Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Виявлення вторгнень на основі аналізу аномалій мережевого трафіку

Виконала:
студентка VI курсу, групи СБмд-61
спеціальності 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

(підпис) Чорна Ю.Р. (прізвище та ініціали)

Керівник (підпис) Баран І.О. (прізвище та ініціали)

Нормоконтроль (підпис) Тимощук Д.І. (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н.В. (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль - 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студентці Чорній Юлії Ростиславівні
(прізвище, ім'я, по батькові)

1. Тема роботи Виявлення вторгнень на основі аналізу аномалій мережевого трафіку

Керівник роботи Баран Ігор Олегович, к.т.н., доц., декан ФІС
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора «22» 11 2024 року № 4/7-1120

2. Термін подання студентом завершеної роботи 27.12.2024 р.

3. Вихідні дані до роботи наукові літературні джерела

4. Зміст роботи (перелік питань, які потрібно розробити)
1. Аналіз предметної області.
2. Мережеві аномалії та методи їх детектування.
3. Практична частина.
4. Охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Тема роботи. 2. Актуальність. 3. Мета, задачі дослідження, об'єкт, предмет дослідження. 4. Наукова новизна, практичне значення роботи. 5. Класифікація СВВ. 6. Зіставлення атак з аномаліями. 7. Систематика методів виявлення аномалій. 8. Виявлення аномалій на основі фрактального аналізу. 9. Алгоритм розрахунку еталонів 10. Порядок дій роботи методу виявлення аномалій на основі обчислення параметра Херста. 11. Базова архітектура СВА. 12. Діаграма варіантів використання. 13. Інтерфейс користувача. 14. Схема мережі для тестування. 15. Результати роботи 16. Висновки. Основні результати дослідження

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., зав. каф. КС		
Безпека в надзвичайних ситуаціях	Стручок В.С., ст. викл. каф. ОХ		

7. Дата видачі завдання 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	22.11 – 23.11	*Виконано*
2.	Підбір джерел про виявлення вторгнень на основі		
	аналізу мережевого трафіку	24.11 – 26.11	*Виконано*
3.	Опрацювання джерел про виявлення вторгнень		
	на основі аналізу аномалій мережевого трафіку	27.11 – 30.11	*Виконано*
4.	Виконання дослідження щодо розробки ПЗ для		
	виявлення вторгнень на основі аналізу аномалій		
	мережевого трафіку	01.12 – 06.12	*Виконано*
5	Розробка алгоритмів функціонування моделей	07.12 – 10.12	
6.	Оформлення розділу «Аналіз предметної області»	11.12 – 13.12	*Виконано*
7.	Оформлення розділу «Аномалії в мережі та методи їх	14.12 – 15.12	*Виконано*
	детектування»		
8.	Оформлення розділу «Практична частина»	16.12 – 18.12	*Виконано*
9.	Виконання завдання до підрозділу «Охорона праці та		
	безпека в надзвичайних ситуаціях»	06.12 – 16.12	*Виконано*
10.	Оформлення кваліфікаційної роботи	14.12 – 19.12	*Виконано*
11.	Нормоконтроль	18.12 – 20.12	*Виконано*
12.	Перевірка на плагіат	16.12 – 19.12	*Виконано*
13.	Попередній захист кваліфікаційної роботи	17.12 – 20.12	*Виконано*
14.	Захист кваліфікаційної роботи	28.12	

Студент _____ Чорна Ю.Р.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Баран І.О.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Виявлення вторгнень на основі аналізу аномалій мережевого трафіку // Чорна Юлія Ростиславівна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем та програмної інженерії, кафедра кібербезпеки, група СБмд-61 // Тернопіль, 2024 // С. – 70, рис. – 9, табл. – 3, слайдів – 16, бібліогр. – 23.

Ключові слова: мережевий трафік, комп'ютерна мережа, аномалія, параметр Херста, Golang, сніффер, виявлення вторгнень

В першому розділі наведено класифікацію систем виявлення вторгнень. Наведено переваги та недоліки описаних систем. Досліджено специфіку різних атак, способи їх втілення і особливості використання.

У другому розділі розглянута систематика аномалій, окремо виділено групи - точкові, контекстні, колективні. Досліджено методи виявлення аномалій (поведінкові, машинного навчання, обчислювального інтелекту, на основі знань). Докладно розглянуто методи на базі фрактального аналізу і самоподібності трафіку мережі. Проаналізовано принципи функціонування двох алгоритмів детектування аномалій мережі із застосуванням параметра Херста.

У третьому розділі було створено базову систему виявлення вторгнень, описано її основні складові частини. Для тестування роботи системи побудовано комп’ютерну мережу. Результати проведених експериментів свідчать, що система може ефективно та якісно виявляти колективні та розподілені в часі атаки. Запропоновано шляхи можливого удосконалення роботи розробленої системи.

У четвертому розділі розглянуто важливі питання охорони праці та безпеки життєдіяльності.

ANNOTATION

Detection of intrusions based on analysis of network traffic anomalies // Chorna Yuliia // Ternopil Ivan Pul'uj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security // Ternopil, 2024 // P. - 70, Fig. - 9, Table - 3, Slides - 16, References - 23.

Keywords: network traffic, computer network, anomaly, Hurst parameter, Golang, snifer, intrusion detection

The first chapter provides a classification of intrusion detection systems. The advantages and disadvantages of the described systems are given. The specifics of various attacks, ways of their implementation and features of use are studied.

In the second chapter, the systematics of anomalies is considered, groups - point, context, collective - are highlighted separately. Methods of detecting anomalies (behavioral, machine learning, computational intelligence, knowledge-based) were studied. Methods based on fractal analysis and self-similarity of network traffic are considered in detail. The principles of functioning of two network anomaly detection algorithms using the Hurst parameter are analyzed.

In the third chapter, a basic intrusion detection system was created and its main components were described. A computer network was built to test the system. The results of the conducted experiments show that the system can efficiently and qualitatively detect collective and time-distributed attacks. Ways of possible improvement of the work of the developed system are proposed.

The fourth chapter deals with important issues of labor protection and life safety.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ СКОРОЧЕНЬ І ТЕРМІНІВ

DoS (denial-of-service attack) – атака на відмову в обслуговуванні.

DDos ((distributed) denial-of-service attack) – розподілена атака на відмову в обслуговуванні.

R2U / R2L – Remote to User / Remote to Local.

U2R – User to Root.

Аномалія – відхилення від норми, загальної закономірності, яке характеризує неправильність поведінки.

БД – база даних.

ГА – генетичний алгоритм.

ГП – генетичне програмування.

Експлойт - комп'ютерна програма, фрагмент програмного коду або послідовність команд, які використовують уразливості у ПЗ та застосовуються для проведення атаки на обчислювальну систему.

ІС – інформаційна система.

МН – машинне навчання.

МСВВ (Network-based IDS) – мережева система виявлення вторгнень.

ПЗ – програмне забезпечення.

СВА – система виявлення аномалій.

СВВ (IDS – Intrusion Detection System) – система виявлення вторгнень (програмний або програмно-апаратний комплекс, який призначений для виявлення аномальних впливів та деяких типів шкідливої активності, які можуть порушити безпеку інформаційної системи).

ХСВВ (Host-based IDS) – хостова система виявлення вторгнень.

ЦП – центральний процесор.

ШНМ – штучна нейронна мережа.

ЗМІСТ

ВСТУП

Актуальність теми. Фактично головним показником сучасного світу можна назвати повномасштабну інформаційну інтеграцію, котра базується на створенні комп'ютерних мереж розмірів підприємства та подальшому їх об'єднанні через Інтернет. Труднощі у логічній і фізичній організації теперішніх мереж веде до справедливих складнощів у вирішенні питань їх керування і забезпечення захисту. Під час розв’язання задач, пов'язаних із діагностуванням і захистом ресурсів мережі, основним питанням постає своєчасне детектування станів мережі, котрі ведуть до станів, при яких мережа стає непридатною для використання, наприклад до втрачення повного чи часткового її працездатного стану, знищення, спотворення або витікання даних. Це наслідок відмов, випадкових відмов або результат одержання зловмисником несанкціоновано мережних ресурсів, проникнення різного роду черв'яків, вірусів і інших загроз інформаційній безпеці. Детектування таких станів на ранніх етапах дасть змогу своєчасно вжити заходів щодо протидії загрозам і, відповідно, запобігатиме можливим катастрофічним наслідкам.

Щоб детектувати загрози застосовується широкий набір спеціалізованих засобів. Зокрема, при вирішенні складних проблем із діагностуванням мереж використовуються інструменти систем керування, сніффери, системи тестування навантаження, інструменти для моніторингу і аналізу трафіку мережі та ін. Питання захищеності мережевих інформаційних ресурсів вирішуються при допомозі firewalls, антивірусів, СВВ, засобів контролювання цілісності, криптографічних засобів захисту. Специфічними ознаками їх застосування є чи їх періодичне та нетривале застосування з метою вирішення якоїсь визначеної проблеми, чи безперервне застовування, проте зі статичними налаштуваннями. Як наслідок, методи аналізу, котрі застосовуються в сучасних системах, скеровані на детектувнаня існуючих і чітко описаних типів впливів, однак досить часто не є в змозі детектувати їх модифікації чи нові типи, а це робить їх використання практично неефективним.

Підхід, котрий є основою більшості праць, це відшукання методів аналізу

трафіку, котрі ефективно детектують аномальні стани інформаційних засобів. Він дає змогу детектувати відомі та свіжі типи вторгнень. Наявні СВВ часто орієнтовані на використання на конкретній системі чи обладнанні, що накладає обмеження на застосування таких систем у широкому масштабі.

Мета дослідження: розробити СВВ, в основі якої використовуються методи детектування аномалій трафіку мережі. Розроблювана система має бути простою для використання та налаштування, окрім того повинна легко переноситися між різноманітними програмними системами.

Задачі дослідження:

– здійснити аналіз відомих методів детектування аномалій;

– систематизувати загрози в ІС;

– побудувати та реалізувати архітектуру ПЗ для ефективного виявлення аномалій;

– тестування та коригування параметрів системи для виявлення конкретного типу загроз.

Об’єкт дослідження: мережевий трафік у комп'ютерних мережах.

Предмет дослідження: механізми виявлення аномалій мережевого трафіку.

Методи дослідження: наукові роботи українських та зарубіжних вчених за темою дослідження, фундаментальні положення інформаційної безпеки; методи - аналітичний, порівняльний, системного аналізу, індукції та проектування.

Наукова новизна отриманих результатів:

– запропоновано для розрахунку оцінки аномальності трафіку використовувати показник Херста;

– реалізовано два алгоритми розрахунку параметра Херста - RS-метод та метод обчислення параметра Херста на основі самоподібності мережевого трафіку.

Практичне значення одержаних результатів. Отримані в роботі результати знайдуть своє застосування для виявлення колективних та розподілених атак на систему в різних установах та організаціях.

Апробація. Окремі результати дослідження апробовано на XII науково-технічній конференції «Інформаційні моделі, системи та технології» у вигляді

опублікованих тез.

Структура роботи. Робота складається з пояснювальної записки та графічної частини. Пояснювальна записка складається з вступу, 4 розділів, висновків, списку використаної літератури та додатків. Обсяг роботи: пояснювальна записка – 70 арк. формату А4, графічна частина – 16 слайдів.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Поняття СВВ та їх характеристики

Вторгнення в ІС є діями, котрі здатні порушити безпекову систему принципів, а детектування вторгнень – це процес, який використовується для розпізнавання вторгнень. Детектування вторгнень розглядається упродовж десь років тридцяти. Стандартний підхід базується на переконаннях, за якими поведінка зловмисника буде істотно відрізнятися від поведінки звичайного юзера і що множина несанкціонованих операцій буде виявлена.

Аномальними впливами можуть бути мережеві атаки різного роду, неавторизований доступ до системи або дії шкідливого ПЗ. Сама власне система виконує роль пасивного захисту. Усі інциденти інформаційної безпеки, що виникають, фіксуються і передаються у звітному вигляді кінцевому користувачеві або адміністратору комп'ютерної мережі. Сигнали щодо загроз у подальшому не будуть опрацьовуватися у таких системах. Для їх опрацювання вже застосовуються системи запобігання вторгненням, котрі вже є власне активними елементами захисту.

Можна класифікувати СВВ за різними ознаками [1]. Наприклад, за розміщенням агента системи в конкретний момент. Є сукупність засобів СВВ, котрі оперують інформацією, отриманою від одного хоста, ХСВВ та такі СВВ, котрі оперують інформацією, одержаною із цілого фрагменту локальної мережі (МСВВ)) та комбінована гібридна СВВ.

Класифікація систем виявлення вторгнень наведена нижче:

- ХСВВ;
- МСВВ;
- гібридна СВВ.

ХСВВ розміщена сервері або робочій станції, і опрацьовує ті дані, котрі одержані із середини самої системи, і майже не застосовує зовнішні пристрої. ХСВВ детектує порушення через внутрішню активність системи. Як приклад таких активних дій можна розглянути раптову спробу редактора тексту

користувача через завантаження даних спробувати змінити БД системних паролів. Також така система має спостерігати за станом застосування оперативної пам'яті, часу процесора та ін. ХСВВ можна уявити у комп'ютерній системі агентом, котрий пильнує внутрішні прагнення обійти встановлену політику безпеки. ХСВВ здатні відслідковувати стани лише деяких робочих машин, де інстальовані агенти, та не здатні займатися моніторингом всієї мережі.

Недоліки ХСВВ:

– складність аналізу спроб вторгнення кілька комп'ютерів;

– складність підтримування єдиної ХСВВ у потужній мережі, котра має різні варіанти операційних систем та конфігурацій;

– можуть перестати працювати, як тільки систему зламають.

Наведемо приклади тізних СВВ.

Системи, котрі відзначають намагання під’єднаня (RealSecure Agent, PortSentry). Вони перевіряють вхідні та вихідні мережеві підключення хоста. Системи особливо ефективні при детектування неавторизованих спроб встановлення TCP і UDP з'єднань, і навіть детектування спроб сканування портів.

Системи, котрі перевіряють мережевий вхідний трафік. Вони захищають хост, шляхом перехоплення підозрілих мережевих пакетів та аналізуючи їх на присутність у них корисного навантаження (якогось шкідницького коду).

Системи, що слідкують за активністю входу в систему на мережному рівні свого хоста (HostSentry). Їхня роль полягає у відслідковуванні спроб входу та виходу з системи, відшуканні нестандартної активності, котра трапляється у якийсь несподіваний час, у певних місцях у мережі, чи детектуванні надзвичайно частих спроб входження в систему (саме невдалих).

ХСВВ, які спостерігають лише за локальним трафіком, здатні досить просто виявити local-to-local або local-to-root атаки, так як їм притаманне чітке представлення щодо локальної доступної інформації, для прикладу, вони здатні використовувати СВВ юзера. Більше того, засоби детектування аномалій значно краще розуміються на внутрішніх проблемах, так як їхня спосібність

детектування базується на нормальній поведінці користувача.

