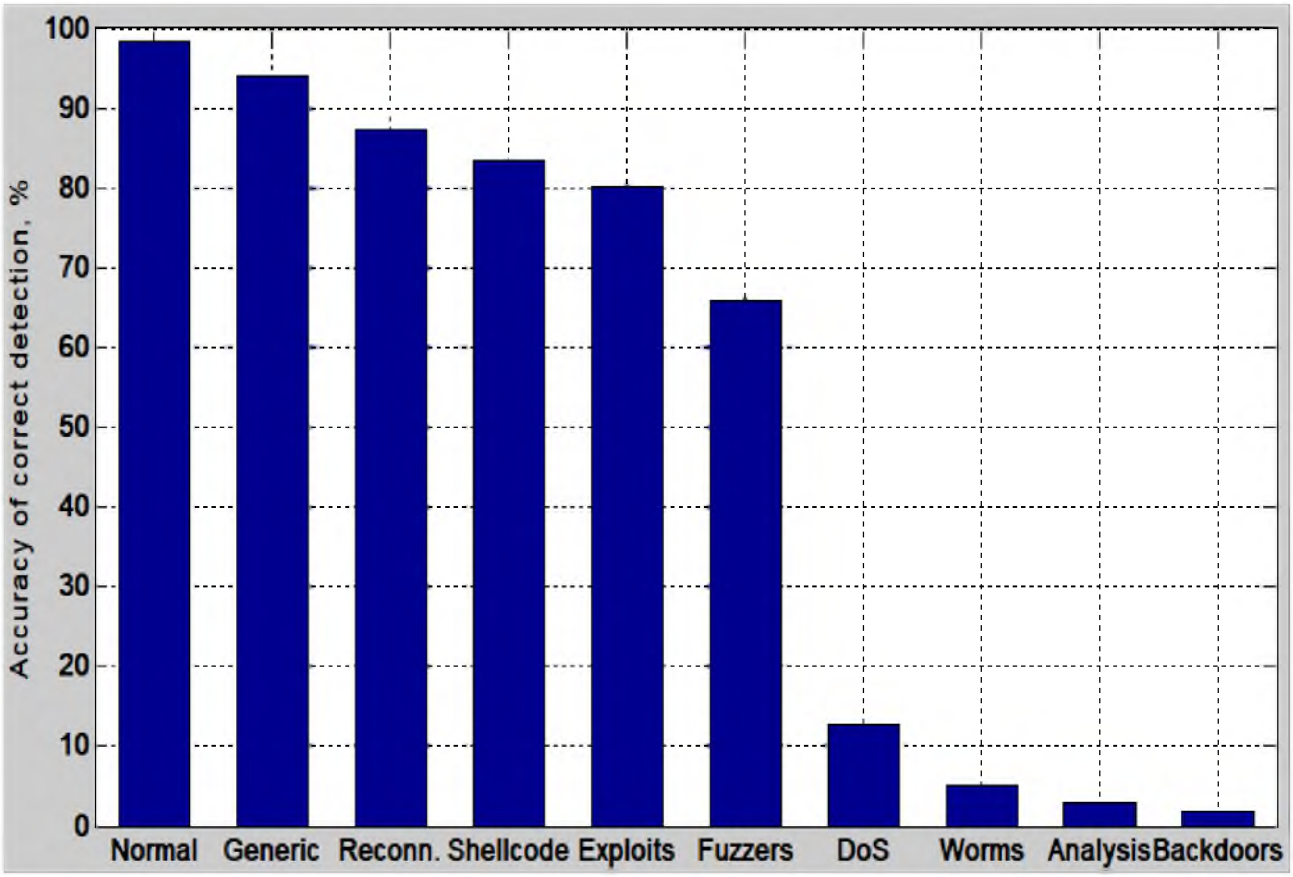


Рисунок 2.3 – Результати роботи класифікатору на основі субтрактивної кластеризації (з діапазоном впливу кластерного центру R_c=0,63) за видами атак

2.3 Висновок

В розділі запропоновано підхід до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі, який полягає у використанні однопараметричної оптимізації (методу Фібоначчі) для вибору параметрів інтелектуальних класифікаторів (на основі алгоритмів субтрактивної кластеризації та нечіткої кластеризації C-середніх).

Оцінка ефективності запропонованого підходу виконувалась в середовищі Matlab/Simulink за допомогою стандартних і розроблених програм.

Як експериментальні дані було обрано базу UNSW-NB15, яка достатньо нова (була створена у 2015 р.), у ній були виправлені недоліки попередніх баз – KDD CUP 99 та NSL KDD, а також додано нові сучасні види атак.

