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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Шляхова Владислава Ігоровича*

академічної групи *125м-20-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Фрактальний аналіз трафіку в інформаційно-комунікаційних мережах для систем виявлення атак*

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

Дніпро
20__

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту *Шляхову Владиславу Ігоровичу* **академічної групи** *125м-20-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Фрактальний аналіз трафіку в інформаційно-комунікаційних мережах для систем виявлення атак*

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

Розділ	Зміст	Термін виконання
Розділ 1	Дослідження систем виявлення атак та методів аналізу мережевого трафіку, а також його фрактальних властивостей.	03.09.2021 – 10.10.2021
Розділ 2	Розробка підходу до визначення аномалій телекомунікаційного трафіку, що базується на розрахунку фрактальних параметрів і визначення фазового портрета, та оцінка його ефективності.	11.10.2021 – 24.11.2021
Розділ 3	Розрахунки капітальних витрат, економічного ефекту та терміну окупності капітальних інвестицій застосування запропонованих рішень.	25.11.2021 – 04.12.2021

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

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Шляхов В.І.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 87 с., 33 рис., 4 додатки, 47 джерел.

Об’єкт дослідження – телекомунікаційний трафік.

Предмет дослідження – підходи до оцінювання стану телекомунікаційного трафіку на основі його фрактального аналізу.

Мета кваліфікаційної роботи – визначення мережевих атак за допомогою фрактальних методів оцінки мережевого трафіку, що ґрунтуються на ознаках його самоподібності.

Наукова новизна результатів – було доведено, що за значеннями показника Херста та кореляційної розмірності не можна однозначно судити про наявність мережевої атаки; за будь-яких ситуаціях про це можна судити за формою фазового атрактора системи.

У першому розділі досліджено системи виявлення атак та методи аналізу мережевого трафіку, а також його фрактальні властивості.

У спеціальній частині роботи запропоновано підхід до визначення аномалій телекомунікаційного трафіку, що базується на розрахунку фрактальних параметрів та визначення фазового портрета та оцінено його ефективність. За наслідками досліджень зроблено висновки щодо рішення поставленої задачі.

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

ПОКАЗНИК ХЕРСТА, ТЕЛЕКОМУНІКАЦІЙНИЙ ТРАФІК, ФАЗОВИЙ АТРАКТОР, СИСТЕМИ ВИЯВЛЕННЯ АТАК, КОРЕЛЯЦІЙНА РОЗМІРНІСТЬ, ВИЯВЛЕННЯ МЕРЕЖЕВИХ АНОМАЛІЙ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

РЕФЕРАТ

Пояснительная записка 87 с., 33 рис., 4 приложения, 47 источников.

Объект исследования – телекоммуникационный трафик.

Предмет исследования – подходы к оценке состояния телекоммуникационного трафика на основе его фрактального анализа.

Цель квалификационной работы – определение сетевых атак с помощью фрактальных методов оценки сетевого трафика, основанных на признаках его самоподобия.

Научная новизна результатов – доказано, что по значениям показателя Херста и корреляционной размерности нельзя однозначно судить о наличии сетевой атаки; при любых ситуациях об этом можно судить по форме фазового аттрактора системы.

В первой главе исследованы системы обнаружения атак и методы анализа сетевого трафика, а также его фрактальные свойства.

В специальной части работы предложен подход к определению аномалий телекоммуникационного трафика, который базируется на расчете фрактальных параметров и определении фазового портрета и оценена его эффективность. По результатам исследований сделаны выводы о решении поставленной задачи.

В экономическом разделе выполнены расчеты капитальных затрат, экономического эффекта и срока окупаемости капитальных инвестиций по применению предложенных решений.

ПОКАЗАТЕЛЬ ХЕРСТА, ТЕЛЕКОММУНИКАЦИОННЫЙ ТРАФИК, ФАЗОВЫЙ АТРАКТОР, СИСТЕМЫ ВЫЯВЛЕНИЯ АТАК, КОРРЕЛЯЦИОННАЯ РАЗМЕРНОСТЬ, ВЫЯВЛЕНИЕ СЕТЕВЫХ АНОМАЛИЙ, ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ

ABSTRACT

Explanatory note: p. 87, fig. 33, 4 additions, 47 sources.

The object of research is telecommunication traffic.

The subject of research – approaches to assessing the state of telecommunications traffic based on its fractal analysis.

The purpose of the qualification work is to determine network attacks using fractal methods of network traffic estimation, based on the signs of its self-similarity.

Scientific novelty of the results – it was proved that the values of the Hurst parameter and the correlation dimension can not be unambiguously judged on the presence of a network attack; in any situation this can be judged by the shape of the phase attractor of the system.

The first section examines attack detection systems and methods of network traffic analysis, as well as its fractal properties.

In a special part of the work the approach to definition of anomalies of telecommunication traffic based on calculation of fractal parameters and definition of a phase portrait is offered and its efficiency is estimated. Based on the results of research, conclusions were made regarding the solution of the problem.

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

HURST INDICATOR, TELECOMMUNICATION TRAFFIC, PHASE ATTRACTOR, ATTACK DETECTION SYSTEMS, CORRELATION DIMENSION, DETECTION OF NETWORK ANOMALIES, SIMULATIVE MODELING

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІБ – Інформаційна безпека;

ІАД – Інтелектуальний аналіз даних;

ІС – Інформаційна система;

ІКМ – Інформаційно-комунікаційна мережа;

ПЗ – Програмні засоби;

СВА – Системи виявлення атак;

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

DoS attack – Denial of Service attack – Атака на відмову в обслуговуванні.

ЗМІСТ

ВСТУП

Стрімкий розвиток інформаційно-комунікаційних систем і мереж (ІКМ) та інформаційних технологій викликає ряд проблем, пов'язаних з безпекою мережевих ресурсів. Тому актуальною є розробка та вдосконалення систем виявлення та запобігання вторгнень, головним завданням яких є розпізнавання мережевих атак, спроб несанкціонованого доступу та використання ресурсів мережі [1, 2].

Ця проблема вирішується шляхом використання засобів моніторингу, здатних аналізувати трафік мережі в режимі реального часу. До таких засобів моніторингу відносяться системи виявлення та запобігання атак (СВА).

Захист критично важливих об'єктів інфраструктури від навмисних кібернетичних вторгнень зі сторони окремих осіб, організацій або країн є надзвичайно актуальним. Наприклад, до основних загроз для промислових систем управління відносяться, зокрема: мережеві атаки через корпоративні мережі; атаки на стандартні мережеві компоненти; атаки типу «відмова в обслуговуванні» [3].

Засобом захисту ІКМ від інформаційно руйнівних утручань у вигляді кібернетичних вторгнень є системи СВА, основне завдання яких полягає в оперативному їх виявленні та в ініціюванні ефективного захисного сценарію щодо припинення факту порушення конфіденційності, доступності та цілісності інформаційних ресурсів та сервісів.

Наразі сформувались два напрямки протидії вторгнень: виявлення зловживань та виявлення аномалій [4, 5].

При виявленні мережевих аномалій [1] даними для аналізу є мережевий трафік, представлений як швидкість передачі даних або набір мережевих пакетів, в загальному випадку фрагментованих на рівні IP. Дані можуть бути агреговані за певний часовий інтервал і нормалізовані, по ним оцінюються характеристики (набір ознак) трафіку. Створений набір ознак порівнюється із набором характеристик нормальної діяльності об'єкта (користувача або

системи) – шаблоном нормальної поведінки. Якщо спостерігається суттєва розбіжність порівнюваних наборів, то фіксується мережева аномалія. В іншому випадку відбувається уточнення шаблону нормального трафіку за допомогою зміни параметрів його настройки з урахуванням поточного спостережуваного профілю мережевої активності.

На такий алгоритм виявлення аномалій орієнтуються поведінкові методи аналізу мережевого трафіку, до яких можна віднести: вейвлет-аналіз; статистичний аналіз; аналіз ентропії; спектральний аналіз; фрактальний аналіз; кластерний аналіз [1, 6, 7].

Трафік в ІКМ є нелінійним стохастичним процесом з властивостями самоподоби та з хаотичною і фрактальною динамікою. Крім того, встановлено, що агрегований трафік від різних джерел на малих часових масштабах проявляє мультифрактальний характер [8].

Таким чином, комплексне спостереження інформативних ознак мережевого самоподібного трафика для визначення аномалій в системах виявлення атак, наразі є актуальною задачею.

Метою роботи є визначення мережевих атак за допомогою фрактальних методів оцінки мережевого трафіку, що ґрунтуються на ознаках його самоподібності.

Постановка задачі:

• провести аналіз систем виявлення атак в мережевому трафіку;

• провести огляд методів аналізу мережевого трафіку (зокрема поведінкових);

• дослідити фрактальні властивості телекомунікаційного трафіку;

• запропонувати підхід до визначення аномалій телекомунікаційного трафіку, що базується на розрахунку фрактальних параметрів та визначення фазового портрета;

• оцінити ефективність розробленого підходу.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Огляд систем виявлення атак в мережевому трафіку

1.1.1 Системи аналізу захищеності

Системи аналізу захищеності досліджують налаштування елементів захисту операційних систем робочих станцій і серверів, аналізують топологію мережі, шукають незахищені мережеві з'єднання, досліджують налаштування міжмережевих екранів. Дані системи дозволяють значно знизити ризик наявності невиявлених загроз у системі захисту мереж [2, 9-14].

До сучасних засобів моніторингу комп'ютерних атак відносяться аналізатори трафіку, такі як «сніфери» і системи виявлення атак. Істотним недоліком даних систем є те, що аналіз трафіку адміністратором безпеки здійснюється практично вручну із застосуванням лише найпростіших засобів автоматизації, таких як аналіз протоколів. У зв'язку з цим дані системи не підходять для моніторингу великих обсягів трафіку мереж масштабу міста. Рішенням цієї проблеми є застосування засобів моніторингу, здатних аналізувати трафік великого об'єму в режимі реального часу. До таких засобів моніторингу відносяться системи виявлення атак.

Системи виявлення атак являють собою окремий клас програмних засобів (ПЗ), під яким розуміють програми, процедури, правила, а також, якщо передбачено, супутніх їм документації та даних, що відносяться до функціонування системи обробки інформації. Повна назва СВА – це системи виявлення і запобігання атак, оскільки саме в можливості автоматизованої протидії атакам полягає одна з основних переваг таких систем, у порівнянні, наприклад, із засобами, заснованими на людському факторі. Проте надалі буде використовуватися найбільш усталена назва – система виявлення атак.

Використання СВА дозволяє вирішити цілий ряд завдань, що забезпечують досягнення цілей інформаційної безпеки:

• розпізнавання відомих і, по можливості, невідомих атак та попередження персоналу, що відповідає за забезпечення інформаційної безпеки (ІБ);

• статистичний аналіз шаблонів аномальних дій;

• моніторинг і аналіз користувацької, мережевої та системної активності;

• контроль цілісності файлів та інших ресурсів інформаційної системи (ІС);

• аудит системної конфігурації і виявлення вразливостей;

• інсталяція і підтримка роботи серверів-пасток для запису інформації про порушників;

• зниження навантаження на персонал (або звільнення від нього), що відповідає за ІБ, від поточних рутинних операцій з контролю за користувачами, системами і мережами, які є компонентами ІС;

• надання можливості управління функціями захисту не спеціалістам в області інформаційної безпеки.

1.1.2 Сучасні технології виявлення атак

Під виявленням атак розуміють процес оцінки подій ІС та її інформаційних потоків, який реалізується за допомогою аналізу журналів реєстрації операційних систем (ОС) і додатків або мережевого трафіку. Реалізація більшості мережевих атак здійснюються в три етапи [2, 9-14].

Перший, підготовчий, етап полягає в пошуку передумов для здійснення тієї чи іншої атаки. На даному етапі шукають вразливості, використання яких робить можливим в принципі реалізацію атаки, яка і складає другий етап. На третьому етапі атака завершується. При цьому перший і третій етапи самі по собі можуть бути атаками. Наприклад, пошук порушником вразливостей за допомогою сканерів безпеки вже вважається атакою.

Технології виявлення атак постійно розвиваються і удосконалюються, і ця область постійно залучає нових виробників і розробників. Незважаючи на

брак теоретичних основ технології виявлення атак, існують досить ефективні методи, що використовують на сьогодні.