ХСВВ міститься на визначеній машині і забезпечує захист визначеної системи. Вони не тільки мають засоби моніторингу системи, а і також мають інші елементи усталеної СВВ. Snort, Dragon Squire, Emerald eXpert-BSM, NFR HID, Intruder Alert призначені для здійснення такого типу моніторингу.

МСВВ зазвичай складаються з мережного пристрою (або давача) з картою мережного інтерфейсу (NIC), що працює в нерозбірливому режимі, та своїм інтерфейсом керування. СВВ розміщується вздовж фрагмента чи межі мережі та відстежує весь трафік у цьому фрагменті. МСВВ здатні виконувати збір та аналіз даних для детектування відомих атак через зіставлення сигнатур чи шаблонів у БД або детектування незаконних операцій через проведення сканування трафіку на присутність аномальної активності. МСВВ надає інформацію щодо використання всього сегмента мережі, до котрого вона під'єднана. МСВВ знову збирає та аналізує всі мережеві пакети, що надходять на карту мережного інтерфейсу, що працює в нерозбірливому режимі. Справа не лише у тих пакетах, котрі йдуть до визначеного хосту, так як всі комп'ютери в сегменті мережі користуються захистом МСВВ. Також МСВВ можна встановити на активних складових частинах мережі, як варіант - на маршрутизаторах. Так як при детектуванні вторгнень (для прикладу, якоїсь flood-атаки) застосовуються дані статистики мережевого навантаження, конкретний тип МСВВ можна сконфігурувати на детектуванні тільки цього типу властиво вторгнень (Novell Analyzer, Microsoft Network Monitor). Будуть захоплені всі пакети, котрі бачать у фрагменті мережі, не проводячи їх аналіз, а тільки зосереджуючись на створенні статистики мережного трафіку. Типовими МСВВ є: Cisco Secure IDS (раніше NetRanger), Hogwash, Dragon, E-Trust IDS.

Керування та оповіщення як від мережевих, так і від хостових пристроїв детектування вторгнень, та створення їх чіткоє спільної конфігурації приведе до єдиної схеми - централізованого керування детектуванням вторгнень. І мережеві, і хостові СВВ володіють своїми унікальними перевагами та недоліками. СВВ на основі мережі простіше у розгортанні та дешевша у купівлі та обслуговуванні. Проте їхня продуктивність залежить від відомих експлойтів безпеки та сигнатур.

Якщо застосовується новий експлойт, про який СВВ нічого не відомо, тоді система здатна просто не детектувати атаку. ХСВВ, в більшості, перебуває в залежності від рівня адміністратора безпеки, котрий формує конфігурацію та слідкує за функціонуванням даної системи. Надбання скілів щодо роботи з цим ПЗ, його обслуговування та моніторинг можуть стати складною задачею. Отже, самий кращий підхід – це застосування комбінації найкращих можливостей СВВ на базі мережі і хоста для покращення стійкості до атак та гарантування більшої гнучкості. Зазвичай, такий підхід зветься гібридною СВВ.

Методи, котрі застосовуються у існуючих СВВ, можна представити так:

– сигнатурні;
– аномально-орієнтовані;
– гібридні.

СВВ на базі сигнатур функціонує завдяки відшуканню за шаблонами атак, котрі вже відомі. Така система є залежною від одержання стабільних по часу оновлювань для шаблонів і не здатна детектувати невідомі старі загрози, котрі відсутні у базі шаблонів, чи вже нові атаки. Однією із найбільших проблем такого типу СВВ є те, що кожна сигнатура потребує запису у БД, тому повна БД ймовірно може мати сотні чи, можливо, і тисячі записів. Будь-який пакет вимагає порівняння із усіма записами у БД. Це може бути дуже ресурсомістким процесом, і це призведе до уповільнення пропускної спроможності та ускладнення у функціонуванні СВВ. Створення шаблонів, котрі б описували всі ймовірні варіації атак визначеного типу, так і є невирішеною задачею. На додачу такі системи надзвичайно уразливі для DoS-атак. Окремі інструменти обходу СВВ здатні використати таку вразливість і заповнити системи СВВ на базі сигнатур завеликим числом пакетів настільки, що СВВ не здатна справитися з трафіком Це веде до тайм-ауту СВВ та ігнорування пакетів і, в результаті, можлива атака буде пропущена чи трапиться відмова у функціонуванні мережі. На додачу до всього, такі СВВ, як і раніше, уразливі для атак, котрі є невідомими, так як для їх детектування система застосовує сигнатури, котрі є в цей час в БД.

В основі другого типу систем лежить твердження, що абсолютно всі атаки

чимось несхожі на нормальну поведінку. Такий тип детектування перебуває в залежності від класифікації мережі на, властиво, нормальну і аномальну. Так як така класифікація базується на положеннях або евристиці, а не на шаблонах чи сигнатурах, і для втілення такої системи перш за все необхідно знати поведінку мережі, яка є звичайною. З цією метою система на старті свого функціонування створює профілі нормальної поведінки.

СВВ на базі аномалій на противагу попередньому виду систем здатна детектувати раніше невідомі загрози, проте ймовірність помилкового спрацьовування вище. Сигнатура нової атаки невідома доти, доки її не буде виявлено і ретельно проаналізовано. Тож важко щось точно сказати маючи лише малу кількість пакетів. Тут системи на основі аномалій детектують аномальну поведінку і виробляють сигнали тривоги на базі відмінності мережного трафіку від нормального профілю трафіку чи поведінки застосунків. Характерна аномальна поведінка, котра може бути виявлена, містить

– використання нестандартних портів;
– різке збільшення UDP, TCP пакетів;
– аномальне звертання до ресурсів системи.

Значними проблемами СВА є встановлення нормальної поведінки мережі, встановлення порогу спрацьовування тривоги і уникнення помилкових тривог. Користувачами мережі, як правило, є люди, а їх поведінка в окремих випадках не піддається передбаченню. За умови, що нормальна модель не детектована чітко, значить буде значне число помилкових спрацьовувань, і така СВА зазнаватиме проблем через зменшення продуктивності.

1.2 Класифікація загроз

Атакою на ІС називаються навмисні дії зловмисника, які використовують уразливості ІС та ведуть до відхилення від встановлених правил для доступності, цілісності та конфіденційності даних, котрі опрацьовуються [2].

Усунення вразливості ІС призводить до усунення і можливості, властиво,

реалізації атак.

Згідно з [3] fтаки поділяються на такі типи.

Розвідка. Містять ping sweeps, передачу DNS -зони, розвідку за допомогою e-mail, сканування TCP або UDP портів, проведення аналізу публічно доступних серверів з метою знаходження cgi -дірок. Такі атаки є достатньо поширеними способами збирання інформації щодо апаратного- та ПЗ комп'ютерів, під'єднаних до мережі, а також дізнатися число таких пристроїв. Якщо така атака хостова, то ймовірне перевіряння можливості втілення визначених типів вразливостей, котрі одержані при збиранні інформації. Цей вид атаки застосовується для одержання корисної інформації щодо хостів, дійсних IP -адрес, ОС і т. д. через сканування мережі у визначеному режимі. Атакуючий застосовує таку інформацію для відшукання потенційних вразливостей системи для їх наступного застосування при втіленні атак щодо комп'ютерів та служб. Стандартними прикладами атаки може бути таке сканування:

– мережі, я варіант, утилітою nmap, що дозволить здійснити перевірку відкритості порту, котрий цікавить;

– усіх наявних портів для одержання інформації щодо типу хоста жертви та які сервіси на ньому запущені та доступні;

– повної мережі.

Експлойт прямо не втілюється, так зловмисник уже має мати хоча б якийсь доступ до системи. Проте може застосовуватися зголом при втіленні DDoS -атак як вузл ботнет мережі.

U2R – атака, за якої зловмисник хоче одержати незаконним шляхом доступ до акаунту адміністратора, щоб маніпулювати чи зловживати необхідними засобами. Такі порушення складно розпізнати серед стандартного трафіку серез те, що вони хочуть одержати привілегії в системі, на що здатні лише авторизовані користувачі. Перш за все при втіленні цієї атаки зловмиснику необхідно отримати дані для автентифікації якого-небудь юзера або сервісу, що працює в системі. Для цього застосовують брутфорс, фішинг, соціальну інженерію, іншими словами можна навіть не застосовувати саму мережу машин, де функціонує система. Щойно зловмисник одержав дані для аутентифікації,

проходить більш детальний аналіз ПЗ, що використовується, в подальшому відшукання способів втілення уразливостей, щоб підвищити свій рівень доступу аж до адміністраторського. Ці атаки можуть належати до різних типів: переповнення буфера, при якому програма атакуючого відправляє в буфер великі обсяги даних без перевірки його ємності, використання руткітів, завантажувачів та інші.

R2U (R2L) втілюється, коли зловмисник прагне одержати локальний доступ як локал-юзера цільової машини, для отримання привілею надсилати мережеві пакети. Такі атаки схожі на атаки на перевищення прав доступу. Містить відправлення віддаленому комп'ютеру чи хосту мережевих пакетів, законним юзером якої система не може бути. Потім аналогічно до адміністратора чи користувача, атакуючий хоче здобути доступ до системи та виконати шкідливі дії. Двома її варіантами, які найчастіше зустрічаються є переповнення буфера та атака із вхідними даними, котрі неперевірені. Також вони вчиняються проти громадських сервісів чи через з'єднання із захищеними службами.

DoS. Такою атакою зловмисник пробує зруйнувати службу (або машину), перевантажити мережу, центральний процесор чи переповнити диск. DoS -атаки часто трапляються і володіють безліччю різновидів. Ці атаки вчиняються, щоб заблокувати доступ до визначених ресурсів, з цією метою стають недоступними визначені мережеві служби або на деякий час скидаються усі мережеві з'єднання. Незважаючи на сьогоднішні реалії при покупці сервісу захисту від DoS -так ваша служба буде, ймовірно, недоступною, оскільки провайдер захисту (cloudflare, amazon shield) сам зробить ваші сервіси такими, щоб захистити власні ресурси. Як правило DoS- атаки обтяжують ресурси цільової системи дуже великою кількістю запитів, що потрібна послугу не можливо їй надати. Однак перевантажуються не тільки ресурси системи, а й сам системний канал доступу та відповідних сервісів, що може призвести до ще гірших наслідків. Інколи такі атаки можуть на деякий час припинити доступ до ресурсів значному числу їх повноправних юзерів. За успішного їх втілення DoS- можуть швидко поширюватися вітками мережі та можуть стати причиною серйозних проблем у

її функціонуванні. Як варіант, за перевантаженогоі каналу може перестати надаватися якісний доступ не тільки до системи, котра атакується, навіть і до усієї підмережі. Як приклад типовості таких атак – переповнення буфера, перевантаження пінгом, TCP SYN та інші. Проте не треба забувати, що даний тип атак може застосовуватись для «відведення очей» від атак інших типів.

При поданні атак як аномалії в комп'ютерних мережах, що демонструє рис. 1.1, то розвідка представляється як контекстна аномалія, так як ця атака базується на визначеному намірі досягти інформації та розвідки.

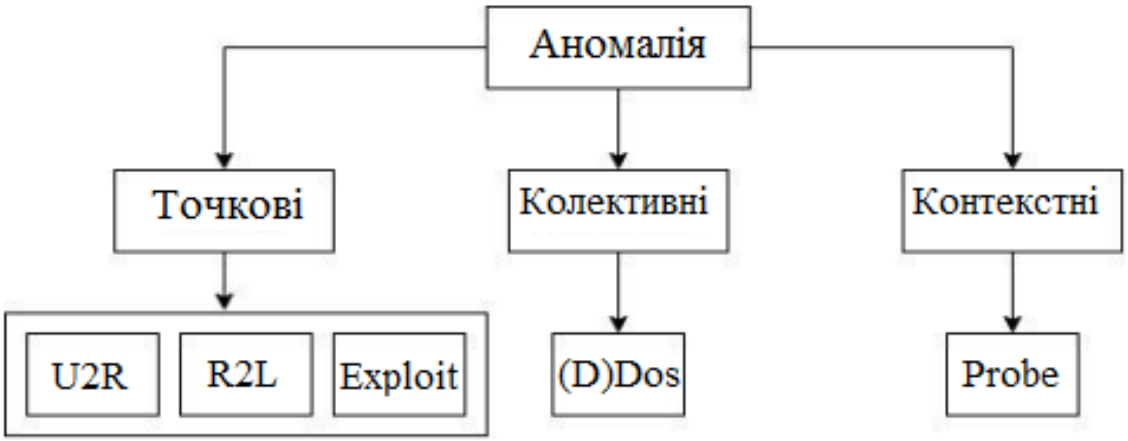

Рисунок 1.1 – Порівняння атак та аномалій

Можна виділити такі етапи реалізації атаки [3]:

- попередні дії перед атакою чи «збір інформації»;
- "реалізація атаки";
- завершення атаки.

Як правило, коли мова йде про якусь атаку, говорять про другий етап, чомусь забуваючи про інші. Збирання інформації та закінчення атаки (відоме як «замітання слідів») власне також є самою атакою, їх ймовірно розділити на декілька стадій.

Саме на стадії зюоу даних ефективність функціонування зловмисника є гарантією успішності власне атаки. Перш за все визначається ідея атаки і проходить збір даних про неї.

Опісля відбувається ідентифікація найуразливіших місць системи, котру атакують, дія на ці місця веде до необхідного результату для зловмисника. Зловмисник старається детектувати усі канали взаємозв'язку ідеї атаки з якими-небудь вузлами. Саме це і даї змогу не лише обрати тип реалізованої атаки, та й джерело її втілення.

Звичні інструменти захисту, такі як Firewall чи механізми фільтрації у мережевих роутерах, починають працювати тільки на наступноій стадії втілення атаки, повністю ігноруючи два інші етапи. Як наслідок досить часто атаку надзвичайно складно припинити хоч і за присутності дороговартісних інструментів захисту.

Стадією закінчення атаки є так зване «замітання слідів» власне зі сторони зловмисника. Перевадно це втілюється через знищення належних записів із реєстраційних журналів чи дій іншого роду, котрі відновлюють атаковану систему у стан, в якому вона властиво перебувала до атаки.

1.3 Висновки до першого розділу

Розглянуто питання визначення СВВ, та їх класифікація по різних ознаках. Враховуються методи, які є у алгоритмах виявлення вторгнень, і основі топології одержуваної інформації. Були розглянуті переваги та недоліки відповідних СВВ.

Також наведено приклади існуючих утиліт, які репрезентують кожну категорію. Головними видами атак є розвідка, U2R, R2U, експлоїт та DoS-атаки. Розглянуто їх особливості, способи реалізації та специфіка застосування. Насамкінець описано загальну стратегію втілення кожної з них.

2 АНОМАЛІЇ В МЕРЕЖІ ТА МЕТОДИ ЇХ ДЕТЕКТУВАННЯ

2.1 Типи аномалій

У процесі інформатизації суспільства швидко розгортаються мережеві послуги і проходить процес їх впровадження у майже всі верстви суспільства. Перед адміністраторами ІС постає задача забезпечити керованість таких систем, та, на додачу, цілісність, доступність та конфіденційність даних. Врешті решт надати штатну роботу системи за максимального виключення поведінки системи, котра є нестандартною (мережеві власне аномалії).