Як метод параметричної оптимізації використовувався метод Фібоначчі, який налаштовував наступні параметри алгоритмів нечіткої кластеризації: для субтрактивної кластеризації – діапазон впливу кластерного центру R_c; для нечіткої кластеризації C-середніх – число кластерів k_c.

Як критерій параметричної оптимізації використовувався критерій регулярності. Встановлено, що його мінімуму ($C_{рег}$=0,034) відповідає алгоритм субтрактивної кластеризації з діапазоном впливу кластерного центру, що дорівнює 0,63 (R_c=0,63). Також мінімуму критерію регулярності ($C_{рег}$=0,038) відповідає алгоритм нечіткої кластеризації C-середніх з використанням структури алгоритму Сугено і 9 кластерами (k_c=9).

Як метрика оцінки якості отриманих інтелектуальних класифікаторів використовувалась Accuracy. Встановлено, що найкращі результати – найменша похибка перевірки Accuracy (97,02%) показав класифікатор на основі алгоритму субтрактивної кластеризації з діапазоном впливу кластерного центру R_c=0,63.

В результаті моделювання для цього класифікатору встановлено, що, незважаючи на високу точність перевірки, визначення окремих видів атак відбувається важко (DoS, Worms, Analysis, Backdoors). Лише 6 із 10 видів з'єднань (Normal, Generic, Reconnaissance, Shellcode, Exploits, Fuzzers) вдається визначити з точністю понад 65%. При цьому розпізнавання нормального трафіку відбувається вірно в переважній більшості випадків (98,34%).

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Запропоновано підхід до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі, який може бути використаний в засобах моніторингу, здатних аналізувати мережевий трафік в режимі реального часу.

Метою даного розділу є обґрунтування економічної доцільності запропонованого підходу до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі.

Для досягнення цієї необхідно здійснити наступні розрахунки:

• капітальні витрати 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 атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі

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 до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі, $t_{тз}=26$;

$t_в$ – тривалість вивчення технічного завдання, літературних джерел за темою тощо, $t_в=36$;

$t_а$ – тривалість моделювання розробленого підходу до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі, $t_а=35$;

$t_р$ – тривалість розробки підходу до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі, $t_м=54$;

$t_д$ – тривалість підготовки технічної документації, $t_д=12$.

Отже,

$$t = t_{тз}+ t_в+ t_а+ t_р+ t_д = 26+36+35+54+12= 163 \text{ години.}$$

Розрахунок витрат на розробку підходу до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі

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 $З_{мч}$.

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 35208 + 1077{,}43 = 36285{,}43 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 163*216 = 35208 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, 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:

$$З_{мч} = t*С_{мч} = 163*6,61 = 1077,43 \text{ грн.}$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = 0,8 \cdot 6 \cdot 1,68 + \frac{7400 \cdot 0,25}{1920} + \frac{6800 \cdot 0,2}{1920} = 6,61 \text{ грн.}$$

Оцінка ефективності запропонованого підходу до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі виконувалась за допомогою стандартних та розроблених програм в середовищі Matlab/Simulink із використанням експериментальних даних – загальнодоступного набору даних мережевих атак. При цьому використовувалась безкоштовна навчальна версія пакета прикладних програм Matlab/Simulink, тому додаткові капітальні витрати не виникають.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки становитимуть 5000 грн.

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

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} =$$
$$= 36285,43 + 5000 = 41285,43 \text{ грн.}$$

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.).

Середовище MATLAB/Simulink, яке застосовується для оцінки ефективності запропонованого підходу щодо класифікації атак в інформаційно-комунікаційних мережах з використанням систем нечіткого висновку, вже використовується на підприємстві, тому додаткові 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 10000 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 18500 грн. Додаткова заробітна плата – 5% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,1 ставки. Отже,

$$С_з = (18500*12 + 18500*12*0,05)*0,1= 23310 \text{ грн.}$$

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

$$С_{єв} = 23310*0,22 = 5128,2 \text{ грн.}$$

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=0,9 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:

$$С_{ел} = 0,9*6*1920*1,68 = 17418,24 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 2%

$$С_{тос} = 41285,43*0,02 = 825,7 \text{ грн.}$$

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

$$С_к = 10000+23310+5128,2+17418,24+825,70 = 47682,14 \text{ грн.}$$

Витрати, які 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 20%.

Тому:

$С_{ак}$= 41285,43*0,2=8257,09 грн.

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

С = 47682,14 + 8257,09 = 55939,23 грн.