Існує кілька способів класифікації систем виявлення атак, кожен з яких заснований на різних характеристиках. Тип слід визначати, виходячи з таких характеристик:

• Спосіб контролю за системою. За способами контролю за системою поділяються на network-based, host-based і application-based.

• Спосіб аналізу. Це частина системи визначення проникнення, яка аналізує події, отримані з джерела інформації, і приймає рішення, чи відбувається проникнення. Способами аналізу є виявлення зловживань (misuse detection) та виявлення аномалій (anomaly detection).

• Затримка в часі між отриманням інформації з джерела та її аналізом і прийняттям рішення. Залежно від затримки в часі, системи виявлення атак діляться на interval-based (або пакетний режим) і real-time.

Більшість комерційних систем виявлення атак є real-time network-based системами.

Виявлення атак вимагає виконання однієї з двох умов: або знання всіх можливих атак та їх модифікацій, чи розуміння очікуваної поведінки контрольованого об'єкта системи. Всі існуючі технології виявлення мережевих атак можна розділити на два типи: методи на основі сигнатур (зразків і правил); методи на основі аномалій.

Зазвичай в СВА намагаються поєднувати обидві технології, щоб усунути недоліки, властиві кожній окремо. Перевага «аномальних» систем – виявлення невідомих або нових видів атак, які можуть «обійти» СВА. Реєстрація такого роду подій тягне за собою їх аналіз адміністратором, створення для них шаблону і внесення останнього до бази даних СВА. Системи, засновані на методі аномалій, вважаються досить перспективними, але ще розвиваються і перебувають у стадії дослідження.

Особливістю технології виявлення атак на основі сигнатур є процес опису атаки у вигляді шаблону або сигнатури і пошуку даного шаблону в

контрольованому просторі (наприклад, мережевому трафіку або журналі реєстрації). Така СВА може виявити всі відомі атаки, але вона мало пристосована для виявлення нових, ще невідомих, атак.

При розробці СВА, заснованих на цьому підході, виникають дві основні проблеми. Перша полягає у створенні механізму опису сигнатур, тобто мови опису атак, а друга проблема виражається в наступному: як записати атаку, щоб зафіксувати всі можливі її модифікації? Схема технології виявлення атак на основі сигнатур показана на рис. 1.1.

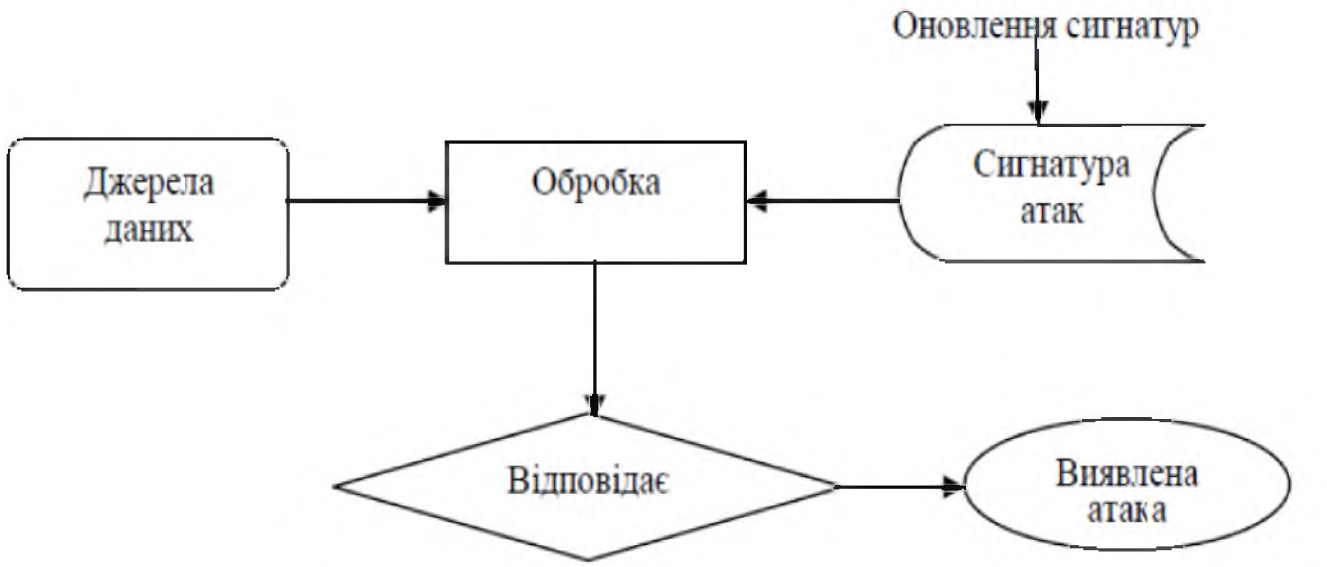

Рисунок 1.1 – Схема виявлення атак на основі сигнатур

Переваги технології виявлення атак на основі сигнатур:

• детектори зловживань ефективно визначають атаки й дуже рідко створюють помилкові повідомлення;

• детектори зловживань швидко й надійно діагностують використання конкретного інструментального засобу або технології атаки; це дає змогу адміністратору скоригувати заходи для забезпечення безпеки;

• швидкість аналізу.

Недоліки технології виявлення атак на основі сигнатур:

• оскільки детектори зловживань виявляють лише відомі їм атаки, слід постійно оновлювати їхні бази даних для отримання сигнатур нових атак;

• більшість детекторів зловживань розроблено так, що вони використовують лише певні сигнатури, а це не дає виявити можливі варіанти атак.

Технологія виявлення атак на основі аномалій побудована на припущенні, що аномальна поведінка суб'єкта ІС (системи, програми, користувача), тобто, як правило, атака або яка-небудь ворожа дія часто проявляється як відхилення від нормальної поведінки. Зазвичай системи виявлення аномальної активності використовують як джерело даних журнали реєстрації і поточна діяльність користувача, хоча існують приклади системи виявлення аномалій в мережевому трафіку [4-5, 15-17].

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

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

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

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

Підкатегорією методу «пропуск атаки» є аналіз на основі профілів, коли нормальна поведінка визначається для окремих суб'єктів (користувачів / систем).

Іноді елементи такого аналізу зустрічаються і в інших методах, скажімо, в розшифровці протоколу, коли виявлений елемент, що не належить наперед визначеному протоколу або порушує правила використання протоколів. Схема типової системи виявлення аномалій показана на рис. 1.2.

Прикладами аномальної поведінки є велика кількість з'єднань за короткий проміжок часу, високі завантаження центрального процесора і

коефіцієнт мережевого навантаження або використання периферійних пристроїв, які зазвичай не використовуються.

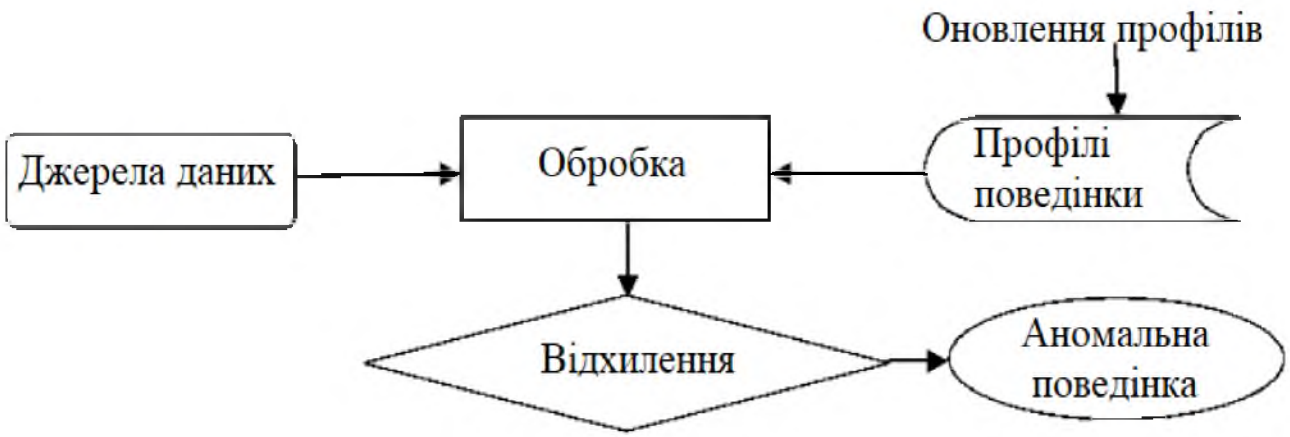

Рисунок 1.2 – Схема системи виявлення аномальної поведінки

Якщо описати профіль нормальної поведінки суб'єкта, то будь-яке відхилення від нього можна охарактеризувати як аномальна поведінка.

Переваги технології виявлення атак на основі аномалій:

• СВА, що виявляють аномалії, фіксуючи несподівану поведінку системи, отримують можливість визначати симптоми атак, не маючи відомостей про їхні конкретні деталі;

• детектори аномалій збирають інформацію, якою в подальшому можуть скористатися детектори зловживань для визначення сигнатур.

Недоліки технології виявлення атак на основі аномалій:

• під час виявлення аномалій, як правило, створюється велика кількість помилкових сигналів про атаки у разі непередбачуваної поведінки користувачів і мережної активності;

• цей метод часто потребує певного етапу навчання системи, під час якого визначаються характеристики нормальної поведінки; якість проведення цього навчання суттєво впливає на подальшу ефективність СВА;

• не можна реалізувати опис атаки за елементами; повідомляється те, що відбувається щось підозріле;

• дана технологія значно залежить від середовища функціонування як визначального фактор анормальної поведінки;

• відносно низька швидкість аналізу;

• трудомістке завдання побудови профілів суб'єктів ІС.

Порівняння методів СВА наведено у табл. 1.1

Таблиця 1.1 – Порівняння методів СВА

Характеристика	**Сигнатурні методи**	**Методи аномалій**
Множина виявлених атак	обмежується відомими видами атак	обмежується можливостями налаштування і методами аналізу СВА
Ймовірність пропуску атаки	середня	низька
Ймовірність помилкового спрацьовування	дуже низька	висока
Вимоги до обчислювальних ресурсів ІС	середні	високі

1.1.3 Переваги використання СВА порівняно з firewall'ами

Кожен засіб захисту адресовано конкретній загрозі в системі. Більш того, кожен засіб захисту має слабкі та сильні сторони. Тільки комбінуючи їх, можна захиститися від максимально великого спектру атак.

Firewall'и є механізмами створення бар'єру, заступаючи вхід деяких типів мережевого трафіку і дозволяючи інші види трафіку. Створення такого бар'єру відбувається на основі політики firewall'а. Системи виявлення атак служать механізмами моніторингу, спостереження активності та прийняття рішень про те, чи є спостережувані події підозрілими. Вони можуть виявити атакуючих, які обійшли firewall, і видати звіт про це адміністратору, який, у свою чергу, зробить кроки щодо запобігання атаки.

Системи виявлення атак стають необхідним доповненням інфраструктури безпеки в кожній організації. Технології виявлення проникнень не роблять систему абсолютно безпечною. Проте практична користь від систем виявлення атак існує, і не маленька, що доведено експертним методом оцінювання у табл. 1.2.

Таблиця 1.2 – Ймовірності подолання загроз різними засобами захисту

Вид атакуючої дії	Засіб захисту			
	Між-мережевий екран	VPN шлюз	СВА	Анти-вірус
Троянські програми				0,96
Віруси				0,92
DoS-атаки	0,81	0,98	0,98	
DDoS-атаки	0,62	0,79	0,97	
Макровіруси				0,6
IP Spoofing	0,69	0,96	0,95	
DNS Spoofing			0,92	
WEB Spoofing			0,54	
Захоплення мережевих підключень	0,51	0,97	0,93	
Різні види сканування мережі	0,59		0,89	
Порушення конфіденційності даних		0,95		
Автоматичний підбір паролів	0,75		0,91	
Атаки на протоколи			0,79	
Неавторизоване використання прав	0,32		0,91	
Неконтрольоване використання ресурсів	0,53	0,61	0,81	0,64
Неавторизоване використання АС	0,62	0,73	0,79	0,67
Прослуховування мережі		0,92		
Шпигунське ПЗ			0,54	0,97

1.1.4 Швидкість реакції

Важливим елементом в системах виявлення атак є швидкість реакції, що відбувається через певні проміжки часу, тобто пакетно. Швидкість реакції вказує на час, що минув між подіями, які були виявлені монітором, аналізом цих подій і реакцією на них.