Звичайним видом аномалії трафіку може бути перехід інформативного параметра сигналу за межі діапазону його допустимих значень, властиво як і за величиною, так і за його швидкістю зміни часу [4].

У розумінні мережевої безпеки аномалії поділяються на точкові, контекстні та колективні [5].

Перші з них характеризуються появою окремого об'єкта, який не узгоджується з рештою набору даних. Прикладом може бути ізольований екземпляр мережного трафіку, який відрізняється від нормальних екземплярів, упродовж певного часового відрізку.

Другий тип визначається появою екземпляра даних, що є аномалією у цьому контексті. Контекст формується з урахуванням структур у наборах даних. Щоб його писати застосовуються два основних набори змінних, це контекстні та поведінкові. Перші використовуються визначення оточення кожному за екземпляра. Другі - визначають всі характеристики, що відносяться до конкретного примірника даних.

Останній тип визначається існуванням пов'язаних екземплярів даних, котрі визнані як аномальні у порівнянні з іншими даними. Якийсь екземпляр може і не визначитися як відхилення, однак спільна поява таких властиво екземплярів вже буде колективною аномалією. Як приклад – поява подій «переповнення буфера», а також «копіювання файлів за протоколом ftp», котрі є звичайними явищами у певній системі, однак їхня спільна поява може слугувати про віддалену атаку на

комп'ютерну систему.

Існую детектування аномалій на із застосуванням продуктивності системи та зміни станів окремих додатків [4].

Аномалія у продуктивності. За ними можна судити про те, що поведінка програми, що спостерігається (наприклад, поточне використання ЦП) не може бути пояснено робочим навантаженням програми, що спостерігається (наприклад, тип і обсяг транзакцій, оброблюваних додатком, передбачає різний рівень використання ЦП).

Зміна у продуктивності транзакцій програми. Зазвичай, мають на увазі значну зміну (збільшення або зменшення) упродовж опрацювання транзакцій, як варіант, в результаті оновлення програми.

Звичайно, що важливим є здатність розрізняти аномалію продуктивності та зміну навантаження функціонування. Аномалія продуктивності демонструє на ненормальну ситуацію, котру потрібно досліджувати та вирішувати. Але навпаки, змінення робочого навантаження (фактично зміни змішування транзакцій і навантаження) типова для веб-додатків. Тому вкрай бажано уникати помилкових тривог, викликаних алгоритмом через зміни робочого навантаження, з врахуванням того, що інформація щодо зміни робочого навантаження, що спостерігаються, може бути надана постачальнику послуг [6].

2.2 Методи виявлення аномалій

2.2.1 Загальна структура методів

Методика детектування аномалій у трафіку мережі на початковому етапі передбачає перехоплення вхідного та вихідного трафіку. Водночас в перехопленому трафіку проводиться відшукання заголовків IP-пакетів, з котрих видобуваються всі необхідні атрибути: обсяг IP пакета, IP -адреса джерела, IP - адреса призначення, дата одержання IP -пакета, час одержання IP -пакета. Отримана інформація зберігається як мережева статистика у БД.

Методи детектування аномалій можна поділити на 4 великі групи (рис. 2.1):

– поведінки;
– МН;
– обчислювального інтелекту;
– на основі знань.

Рисунок 2.1 – Систематика методів виявлення аномалій

2.2.2 Поведінкові методи

Базуються на застосуванні інформації щодо нормального функціонування системи та її зіставлення із поведінковими параметрами, котрі спостерігаються. Такі методи спрямовані на формування моделі штатної діяльності системи чи користувача. Під час функціонування системи, котрі застосовують такий підхід, співставляють поточні атрибути активності із параметрами нормальної роботи. Подія суттєвих відхилень може бути свідченням присутності аномалій [7]. Далі наведено деякий огляд функціонування кожного з методів.

Вейвлет-аналіз. Надходження сигналу розкладається із застосуванням базисних функцій, у подальшому потрібно зробити розрахунок відповідних коефіцієнтів. Сигналом може бути велика кількість параметрів: кількість пакетів за 1 секунду, інтенсивність трафіку у визначений час доби. Проведення вейвлет-

перетворення дає змогу більш явно визначити складову сигналу, котра має більшу амплітуду та знизити вплив малих амплітуд, котрі, здебільшого, є шумовими частинами сигналу.

Статистичні методи використовують певну статистичну модель до вихідних даних (зазвичай, які визначають нормальну поведінку) та застосовують статистичний висновок у тому, щоб визначити, є спостереження аномалією або, все ж таки, ні.

Спостереження, можливість яких з'явитися в даній моделі є надзвичайно низькою, детектуються аномаліями. Дане визначення визначає основні переваги та недоліки даних методів: якщо трафік розподілено за певним законом, ми отримаємо хороший результат, у іншому випадку, результати вже будуть не дуже задовільними.

Головний принцип статистичних методів детектування аномалій такий: елементи вибірки розподілені за визначеним законом, а аномалія є спостереження, котре чітко відрізняється у наборі даних, у котрому воно є, та значно різниться з іншими складовими вибірки, так як, імовірніше, належить якомусь іншому закону.

Тобто припущення, за яким функціонують статистичні методи, є таким – нормальні спостереження попадають до районів стохастичної моделі за високої імовірності, а самі аномалії – до районів з низькою ймовірністю. Статистичні підходи щодо відшукання аномалій володіють рядом переваг, так як не потребують апріорної інформації щодо ознак аномалій. Однак перед нами постає завдання вибору більш підходящої стохастичної моделі.

Самі методи статистичного аналізу поділяються ще на такі типи, як то параметричні та непараметричні.

Припущення перших – для генерування нормальних даних використовується параметричний розподіл з параметром θ і, відповідно, функцією щільності імовірності $P(x,\theta)$, де x - одержаний сигнал. Дуже часто дані методи ґрунтуються на гауссовому розподілі та регресійній моделі.

Для непараметричних методів функція щільності ймовірності P невідома і визначається з урахуванням даних за при допомозі методів гістограм і функцій

ядра.

Спектральні же методи детектування аномалій намагаються віднайти наближення даних із застосуванням набору атрибутів таким чином, щоб відобразити всю різноманітність даних. Основне припущення спектральних – дані можна подати з іншою розмірністю, в іншому просторі та різниця у новому представлені між нормальними та аномальними даними буде значною. Як наслідок, головним завданням при використанні даного методу є відшукання такого простору, в якому відмінності будуть видимі опісля перетворення. Даний метод може застосовуватися в комбінації з якин-небудь іншим, як метод передобробки одержуваних даних.

Аналіз ентропії застосовується при детектуванні атак для побудови статистичного критерію для перевіряння належності досліджуваного екземпляра аномального класу. Суть методу – створення такої моделі, котра б максимізувала ентропію. Це повністю корелюється із припущенням, що при збільшені числа унікальних записів проходить їх рівномірний розподіл щодо вибраних множинних класів, що веде до збільшення ентропії.

Фрактальний же аналіз ґрунтується на припущенні, за якого трафік мережі задовольняє властивості самоподібності [11]. Фундаментальними поняттями такого аналізу є фрактальна розмірність Хаусдорфа D та зв'язаний із нею показник Херста H [10]. D та H входять до співвідношення D = 2 - H.

Всі методи статистичного аналізу володіють схожими недоліками. Перш за все, в царині розробки шкідливого ПЗ проходить адаптація програм під роботу звичайного юзера. Саме тому статистичні методи, ймовірно, будуть абсолютно безсилі. Наступний – складність визначення порогу, котрий дасть змогу ідентифікувати аномалії і різні вторгнення досить ефективно (за незначної кількості помилкових спрацьовувань). І крім цього статистичним методам потрібно дізнаватися усю необхідну інформацію про процес, котрий проходить, за умов обмеженості самих цих даних.

2.2.3 Методи МН

Методи обчислювального інтелекту застосовуються з метою виявлення

аномалій, зловживань в комп'ютерної мережі. Це можливо при використанні в даних методах шаблонів як нормальної, так і, власне, аномальної поведінки в мережі.

МН визначається як можливість програми чи системи навчатися та вдосконалювати свої можливості залежно від завдання. На противагу статистичним методам, котрі прагнуть сфокусуватися на розумінні власне процесу, МН передбачає побудову такої системи, яка вдосконалюється на основі попередніх знань. Системи, котрі базуються на парадигмі МН, мають можливість змінити стратегію опрацювання даних на базі нової інформації. До недоліків методів МН відносять високі обчислювальні витрати та складність їхньої адаптації до визначеної предметної області.

Процес МН, зазвичай, містить такі етапи:

– з’ясування атрибутів класу (ознак) та самих класів у навчальних даних;

– встановлення підмножини атрибутів, потрібних класифікації (тобто зменшення розмірності);

– навчання моделі при застосуванні з метою класифікації невідомих даних у режимі тестування.

У випадку детектування будь-якої атаки на етапі навчання, кожен з її типів досліджується при допомозі екземплярів з навчального набору. У подальшому на етапі тестування через модель надходять нові дані, які поділяються на конкретні екземпляри. Примірники класифікуються за належністю до якогось типу атак. Коли зразок не належить до жодного з класів, тоді робиться висновок про те, що властиво трафік є нормальним.

При детектуванні аномалії на початковому етапі встановлюється профіль нормального трафіку. На етапі вже тестування раніше ж навчена модель використовується до нових даних, і кожен екземпляр у наборі даних буде класифікований як нормальний чи аномальний. Але також варто згадати ще один етап при роботі методів МН - валідація. Після закінчення навчання ми можемо отримати кілька моделей, які можуть переходити до наступного етапу. З метою вирішення проблеми про те, котру модель необхідно використовувати надалі, та забезпечити на тестовому наборі малу похибку, необхідно використовувати ще

один набір даних – власне набір для валідації. Використовується та модель, котра продемонструвала кращі результати на валідаційних даних, але вона не має змінюватись в залежності від показників точності на множині даних для тестування. В іншому випадку точність буде іншою за інших даних.

Використовують три базові типи підходів до МН:

– без вчителя (unsupervised);
– з учителем (supervised);
– їхня комбінація (semi-supervised).

У неконтрольованих завданнях навчання основна задача полягає у знаходженні шаблонів, структур або знань у непомічених даних. Коли частина даних маркована під час їх одержання або самими експертами, проблема буде такою, що напівнавчається. Додавання зазначених даних значною мірою допомагає вирішити цю проблему.

За умови ж, коли дані повністю позначені, проблема називається піднаглядовим навчанням, а загалом завдання в тому, щоб віднайти таку функцію чи модель, котра інтерпретує аналізовані дані. Щойно модель класифікації розроблена при допомозі навчання та перевірки даних, вона вже може бути збережена та використовуватись згодом чи в іншій системі.

Поміж методів детектування аномалій, котрі ґрунтуються на класифікації, виділяють методи, котрі застосовують:

– байєсовські мережі;
– метод опорних векторів;
– продукційні правила.

Байєсівськаю мережа містить дві частини: графічна структура, котра встановлює комплекс залежностей у множині випадкових значень, котрі є суб'єктами предметної області, та комплекс ймовірнісних розподілів, які визначають властиво силу взаємовідносин залежності, що предствалені як код у графічній структурі.

Методи, котрі ґрунтуються на кластеризації, роблять оцінку відстані до об'єктів виходячи з інформації про кластері, котрим належать об'єкти, тоді як методика застосування найближчих сусідів використовує локальне оточення

кожного об'єкта. При застосуванні цього класу методів беруть до уваги одне з таких припущень про нормальні об’єкти:

– вони є у розпорядженні кластера, аномальні ж не є;

– перебувають близько до центру кластера, тоді як аномальні є далекими від нього;

– належать великим, щільним кластерам, на противагу - аномалії належать невеликим та розрідженим. Перевагами даного класу методів є ймовірність навчання без вчителя, адаптація методів щодо різних типів даних і невелика кількість розрахунків при віднесенні об'єктів до нормальних чи аномальних (бо число кластерів зазвичай незначне). Недоліками є сильна залежність від обраного алгоритму кластеризації і характерними моментами його функціонування (метод кластеризації не оптимізований для детектування аномалій, аномалії - тільки побічний результат від функціонування алгоритму кластеризації тощо).

2.2.4 Методи обчислювального інтелекту

За їх допомогою можна вирішити проблему точної ідентифікації атаки за її розподілом в часі або при проведенні кількома зловмисниками. До плюсів цих методів можна належать здатність розв'язання задачі за невідомих зв’язків між об’єктами, у вхідних даних шумостійкість, пристосування до варіацій у середовищі, відмовостійкість для апаратної реалізації ШНМ. і т.д, і т.п.

ШНМ [14]. Більша частина теперішніх методів детектування атак застосовують якусь форму аналізу контрольованого території беручи до уваги правила або статистичний підхід. Такою контрольованою територією можуть бути реєстраційні журнали чи трафік мережі. Аналіз базується на наборі наперед уточнених правил, котрі формуються адміністратором або системою детектування атак.

Які-небудь розподілені часові атаки або атаки, в котрих бере участь велика кількість зловмисників, є важкими для виявлення експертними системами. З огляду на значну кількість атак та хакерів навіть особливі безперевні оновлення БД вимог експертної системи нізащо не зможуть гарантувати точну

ідентифікацію повного об’єму атак.

Застосування нейромереж є всього лиш одним із багатьох елементів ліквідації згаданої вади експертних систем. Властиво на противагу експертним системам, котрі здатні надати користувачеві визначену відповідь щодо відповідності цих ознак закладеним у БД умовам, ШНМ аналізує дані і дає змогу оцінити, власне чи узгоджуються ці дані із ознаками, котрі її навчили розпізнавати.

Метод детектування аномалій на основі ШНМ містить два етапи. На першому ШНМ навчається розпізнавати класи нормальної поведінки на тренувальній вибірці. На другому кожен екземпляр надходить як вхідний сигнал нейромережі. Система, заснована на ШНМ, може розпізнавати як один, і кілька класів нормальної поведінки. Для відшукання аномалій за допомогою розпізнавання лише одного класу використовують реплікативні ШНМ. Також можуть застосовуватися технології глибокого навчання з метою ефективного детектування аномалій у цих системах.

Дія ШНМ зумовлена множиною функцій наближення, що залежать від вхідної інформації та спочатку невідомих. Головна перевага ШНМ – вони знаяно менш чутливі до неточних даних на вході, а також можливість формування рішення без наявності інформації про залежність, закономірності у вхідних даних.

Найбільш поширеними серед методів еволюційного моделювання [14] є ГА та ГП. Вони обидва базуються на принципі «виживає найсильніший» та використовують населення особин (хромосоми), застосовуючи певні оператори. Головні оператори – це відбір, кросовер (кросинговер) і мутація. Працювати алгоритми починають із випадково зґенерованою популяцією, котра не обов'язково є життєздатною. Для кожної особини розраховується параметр пристосованості, котрий відображає, як конкретний фенотип здатен вирішувати поставлене завдання. Особи з найбільшими параметрами пристосованості отримують більший шанс стати батьками. Вже двоє батьків можуть проводити кросовер і також кожен з них може мутувати. Особи з найкращими показниками пристосованості будуть копіюватися в наступне покоління.