3.3 Оцінка можливого збитку

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

Оцінка можливого збитку від атаки на вузол або сегмент мережі

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, 2 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 3 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 25000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 18000 грн./міс.;

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

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 5 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 500 тис. грн. на рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, 0 грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 30.

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:

$$П_п = \frac{\sum З_с}{F} t_п = \frac{18000 * 5}{176} * 2 = 1022{,}72 \text{ грн},$$

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 $t_{ви}$:

$$П_{ви} = \frac{\sum З_с}{F} t_{ви} = \frac{18000 * 5}{176} * 3 = 1534{,}09 \text{ грн.}$$

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

$$П_{пв} = \frac{\sum З_в}{F} t_в = \frac{25000*1}{176} * 2 = 284{,}09 \text{ грн.}$$

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

$$П_в = 1534{,}09+284{,}09 = 1818{,}18 \text{ грн.}$$

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:

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ})$$

$$V = \frac{500000}{2080} \cdot (2 + 2 + 3) = 1682{,}69 \text{ грн.}$$

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

$$U = 1022{,}72+1818{,}18+1689{,}69 = 4530{,}59 \text{ грн.}$$

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

$$B = \sum_i \sum_n U = \sum_1 \sum_{30} 4530{,}59 = 135917{,}7 \text{ грн.}$$

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

R – вірогідність успішної реалізації загрози (60%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$$E = 135917,7*0,6- 55939,23 = 25611,39 \text{ грн.}$$

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 Е – загальний ефект від впровадження системи інформаційної безпеки грн.;

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI=25611,39 / 41285,43=0,62, \text{ частки одиниці.}$$

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, (6%); $N_{інф}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,62 > (6 – 5)/100 = 0,62 > 0,01.$$

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

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

$$T_0= 1 / 0,62 = 1,61 \text{ років.}$$

3.6 Висновок

Отже, згідно з наведеними розрахунками можливо зробити висновок, що розробка підходу до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі є економічно доцільною.

Капітальні витрати, які складають 41285,43 грн, дозволяють отримати ефект величиною 25611,39 грн. Відповідно до отриманих значень показників економічної можна зазначити, що запропонований підхід дозволить отримувати 0,62 економічного ефекту на 1 грн. капітальних витрат (коефіцієнт повернення інвестицій ROSI складає 0,62 грн.). Термін окупності при цьому складатиме 1,61 років.

ВИСНОВКИ

Основні результати кваліфікаційної роботи полягають у наступному:

1. Встановлено, що 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.

Питання забезпечення необхідного рівня мережевої безпеки та захисту від атак активно вивчаються різними дослідниками у галузі систем штучного інтелекту, оскільки такі системи дозволяють вирішувати завдання пошуку аномалій, виявлення взаємозв'язків усередині даних тощо. Однак, у будь-якій з таких систем формування інтелектуальних рішень, результат, як правило, залежить як від інструментів і алгоритмів навчання, що використовуються, так і від якості даних, на яких будується інтелектуальна модель.

2. 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 класифікації інцидентів кібербезпеки на реальному мережевому трафіку.

3. В результаті аналізу найбільш відомих спеціалізованих загальнодоступних наборів розмічених даних, що використовуються для оцінки виявлення мережевих атак встановлено, що більшість з них було розроблено з головною метою – надати дослідникам можливість порівняти різні методи виявлення в однакових умовах. Встановлено основні вимоги до цих наборів даних. Для подальших досліджень було обрано базу UNSW-NB15, яка достатньо нова (була створена у 2015 р.), у ній були виправлені недоліки

попередніх баз – KDD CUP 99 та NSL KDD, а також додано нові сучасні види атак.

4. Запропоновано підхід до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі, який полягає у використанні однопараметричної оптимізації (методу Фібоначчі) для вибору параметрів інтелектуальних класифікаторів (на основі алгоритмів субтрактивної кластеризації та нечіткої кластеризації C-середніх). Метод Фібоначчі налаштовував наступні параметри алгоритмів нечіткої кластеризації: для субтрактивної кластеризації – діапазон впливу кластерного центру R_c; для нечіткої кластеризації C-середніх – число кластерів k_c.

5. Оцінка ефективності запропонованого підходу виконувалась в середовищі Matlab/Simulink за допомогою стандартних і розроблених програм. На прикладі експериментальних даних (набору даних UNSW-NB15) оцінено ефективність отриманих класифікаторів на основі алгоритмів нечіткої кластеризації.

ПЕРЕЛІК ПОСИЛАНЬ

1. 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.

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

3. 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.