У системах, реакція яких відбувається через певні проміжки часу, інформаційний потік від точок моніторингу до інструментів аналізу не є безперервним. У результаті інформація обробляється способом, аналогічним комунікаційним схемами «зберегти і перенаправляти». Багато ранніх host-based систем виявлення атак використовують дану схему хронометражу, тому що вони залежать від записів аудиту в ОС. Засновані на інтервалі системи не виконують ніяких дій, які є результатом аналізу подій.

Real-Time (безперервні) системи виявлення атак обробляють безперервний потік інформації від джерел. Найчастіше це є домінуючою схемою в network-based системах, які отримують інформацію з потоку мережевого трафіку. Термін «реальний час» використовується в тому ж сенсі, що і в системах управління процесом. Це означає, що визначення проникнення, що виконується системами виявлення атак в "реальному часі призводить до результатів досить швидко, що дозволяє виконувати певні дії в автоматичному режимі.

1.2 Поведінкові методи аналізу мережевого трафіку

Класифікація методів виявлення атак схематично представлена на рис. 1.3. Дана схема розбиття є умовною і не претендує на повноту: деякі з підходів можуть належати до кількох груп. Зокрема, експертні системи та кінцеві автомати можуть використовуватися для виявлення аномалій, але у більшості випадків вони застосовуються саме для виявлення зловживань. Також такі методи обчислювального інтелекту, як нейронні мережі та метод

опорних векторів, найчастіше зараховують до методів машинного навчання. У схемі, що відповідає рис. 1.3, обрано таке розбиття, при якому методи інтелектуального аналізу даних (ІАД) класифікуються за критерієм їх належності до біоподібних алгоритмів і тому містять два класи: методи обчислювального інтелекту і методи машинного навчання [1, 18-23].

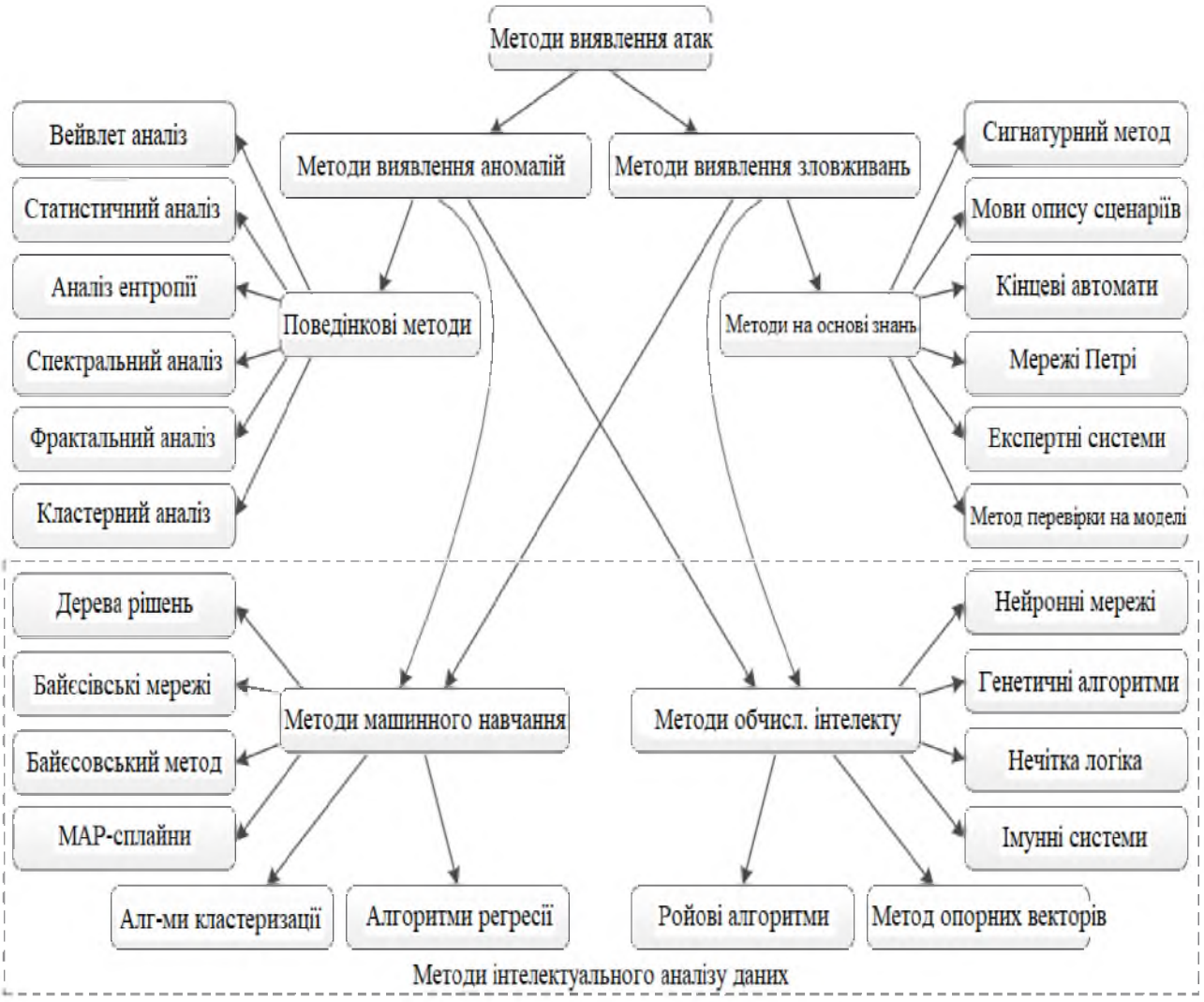

Рисунок 1.3 – Класифікація методів виявлення атак

Поведінковими методами [24] називаються методи, що ґрунтуються на використанні інформації про нормальну поведінку системи та її порівняння з параметрами спостережуваної поведінки. Представлена група методів орієнтована на побудову моделі штатного, або нормального, функціонування системи або користувача. У процесі роботи системи, які використовують даний

підхід, порівнюють поточні показники активності з профілем нормальної діяльності, і випадок значних відхилень може розглядатися як свідчення наявності атаки.

Дані методи характеризуються наявністю хибно-позитивних спрацьовувань, які пояснюються насамперед складністю точного та повного опису безлічі легітимних дій користувачів. Крім того, для більшості подібних систем характерне і необхідне проведення етапу попереднього налаштування, під час якого система «набирається досвіду» для створення моделі нормальної поведінки. Тривалість такого інтервалу для збору даних може тривати кілька тижнів, а іноді й декілька місяців. Зазначені недоліки найчастіше є основними причинами відмови від застосування систем, побудованих на основі поведінкових методів, на користь тих систем, які використовують точне уявлення про порушення безпеки в мережі.

До поведінкових методів віднесено такі методи виявлення атак:

- вейвлет-аналіз;
- статистичний аналіз;
- аналіз ентропії;
- спектральний аналіз;
- фрактальний аналіз;
- кластерний аналіз.

Вейвлет-аналіз полягає у побудові коефіцієнтів, що використовуються у розкладанні вихідного сигналу за базовими функціями. Як сигнал може розглядатися інтенсивність мережевого трафіку або дані про кореляцію IP-адрес призначення. Виконання вейвлет-перетворення дозволяє виділити найбільш вагому інформацію як сигнал, що відповідає коливанням з високою амплітудою, та ігнорувати менш корисну інформацію в коливаннях з низькою амплітудою як шумову складову.

У роботі [25] як початкові дані використовувались агреговані за п'ятихвилинні інтервали середні значення наступних величин: кількість байт на секунду, кількість пакетів на секунду, кількість потоків на секунду, величина

середнього розміру TCP-пакета. У кожному випадку зібрані дані були дискретною послідовністю частотно-часового сигналу, який згідно з запропонованим алгоритмом вейвлет-аналізу був декомпозований у вигляді ієрархії декількох шарів (strata). Для кожного із вилучених сигналів змінна часу була незалежною. Наявність різких амплітуд у кожному представлених сигналів відповідало певним групам аномалій. Так, було виділено такі групи мережевих аномальних подій:

• аномалії, викликані помилками у налаштуваннях мережного обладнання, а також збоєм у роботі обладнання (G1);

• мережеві атаки, представлені класом «відмова в обслуговуванні» (G2);

• перевантаження в мережі (flash crowd), які виникають внаслідок різких сплесків, наприклад, у моменти збільшення легітимних запитів на завантаження нових релізів програмного забезпечення (G3);

• інші аномалії, до яких відносяться обмін великою кількістю даних, помилки під час запису трафіку на сенсорі або надсилання даних колектору NetFlow, що дає можливість аналізу мережевого трафіку на рівні сеансів (G4);

Було виділено три складові компонента первинного сигналу [25]. Низькочастотний компонент сигналу захоплював тривалі мережні аномалії, які можуть тривати від декількох днів. Середньочастотна частина мала нульове математичне очікування і була призначена для аналізу коливань в межах одного дня. Високочастотна частина відповідала невеликим короткостроковим змінам, які можна розглядати як шум.

Після розбиття початкового сигналу було застосовано до першим двом його компонентам процедуру обчислення локальної дисперсії в рамках ковзного вікна розміром 3 години. Далі застосовувався метод граничного аналізу до виваженої суми цих компонентів. Аномалія ідентифікується у разі, якщо пікова точка останнього сигналу перевищила заданий поріг.

У результаті було зроблено висновок у тому, що представлені типи аномальних подій може бути ідентифіковані на конкретних, властивих їм частотах. Так, крупнозернисті аномалії класів G1, G2 і G4 розпізнаються на

високих і середніх частотах, тоді як аномалії класу G3 відповідають низькочастотні та середньочастотні сигнали.

Недоліками вейвлет-аналізу є неоднозначність вибору базисних функцій, велика обчислювальна складність для розрахунку коефіцієнтів розкладання сигналу. Крім того, нетривіальною є завдання правильного завдання розміру вікна. Як було зазначено в [25], якщо розмір ковзного вікна набагато перевищує тривалість аномалії, то відповідний частотний сплеск може бути згладжений, і тим самим атака буде пропущена. В іншому випадку, якщо величина вікна занадто мала, то неминучий потік безглуздих аномалій.

Статистичний аналіз [26] є ядром методів виявлення аномалій у мережі. До цієї групи відносять такі методи:

- ланцюги Маркова;
- метод хі-квадрат (χ^2);
- метод середньоквадратичних відхилень;
- аналіз розподілів інтенсивності передачі/прийому пакетів;
- аналіз часових рядів;
- пороговий аналіз.

Зазначимо, що у статистичних системах важливу роль відіграє правильний вибір контрольованих параметрів, що характеризують відмінності у нормальному та аномальному трафіках. Може вийти так, що через неправильний вибір кількості параметрів, що спостерігаються, модель опису поведінки суб'єктів у системі виявиться неповною або надмірною. Це призводить до пропуску атак або помилкових спрацьовувань у системі.

Перевагами статистичних систем є їх адаптація до зміни поведінки користувача, а також здатність до виявлення модифікацій атаки. Серед недоліків можна відзначити високу ймовірність виникнення хибних повідомлень про атаки та залежність від порядку слідування подій.

Аналіз ентропії використовується у виявленні атак для формування статистичного критерію з метою перевірки належності досліджуваного екземпляра аномальному класу.

Ентропія безлічі X визначається таким чином [27]:

$$H(X) = -\sum_{x \in X} P(x) \cdot \log_2 P(x), \tag{1.1}$$

де P(χ) – ймовірність появи елемента в множині.

Суть методу полягає у побудові моделі, яка б максимізувала значення ентропії. Це відповідає тому припущенню, що зі збільшенням числа унікальних записів відбувається їх рівномірний розподіл щодо вибраних множинних класів, що призводить до збільшення ентропії.

Для виявлення аномалій також може спершу застосовуватися метод максимуму ентропії для створення нормальної моделі, в якій виділені класи мережевих пакетів мають найкращий рівномірний розподіл. Далі застосовується умовна ентропія для виявлення відмінностей між розподілом класів пакетів у поточному трафіку порівняно з розподілом, знайденим у результаті методу максимуму ентропії.