Основна відмінність між ГА та ГП є у поданні особин. По-перше, вони представлені як набір бітових стрічок і всі операції є надзвичайно простими. Для ГП особини – це програмний код і тому представляються як дерева, де внутрішні вузли це оператори додавання, віднімання, ділення, множення, кон'юкція, диз'юнкція, інверсія, а також різні програмні структури, зокрема: оператор розгалуження, цикли та інші. У ГП всі операції видаються набагато складнішими, ніж у ГА.

Головними перевагами ГА детектування аномалій є їх значна гнучкість і стійкість щодо випадкових шумових змін набору даних на вході. На додачу до цього особливістю даних алгоритмів є прагнення оптимального вирішення проблеми з урахуванням ймовірнісних правил відбирання найкращих шляхів вирішення. У протилежність до більшості методів відшукання аномалій, ГА є математично спрощеними та легко сприймаються. Існує й низка недоліків ГА детектування викидів. Зокрема складність підбирання правил відбирання найкращих рішень, а також варіювання часу обрахунку від ситуації до ситуації. Більш того, відсутня гарантія, що ГА дозволить відшукати глобальне оптимальне рішення.

Гібридні методи. Властиво останні досягнення у царині детектування аномалій пов'язані саме з ними. Ці методи містять, щонайменше, два алгоритми, котрі відносяться до різних класів відшукання аномалій. Гібридизація застосовується, щоб подолати недоліки одного методу через використання переваг іншого, узгодивши їх функції.

Властиво гібридні методи детектування аномалій дають змогу поєднувати успішно переваги різних підходів. За цих обставин, задля досягнення середніх результатів можуть використовуватися різні технології як послідовно, так і паралельно. Як приклад гібридних систем можна навести [15]:

– спільне використання кластеризації із алгоритмом найближчого сусіда;

– поєднання суміщених алгоритмів, як варіант, баєсових мереж і дерев рішень, та алгоритму найближчого сусіда із класифікацією на базі правил;

– метод опорних векторів та ШНМ.

2.2.5 Методи, що ґрунтуються на знаннях

Тут як процедуру пошуку можна використати співставлення за зразком, апарат регулярних виразів, аналізування переходу станів та ін. Власне і назвою методи завдячують тому, що системи, котрі базуються на їх використанні, взаємодіють із базою знань, до котрої входять описи раніше відомих атак [8]. У цьому випадку в основі бази знань є сховище, у котрому наявні записи експертів при допомозі логіки їх опрацювання і представлення.

Сигнатурні методи (інколи застосовується назва методи контекстного пошуку) полягають у визначенні у вихідних даних якоїсь множини символів. Зокрема, як приклад, для детектування атаки на Web -сервер під управлінням ОС сімейства Unix, спрямованої на одержання несанкціонованого доступу до парольного файлу, здійснюється відшукання відповідності символів «GET*/etc/passwd» у заголовку HTTP -запиту, або ж «GET* /.htaccess». Також може проходити запис станів системи, де будуть формуватися сигнатури атак як набору переходів ІС із одного стану в інший. Фактично, кожен такий перехід описується настанням в ІС визначеної події, а властиво набір таких подій встановлюється параметрами сигнатури атаки.

Властиво сигнатурне виявлення містить пошук мережного трафіку з рядом шкідливих байтів чи сукупністю пакетів. Основною перевагою даного методу є те, що сигнатури є такими, дуже легко розробляються та розуміються, якщо відомо, котру мережеву поведінку потрібно ідентифікувати. Наприклад, можна використовувати сигнатуру, яка шукає певні рядки в межах або перевіряє, чи використовують певну вразливість переповнення буфера. СВВ, які ґрунтуються на цих методах, можуть з високою точністю вказати на причину тривоги. Так як зіставлення відбувається за конкретними типами сигнатур. Також варто зауважити, якщо система використовує лише визначений тип комунікації в мережі (DNS, SMTP, ICMP, HTTP), додаткові сигнатури можна від’єднати для більш гнучкого і ефективного використання даної системи.

Існує кілька способів зіставлення сигнатур із реальними даними [16]:

- збіг із шаблоном;

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

Перший спосіб передбачає виявлення, що базується на відшуканні визначеної послідовності байтів у даних, котрі опрацьовуються. Як результат одержується простота завдання правил і є змога створити прямий зв'язок із аномалією. Також збіг з шаблоном буде застосований до майже всім типів протоколів. Проте також трапляються й недоліки: можливість помилкового спрацьовування, необхідність створення великої кількості шаблонів, обмеженість у застосуванні, а також значна кількість таких умов, за яких аномалії не будуть детектовані.

Другий спосіб по одним пакетам встановлює біжучий стан потоку даних, а з появою інших пакетів формує меседж про існування аномалії. Фактично має всі переваги збігу із шаблоном, проте показує вищу надійність. Хоча володіє аналогічними недоліками: потреба у наявності широкої бази шаблонів та за зміни аномалії здатен призвести до пропуску її детектування.

Третій спосіб застосовується для оцінки стану визначеного типу протоколу чи його різних станів. Перевагами даного способу є прямий зв'язок із аномаліями і здатність детектування значних, розподілених аномалій. Недоліки - велика кількість перепусток, а також складність створення сигнатур для визначених систем.

Третій спосіб передбачає, що у часовий проміжок сигнатури описують ситуації, у яких частота якихось подій перевищує встановлений поріг.

Перевагами є можливість опису комплексних взаємозв'язків, і навіть виявлення нових типів аномалій. Недоліки - складність у реалізації та пристосуванні сигнатур відносно певного виду трафіку мережі.

2.3 Детектування аномалій на базі фрактального аналізу

2.3.1 Поняття про фрактали

Визначення "фрактал" вперше використовував Бенуа Мандельброт [4].

Ним він називав геометричні фігури, котрі володіють дуже порізаною формою, та можуть мати властивості самоподібності. Можливо узагальнити це поняття стосовно якого-небудь об'єкта (зображення, мова, трафік мережі), окремі параметри якого зберігаються за зміни масштабу чи часу. Самоподібність значить, що частини об’єкта за збільшення є подібними (у певному сенсі) до його цілого образу. Щодо мережного трафіку, фрактальність – це практична постійність розподілу трафіку упродовж часу за масштабування тимчасової шкали.

Для кількісного опису фракталів достатньо величини фрактальної розмірності (розмірності Хаусдорфа), яка визначається за (2.1):

$$D_f = -\lim_{\delta \to 0} \frac{\ln N(\delta)}{\ln(1/\delta)}, \qquad (2.1)$$

де $N(\delta)$ - мінімальна кількість n-вимірних умовних одиниць, котрі покривають множину, δ – розмір окремої умовної одиниці.

Властивість точної самоподібності правильна лише для регулярних фракталів. Крім регулярних фракталів є ще окремий клас фрактальних об'єктів, у яких розподіл точок множини є неоднорідним. Підставою такого роду неоднорідності є відмінні ймовірності заповнення геометрично ідентичних елементів фракталу чи на загал невідповідність ймовірностей заповнення геометричним розмірам визначених областей. Властиво ці неоднорідні об'єкти вже матимуть назву мультифрактали. Щоб повністю описати такі об'єкти вже не досить однієї величини D_f, а потрібно значно більше [9].

2.3.2 Самоподібність даних мережевого трафіку

В даний час сильно зростає попит клієнтів на хмарний та мережевий бізнес, а у зв’язку з цим збільшує зацікавленість хакерів до даних систем. Виявляються дедалі більше нових вразливостей у системі, котрі стабільно експлуатуються, що, водночас, веде до складності управління безпекою. Відстеження трафіку реалі та швидке виявлення в ньому аномалій є важливим

для підвищення надійності та доступності мережі.

Зараз відомо, що велика кількість мережевих потоків, котрі представлені трафіком в LAN, WAN, WWW, показують високі показники самоподібності [19], а це свідчить про існування схожості форми мережевого трафіку у широкому часовому масштабі. Показник Херста, котрий і характеризує монофрактальну розмірність, є основним показником оцінювання власне самоподібності мережевого трафіку. Така оцінка широко застосовується у керуванні проходження трафіку по мережі та контролю доступу. Таким чином, його точне та швидке оцінювання має важливе значення надалі для більш точного управління мережі.

Аномальний пакетний трафік здатен сильно спотворити функцію самоподібності трафіку за певний проміжок часу. Це було показано за допомогою тестової вибірки трафіку із датасету DARPA99 [13]. Це значить, що показник Херста можна використовувати для детектування аномалії пакетного трафіку мережі.

2.3.3 Показник Херста

Для оцінювання фрактальних ознак різних процесів широкого поширення набув показник Херста *H*, котрий напряму пов'язаний із розмірністю Хаусдорфа D_f (2.2):

$$D_f = 2 - H, \tag{2.2}$$

Показник ступеня Херста обчислюється в термінах асимптотичної поведінки визначеного масштабованого діапазону як функції відрізка часу часового ряду як (2.3):

$$E\left[\frac{R(n)}{S(n)}\right] = Cn^H, \tag{2.3}$$

де $R(n)$ - розмах накопичених відхилень перших n значень від обчисленого середнього значення ряду; $S(n)$ - стандартне відхилення; E - математичне сподівання, n - число точок у відрізку часового ряду, C – константа.

Мандельброт показав [10], що з параметра Херста можна розрахувати розмірність простору ймовірностей. З цього отримуємо такі варіації:

– якщо $0 \leq H < 0.5$, то ряд має схильність до змін. Виникає зворотна залежність власне поточного стану від часу. Властиво Стійкість системи перебуває у залежності від того, наскільки близько показник Херста розміщений до 0;

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

– якщо $0.5 < H \leq 1$, ряд є трендостійким. Ряд зберігає пряму залежність.

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

Показник Херста може оцінюватись декількома способами: R/S, метод періодограм та методами вейвлет-аналізу. Однак у деяких випадках використовують інші методи [4].

Перевагою застосування показника Херста можна назвати швидкість опрацювання даних навіть при значних розмірах рядів, але це, водночас, і є його недоліком: для одержання достовірних результатів необхідні великі розміри рядів; за малих значень може одержатися помилка.

2.3.4 Розрахунок показника Херста R/S методом

За основу було взято метод, який використовувався у роботі [5]. Алгоритм містить два етапи: розрахунок еталонів та виявлення аномалій у реальному часі. Для розрахунки оцінки аномальності застосовується інформація із заголовків пакетів рівнів моделі OSI (транспортного і мережевого) за 1 с.:

– порт джерела/призначення;

– IP-адреса джерела/призначення;

– кількість пакетів IPv4;

– розмір корисного навантаження.

Дані, розрахунок котрих здійснюється на етапі обчислення еталонних значень, будуть співставлятися із тими даними, котрі розраховуються в реальному часі на етапі детектування. Для оцінки аномальності цим методом застосовується показник Херста. Етап обчислення еталонів є кінцевою процедурою, це наведено на рис. 2.2, та її тривалість становить для звичайного режиму чотири хв. Як результат, одержується два масиви з 4 значеннями: значення показників Херста для різних часових інтервалів та їхнє середньоквадратичне відхилення.

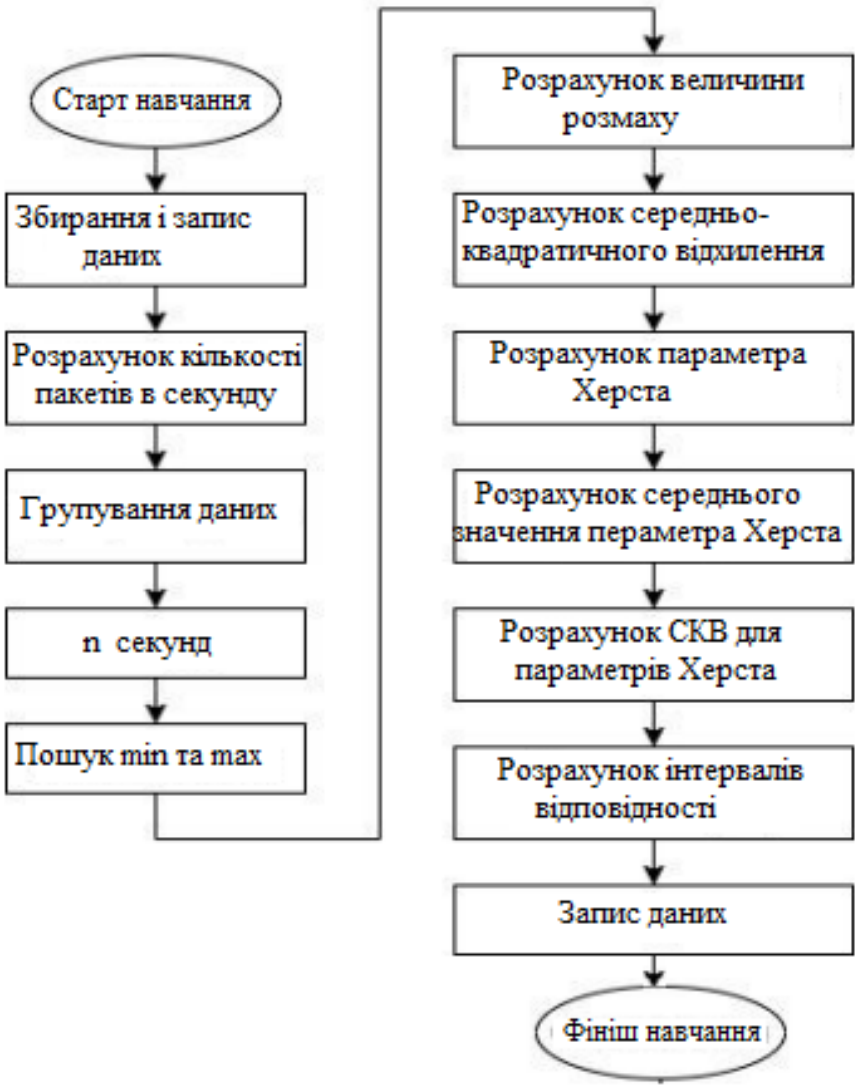

Рисунок 2.2 – Алгоритм розрахунку еталонів

Оцінювання параметра Херста проходить за методом R/S, в основі якого

лежить формула (2.3).

Загальновідомо, що основною формулою RS-аналізу є відношення (2.4):

$$R/S = (a \cdot N)^H, \tag{2.4}$$

де H – показник Херста; S - стандартне відхилення послідовності спостережень; R – розмах нагромадженого відхилення; N - дискретний час (обсяг вибірки); a – задана позитивна константа.

R є головним елементом для обчислення параметра Херста. У загальному R обраховують способом за формулою (2.5):

$$R = \max_{1 \le U \le N}(Z_U) - \min_{1 \le U \le N}(Z_U), \tag{2.5}$$

де Z_U – нагромаджене відхилення ряду від середнього X_{CP}.