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

5. Карачанская Е.В. Метод выявления аномалий сетевого трафика, основанный на его самоподобной структуре / Е.В. Карачанская, Н.И. Соседова // Безопасность информационных технологий. – 2019. – С. 98-110.

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

7. Jin S. Intrusion Detection System Enhanced by Hierarchical Bidirectional Fuzzy Rule Interpolation / S. Jin, Y. Jiang, J. Peng. // 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC). – Miyazaki, Japan, 2018. – Pp. 6-10. – DOI 10.1109/SMC.2018.00010.

8. Бекетова Г., Ахметов Б., Корченко А., Лахно В. Разработка модели интеллектуального распознавания аномалій и кибератак с использованием логических процедур, базирующихся на покрытиях матриц признаков //

Ukrainian Scientific Journal of Information Security. – 2016. – Vol. 22, issue 3. – P. 242-254.

9. Петров О., Корченко О., Лахно В. Метод та модель інтелектуального розпізнавання загроз інформаційно-комунікаційному середовищу транспорту // Ukrainian Scientific Journal of Information Security, 2015. – Vol. 21, issue 1. – P. 26-34

10. 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.

11. 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.

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

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

14. Carbonneau M.A. Multiple instance learning: A survey of problem characteristics and applications / M.-A. Carbonneaua, V. Cheplygina, E. Grangera, G. Gagnon // Pattern Recognition. – 2018. – Vol. 77. – P. 329– 353.

15. Kuncheva L. Combining pattern classifiers: methods and algorithms / L. Kuncheva. – John Wiley & Sons, 2004. – 350 p.

16. Shtovba S., Shtovba O., Petrychko M. Detection of Social Network Toxic Comments with Usage of Syntactic Dependencies in the Sentences / Proc. of the Second International Workshop on Computer Modeling and Intelligent Systems, Zaporizhzhia, Ukraine, April 15-19, 2019. CEUR Workshops Proceeding, Vol. 2353. – 2019. – P. 313-323

17. Zambon, M., Lawrence, R., Bunn, A., Powell, S. Effect of alternative splitting rules on image processing using classification tree analysis // Photogrammetric Engineering & Remote Sensing. – 2006. – Vol. 72, №1, P. 25- 30.

18. Zhang M. L., A review on multi-label learning algorithms / M.L. Zhang, Z. H. Zhou // IEEE transactions on knowledge and data engineering. – 2014. – Vol. 26. – №.8. – P. 1819-1837.

19. Anderson James P. Computer Security Threat Monitoring and Surveillance: Technical Report / James P. Anderson // James P. Anderson Company, Fort Washington, 1980.

20. Axelsson Stefan. Intrusion detection systems: A survey and taxonomy. / Stefan Axelsson // Technical report, 2000. – Vol. 99. – P. 101-127.

21. Debar H. A revised taxonomy for intrusion detection systems / H. Debar, M. Dacier, A. Wespi // In Annales des télécommunications. – 2000. – Vol. 55. – No. 7-8. – P. 361-378.

22. Liao H.-J. Intrusion detection system: a comprehensive review / Liao H.-J., Lin C.-HR., Lin Y.-C., Tung K.-Y. // Journal of Network and Computer Applications. – 2013. – Appl 36(1). – P. 16-24.

23. Павлов І.М. Аналіз таксономії систем виявлення атак у контексті сучасного рівня розвитку інформаційних систем / І.М. Павлов, С.В. Толюпа, В.І. Ніщенко // Сучасний захист інформації. – 2014. – №4. – С. 44-52.

24. Ghorbani Ali A. Network Intrusion Detection and Prevention: concept sand techniques. / Ali A. Ghorbani, Wei Lu, Mahbod Tavallaee // London: Springer. – 2010. – P. 27-49.

25. Manasi G. Taxonomy of Anomaly Based Intrusion Detection System: A Review / G. Manasi, Yadav Rana // International Journal of Scientific and Research Publications. – 2012. – Vol. 2, Issue 12. – P. 122-131.

26. Luo J. Mining fuzzy association rules and fuzzy frequency episodes for intrusion detection / J. Luo, S.M. Bridges // International Journal of Intelligent Systems, 2000. – Vol. 15, No. 8. – P. 687-704.

27. Sundaram A. An introduction to intrusion detection / A. Sundaram. – 1996. [Електронний ресурс]. – Режим доступу: http://www.cs.purdue.edu/coast/archive/data/categ24.html.

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

29. Lunt T. A prototype real-time intrusion-detection expert system / T. Lunt, R. Jagannathan // Proceedings of 1988 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, California. – April 18-21, 1988. – P. 59-66.