Спектральний аналіз є окремим випадком вейвлет-перетворення та дозволяє виділяти найбільш інформативні складові досліджуваного процесу за допомогою зміни розмірності початкового простору ознак. Для цих цілей аналізується коваріаційна матриця елементів досліджуваного процесу за допомогою методу основних компонентів, гусениці чи сингулярного спектрального аналізу.

Цей підхід ґрунтується на тому припущенні, що отримані компоненти аномального трафіку відрізняються від компонентів звичайного трафіку. Головні компоненти обираються в такий спосіб, щоб вони відповідали найбільшої мінливості початкового процесу. Інші компоненти можуть бути розглянуті як складові шуму.

Фрактальний аналіз заснований на припущенні, що мережевий трафік задовольняє властивості самоподібності [28], ключовими поняттями в якому є параметр Херста H та фрактальна хаусдорфова розмірність D. При чому, для самоподібних процесів виконується співвідношення $0.5<H<1$.

На малих часових відрізках аномальний та нормальний трафіки характеризуються різними значеннями показника Херста [29].

Суть кластерного аналізу полягає у виділенні таких характеристик з мережевого трафіку, які дозволять розбити об'єкти (пакети, з'єднання), що класифікуються, на групи, які відповідають нормальному функціонуванню мережевої взаємодії. Усі інші екземпляри, які потрапляють у побудовані області, класифікуються як аномальні [30].

1.3 Фрактальний аналіз

1.3.1 Фрактальний метод нормованого розмаху Херста (R/S-аналіз)

Стандартна гаусова статистика добре працює при деяких обмежуючих припущеннях [8]. Центральна гранична теорема (закон великих чисел) стверджує, що по мірі проведення дедалі більшої кількості випробувань граничний розподіл випадкової системи буде мати нормальний розподілом. Досліджувані події повинні бути незалежними та ідентично розподілені. Але що робити, якщо для системи не виконуються ці умови? На щастя, існує непараметрична методологія, відкрита ще у 1951 р. Х.Е. Херстом, знаменитим британським гідрологом. Він розробив метод нормованого розмаху (*R*/*S*-аналіз), який використовується для розрізнення випадкового часового ряду і фрактального ряду. Нижче опишемо цю методику на прикладі резервуара річки Ніл.

Протягом кожного проміжку часу t такий резервуар приймає приплив $\xi(t)$ з озера, в той час, як регульований обсяг води (стік) спускається з водосховища. Необхідно знайти потрібну кількість води в резервуарі, щоб щорічно можна було спускати з нього кількість води, яка дорівнює середньому припливу за цей період.

Середній приплив за період в τ років дорівнює:

$$\langle \xi \rangle_r = \frac{1}{\tau} \sum_{t=1}^{\tau} \xi(t). \quad (1.2)$$

Тоді $X(t)$ – накопичене відхилення припливу $\xi(t)$ від його середнього значення є сумою

$$X(t,\tau) = \sum_{u=1}^{t} (\xi(u) - \langle \xi \rangle_r). \quad (1.3)$$

Розмах відхилень буде визначатися як

$$R(\tau) = \max_{1 \le \tau \le \tau} X(t,\tau) - \min_{1 \le t \le \tau} X(t,\tau). \quad (1.4)$$

Стандартне відхилення можна отримати за формулою квадратного кореня з дисперсії

$$S(\tau) = \sqrt{\frac{1}{\tau} \sum (\xi(t) - \langle \xi \rangle_r)^2}. \quad (1.5)$$

Як виявив Херст, для багатьох часових рядів, що спостерігаються, нормований розмах R/S дуже добре описується емпіричним співвідношенням у вигляді степеневого закону:

$$R / S = (a\tau)^H, \quad (1.6)$$

де H – показник Херста. Тут слід зазначити, що розмах іменується нормованим, оскільки він за задумом Херста повинен ділитися на квадратний корінь з дисперсії. Це дозволяє застосовувати метод до самих різних систем. Показник Херста є стійкою мірою деяких статистичних явищ, для яких дисперсія такою не є.

1.3.2 Фрактальна розмірність

Ми схильні думати про всі об'єкти, які мають глибину, як про «тривимірні». З точки зору математики це невірно. Лінія, прокреслена в тривимірному просторі, має глибину, але ця лінія залишається одновимірною. Істинно тривимірний об'єкт – суцільне тіло, яке не має отворів або тріщин на

своїй поверхні. Ось чому уявлення природних форм за допомогою евклідової геометрії є настільки важким. Більшість реальних об'єктів не суцільні в класичному, евклідовому сенсі – вони мають проломи в порожнині. Вони просто розташовуються в тривимірному просторі [8].

Нездатність евклідової геометрії описати більшість природних об'єктів обмежує нашу здатність зрозуміти те, як об'єкт влаштований. Для випадку часових рядів класична геометрія не може надати суттєвої допомоги в розумінні походження їх структури, якщо тільки це не випадкове блукання – система настільки складна, що передбачити її поведінку неможливо. У термінах статистики число ступенів свободи, або факторів впливу на систему дуже велике.

Фрактальна розмірність, яка описує об'єкт (або часовий ряд) заповнює свій простір, є продуктом всіх тих факторів впливу на систему, які й породжують цей об'єкт (або часовий ряд). Часовий ряд буде тільки тоді випадковий, коли він є наслідком великої кількості рівно можливих подій. У термінах статистики – він має велику кількість ступенів свободи. Невипадковий часовий ряд буде відображати невипадкову природу впливів. Скачки даних будуть відповідати стрибкам факторів, що впливають, відображаючи притаманну їм кореляцію. Іншими словами, часовий ряд буде фракталом.

Зазвичай ми поміщуємо об'єкт в простір, більший ніж фрактальна розмірність цього об'єкта. Ми вважаємо, що кулька зім'ятого паперу є тривимірною, хоча вона і не заповнює весь відведений їй тривимірний простір. Це простір, що розглядається як об'єкт, називається розмірністю вкладення, або топологічною розмірністю. Коли об'єкти мають розмірність між двома і трьома, ми схильні думати про них як про тривимірні. Прикладами можуть служити гори і хмари.

Ми думаємо про берегову лінію як про двовимірну, в той час як в дійсності її розмірність менше. Часовий ряд відноситься до тієї ж категорії об'єктів. Тільки випадковий часовий ряд, який би суцільно покрив площину, був би істинно двовимірним.

Одна з характеристик фрактальних об'єктів полягає у тому, що вони залишають собі свою власну розмірність, будучи поміщені в простір розмірності, більше ніж їх фрактальна розмірність. Випадкові розподіли (білий шум) не мають цієї характеристики. Білий шум заповнює свій простір подібно до того, як газ заповнює обсяг. Якщо певну кількість газу помістити в контейнер більшого обсягу, газ просто розтечеться в більшому просторі, оскільки молекули газу ніщо не пов'язує між собою. З іншого боку, тверде тіло має молекули, зчеплені одна з одною. Аналогічно цьому у фрактальному часовому ряді положення точок визначені кореляціями, але таких кореляцій не існує у випадковому ряді. У фракталі, подібному трикутнику Серпінського, кожна точка корельована з точкою, нанесеною до неї. Якщо ми збільшимо розмірність простору вкладення трикутника, то кореляції залишаться незмінними і будуть стягувати точки в групи. Розмірність трикутника залишиться незмінною, так само як залишилася б незмінною розмірність часового ряду.

У випадковому часовому ряді немає кореляцій точок. Ніщо не утримує точки в тому ж сусідстві, зберігаючи їх розмірність. Замість того вони цілком заповнюють відведений їм простір.

Фрактальна розмірність визначається тим, як об'єкт або часовий ряд заповнює простір. Фрактальний об'єкт заповнює простір нерівномірно, оскільки його частини залежні, або корельовані. Щоб визначити фрактальну розмірність, ми повинні визначити, яким чином об'єкт групується в єдине ціле в своєму просторі.

Берегові лінії є хорошим прикладом, особливо якщо провести паралель між ними та часовими рядами. Мандельброт висунув постулат про те, що ми ніколи не зможемо виміряти дійсну довжину берегової лінії, оскільки вимірювана довжина залежить від довжини використовуваної для вимірювання лінійки.

Припустимо, наприклад, що ми хочемо виміряти довжину узбережжя. Ми почнемо з самої північної точки і будемо міряти, накладаючи на поверхню

землі лінійку метрової довжини. Ми будемо складати метрові збільшення, рухаючись вниз по березі, і прийдемо до якогось числа. Потім ми повторимо цю процедуру, використовуючи півметрову лінійку. На цей раз ми зможемо вловити більше деталей, оскільки наша лінійка коротше. Оскільки ми зможемо врахувати більшу кількість бухт і фіордів, ми в результаті отримаємо велику довжину узбережжя. Якщо ми вкоротити лінійку ще в два рази, то отримаємо ще більше деталей і ще більшу довжину. Чим коротше буде ставати лінійка, тим довше берегова лінія. Виходить, що довжина берегової лінії залежить від розмірів лінійки!

З огляду на те, що це справедливо для усіх берегових ліній, довжина як міра не годиться для порівняння берегових ліній. Замість неї Мандельброт запропонував використовувати фрактальну розмірність. Берегові лінії являють собою зазубрені криві, тому їх фрактальна розмірність більше одиниці (тобто їх евклідової розмірності); те, наскільки вона більше одиниці, залежить від ступеня зазубреності. Чим вона більше, тим ближче розмірність берегової лінії до двох – розмірності площини.

Фрактальна розмірність розраховується за допомогою вимірювання цієї властивості зазубреності. Ми підраховуємо кількість кіл певного діаметра, яке необхідно для покриття берегової лінії. Ми збільшуємо їх діаметр і знову рахуємо їх кількість. Продовжуючи цю процедуру, ми знайдемо, що кількість кіл і їх радіус пов'язує показова залежність:

$$N(2r)^D = 1, \tag{1.7}$$

де N – кількість кіл, r – радіус кола, D – фрактальна розмірність.

Рівняння (1.7) може бути приведене до відношенню логарифмів

$$D = \frac{\log N}{\log(r/2)}. \tag{1.8}$$

Фрактальна розмірність показує нам, як форма або часовий ряд заповнюють простір. Спосіб заповнення об'єктом простору визначається тими силами, які визначили його формування. Для берегової лінії такими силами виступає геологічна активність, яка обумовлює її формування: тиск вітру,

вулканічні явища тощо. Зауважимо, що метод кіл для визначення фрактальної розмірності незручний в практичному відношенні.

Безумовною цінністю розмірності Хаусдорфа є можливість її експериментального визначення. Деяка множина може бути виміряна d-вимірними (d – ціле) зразками зі стороною ε_1. Тоді, кількість зразків N_1, які покривають множину буде: $N_1 = A / \varepsilon_1^d$. Значення d має ґрунтуватися на попередніх відомостях про розмірності множини, теоретично, якщо d буде менше топологічної розмірності, то $N_1 \neq 0$, а якщо $d>R^n$, де R^n – евклідів простір, то $N_1 \to 0$.

Зразок з розміром ε_2 дасть оцінку $N_2 = A / \varepsilon_1^d$, тоді розмірністю подібності буде:

$$D = -\log_{\varepsilon_2/\varepsilon_1} \frac{N_2}{N_1}. \qquad (1.9)$$

Наприклад, лінія довжиною A=100 одиниць може бути покрита N=10 відрізками ε_2 довжиною 10 одиниць, або 100 відрізками ε_1 довжиною в 1 одиницю довжини. Тоді, розмірність лінії, згідно (1.9) буде: $D = -\log_{10/1} \frac{10}{100} = 1$.

Прямокутник площею A=64 одиниці, може бути покритий 16-ю майданчиками ε_2^2 площею 4 одиниці (сторона 2) або 64 майданчиками ε_1^2 площею в 1 одиницю (сторона 1). Тоді, розмірність прямокутника буде $D = -\log_{2/1} \frac{16}{64} = 2$.

Слід зазначити, що використання розмірності подібності зручно в разі об'єктів, які мають явну масштабну подобу. Такими об'єктами, перш за все, є само подібні фрак тали – крива Коха, множина Мандельброта, Жюліа та інші. В тих же випадках, коли подобу важко встановити навіть при її наявності, зручно застосовувати наближене обчислення розмірності Хаусдорфа. Тут, як приклади,

можна розглянути стохастичні само афінні фрактали, динамічні відображення – дивні атрактори тощо.