Херст емпіричним шляхом порахував константу, для порівняно короткотермінових тимчасових рядів у природних подій. Отже, формула (2.4) набуде вигляду (2.6):

$$R/S = (N/2)^H. \tag{2.6}$$

Знаходження значення параметра H можна розбити на такі етапи:

– вихідний часовий ряд розбивається на блоки з однаковою довжиною;

– для кожного блоку обраховується розмах R;

– розраховуємо для кожного блоку властиво середньоквадратичне відхилення за (2.7):

$$S = \sqrt{N^{-1}} \sum_{i=1}^{N} (X_i - X)^2; \tag{2.7}$$

– приймаємо за N обсяг вибірки (дискретний час);
– логарифмуємо отриманий вираз;
– отримуємо шуканий параметр за (2.8):

$$H = \log(R/S)/\log(N/2). \quad (2.8)$$

Оскільки попередньо відомо, що тривалість етапу обчислення еталонів - 4 хвилини, тому можна для обчислень використовувати наступну схему розбивання на інтервали, один раз на n секунд:

– на 5 с;
– на 15 с;
– на 60 с;
– на 120 с.

Схема «раз на n» секунд означає, що весь часовий відрізок, що дорівнює ; хв (240 с), розбивається по інтервалах по n секунд, і в кожному такому інтервалі проходить розрахунок показників Херста. Як підсумок, для позиції «раз на 5 с» будемо мати сорок вісім інтервалів, обчислюємо для кожного з них показник Херста та середнє значення цих показників. Так само для позиції «раз в 15 с» одержуємо шістнадцять таких інтервалів, для позиції «раз в 60 с» - відповідно чотири інтервали, за тим самим принципом для позиції «120 с» - два інтервали.

Провівши розрахунок еталонів, під час безпосереднього відшукання аномалій відбувається порівняння з еталонними значеннями для трафіку, котрий одержаний за 5 с, 15 с, 60 с і 120 с.

Після отримання значень у реальному часі (5 секундний інтервал) дані записуються у часовій змінній. Відбувається перерахунок кожного із чотирьох значень параметрів Херста. У подальшому перевіряється розмір відхилення. За умов, коли не входимо в інтервал "трьох сигм", тоді відображується попередження про проблеми в мережі.

2.3.5 Алгоритм розрахунку параметра Херста на базі властивостей стаціонарності трафіку

Базовий метод описується у роботі [20]. Хай X_i кількість бітів, байтів чи пакетів, котрі зафіксовані за і-й інтервал часу. Дана послідовність X_I вважатиметься стаціонарною другого порядку, коли її математичне сподівання $E(X_i)$ не залежить від i, а функція автоковаріації (2.9) залежить лише від різниці k = i - j:

$$CovX = E[(X_i - E(X_i))(X_j - E(X_j))] \tag{2.9}$$

Потім можна провести заміну самої автоковаріації на γ(к). Позначимо дисперсію через (2.10):

$$\sigma^2 = \gamma(0) = E[(X_i - E(X_i))^2] \tag{2.10}$$

Нормовану кореляційну функцію послідовності знаходимо за (2.11):

$$\rho(k) = \frac{\gamma(k)}{\sigma^2} \tag{2.11}$$

Стаціонарний процес є властиво самоподібним другого порядку з покказником Херста 0 < H < 1, коли його коефіцієнт кореляції виглядатиме як (2.12):

$$\rho(k) = \frac{1}{2}(|k+1|^{2H} - 2|k|^{2H} + |k-1|^{2H}) \tag{2.12}$$

Оскільки X_i є самоподібною послідовністю властиво другого порядку, з (2.12) ми отримаємо рівняння (2.13):

$$\rho(1) = 2^{2H-1} - 1 \tag{2.13}$$

Розв’язуючи рівняння (2.13) можемо отримати H за (2.14)

$$H = \frac{1}{2}(1 + \log_2(1 + \rho(1))) \tag{2.14}$$

У подальшому за припущення, що для визначеного ряду X_1, X_2, ... X_n його середнє значення вибірки (2.15), вибіркова коваріація (2.16) і автокореляційна функція (2.18) мають наступний вигляд

$$\mu'_n = \frac{1}{n}\sum_{i=1}^{n} X_i \tag{2.15}$$

$$\gamma'_n(k) = \frac{1}{n-k}\sum_{i=1}^{n-k}(X_i - \mu')(X_{i+k} - \mu') \tag{2.16}$$

$$\sigma'^2_n = \gamma'_n(0) \tag{2.17}$$

$$\rho'_n(k) = \frac{\gamma'_n(k)}{\sigma'^2_n} \tag{2.18}$$

$$H' = \frac{1}{2}(1 + \log_2(1 + \rho(1))) \tag{2.19}$$

Таким чином одержуємо кінцеву формулу для знаходження показника Херста для послідовності X_i.

Алгоритм наведено на рис. 2.3.

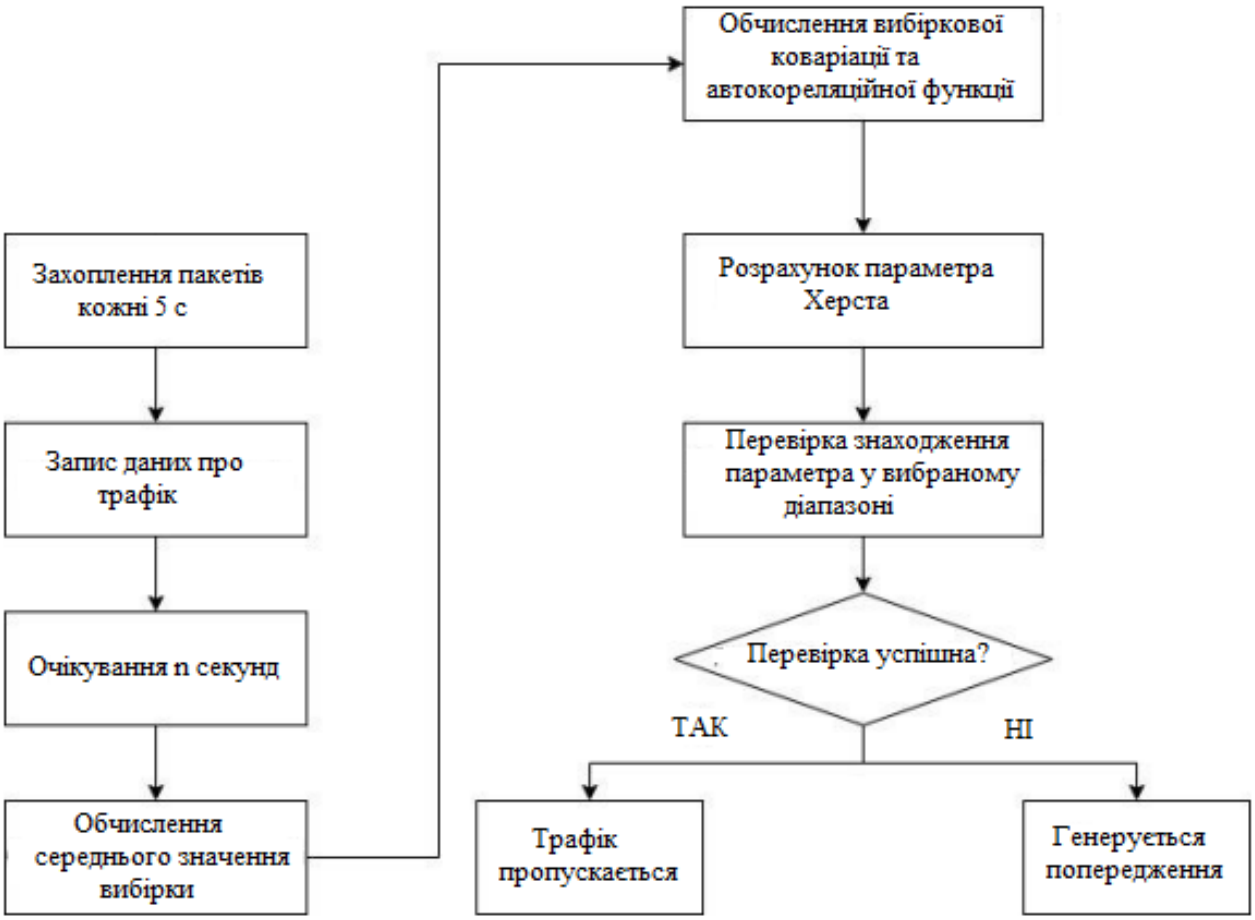

Рисунок 2.3 – Порядок дій роботи методу детектування аномалій на базі розрахунку показника Херста

Щоб обчислити еталони, треба вибрати достатній час, при якому ми матимемо допустиму кількість помилкових спрацьовувань, і навіть достатньо швидкий час одержання оцінки показника Херста. Для оцінки показника застосовувалися часові інтервали, котрі більше восьми і крані чотирьом, це 8, 12, 16 хв. Фінальна послідовність розбивається на проміжки, що дорівнюють 5 і потім обраховується показник Херста для таких інтервалів: 30, 60, 120 і 240 с. Потім обчислюється середньоквадратичне відхилення і математичне сподівання для всіх проміжків та на базі цих величин встановлюються межі інтервалу відповідності. Такий процес схожий на те, що використовувався в попередньому підпункті.

У подальшому для обрахунку показника Херста в реальному часі будуть

використовуватись послідовності трафіку за інтервал у 5 секунд. Для оцінювання аномальності застосовуватиметься величина кількості пакетів. Проте можуть застосовуватися також і інші метрики, зокрема, ті, котрі були у методі вище. Як наслідок одержуватимемо ряд значень за такі інтервали часу (один раз на n секунд):

- на 30 с;
- на 60 с;
- на 120 с;
- на 240 с.

Потім обраховуємо відповідні необхідні показники: середню величину, вибіркова коваріація і автокореляційна функція. На їх базі обчислюємо значення показника Херста та перевіряємо знаходження значення у допустимих межах.

2.3.6 Динамічна зміна значень еталонів

За нормальних умов трафік у мережі показує добові коливання, так як у певній мірі мережа зайнята нерівномірно та з малим добовим періодом. Для зменшення впливу періодичності мережевого трафіку на оцінювання параметра Херста, потрібно обробляти трафік у різні часи. Врешті решт треба володіти набором еталонних даних певного часу доби.

До того ж трафік може показувати коливання у той самий проміжок застосування. Для мінімізації цих коливань на точність визначення аномалій ймовірно використовувати алгоритм оновлення еталонів, котрий використовується у [12]:

H_{cur} - поточне значення показника Херста, H_{nor} – його еталонне значення; H_{norup} - верхня границя 98% довірчого інтервалу, $H_{nordown}$ - нижня границя такого інтервалу. Стартові значення H_{nor}, H_{norup} та $H_{nordown}$ розраховуються циклічно для нормального трафіку мережі (для значного часового проміжку).

Після отримання поточного розрахованого значення H_{cur} :

– одержати відповідні H_{nor}, H_{norup} та $H_{nordown}$ від моделі трафіку, який є нормальним;

– перевірка на аномалію H_{cur}: якщо правильно - завершуємо;

– перевірити умову $H_{nordown} < H_{cur} < H_{norup}$: якщо неправильно - завершуємо;

– оновити H_{nor}: $H_{nor} = (H_{nor} + H_{cur}) / 2$;

– обчислити 95 % довірчий інтервал H_{nor} : $95(H_{nor})$ %;

– оновити межі довірчого інтервалу.

2.4 Висновки до другого розділу

Розглянуто поняття про аномалію та їх класифікацію. Можна виділити кілька груп: точкові, контекстні та колективні. Дальше були досліджені методи детектування аномалій: методи поведінки, МН, методи обчислювального інтелекту та методи на базі знань. Були наведені загальні принципи функціонування кожної групи методів, наведені переваги, недоліки та кращі варіанти застосування кожного з них. Більш детально було розглянуто методи на базі фрактального аналізу та властивостей самоподібності мережевого трафіку.

Розглянуто принципи функціонування двох алгоритмів детектування аномалій мережі на основі показника Херста: R/S метод та метод на базі стаціонарності трафіку. Наприкінці розглянуто алгоритм динамічного змінення еталонів аналізованої системи.

3 ПРАКТИЧНА ЧАСТИНА

3.1 Опорна архітектура СВА

3.1.1 Архітектура

У цьому розділі буде розглянуто побудову базової архітектури СВА. Схема даної архітектури показано на рис. 3.1.

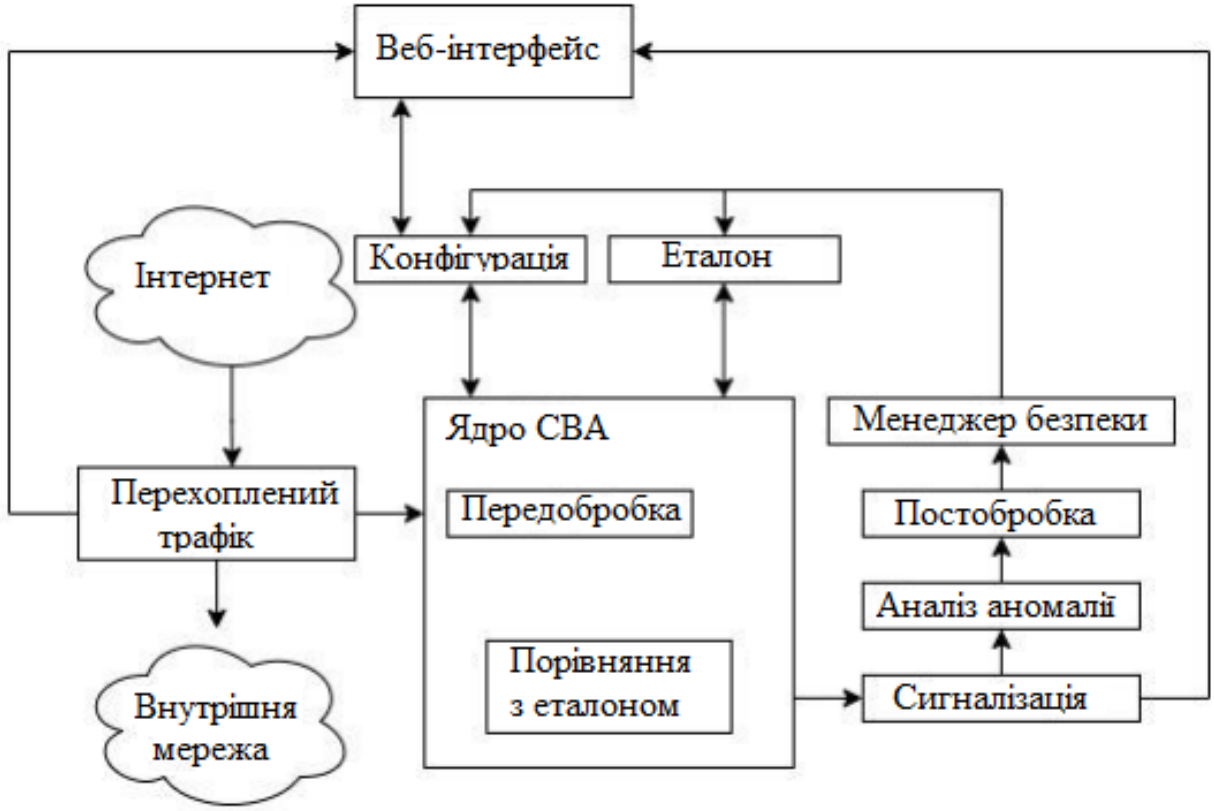

Рисунок 3.1 – Базова архітектура СВА

Основними складовими цієї моделі є:

- підсистема захоплення трафіку;
- ядро СВА;
- довідкові дані;
- менеджер безпеки;
- веб-інтерфейс.