30. Teng H. Adaptive real-time anomaly detection using inductively generated sequential patterns / H. Teng, K. Chen, S. Lu // Proceedings of 1990 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, California. – May 7-9, 1990. – P. 278-84.

31. Debar H. A neural network component for an intrusion detection system / H. Debar, M. Becker, D. Siboni // In Proceedings of 1992 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, California. – May 4-6, 1992. – P. 240-50.

32. 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.

33. Моделювання та аналіз безпеки розподілених інформаційних систем / В.В. Литвинов, В.В. Казимир, І.В. Стеценко [та ін.]. – Чернігів: Чернігівський національний технологічний університет, 2017. – 206 с

34. Толюпа С.В. Класифікаційні ознаки систем виявлення атак та напрямки їх побудови. / С.В. Толюпа, С.С. Штаненко, Г. Берестовенко // Збірник наукових праць Військового інституту телекомунікацій та інформатизації ім. Героїв Крут. – № 3. – 2018. – С. 56-66.

35 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.

36. Зоріна Т.І. Системи виявлення і запобігання атак в комп'ютерних мережах / Т.І. Зоріна // Вісник східноукраїнського національного університету ім. В. Даля. – № 15 (204), ч.1. – 2013. – С. 48-54.

37. Valdes A. Adaptive model-based monitoring for cyber attack detection / A. Valdes, K. Skinner // In: Proc. of the Recent Advances in Intrusion Detection (Toulouse, France, 2000) – 2000. – P. 80-92.

38. 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.

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

40. 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.

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

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

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

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

45. Baddar S.A.-H., Merlo A., Migliardi M. Anomaly Detection in Computer Networks: A State-of-the-Art Review // Journal of Wireless Mobile Networks,

Ubiquitous Computing, and Dependable Applications. – 2014. – Vol. 5. no. 4. – P. 29–64.

46. Gyanchandani M. Taxonomy of Anomaly Based Intrusion Detection System: A Review / M. Gyanchandani, J.L. Rana, R.N. Yadav // International Journal of Scientific and Research Publications. – 2012. – Vol. 2. Issue 12. – P. 1-13.

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

48. Ring M. A Survey of Network-based Intrusion Detection Data Sets / M. Ring, S. Wunderlich, D. Scheuring, D. Landes, A. Hotho // Computers & Security. – 2019. – Vol. 86. – P. 147-167.

49. A Detailed Analysis of Benchmark Datasets for Network Intrusion Detection System / Reem Alshamy, Suad Othman Mossa Ghurab, Ghaleb Gaphari, Faisal Alshami // Asian Journal of Research in Computer Science. – 2021. – Vol. 7. – Issue 4. – P. 147-167.

50. Sarker I.H. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions / Sarker I.H., Furhad M.H., Nowrozy R. // SN Computer Science. – 2021. – Vol. 2. – Issue 3. –P. 173-197.

51. Sharafaldin I. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. / I. Sharafaldin, A.H. Lashkari, Ali A. Ghorbani // Proc. of the 4th International Conference on Information Systems Security and Privacy (ICISSP), 2018. – P. 108-116.

52. Moustafa Nour, Jill Slay. The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. // Information Security Journal: A Global Perspective (2016): 1-14

53. Ivakhnenko A.G. Inductive learning algorithms for complex systems modeling / A.G. Ivakhnenko, H.R. Madala – London, Tokyo: CRC Press, 1994. – 384 p.

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	44	
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	2	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація Старостенко.ppt

2 Диплом Старостенко.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 125м-21-1 Старостенко А.О. на тему: «Виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 88 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на дослідження та обґрунтування алгоритмів нечіткої кластеризації, що дозволяють виконувати класифікацію вхідного трафіку мережі для ідентифікації різних інцидентів кібербезпеки.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу сучасних систем виявлення вторгнень і атак в інформаційно-комунікаційних системах і мережах, основ нечіткої логіки та алгоритмів нечіткої кластеризації, а також існуючих наборів даних для оцінки виявлення мережевих атак в ній сформульовані задачі, вирішенню яких присвячений спеціальний розділ. У ньому було запропоновано підхід до виявлення атак в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації та методу Фібоначчі та шляхом моделювання оцінено його ефективність.

Наукова новизна результатів полягає у тому, що було запропоновано виявляти атаки в інформаційно-комунікаційних мережах з використанням алгоритмів нечіткої кластеризації; при цьому параметри цих інтелектуальних класифікаторів було налаштовано методом Фібоначчі

Практична цінність роботи полягає в тому, що отримані інтелектуальні класифікатори 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 відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

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

Керівник роботи,
к.т.н., доцент **С.М. Мацюк**