Для наближеного вимірювання розмірності Хаусдорфа, на початковій множині (вибірці) $x(t)$ встановлюється деяка «міра» – наприклад, довжина графіка вибірки. Далі вибірку треба виміряти за допомогою зразка фіксованої довжини δ (рис. 1.4). Вибірка, в даному випадку повинна бути упорядкованою.

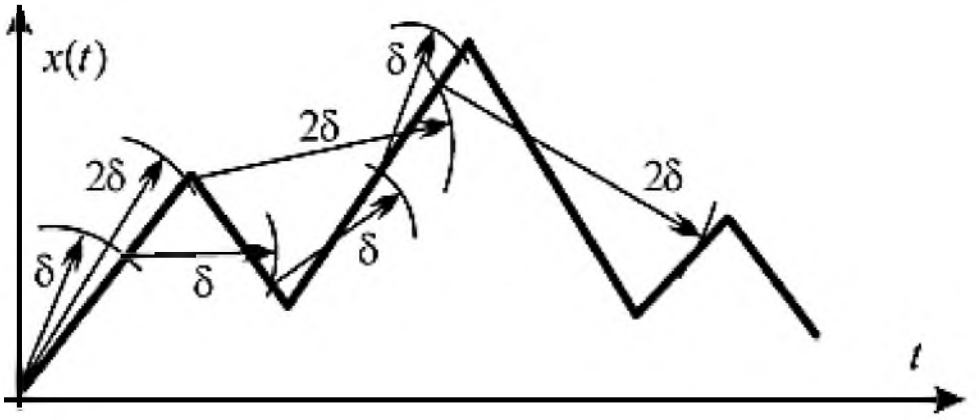

Рисунок 1.4. – Експериментальне вимірювання розмірності Хаусдорфа

Далі потрібно виміряти вибірку зразком довжини в 2δ. У підсумку ми отримаємо дві оцінки довжини A на «масштабі» δ – у вигляді A_1 і на «масштабі» 2δ – у вигляді A_2.

Розмірність кривої на рис. 6.8 обчислюється за формулою:

$$D_{x(t)} = \log_2 \frac{A_1}{A_2}. \qquad (1.10)$$

Якщо довжина вимірюється тільки цілим числом зразків, то розмірність може бути обчислена за формулою (1.9), що є аналогом фізичної подібності у відрізках.

Практична реалізація описаного методу, наштовхується на труднощі, обумовлені великим обсягом обчислень. Пов'язано це з тим, що для обчислення розмірності Хаусдорфа, потрібно вимірювати не просто співвідношення, а верхню границю цього співвідношення.

1.4 Мережеві атаки

Наразі актуальним завданням є захист від мережевих атак, заснованих на використанні протоколів транспортного та мережевого рівнів стека TCP/IP. Існуючі засоби захисту не завжди справляються з новими видами таких атак, тому важливим напрямком досліджень та розробок є створення систем захисту, здатних захищати не від конкретних атак, а від цілих класів атак. Складність процесів виявлення та блокування атак суттєво збільшується внаслідок сучасних тенденцій розвитку інформаційно-телекомунікаційних технологій, у тому числі пов'язаних із зростанням розмірів та продуктивності мереж, ускладненням їхньої топології, зростанням обсягу «швидкого трафіку», обумовленого функціонуванням peer-to-peer додатків, VoIP-трафіком, роботою сканерів безпеки тощо.

Існуючі мережеві атаки можна поділити на чотири основні класи:

• збір інформації, що використовує аналіз результату обробки пакетів;

• атаки, що ґрунтуються на помилках в обробці пакетів;

• сканування хостів та мереж, що базується на використанні помилок в обробці сесій;

• сканування, засноване на коректному встановленні з'єднань.

Взагалі мережеві атаки є вторгненням в операційну систему віддаленого комп'ютера [102]. По суті, це шкідливі дії, які виконані зловмисником та/або дії, виконані шкідливими програмами, встановленими на атакованому комп'ютері. До шкідливих програмам, що беруть участь у мережевих атаках, відносять деякі троянські програми, інструменти DoS-атак, шкідливі скрипти та мережеві хробаки.

Найчастіше мережеві атаки ділять на три основні типи:

• сканування портів;

• DoS-атаки;

• мережеві атаки-вторгнення.

DoS-атаки (Denial of Service) – це атаки, що призводять до паралізації роботи сервера або персонального комп'ютера внаслідок величезної кількості запитів, які з високою швидкістю надходять на ресурс, що атакується. Якщо подібна атака проводиться одночасно відразу з великої кількості комп'ютерів, то в цьому випадку говорять про DDoS-атаку (Distributed Denial of Service), завдяки чому атаці можуть бути піддані сервера навіть з дуже великою пропускною спроможністю інтернет-каналів.

Іноді ефект DDoS-атаки «спрацьовує» випадково. Це відбувається в тому випадку, якщо, наприклад, на сайт, що знаходиться на сервері, було поставлене посилання в популярному інтернет-ресурсі. Це викликає потужний сплеск відвідуваності сайту (сплешдот-ефект), який діє на сервер аналогічно до DDoS-атаки.

Класифікація DoS та DDoS атак [31-33]:

• насичення смуги пропускання – атака, пов'язана з великою кількістю безглуздих запитів до сайту, з метою його відмови через вичерпання системних ресурсів – процесора, пам'яті чи каналів зв'язку.

• HTTP-флуд та PING-флуд – примітивна DoS атака, метою якої є насичення смуги пропускання та відмова сайту в обслуговування; успіх цієї атаки безпосередньо залежить від різниці розмірів ширини каналу сайту, що атакується, і атакуючого сервера.

• SMURF-атака (ICMP-флуд) – одна з найнебезпечніших DDoS атак, коли атакуючий використовує широкомовне розсилання для перевірки функціонуючих вузлів мережі з відправкою ping-запиту.

• FRAGGLE-атака (UDP-флуд) – атака, аналогічна SMURF-атаці, де замість ICMP пакетів використовуються пакети UDP.

• атака пакетами SYN – суть атаки полягає в наступному: два сервери встановлюють TCP з'єднання, на встановлення якого виділяється невелика кількість ресурсів. Надіславши кілька помилкових запитів, можна витратити всі ресурси системи, відведені встановлення з'єднання. Робиться це заміною істинного IP на неіснуючу IP адресу атакуючого сервера при відправленні SYN

пакетів. Сервер – жертва створюватиме чергу з необроблених з'єднань, яка вичерпає його ресурси. Визначити джерело такої атаки дуже складно, оскільки справжні адреси атакуючих серверів замінюються на неіснуючі.

Слід зазначити, що наразі багато сучасних способів виявлення атак у мережі недостатньо надійні, що, у першу чергу, пов'язано з недостовірним визначенням часу початку атаки. Дослідження фрактальних методів аналізу спрямовано на виявлення не властивих для звичайного трафіку структурних особливостей, викликаних аномальними змінами, що, у свою чергу, дозволить потім своєчасно блокувати атаку відомими методами.

1.5 Фрактальна модель та самоподібність телекомунікаційного трафіку

Трафік – це обсяг переданої в одиницю часу інформації, виражений, наприклад, в біт/с. Трафік у мережі зв'язку є процесом надходження та обслуговування заявок користувачів. Процес надходження заявок, найчастіше, є випадковим процесом.

Телекомунікаційний трафік, що є по суті часовим дискретним рядом, має фрактальні властивості [34].

Телекомунікаційний трафік, має фрактальну природу, тому що його кореляційна розмірність не є цілим числом. Для оцінки фрактальності того чи іншого фізичного процесу може бути використаний показник Херста, що дозволяє визначити рівень детермінованого хаосу в досліджуваній системі. Однак використання єдиного фрактального параметра для опису телекомунікаційного трафіку за наявності мережевих атак є недостатнім і не завжди повністю інформативним.

Фрактальний аналіз трафіку дозволяє виявляти не властиві для звичайного трафіку властивості для своєчасного блокування мережевої атаки.

Як відомо, фрактали мають властивості самоподібності, тобто властивості точного або ймовірнісного повторення властивостей об'єкта при розгляді його в різних масштабах простору або часу. Це призводить до закономірностей у

статистичній поведінці трафіку. З викладеного також випливає, що необхідно застосування ймовірнісного підходу до складних стохастичних процесів. Під стохастичним процесом розуміється процес, у якому є елемент випадковості.

Самоподібним називається трафік, часові реалізації якого є фракталами. Варто зазначити, що зазвичай немає одного причинного фактору, що викликає самоподібність мережевого трафіку.

З робіт [35-36] відомо, що трафік телекомунікаційних систем необхідно описувати моделями, що враховують властивості його самоподібності.

Ця проблема розглядається у значній кількості робіт, наприклад, [36-39]. Результати цих досліджень дають змогу розрахувати деякі параметри телекомунікаційного трафіку. Однак недоліком багатьох моделей є значні часові витрати на збирання та обробку інформації, що призводить до неможливості аналізу телекомунікаційного трафіку в режимі реального часу. У зв'язку з вище сказаним є актуальним розробка швидкої методики визначення параметрів трафіку з урахуванням його самоподібності.

Згідно з дослідженнями [39], фрактальність трафіку характеризується показником Херста, значення якого може бути використане для виявлення аномальних змін трафіку, у тому числі для виявлення вторгнень та атак на ІС. Відповідно до [39-40], зменшення значення параметра Херста свідчить про проведення атаки DDoS на інформаційну мережу.

Наразі існують різноманітні статистичні методи аналізу самоподібних випадкових процесів. Найбільш популярний так званий R/S-аналіз (обчислення показника Херста), який дозволяє використовувати як початкові дані різні за тривалістю інтервали вибірки. Різна кількість відліків часто призводить до приблизних оцінок ступеня самоподібності телекомунікаційного трафіку. Для більш точного аналізу використовується, наприклад, методика Віттла [41], що дозволяє визначити довірчий інтервал подальшого застосування R/S-аналізу. Також зауважимо, що відмінності у довжині довірчих інтервалів також мають невеликий вплив на значення обчислюваного показника Херста.

У зв'язку з тим, що самоподібність передбачає значний вплив на мережеві характеристики, важливою проблемою для аналізу мережного трафіку стає розуміння причин та впливів самоподібності трафіку.

Трафік телекомунікаційної компанії, по суті, складається з трафіку локальної мережі (LAN) компанії та трафіку глобальної мережі (WAN). Щоб довести самоподібність трафіку телекомунікаційної компанії, розглянемо його окремо. Самоподібність трафіку LAN веде до структурованих моделей, які, у свою чергу, зводяться до ON/OFF-джерел або так званих пакетних серій. Суперпозиція ON/OFF-процесів виявляє локальний зв'язок між параметрами самоподібності та «важко-хвостовими» розподілами [34]. Мережі WAN служать задля забезпечення взаємодії між просторово-географічно рознесеними користувачами. Самоподібність WAN-трафіку було доведено у роботі [42], у якій шляхом аналізу різних трас WAN трафіку демонструється неадекватність традиційних моделей пуасонівського трафіку із застосуванням опису ключових моментів поведінки цього виду трафіку. У пізніших роботах автори роблять спроби отримання структурних моделей для WAN-трафіку, далі теж саме застосовується для приведення до ON/OFF-моделей для окремих пар джерело-одержувач, WAN трафік описується на рівні окремих додатків.

Відповідно до [43], виникнення самоподібного трафіку може бути викликане високорівневістю комплексної системи, в якій розміри файлів, що передаються через мережу, мають розподіли з «важкими хвостами». Також до самоподібності трафіку призводить ситуація, коли у мережевому оточенні утворюються численні накладення подібних пересилок типу клієнт/сервер, що, у свою чергу, пов'язано зі зміною мережевих ресурсів і топології мережі.

Самоподібність мережевого трафіку LAN та WAN пов'язана з мережевою динамікою на різних рівнях ієрархічної семирівневої моделі.

Наразі немає жодного причинного фактора, що визначає самоподібність мережевого трафіку.

Насправді перевірка на самоподібність і оцінка показника Херста є складними завданнями. Це пов'язано насамперед з тим, що в реальних умовах

завжди відбувається робота з кінцевими наборами даних, тому неможливо перевірити, чи маршрут трафіку є самоподібним. Наслідком цього є потреба у дослідженні різних властивостей самоподібності в реальному виміряному трафіку, не маючи інформації про всі масштаби. Як правило, при аналізі мережевого трафіку (навіть якщо підтвердилися деякі властивості самоподібності) відразу не вдається зробити висновок, що проаналізовані дані мають самоподібну структуру, оскільки існують інші впливи, які можуть призвести до таких властивостей, наприклад, присутність нестаціонарності. У такому разі говорять про самоподібну структуру в заданому масштабному діапазоні заданого набору даних.