3.1.2 Опис складових частин

Модуль захвату трафіку є потрібним складовим елементом такого типу систем. Дані, котрі є необробленими, записуються на обох рівнях – пакетів і потоків. Пакетні дані здатні бути перехоплені яким-небудь інструментом (як варіант, Wireshark) і після передобробки відправлені в ядро системи. Поточні дані у випадку систем з високошвидкісною передачею здатні містити загальну інформацію щодо числа пакетів. Програмними засобами для захоплення покових даних, котрі часто застосовуються, можуть бути Nfpdump, Nfsen, Cisco Netflow. Основні елементи модуля захвату трафіку показані на рис.3.2. Необроблені дані мережного трафіку захоплюються та буферизуються завдяки мережевому адаптеру у файлі tcpdump-формату. Для одержання та обробки фільтрованого трафіку з таким форматом можна використовувати бібліотеку libpcap.

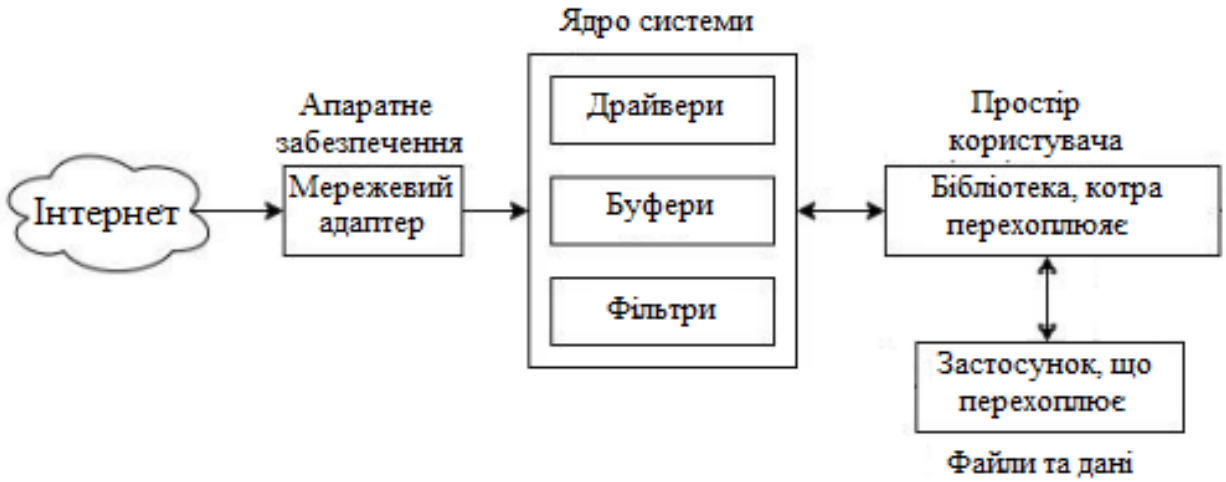

Рисунок 3.2 – Модуль захвату трафіку мережі

Ядро СВА покликане виявляти наявність аномалій у мережевому трафіку. Однак перед відправкою мережного трафіку на ядро треба здіснити його передобробку. Коли така атака вже відома, значить її можна детектувати щодо залучення відповідних ресурсів. По іншому, невідомі атаки може бути виявлено через порівняння поточного стану із еталонним (котрий нормально прогнозований).

Співставлення із еталоном передбачає пошук патерну чи профілю у

графіку мережі, котрі здатні бути побудованими на базі тривалого за часом моніторингу властиво поведінки мережі із вже відомими вразливістю чи експлойтами. При формуванні механізму співставлення з еталоном треба звернути особливу увагу на наступні аспекти:

– кожен новий, котрий не зустрічався перед тим, кадр багатовимірного профілю функціонування мережі оцінюється щодо того, належить він до відомого класу чи ні, співставлення повинно бути незалежним;

– співставлення з талоном повинно бути швидким;

– за ефективної організації профілів швидкість відшукання при порівнянні може підвищитися.

Дані для довідки (еталон і конфігурація) мають такі дані, зокрема інформація щодо розмірів даних, профілі відомих вторгнень або нормальну поведінку. Властиво такі дані мають бути збереженими таким чином, щоб зробити мінімальними обчислювальні затрати для доступу до них та їхню обробку.

У випадку СВА, в основному, вони будуть профілями та сигнатурами. Елементи опрацювання будуть оновлювати профілі по ходу появи нових знань про поведінку, що спостерігається. Ці оновлення здійснюються пакетно-орієнтованим способом через вирішення конфліктів, при їх виникненні.

Еталонні дані є, властиво, інформацією щодо існуючих сигнатур атак чи профілів нормальної поведінки мережі. Вони потребують ефективної організації їхнього зберігання. Що стосується СВА, тут частіше використовуються профілі. Робочі частини системи будуть оновлювати профілі з надходженням нової інформації щодо роботи мережі. Такі оновлення підготовлюються в регулярні проміжки часу із застосуванням пакетно-орієнтованого режиму.

Такі конфігурації можна вважати належними до проміжних результатів, наприклад, частково побудовані сигнатури вторгнень. Сховище, потрібне таким даним, може бути трохи більше. Проміжні дані повинні поєднуватися з наявними знаннями з метою забезпечення стійкості та актуалізації результатів функціонування системи.

Сигналізаційний модуль потрібен для генерації сигнальних повідомлень на

базі тих даних, котрі одержані від ядра СВА.

Основні задачі модуля аналізу – роз'яснення даних щодо аномалій, отримані від ядра СВА, та вжиття потрібних заходів захисту. Завданнями цього модуля також є оновлення профілів і шаблонів при допомозі безпекового менеджера.

Компонент постобробки повинен здійснювати постобробку зґенерованих повідомлень щодо аномалій для діагностування актуальних атак.

Адміністратор безпеки. Ця складова частина оновлює сигнатури, котрі зберігаються при детектування нових вторгнень.

Однозначно, що для ефективної роботи системи повинен бути наявним веб- інтерфейс. Його призначення – візуалізація даних та спрощення системи адміністрування СВА. При його допомозі можна переглядати усі події по загрозах, повністю увесь трафік, що входить за визначений період, за певними протоколами в реальному часі. Адміністратору доступна можливість часткового редагування даних конфігурації, а також налаштування способів візуалізації відображених протоколів, подій.

3.1.3 Діаграма варіантів використання

З метою представлення використання програми застосовується дана діаграма активностей, яка наведена на рис. 3.3.

Її основним учасником є адміністратор системи. Як вже вище йшлося він буде взаємодіяти з внутрішньою системою завдяки веб-інтерфейсу.

Адміністратору доступні чотири основні варіанти використання:

– зміна конфігурації;
– запуск навчання;
– перегляд статистики трафіку, що передається;
– запускання моніторингу трафіку.

У межах змінювання конфігурації системи адміністратор проводить вибір параметрів якого саме внутрішнього методу потрібно змінити. Для прикладу, для методів на базі самоподібної структури трафіку - це вибір інтервалу обчислень еталонів, ймовірне коригування допустимих меж показника Херста. Для методів

на базі ШНМ – це зміна числа нейронів, котрі відповідальні за атаку чи нормальну поведінку, зміна способу вибірки імунних детекторів.

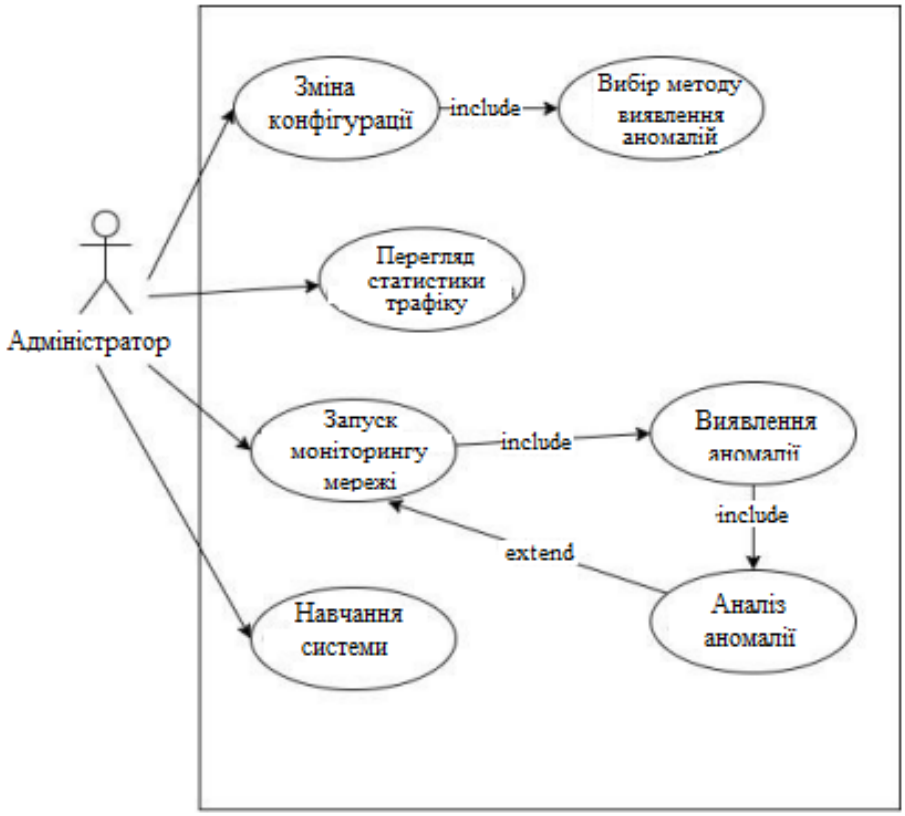

Рисунок 3.3 – Діаграма варіантів використання

За перегляду статистики трафіку доступною буде як статистика по вхідному, так і по вихідному трафіку з вибором типів пакетів, що передаються. Доступний як у реальному часі, так і частково переглядання статистичних даних пакетів, що передаються при появі аномалії.

Вслід за запуском моніторингу мережі система самостійно запустить метод, котрий визначений у конфігурації, з певними характеристиками та відповідним зразком. У разі аномальної ситуації буде проведено попередній аналіз такої ситуації, з подальшим записом їх у журнал. У подальшому адміністратор отримуватиме повідомлення щодо аномальної ситуації.

3.2 Реалізація базової архітектури

3.2.1 Модуль перехоплення трафіку

Tcpdump утиліта UNIX, котра дає змогу захоплювати та здійснювати аналіз трафіку мережі, котрий проходить через машину, на якому працює цей застосунок [17].

Інструмент містить два основні блоки: захват пакетів (через звертання до бібліотеки libpcap (Unix) чи Pcap (Windows)) та відтворення цих пакетів.

tcpdump дані. Класифікатори, що породжуються, використовують дані tcpdump, з метою відрізнити мережеві атаки від властиво нормального трафіку. TCPdump (або Windump для Windows) є популярним і широко застосовуваним програмним засобом, що дозволяє детально дослідити процес передавання інформації в мережі. Результат роботи tcpdump має дані пакетів мережевих з'єднань у порядку появи пакета мережі. Перед збиранням інформації ці пакети повинні попередньо опрацьовуватися. Конвертори tcpdump даних обертають записи з'єднання на множину особливостей (іншими словами, атрибутів), для прикладу, time (час початку з'єднання, мається на увазі позначка часу першого пакета), dur (тривалість з'єднання), src та dst (хост-джерело і хост -адресат), bytes (кількість байтів даних, відправлених із джерела адресату), srv (сервіс, тобто порт адресата), flag (яким чином з'єднання відповідає мережному протоколу) і т.д. Ці суттєві особливості фактично підсумовують інформацію рівня пакетів у межах з'єднання.

Сніффер tcpdump був використаний у багатьох працях у галузі комп'ютерних мереж та де-факто є стандартним інструментом для захоплення трафіку. За його допомоги встановлено вихідний формат файлів PCAP, котрий є файловим форматом, що найбільш використовується для захвату та збереження пакетів. Цей сніффер пропонує механізм фільтрації, котрий дає змогу захоплювати тільки ті пакети, котрі відповідають визначеному критерію, як приклад, TCP-пакети із зафіксованим номером для порту призначення, що дорівнює 80. Проте, даний механізм не має можливості вибрати пакети лише однієї програми, особливо якщо процес, що спостерігається, є peer- to-peer

програмою, котра призначає нові порти динамічно упродовж кожних кількох секунд. Однак це можна втілити при застосуванні мов програмування, котрі підтримують роботу з даним сніффером, при допомозі аналізу заголовків пакетів вищого рівня.

Блок захоплення пакетів (під час його запуску) надсилає повідомлення щодо логіки захвату (що йде після всіх параметрів командного рядка) напряму бібліотеці захоплення пакетів, котра проводить перевірку синтаксису, здійснює його компіляцію, після цього копіює у внутрішній буфер інструменту пакети мережі, котрі проходять через визначений інтерфейс та відповідають сукупності фактів у ньому.

Блок відображення пакетів бере по одному захоплені раніше пакети із буфера, та виводить їх (у легкочитаному вигляді) на стандартний висновок порядково відповідно визначеному рівню деталізації.

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

Програмне втілення сніффера трафіку проходить із застосуванням мови Go та інструмента tcpdump із відповідним драйвером libpcap. З метою взаємодії з tcpdump використається відповідний модуль gopacket [18], котрий надає оболонку Go для libpcap, котра написана на C. Однак це більше, аніж звичайна оболонка. Модуль надає додаткову функціональність і застосовує спеціальні інтерфейси, саме тому він є надвичайно потужним.

3.2.2 Ядро СВА

Цей компонент відповідає за обробку мережного трафіку, що одержаний від сніффера. У реалізації застосовується два методи на базі показника Херста, котрі описані вище. Як метрики, що використовуються для підрахунку, застосовується кількість IP -пакетів, одержаних за 5 с. Проте також можуть застосовуватися дані щодо протоколів, портів призначення та прийому, що використовуються, та також IP- адреса призначення і прийому.

Модуль розрахунку еталонних даних та їх захоплення схожий на підхід, який застосовується для обрахунку показника Херста в реальному часі. Основна

відмінність – завдання фінального часового інтервалу, з метою одержання великої кількості відліків у послідовності. У межах навчання відбувається обчислення необхідних параметрів застосовуваних методів та вподальшому запис еталонних даних. Має бути хоча б один раз запущено для правильної роботи системи.

Модуль оповіщення описується окремою функцією, котра відповідає за загальний підрахунок числа виходів за границі допустимих інтервалів. Як описувалося вище, у статистичних методах одними з основних проблем є вибір границь таких допустимих значень і, отже, досить багато хибних спрацьовувань.

3.2.3 Серверна частина

З метою втілення серверної частини застосовувася стандартний модуль Go net/http і виведення логів сервера модуль log. Існуючий HTTP -сервер запущено на 5000 порту інтерфейсу localhost, є потреба запуску «під адміністратором» чи з правами root -користувача (залежно від ОС, що використовується), для можливості прослуховування всіх інтерфейсів та портів у системі. Клієнт-серверна взаємодія проходить при допомозі GET запитів.

Для обробки запитів можливі наступні маршрути:

- /Devices. Використовується для одержання поточного переілку доступних інтерфейсів мережі в системі.
- /start. Призначений для запуску моніторингу мережного трафіку. Проходить асинхронний запуск ядра системи за допомогою горутину. Застосовує один атрбут deviceName для вибору пристрою прослуховування трафіку.
- /get-data. Використовується для одержання поточної статистики вимірювання параметра Херста. Застосовує параметри type - інформація про методи розрахунку, що використовується, interval - інформація щодо тимчасового інтервалу, котрий цікавить.
- /stop. Призначений для зупинення моніторингу мережі та оновлення даних, отриманих у реальному часі.
- /get-test-data. Використовується з метою оновлення тестового файлу,

котрий береться для обчислення початкових еталонів. Застосовує атрибут deviceName для вибору пристрою прослуховування трафіку.

- /get-anomaly-count. Застосовується для одержання та оновлення статистики за ситуаціями, що вийшли за границі допустимих значень.

3.2.4 Інтерфейс користувача

На рис. 3.4 представлений зовнішній вигляд користувальницького інтерфейсу системи. Як зазначалося вище, для його відтворення застосовується стек JavaScript/HTML/CSS.

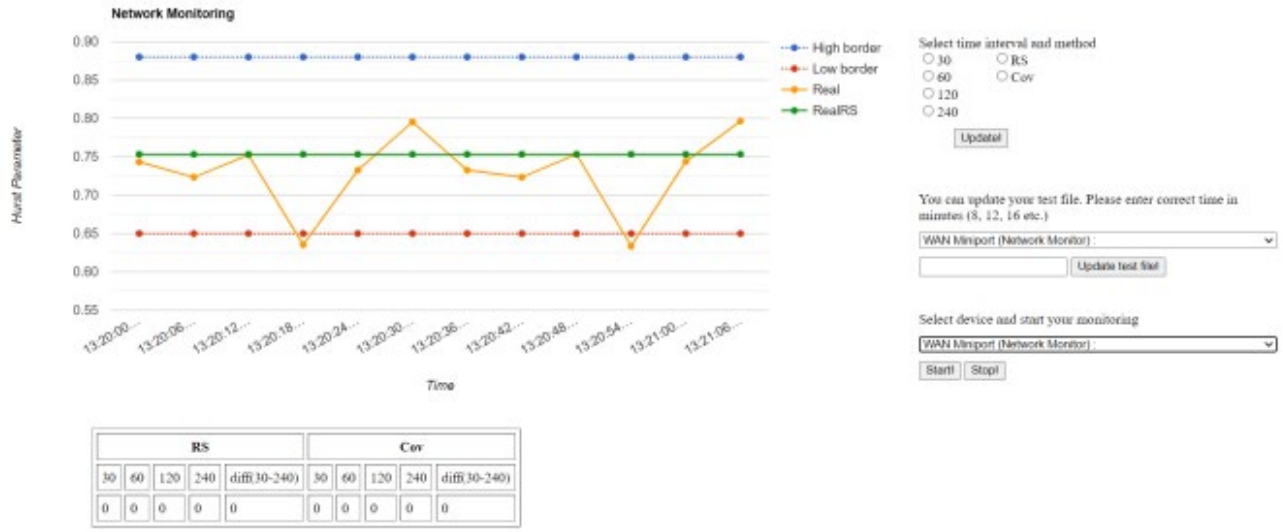

Рисунок 3.4 – Зовнішній вигляд інтерфейсу користувача

Містить три важливі блоки:

– графік залежності параметра Херста від часу;

– таблиця, що відображає кількість попереджень, що виникли;

– блок керування.

Для відображення графіка використовувалася бібліотека Google Charts.

У таблиці відображається кількість виявлених попереджень для кожного інтервалу часу за кожним з методі. Останній стовпчик вказується кількість детектованих попереджень за останні 4 хвилини моніторингу системи. Висновок про проблеми проводиться в мережі робиться з крахуванням

останніх стовпчиків за кожним із методів. Максимальним значенням даного поля буде 15, яка рівна сумі 8 + 4 + 2 + 1. За перевищення визначеного порога в обох методах можна формувати повідомлення та передати ці дані наступним пристроям у периметрі захисту системи.

В блоці керування (конфігурації) вказуються різні параметри виведення і функціонування ядра системи. Верхній блок містить конфігурацію про те, що саме відображатиметься на графіку моніторингу. У другому блоці є змога оновити існуючий .pcap файл, на основі якого розраховуються границі ймовірних допустимих значень. В останньому ж блоці запускається чи зупиняється процес моніторингу мережі системи.

3.3 Модельний опис та тестування СВА

Для тестування роботи СВА було побудовано базову мережу, зображену на рис. 3.5. Це два пристрої з запущеним агентом на різних ОС, а також один пристрій втілення атаки для з ОС Kali Linux на основі Ubuntu.

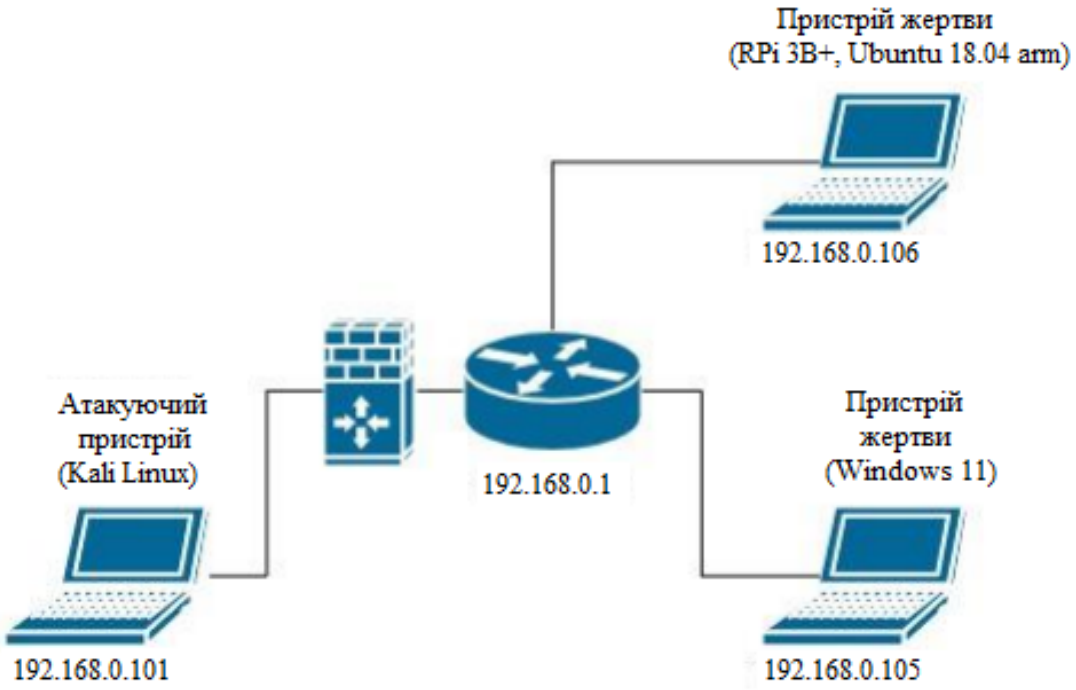

Рисунок 3.5 – Схема мережі

На атакуючій машині втілювалися два типи атак: DoS та розвідка. Перша з них запускалася із застосуванням утиліти hping3 , при допомозі якої генерувався трафік таким чином: hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.0.106(105). Є звичайною атакою SYN-flood , в якій відправляється 15000 пакетів по 120 байт у кожному. Для втілення другої застосовувалася утиліта nmap таким чином: nmap 192.168.0.106 (105).

При роботі у звичайному режимі упродовж 45 хв. у середньому одержуємо дані значення щодо кількості попереджень (усереднена величина за 5 проходів), котрі відображені у табл. 3.1. Однак варто зауважити, що при розрахунку величин із надзвичайно розрядженим за часом трафіком, власиво самі алгоритми функціонують не повністю коректно і достатньо часто отримуємо значення показників Херста, які виходять за границі 0 та 1.

Таблиця 3.1 – Результати функціонування за нормального режиму

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

Отримані значення показують, що кількість попереджень стає ближчою до половини від найбільш можливих у 30 -ти та 60-ти секундних інтервалах. В інтервалах 120-ти та 240 секунд отримуємо більш прийнятні значення. Якщо розглянути загальну кількість попереджень за тих таки 4 хвилини, то в середньому отримується 5-6 мінімум до 0 і максимум до 8-9.

Виявлення DoS-атак. За реалізації DoS -атаки упродовж 45 хв. отримуємо такі дані (усереднене значення за 5 проходів), котрі продемонстровані у табл. 3.2. Величини у малих інтервалах змінилися не суттєво, але перейшли 50% бар'єр від максимальної кількості ймовірних попереджень. Для великих часових інтервалів число попереджень значно змінилося (навіть до 4-х разів).

Таблиця 3.2 – Результати функціонування за DoS-атаки

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

Щодо загальної кількості попереджень за кожні 4 хвилини, тут в середньому одержували від 8 до 12, у піку – 13, у мінімумі – 6. Дані результати демонструють ефективність методів у детектуванні колективних та розподілених атак.

Виявлення розвідувальних атак. Так як за нормального режиму фукціонування трапляється досить чимало помилкових попереджень, детектування будь-яких точкових аномалій виглядає фактично неможливим. Результати продемонстрували схожий результат із нормальною роботою, табл. 3.3, за 45 хв.

Таблиця 3.3 – Результати функціонування при розвідці

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

Однак цілком ймовірним є варіант щодо здатності детектування даної атаки, за умови, що вона буде значно розподіленіша за часом.

Використання як метрик не кількості всіх пакетів, а й числа запитів на різні порти вирішить цю проблему, проте з цим стані впоратися і звичайні сигнатурні методи.

Можливі покращення. За одержаними результатами можна стверджувати, що у застосуванні 30-ти та 60-ти секундних інтервалів відсутній значний сенс. Система одержує велику кількість помилкових спрацьовувань, що не дозволяє

ефективно детектувати точкові атаки. Можна побачити, що зі збільшенням інтервалу часу зменшується кількість помилкових спрацьовувань у системі. Даний інтервал, ймовірно, можна збільшувати аж до одного дня чи, навіть, тижня (у залежності мережевого навантаження). Також зростання часового інтервалу зменшить проблему розрахунку показника Херста для розрідженому трафіку за часом. Для детектування точкових аномалій більш ефективно буде використовувати інші методи (як варіант, штучні імунні системи або ГА). І для більш ефективного виявлення колективних аномалій можна використовувати комбінацію деяких методів.

3.4 Висновки до третього розділу

Було сформовано базову СВА. Розглянуто її основні модулі. Також представлено діаграму використання СВА. Також описано засоби і утиліти, котрі застосовувалися для побудови кожного модуля системи. І було дано описи реалізованих модулів та його базовий функціонал.

Побудовано мережу, де тестувалася СВА. Як показали результати, у функціонуванні цих методів наявна проблема щодо грамотного вибору допустимого інтервалу значень показника Херста. Виникає достатньо велика кількість помилкових спрацьовувань, що свідчить про непридатність до детектування точкових атак. Однак дана система здатна надзвичанйо ефективно детектувати колективні та розподілені за часом атаки, зокрема DoS-атаки. Запропоновано способи щодо можливого поліпшення роботи даної системи.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Метою кваліфікаційної роботи магістра є розробити СВВ, в основі якої використовуються методи детектування аномалій трафіку мережі. Розроблювана система має бути простою для використання та налаштування, окрім того повинна легко переноситися між різноманітними програмними системами. Оскільки, проведення такого виду робіт передбачає застосування комп'ютерної техніки, зокрема ПК та периферійних пристроїв, то обов'язковим є дотримання вимог з охорони праці і техніки безпеки.

Для ефективної і безпечної роботи колективу працівників з розробки СВВ необхідно організувати безпечні умови праці. При цьому керівник організації несе безпосередню відповідальність за порушення нормативно-правових актів з охорони праці [21]. Окрім цього, на робочих місцях працівників необхідно забезпечити дотримання вимог, затверджених Наказом Мінсоцполітики від 14.02.2018 за № 207 «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями». Згідно Вимог приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до цих вимог:

– переліку однотипних за призначенням об'єктів, які підлягають обладнанню автоматичними установками пожежогасіння та пожежної сигналізації, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 22.08.2005 N 161, зареєстрованого в Міністерстві юстиції України 05.09.2005 за N 990/11270 (НАПБ Б.06.004-2005);

– Державних будівельних норм "Інженерне обладнання будинків і споруд. Пожежна автоматика будинків і споруд", затверджених наказом Держбуду України від 28.10.98 N 247 (далі - ДБН В.2.5-56:2014, з димовими пожежними

сповіщувачами та переносними вуглекислотними вогнегасниками.

В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Приміщення, де розміщені робочі місця операторів, мають бути оснащені вогнегасниками, кількість яких визначається згідно з вимогами ДСТУ 4297:2004 «Пожежна техніка. Технічне обслуговування вогнегасників». Загальні технічні вимоги і з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог НАПБ А.01.001-2014. Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог ДБН В.2.5-56:2014, ДБН В.2.5-56:2010, НАПБ А.01.001-2014 і вимог нормативно-технічної та експлуатаційної документації виробника. Проходи до засобів пожежогасіння мають бути вільними.

Лінія електромережі для живлення комп'ютера та периферійних пристроїв повинні бути виконаними як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Не допускається використовувати нульовий робочий провідник як нульовий захисний провідник. Нульовий захисний провідник прокладається від стійки групового розподільного щита, розподільного пункту до розеток електроживлення. Не допускається підключати на щиті до одного контактного затискача нульовий робочий та нульовий захисний провідники.

Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі має бути не менше площі перерізу фазового провідника. Усі провідники мають відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам НПАОП 40.1-1.01-97.

У приміщенні, де одночасно експлуатуються понад п'ять комп'ютерів, на помітному, доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Комп'ютери повинні підключатися до електромережі тільки за

допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення.