1.6 Висновок. Постановка задачі

Вибір СВА повинен ґрунтуватись на вимогах, що висуваються до системи захисту інформації в кожному конкретному випадку. Проведене дослідження та порівняльний аналіз сучасних систем виявлення атак та запобігання вторгненням показав, що при вдосконаленні існуючих та проектуванні нових систем необхідно враховувати визначені властивості, зважаючи на особливості реалізації та функціонування інформаційної системи, які підлягають захисту.

Наразі актуальним завданням є захист від мережевих атак, заснованих на використанні протоколів транспортного та мережевого рівнів стека TCP/IP. Існуючі засоби захисту не завжди справляються з новими видами таких атак, тому важливим напрямком досліджень та розробок є створення систем захисту, здатних захищати не від конкретних атак, а від цілих класів атак. Складність процесів виявлення та блокування атак суттєво збільшується внаслідок сучасних тенденцій розвитку інформаційно-телекомунікаційних технологій, у тому числі пов'язаних із зростанням розмірів та продуктивності мереж, ускладненням їхньої топології, зростанням обсягу «швидкого трафіку», обумовленого функціонуванням peer-to-peer додатків, VoIP-трафіком, роботою сканерів безпеки тощо.

Встановлено, що багато з сучасних способів виявлення атак у мережі недостатньо надійні, що, у першу чергу, пов'язано з недостовірним визначенням часу початку атаки. Дослідження фрактальних методів аналізу спрямовано на виявлення не властивих для звичайного трафіку структурних особливостей, викликаних аномальними змінами, що, у свою чергу, дозволить потім своєчасно блокувати атаку відомими методами.

Телекомунікаційний трафік, що є по суті часовим дискретним рядом, має фрактальні властивості. Телекомунікаційний трафік, має фрактальну природу, тому що його кореляційна розмірність не є цілим числом. Для оцінки фрактальності того чи іншого фізичного процесу може бути використаний показник Херста, що дозволяє визначити рівень детермінованого хаосу в досліджуваній системі. Однак використання єдиного фрактального параметра для опису телекомунікаційного трафіку за наявності мережевих атак є недостатнім і не завжди повністю інформативним.

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

Таким чином, для виконання мети кваліфікаційної роботи необхідно:

• запропонувати підхід до визначення аномалій телекомунікаційного трафіку, що базується на розрахунку фрактальних параметрів та визначення фазового портрета;

• оцінити ефективність розробленого підходу.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Підхід до виявлення мережевих атак за допомогою фрактального аналізу

Виявлення мережевих атак за допомогою спеціалізованого програмного забезпечення, як правило, полягає в моніторингу мережевого трафіку між клієнтською системою, на яку здійснюватиметься атака та системою зловмисника (атакуюча система), а також аналізі підозрілого трафіку мережі, з подальшою оцінкою атаки, ризиків її здійснення, збитків та механізмів протидії атакуючій системі. Найчастіше підозрілий трафік виявляється автоматично, і не вимагає постійного спостереження за трафіком з боку експерта, що у свою чергу виключає людський фактор помилковості розпізнавання атаки на ресурси системи. До переважних методів розпізнавання мережевих атак відносять сигнатурний аналіз. Величина ризику мережевої атаки не можлива без експертної думки, на основі цієї величини має бути прийняте рішення про заходи та способи реагування на мережеву атаку. У випадках з мінімальними ризиками, атака може взагалі не заслуговувати на увагу. У протилежних випадках може вимагати швидку реакцію на події.

Залежно від ступеня критичності атаки існують різні рівні реагування на них. Слід зазначити, що за рівнем критичності атаки зазвичай визначається ступінь реакції на неї. У загальному випадку, критичність атаки пов'язана з величиною ризику та можливої шкоди від даної атаки [44].

Для вирішення задачі захисту від мережевих атак необхідна концепція, що визначає об'єкти захисту, цілі, завдання та основні принципи захисту, а також склад та послідовність робіт із попередження, виявлення та реагування на атаки.

У зв'язку з вищесказаним пропонується наступний алгоритм реагування на мережеву атаку.

Етап 1. За допомогою відомих програм для запису трафіку у режимі онлайн проводиться протоколювання телекомунікаційного трафіку (навантаження мережі) залежно від часу. По суті, початкові дані є дискретним цифровим рядом, зручним для подальшого аналізу.

Етап 2. З використанням методів фрактального аналізу за цими значеннями обчислюються показник Херста та спектр потужності. За зниженням значення показника Херста до рівня 0.5-0.55 можна судити про те, що трафік переходить в аномальний стан. Однак судити про те, що в цей момент починається мережева атака, тільки по зниженню цього показника недоцільно. Як показано, наприклад, [39], невелике зниження показника Херста може відбуватися і у разі постійно збільшеного навантаження мережі протягом деякого інтервалу часу.

Етап 3. Виконується побудова фазового портрету, на вигляд якого, можна з великою впевненістю говорити про початок мережевої атаки. Причому самі фазові портрети можуть автоматично оброблятися з використанням програмного забезпечення для обробки зображень.

Відразу зазначимо, що запропонований алгоритм визначення мережевої атаки не дозволяє блокувати мережеву атаку, оскільки не визначає IP-адреси атакуючих мережних вузлів, тому після індикації атаки має бути запущене програмне забезпечення для блокування атакуючих хостів. Для цієї мети можуть бути використані спеціалізовані програмні засоби (iptables, ipwf та ін.).

Отже, запропоновано фрактальний індикатор мережевих атак, що базується на розпізнаванні фазового портрета дискретного телекомунікаційного трафіку.

2.2 Застосування фрактальних заходів до телекомунікаційного трафіку

Побудова достатньої фрактальної моделі телекомунікаційного трафіку дозволяє надалі здійснювати визначення ступеня загрози за величиною параметрів, що характеризують самоподібність. Зокрема, важливо правильно

визначати часовий лаг, на якому система зберігає властивості фрактальності та самоподібності.

Фрактальна модель трафіку є сукупністю різних фрактальних параметрів (розмірностей), поставлених у відповідність деякому (поточному) стану мережевого трафіку. Динаміка зміни фрактальних розмірностей під час проведення низки вимірів стану однієї й тієї ж телекомунікаційного вузла дозволяє будувати висновки про динаміку стану телекомунікаційного трафіку, тобто. про наявність чи відсутність мережевих атак на ресурси ІС телекомунікаційної компанії у цьому місці

2.2.1 Обчислення показника Херста

Однією з основних методик, що використовуються для опису детермінованого хаосу, є розрахунок нормованого розмаху Херста (R/S аналіз). Як основний параметр обчислюється показник Херста, що визначає ступінь хаотичності як усієї системи, так і телекомунікаційного трафіку. За його значенням можна судити про фрактальну природу об'єкта, що досліджується.

Приклади профілів співвідношень LAN-трафіку та WAN-трафіку в одиницю часу наведені на рис. 2.1

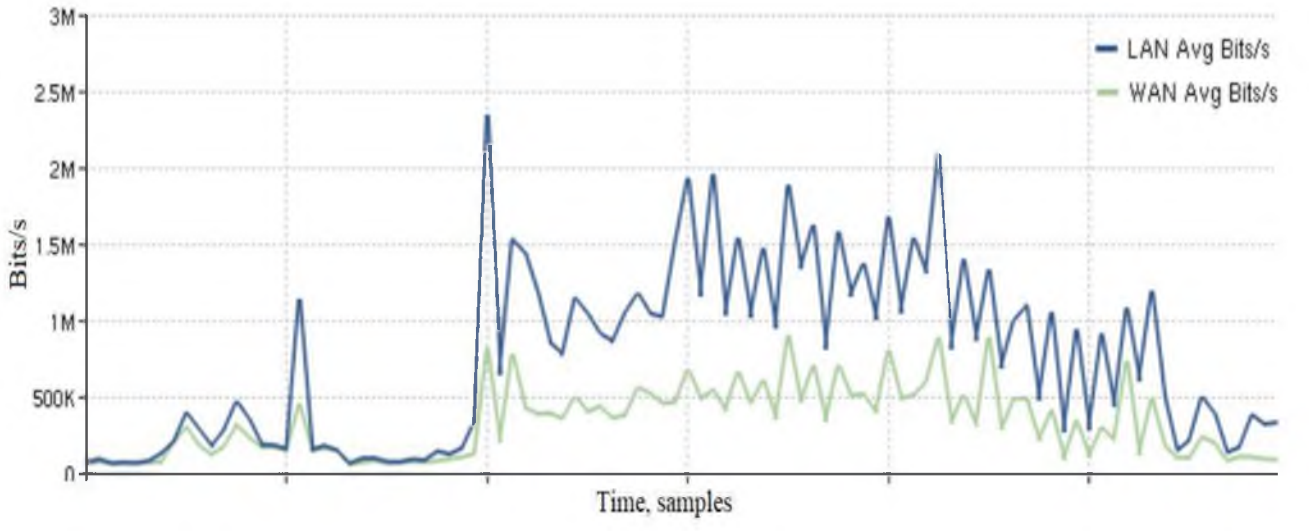

Рисунок 2.1 – Приклади LAN та WAN-трафіків

Графік, показані рис. 2.1 відображає завантаження мережі в байтах за одиницю часу і може бути використаний для виявлення самоподібності. Слід зазначити, що з практичної точки зору найбільш корисною є інформація про рівень завантаженості мережі, якщо ж взяти до розгляду графік, що відображає інформацію про кількість пакетів в одиницю часу (даний графік теж характеризує трафік мережі), його графічне представлення може ввести нас в оману щодо виявлення самоподібності трафіку. Це пов'язано з тим, що в мережі можуть бути численні не об'ємні керуючі пакети, які не несуть у собі корисну інформацію, а також пакети мінімальної довжини, які створюють піки, що не збігаються з піками байтової швидкості. З рис. 2.1 ж можна дійти невтішного висновку, що зображений на ньому процес є пульсуючим у широких межах часового масштабу, що дозволяє говорити про його фрактальну структуру, і як наслідок самоподібність.

Моделювання розв'язання задачі фрактального аналізу трафіку в інформаційно-комунікаційних мережах для СВА згідно запропонованого алгоритму виконувалося за допомогою програми Fractan 4.4 [45]. на основі експериментальних даних – трафіку, що передається через мережу Інтернет [46]. Дані являють собою залежність розміру Ethernet кадрів в байтах від часу. Для їх приведення до еквідистантної шкали за часовою віссю було проведено процедуру агрегації з кроком 5 с.

На рис. 2.2 представлений приклад завантаження мережі, отриманий у результаті запису телекомунікаційного трафіку мережі оператора у момент відсутності мережевої атаки на деякий хост.

Приклад розрахунку нормованого розмаху R/S для трафіку з рис. 2.2, показаний на рис. 2.3. Показник *H* найпростіше знайти як кут нахилу прямої, отриманої шляхом апроксимації (за методом найменших квадратів) відношення R/S (у цьому випадку слід по обох осях системи координат використовувати логарифмічну шкалу).

При цьому по обидва осі використовувались десяткові логарифми, а параметр $\alpha=1$.

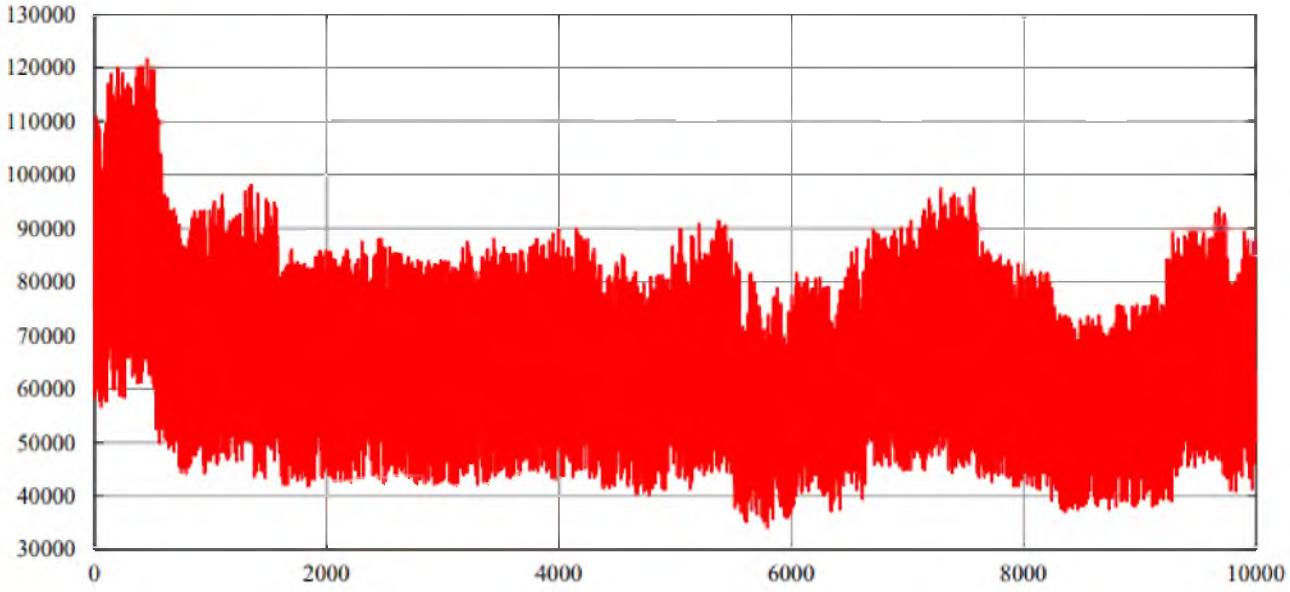

Рисунок 2.2 – Досліджуваний телекомунікаційний трафік

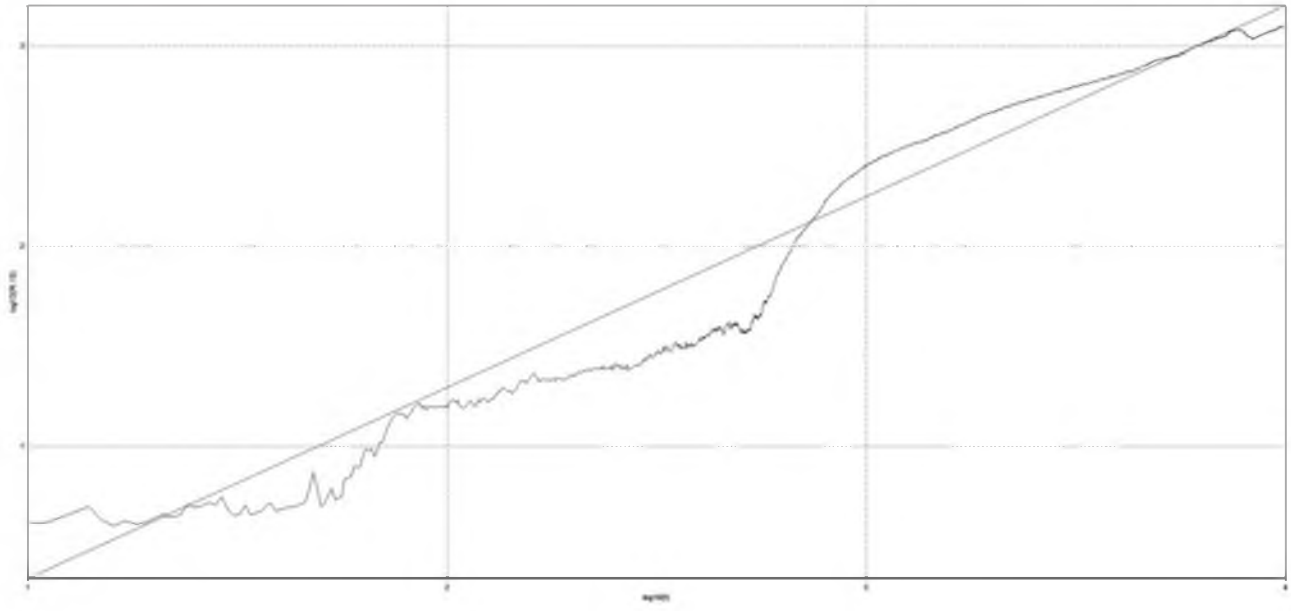

Рисунок 2.3 – Графік залежності R/S-параметра телекомунікаційного трафіку від запізнення N у подвійному логарифмічному масштабі

На рис. 2.3 показано R/S від запізнення N у подвійному логарифмічному масштабі, а також апроксимуюча пряма. Показник Херста для досліджуваного трафіку виявився рівним H=0.94, що говорить про його фрактальну природу.

R/S-метод не надто точний, оскільки він дає лише оцінку рівня самоподібності в часовому ряді. Тому даний метод використовується тільки для

перевірки, чи є часовий ряд самоподібним і, якщо є, отримати деяку оцінку показника Херста H.

Відповідно до теорії фракталів, якщо отримане значення показника Херста H>0.5, це характеризує персистентну поведінку процесу, тобто система має тривалу пам'ять. Тобто, якщо протягом деякого часу в минулому спостерігалися позитивні збільшення мережевого трафіку і відбувалось збільшення, то й надалі у середньому відбуватиметься збільшення. У разі H<0.5 говорять про антиперсистентність процесу. Тут високі значення мережевого трафіку слідують за низькими, і навпаки. При H=0.5 відхилення мережевого трафіку від середнього є справді випадковими і не залежать від попередніх значень.

Однак, як буде показано надалі, у разі мережевих атак рівень самоподібності знижуватиметься. Тому показник Херста можна вважати первинним індикатором стану мережі.

2.2.2 Відновлення фазового простору

Для телекомунікаційного трафіку стан вузла однозначно визначається одновимірною послідовністю часових відліків. Тому інтерес представляє реконструкція фазового простору по одновимірному часовому ряду [47].

Відомо, що система через деякий час повертається у стан, близький до початкового, за деяким циклом (теорема Пуанкаре). Наявність циклічності повернення системі дозволяє зрушити послідовність щодо себе на «половину періоду». «Період» буде значення середнього часу повернення τ.

Відповідно до робіт Такенса [47], можна обчислити так званий кореляційний інтеграл та кореляційну розмірність за знятими значеннями одновимірної часової послідовності.

Для цього потрібно побудувати простір вкладення з m-вимірним вектором за значеннями досліджуваного трафіку $x(i)$:

$$\vec{\mathbf{x}}(i)=\left\{x\left(i-(m-1)\tau\right),x\left(i-(m-2)\tau\right),...,x(i)\right\},\ \left(i=\overline{1,N-(m-1)\tau}\right), \quad (2.1)$$

де τ – часовий зсув; m – розмірність простору вкладень.

Багатовимірні вектори, побудовані за схемою (2.1), утворюють реконструйований фазовий простір розмірності m(R^m).

У побудованому у такий спосіб фазовому просторі розраховується кореляційна розмірність D_C. Фазовий простір, побудований за схемою (2.1), згідно з Такенсом матиме розмірність початкового фазового простору:

$$N \geq \text{int}[D_c] + 1. \tag{2.2}$$

Після реконструкції простору вкладень з'являється можливість визначення розмірності фазового простору m.

2.2.3 Метод хибних найближчих сусідів

Після відновлення фазового простору системи необхідно визначити наскільки подібними є початковий та відновлений атрактори. Найчастіше при цьому використовується метод хибних найближчих сусідів.

Відомо, що фазові траєкторії початкового атрактора не мають самоперетинів, то і у відновленому атракторі траєкторії також не повинні мати перетинів. Умовою того, що перетини будуть відсутні, є те, що точки-сусіди фазового атрактора, сконструйованого в R^m, також є сусідами в (m+1)-просторі. Метод хибних найближчих сусідів служить для визначення найменшої величини розмірності m. При цьому значенні число хибних сусідів у просторах R^m і R^{m+1} буде дуже мало відрізнятися. У результаті знайдене m відповідає найменшій розмірності простору, у якому можливе відновлення фазового простору без самоперетинів.

Розглянемо дискретний телекомунікаційний трафік як набір дискретних часових відліків A(n).

На першому етапі по початковому часовому ряду визначаються:

1. Мінімальне значення min{A(n)}.

2. Інтервал між максимальним та мінімальним значеннями I=maxA(n)}-min{A(n)}.

3. Проводиться нормування:

$$x(n)=\frac{A(n)-\min\{A(n)\}}{\max\{A(n)\}-\min\{A(n)\}}. \tag{2.3}$$

Далі проводиться відновлення фазового простору за допомогою методу затримки. Одномірні вектори у відновленому просторі утворюються із значень вихідного часового ряду з тимчасовим запізненням:

$$\vec{\mathbf{x}}(i)=\{x(i-(m-1)\tau),x(i-(m-2)\tau),...,x(i)\},\ \left(i=\overline{1,N-(m-1)\tau}\right), \tag{2.4}$$

де τ – так званий часовий лаг (зсув за часовими відліками), m – розмірність відновленого фазового простору.

В результаті проводиться перетворення одновимірного ряду нормованого x в багатовимірний вектор $\vec{x}$:

$$x\Rightarrow\begin{pmatrix} x(1-(m-1)\tau),x(1-(m-2)\tau),x(1-(m-3)\tau),...,x(N) \\ x(2-(m-1)\tau),x(2-(m-2)\tau),x(2-(m-3)\tau),...,x(N) \\ ... \\ x(N-2(m-1)\tau),x(N-(m-1)\tau-(m-2)\tau),...,x(N) \end{pmatrix}. \tag{2.5}$$

Якщо вихідний дискретний ряд, що описує завантаження каналу, містить N значень, число векторів визначається як N-(m+1)τ.

Практична реалізація методу хибних найближчих сусідів полягає у послідовній побудові багатовимірних векторів зі збільшеною на 1 розмірністю та оцінка виконання «близькості» розташування фазових траєкторій у початковому та відновленому атракторі.

1. На першому етапі розмірність відновлювального фазового простору m=1.

2. Побудуємо багатовимірний вектор такого виду:

$$\vec{\mathbf{x}}_{m=1}=\begin{pmatrix} \vec{\mathbf{x}}_{m=1}(1) \\ \vec{\mathbf{x}}_{m=1}(2) \\ ... \\ \vec{\mathbf{x}}_{m=1}(N) \end{pmatrix}=\begin{pmatrix} x(1),x(1+\tau),x(1+2\tau)...,x(N) \\ x(2),x(2+\tau),x(2+2\tau),...,x(N) \\ ... \\ x(N),x(N+\tau),x(N+2\tau),...,x(N) \end{pmatrix}. \tag{2.6}$$

3. Далі будуємо багатовимірний вектор у просторі вкладень з розмірністю m=2

$$\vec{\mathbf{x}}_{m=2} = \begin{pmatrix} \vec{\mathbf{x}}_{m=2}(1) \\ \vec{\mathbf{x}}_{m=2}(2) \\ \dots \\ \vec{\mathbf{x}}_{m=2}(N) \end{pmatrix} = \begin{pmatrix} x(1-\tau), x(1), x(1+\tau) \dots, x(N) \\ x(2-\tau), x(2), x(2+\tau), \dots, x(N) \\ \dots \\ x(N-2\tau), x(N-\tau), x(N+\tau), \dots, x(N) \end{pmatrix}. \quad (2.7)$$

Далі при $i = \overline{1,N};\ j = \overline{1,N}$ визначаємо довжини (норми) векторів:

$$\left\| \vec{\mathbf{x}}_{m=1}(i) - \vec{\mathbf{x}}_{m=1}(j) \right\| =$$
$$= \sqrt{\left(\vec{x}_{m=1}(i)_1 - \vec{x}_{m=1}(j)_1\right)^2 + \left(\vec{x}_{m=1}(i)_2 - \vec{x}_{m=1}(j)_2\right)^2 + \dots + \left(\vec{x}_{m=1}(i)_N - \vec{x}_{m=1}(j)_N\right)^2};$$
$$\left\| \vec{\mathbf{x}}_{m=2}(i) - \vec{\mathbf{x}}_{m=2}(j) \right\| =$$
$$= \sqrt{\left(\vec{x}_{m=2}(i)_1 - \vec{x}_{m=2}(j)_1\right)^2 + \left(\vec{x}_{m=2}(i)_2 - \vec{x}_{m=2}(j)_2\right)^2 + \dots + \left(\vec{x}_{m=2}(i)_N - \vec{x}_{m=2}(j)_N\right)^2}. \quad (2.8)$$

5. Потім обчислюється відношення норм векторів у просторах з різною розмірністю:

$$R_{i(12)} = \frac{\left\| \vec{\mathbf{x}}_{m=2}(i) - \vec{\mathbf{x}}_{m=2}(j) \right\|}{\left\| \vec{\mathbf{x}}_{m=1}(i) - \vec{\mathbf{x}}_{m=1}(j) \right\|}. \quad (2.9)$$

У випадку, коли $R_{i(12)} > R_t$, де R_t – поріг «близькості» фазових траєкторій, точка з вектором $\vec{\mathbf{x}}(j)$ є хибним найближчим сусідом по відношенню до точки з вектором $\vec{\mathbf{x}}(i)$. В результаті проводиться підрахунок кількості хибних найближчих сусідів P_{12} для кожної точки з вектором $\vec{\mathbf{x}}(i)$.