У штепсельних з'єднаннях та електророзетках, крім контактів фазового та нульового робочого провідників, мають бути спеціальні контакти для підключення нульового захисного провідника. Їхня конструкція має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше, ніж приєднання фазового та нульового робочого провідників. Порядок роз'єднання при відключенні має бути зворотним. Не допускається підключати комп'ютери до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв. Електромережі штепсельних з'єднань та електророзеток для живлення комп'ютерної техніки повинні бути виконаними за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі. Штепсельні з'єднання та електророзетки для напруги 12 В та 42 В за своєю конструкцією мають відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В. Штепсельні з'єднання та електророзетки, розраховані на напругу 12 В та 42 В, мають візуально (за кольором) відрізнятися від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

При підвищенні ефективності контролю доступу в приміщення, де для забезпечення безпеки мешканців, співробітників і збереження майна використовуються ДС, важливим, з точки зору охорони праці, є забезпечення достатньої величини природного та штучного освітлення, які визначені у НПАОП 0.00-7.15-18.

Організація робочого місця фахівця із дослідження методів та програмно-апаратних засобів оптимізаційних процесів на основі ГА повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги». Відстань від екрана до ока фахівців, які працюють за комп'ютером визначається згідно з вимогами ДСанПіН 3.3.2.007-98.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрана

комп’ютера, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля згідно з вимогами ДСанПіН 3.3.2.007-98.

Таким чином, у результаті аналізу вимог щодо охорони праці користувачів комп’ютерів, визначено особливості організації робочих місць, вимог з електробезпеки, природного та штучного освітлення для ефективної і безпечної роботи фахівців з розробки СВВ, в основі якої використовуються методи детектування аномалій трафіку мережі.

4.2. Планування та порядок проведення евакуації населення з районів наслідків впливу НС техногенного та природного характеру

В умовах неповного забезпечення захисними спорудами в містах та інших населених пунктах, що мають об'єкти підвищеної небезпеки, основним засобом захисту населення є евакуація і розміщення його у зонах, які є безпечними для проживання людей [45].

Евакуації підлягає населення, яке проживає в населених пунктах, що знаходяться у зонах можливого катастрофічного затоплення, можливого небезпечного радіоактивного забруднення, хімічного ураження, в районах виникнення стихійного лиха, аварій і катастроф (якщо виникає безпосередня загроза життю та здоров'ю людей). Залежно від обставин, які склалися на час надзвичайної ситуації, може бути проведено загальну або часткову евакуацію населення тимчасового або безповоротного характеру. Загальна евакуація проводиться за рішенням Кабінету Міністрів України для всіх категорій населення і планується на випадок:

– можливого небезпечного радіоактивного забруднення територій навколо атомних електростанцій (якщо виникає безпосередня загроза життю та здоров'ю людей, які проживають в зоні ураження);

– виникнення загрози катастрофічного затоплення місцевості з чотиригодинним добіганням проривної хвилі.

Часткова евакуація проводиться за рішенням Кабінету Міністрів України у разі загрози або виникнення надзвичайної ситуації техногенного та природного характеру.

Під час проведення часткової евакуації завчасно вивозиться не зайняте у сферах виробництва та обслуговування населення: діти, учні навчальних закладів, вихованці дитячих будинків, разом з викладачами та вихователями, студенти, пенсіонери та інваліди, які утримуються у будинках для осіб похилого віку, разом з обслуговуючим персоналом і членами їх сімей [45].

У сфері захисту населення і територій від надзвичайних ситуацій техногенного та природного характеру евакуація населення планується на випадок:

– аварії на атомній електростанції з можливим забрудненням території; усіх видів аварій з викидом сильнодіючих отруйних речовин; загрози катастрофічного забруднення місцевості :

– лісових і торф'яних пожеж, землетрусів, зсувів, інших геофізичних і гідрометеорологічних явищ з тяжкими наслідкам, що загрожують населеним пунктам.

Загальна евакуація проводиться шляхом вивезення основної частини населення з міст і небезпечних районів усіма видами наявних транспортних засобів на відповідній адміністративній території та виведення найбільш витривалої його частини пішки. Часткова евакуація проводиться з використанням транспортних засобів, що експлуатуються за діючим графіком. На органи виконавчої влади, органи місцевого самоврядування та керівників об'єктів, які проводять евакуацію населення, покладається:

– планування і проведення евакуації працівників та членів їх сімей;

– подання до відповідних транспортних органів розрахунків потреби у транспортних засобах для вивезення працівників і членів їх сімей до безпечних районів;

– контроль за плануванням, підготовкою і проведенням евакуаційних заходів підвідомчими об'єктами;

– визначення та підготовка безпечного району для розміщення евакуйованих працівників і членів їх сімей.

Інші заходи та порядок проведення евакуації викладено у постанові Кабінету Міністрів від 26 жовтня 2001р. № 1432 про затвердження Положення про порядок проведення евакуації населення у разі загрози або виникнення надзвичайних ситуацій техногенного та природного характеру.

У плані евакуації, складовою частиною якого є карта (схема), зазначаються:

– висновки з оцінки обстановки у разі виникнення надзвичайної ситуації;

– порядок оповіщення населення про початок евакуації;

– кількість населення, яке підлягає евакуації, за віковими категоріями;

– терміни проведення евакуації;

– склад евакуаційних органів і терміни приведення їх у готовність;

– кількість населення, яке вивозиться різними видами транспортних засобів окремо і виводиться пішки;

– розподілення об'єктів за збірними евакуаційними пунктами, пунктами посадки, районами (пунктами) розміщення та евакуаційними напрямками; маршрути евакуації;

– райони (пункти) розміщення евакуйованого населення; пункти посадки на транспортні засоби, пункти висадки у безпечному районі, порядок доставки населення з пунктів висадки до районів (пунктів) розміщення;

– заходи щодо організації приймання, розміщення, захисту та життєзабезпечення евакуйованого населення у безпечному районі;

– порядок організації управління і зв'язку.

План приймання і розміщення евакуйованого населення включає також розділ з транспортного забезпечення евакуації, в якому зазначається [26]:

– кількість транспортних засобів кожного виду і термін їх подачі до пунктів посадки;

– кількість населення, яке підлягає евакуації;

– терміни відправлення евакуйованого населення у безпечні райони;

– терміни прибуття евакуйованого населення до пунктів посадки;
– маршрути руху транспортних засобів;
– кількість рейсів.

На всіх громадян, які підлягають евакуації, завчасно складаються списки за об'єктами і житлово-експлуатаційними організаціями у трьох примірниках, один з яких залишається на об'єкті або в житлово-експлуатаційній організації, другий (у разі одержання рішення про проведення евакуації) після уточнення списків надсилається на збірний евакуаційний пункт, третій - до евакуаційної комісії району (пункту) розміщення.

З отриманням рішення (сигналу) про проведення евакуації евакуаційні комісії уточнюють завдання керівникам об'єктів щодо проведення евакуаційних заходів, контролюють стан оповіщення населення, його збору, формування колон (через начальників маршрутів), забезпечують переміщення їх до пунктів евакуації, а також разом з транспортними службами - готовність транспортних засобів до перевезень, уточнюють порядок їх використання, підтримують постійний зв'язок з начальниками маршрутів та з органами виконавчої влади безпечних районів, інформують їх про хід евакуації.

У райони розміщення евакуаційних органів та населення, яке підлягає евакуації, направляються представники евакуаційних комісій для вирішення питань приймання, розміщення і життєзабезпечення евакуйованого населення.

Керівник органу виконавчої влади і евакуаційна комісія безпечного району, організовують підготовку пунктів висадки, розгортають приймальний евакуаційний пункт, уточнюють кількість прибулих і порядок подачі транспортних засобів для їх вивезення з пунктів висадки, а також з проміжних пунктів евакуації до пунктів розміщення, контролюють роботу керівників об'єктів безпечних районів з прийому і розміщення евакуйованого населення.

У разі оголошення евакуації громадяни самостійно на міських транспортних засобах, які у цей період працюють цілодобово, прибувають на збірні евакуаційні пункти. Працівники цих пунктів розподіляють громадян, які підлягають евакуації, за транспортними засобами, інструктують їх і забезпечують посадку на транспортні засоби.

Евакуйовані громадяни повинні мати при собі паспорт, військовий квиток, документ про освіту, трудову книжку або пенсійне посвідчення, свідоцтво про народження, гроші і цінності, продукти харчування і воду на 3 доби, постільну білизну, необхідний одяг і взуття загальною вагою не більш як 50 кілограмів на кожного члена сім'ї. Дітям дошкільного віку вкладається у кишеню або пришивається до одягу записка, де зазначається прізвище, ім'я та по батькові, домашня адреса, а також ім'я та по батькові матері і батька.

4.3. Висновки до четвертого розділу

В цьому розділі проаналізовано важливі питання охорони праці та безпеки в надзвичайних ситуаціях, висвітлено питання планування та порядку проведення евакуації населення з районів наслідків впливу НС техногенного та природного характеру.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було отримано такі результати:

– розглянуто існуючі СВВ, їх класифікацію та сферу застосування. Це класифікація з урахуванням методів, котрі є у алгоритмах виявлення вторгнень, і основі топології одержуваної інформації;

– проведено класифікацію мережевих атак, наведено приклади їх застосування та описано процедуру реалізації атаки. Головні типи атак – це розвідка, U2R, R2U, експлойт та DoS-атаки;

– вивчено методи виявлення аномалій, представлено їх класифікацію, переваги та недоліки. Можна виділити кілька груп аномалій: точкові, контекстні та колективні. Самі ж методи детектування можна розділити на такі групи: поведінкові методи, методи МН, методи із використанням обчислювального інтелекту та методи з урахуванням знань;

– більш детально було розглянуто та реалізовано методи детектування аномалій на базі фрактального аналізу. Для розрахунку оцінки аномальності трафіку застосовується параметр Херста;

– було представлено та реалізовано базову архітектуру СВВ;

– здійснено тестування функціонування системи із застосуванням атак різних типів.

Результати проведеної роботи свідчать, що для детектування колективних і розподілених у часі атак застосування методів на базі фрактального аналізу при застосуванні параметра Херста здатні ефективно детектувати дані впливу.

Для виявлення точкових та контекстних атак необхідно використовувати інші методи, так як складність вибору грамотного інтервалу допустимих значень веде до великої кількості помилкових спрацьовувань. А це, врешті решт, не дає можливості ефективно детектувати даний тип впливу на систему.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Tymoshchuk, V., Vorona, M., Dolinskyi, A., Shymanska, V., & Tymoshchuk, D. (2024). SECURITY ONION PLATFORM AS A TOOL FOR DETECTING AND ANALYSING CYBER THREATS. Collection of scientific papers «ΛΌГОΣ», (December 13, 2024; Zurich, Switzerland), 232-237.

2. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.

3. Tymoshchuk, V., Mykhailovskyi, O., Dolinskyi, A., Orlovska, A., & Tymoshchuk, D. (2024). OPTIMISING IPS RULES FOR EFFECTIVE DETECTION OF MULTI-VECTOR DDOS ATTACKS. Матеріали конференцій МЦНД, (22.11. 2024; Біла Церква, Україна), 295-300.

4. Tymoshchuk, V., Vantsa, V., Karnaukhov, A., Orlovska, A., & Tymoshchuk, D. (2024). COMPARATIVE ANALYSIS OF INTRUSION DETECTION APPROACHES BASED ON SIGNATURES AND ANOMALIES. Матеріали конференцій МЦНД, (29.11. 2024; Житомир, Україна), 328-332.

5. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.

6. Tymoshchuk, V., Pakhoda, V., Dolinskyi, A., Karnaukhov, A., & Tymoshchuk, D. (2024). MODELLING CYBER THREATS AND EVALUATING THE PERFORMANCE OF INTRUSION DETECTION SYSTEMS. Grail of Science, (46), 636–641. https://doi.org/10.36074/grail-of-science.29.11.2024.081

7. Корченко А.О. Методи ідентифікації аномальних станів для систем виявлення вторгнень: Автореф. дис. ... д-ра. техн. Наук. Київ, 2019. 42 с.

8. ТИМОЩУК, Д., & ЯЦКІВ, В. (2024). USING HYPERVISORS TO CREATE A CYBER POLYGON. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (3), 52-56.

9. Ribeiro V. J., Riedi R. H., Baraniuk R. G. Optimal sampling strategies for multiscale models with application to network traffic estimation. IEEE Workshop on

Statistical Signal Processing, 2003, St. Louis, MO, USA. URL: https://doi.org/10.1109/ssp.2003.1289360 (date of access: 14.12.2024).

10. Zagorodna, N., Skorenkyy, Y., Kunanets, N., Baran, I., & Stadnyk, M. (2022). Augmented Reality Enhanced Learning Tools Development for Cybersecurity Major. In ITTAP (pp. 25-32).

11. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.

12. Muzh, V., & Lechachenko, T. (2024). Computer technologies as an object and source of forensic knowledge: challenges and prospects of development. Вісник Тернопільського національного технічного університету, 115(3), 17-22.

13. Derkach, M., Skarga-Bandurova, I., Matiuk, D., & Zagorodna, N. (2022, December). Autonomous quadrotor flight stabilisation based on a complementary filter and a PID controller. In 2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 1-7). IEEE.

14. Tymoshchuk, D., & Yatskiv, V. (2024). Slowloris ddos detection and prevention in real-time. Collection of scientific papers «ΛΌГОΣ», (August 16, 2024; Oxford, UK), 171-176.

15. Booker L. B., Goldberg D. E., Holland J. H. Classifier systems and genetic algorithms. Artificial Intelligence. 1989. Vol. 40, no. 1-3. P. 235–282. URL: https://doi.org/10.1016/0004-3702(89)90050-7 (date of access: 14.12.2024).

16. Orobchuk, O. (2019). Methodology of development and architecture of ontooriented system of electronic learning of Chinese image medicine on the basis of training management system. Вісник Тернопільського національного технічного університету, 92(4), 83-90.

17. Home | TCPDUMP & LIBPCAP. Home | TCPDUMP & LIBPCAP. URL: https://www.tcpdump.org (date of access: 14.12.2024).

18. gopacket package - github.com/google/gopacket - Go Packages. Go Packages - Go Packages. URL: https://pkg.go.dev/github.com/google/gopacket (date of access: 14.12.2024)..

19. On the self-similar nature of Ethernet traffic / W. E. Leland et al. ACM SIGCOMM Computer Communication Review. 1993. Vol. 23, no. 4. P. 183–193. URL: https://doi.org/10.1145/167954.166255 (date of access: 14.12.2024).

20. Muzh, V., & Lechachenko, T. (2024). Computer technologies as an object and source of forensic knowledge: challenges and prospects of development. Вісник Тернопільського національного технічного університету, 115(3), 17-22.

21. Заікіна Д., Глива В. Основи охорони праці та безпека життєдіяльності. 2019. URL: https://doi.org/10.31435/rsglobal/001 (дата звернення: 14.12.2024).

22. Кучма М.М. Цивільна оборона (цивільний захист). Навчальний посібник. Львів : Магнолія 2006 . 2024. 296 с.

ДОДАТОК А

Тези конференції