6. Обчислюється значення відношення P_{12}/N.

7. Будуємо багатовимірний вектор у просторі вкладень з розмірністю m=3:

$$R_{i(23)} = \frac{\left\| \vec{\mathbf{x}}_{m=3}(i) - \vec{\mathbf{x}}_{m=3}(j) \right\|}{\left\| \vec{\mathbf{x}}_{m=2}(i) - \vec{\mathbf{x}}_{m=2}(j) \right\|}. \quad (2.10)$$

8. Обчислюється співвідношення P_{23}/N.

9. Далі п. 2-8 повторюються для $m = \overline{4,\dots m_d}$ (m_d – максимальне значення простору вкладень).

Таким чином, в результаті обчислень визначається залежність відношення P/N від розмірності відновленого фазового простору m.

Для телекомунікаційного трафіку при нормальному функціонуванні сегмента мережі, показаного рис. 2.2, розмірність фазового простору дорівнює 13.

Таким чином, другим, після показника Херста, параметром, який буде використаний для оцінки стану мережі є розмірність відновленого фазового простору.

На рис. 2.4 наведено результат розрахунку фазового простору (траєкторій у фазовому просторі) для телекомунікаційного трафіку при нормальному функціонування сегмента мережі (див. рис. 2.2). Як видно з рис. 2.4, основний атрактор системи займає досить велику площу і зміщений в область початку системи координат.

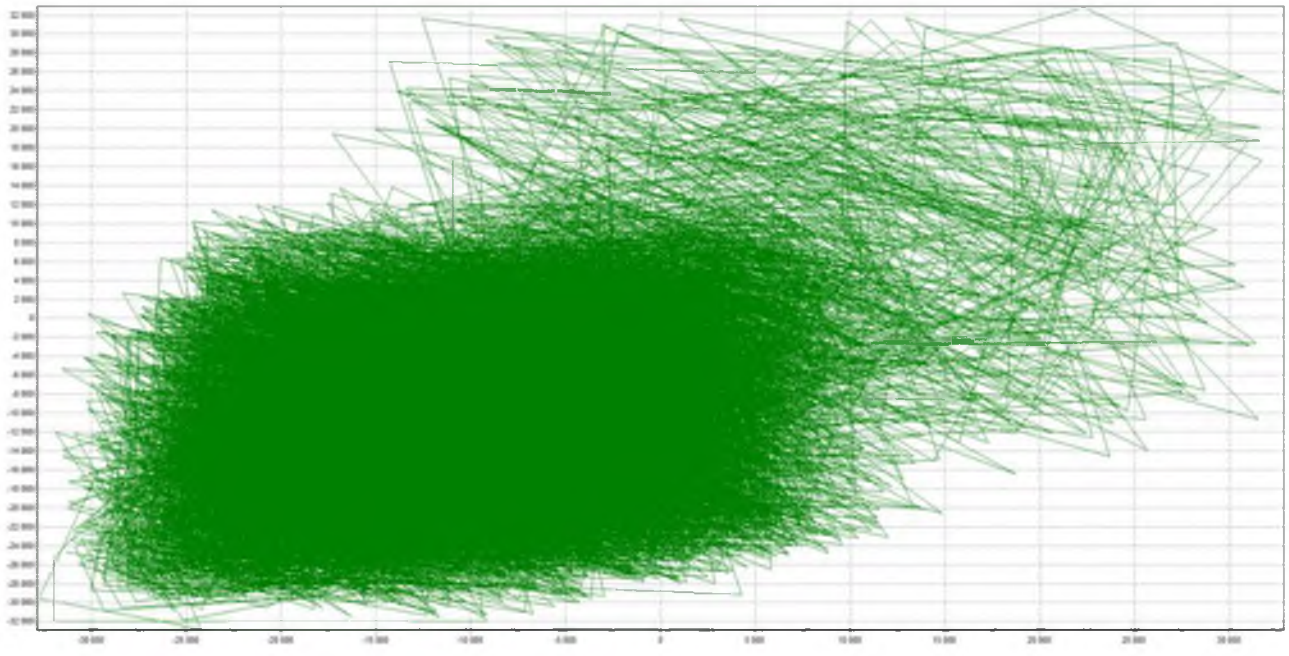

Рисунок 2.4 – Фазовий портрет телекомунікаційного трафіку в нормальному стані

2.2.4 Обчислення кореляційного інтеграла та кореляційної розмірності

За допомогою розглянутого методу затримок сконструюємо з досліджуваного одновимірного ряду такі багатовимірні вектори:

$$\vec{\mathbf{x}}(i)=\{x(i-(m-1)\tau),x(i-(m-2)\tau),...,x(i)\},\ \left(i=\overline{1,N-(m-1)\tau}\right), \tag{2.11}$$

де τ – часовий лаг, m – розмірність відновленого фазового простору, визначена у попередньому розділі.

Кореляційний інтеграл обчислюється наступним чином:

$$C(\varepsilon,N)\big|_m=\lim_{N\to\infty}\frac{1}{N(N-1)}\sum_i^N\sum_j^N\theta\left(\varepsilon-\left|\vec{x}_m(i)-\vec{x}_m(j)\right|\right),\ \left(i\neq j;\ m=\overline{1,m_d}\right), \tag{2.12}$$

де N – кількість відліків у тимчасовому ряді; $\left|\vec{\mathbf{x}}_m(i)-\vec{\mathbf{x}}_m(j)\right|$ – відстань за нормою між i-ю та j-ю точками фазової траєкторії в m-вимірному просторі R^m; ε – точність розрахунку; θ(x) – θ-функція Хевісайду, яка визначається наступним чином:

$$\theta(x)=\begin{cases}0, & x<0;\\ 1, & x\geq 0.\end{cases} \tag{2.13}$$

Кореляційний інтеграл C(ε, N) представляє функцію, яка залежить від кількості точок атрактора у просторі R^m, відстань між якими менша наперед заданої точності ε.

У формулі (2.12) норма відстані між i-ю та j-ю точками обчислюється як

$$\left|\vec{\mathbf{x}}_m(i)-\vec{\mathbf{x}}_m(j)\right|=\sqrt{\left(\vec{x}_m(i)_1-\vec{x}_m(j)_1\right)^2+...+\left(\vec{x}_m(i)_N-\vec{x}_m(j)_N\right)^2}. \tag{2.14}$$

Далі для всіх отриманих при різних m кореляційних інтегралів обчислюється похідна D_C, що є кореляційною розмірністю:

$$D_C=\lim_{\varepsilon\to 0}\lim_{N\to\infty}\left[\frac{d\lg C(\varepsilon,N)}{d\lg\varepsilon}\right]. \tag{2.15}$$

Зазвичай цю похідну не обчислюють, а кореляційна розмірність D_C визначається як тангенс нахилу дотичної графіка залежності D_C від розмірності простору вкладень до вісі абсцис.

На рис. 3.5 наведено залежність кореляційної розмірності D_C від розмірності простору вкладень, а також наведено дотичну до графіку даної функції.

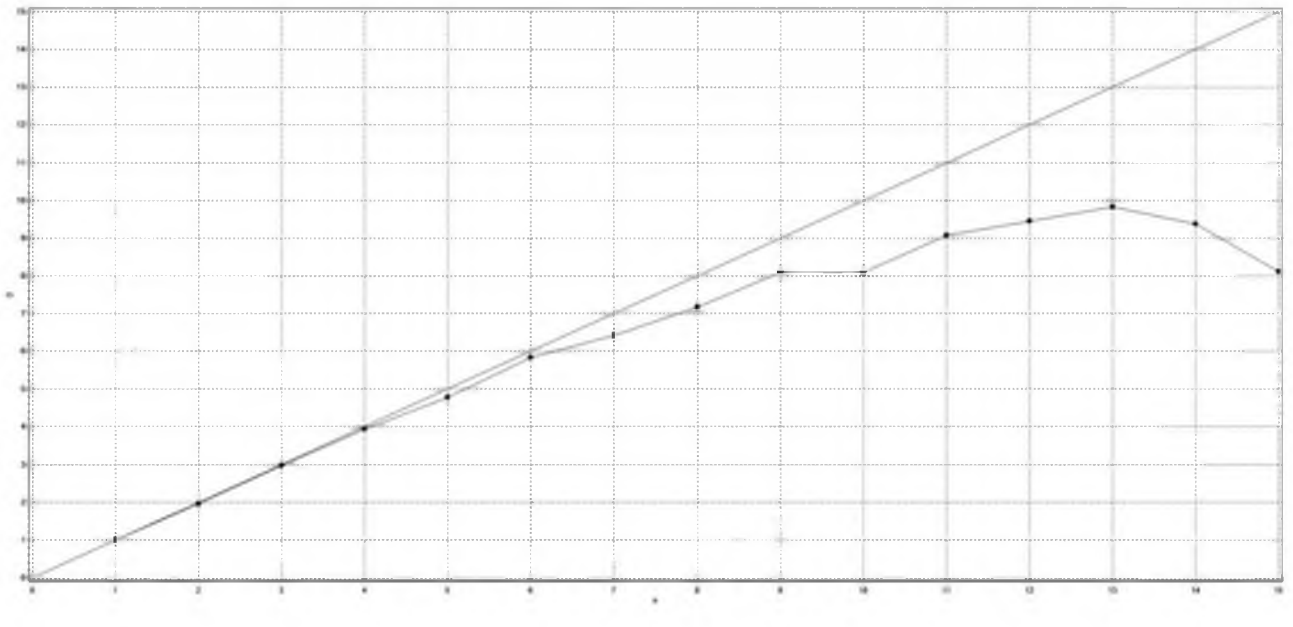

Рисунок 2.5 – Залежність кореляційної розмірності D_C від розмірності відновленого фазового простору

За графіком залежності (рис. 2.5) $D_C(m)$ визначається максимум кореляційної функції. Значення $m=m_c$, при якому функція має максимум, буде відповідати розмірності простору вкладення m_d, а значення D_C відповідатиме кореляційній розмірності.

Таким чином, з рис. 2.5 нескладно визначити, що розмірність відновленого фазового простору в нормальному стані мережі 13, що доводить результат, раніше отриманий методом найближчих помилкових сусідів. Також можна помітити, що значення кореляційної розмірності дорівнює в даному випадку 9,819.

Таким чином, для оцінки стану сегмента мережі пропонується використовувати наступний набір фрактальних параметрів:

1) показник Херста (первинний індикатор для оцінки самоподібності);

2) кореляційна розмірність;

3) розмірність фазового простору;

4) тип фазового простору.

Далі буде показано, що показник Херста у разі нормального стану телекомунікаційного трафіку більший за 0,8; кореляційної розмірності – більше 9: розмірність фазового простору – більше 13.

Таким чином, в основі фрактального індикатора стану мережі пропонується використовувати набір трьох фрактальних заходів (показник Херста, кореляційна розмірність, розмірність фазового простору), а також вид фазового портрета телекомунікаційного трафіку.

2.3 Оцінка ефективності підходу до виявлення мережевих атак за допомогою фрактального аналізу

Під час проведення моделювання важливо розглянути різні ситуації під час захоплення трафіку:

1. Протягом усього часу захоплення трафіку DDoS-атака не відбувалася (нормальний режим).

2. Протягом частини часового інтервалу мережевої атаки не було, а в іншій частині часового інтервалу відбувалася DDoS-атака.

3. Протягом усього часу захоплення трафіку відбувалася DDoS-атака.

Для аналізу використовувалися часові ряди з числом вибірок не менше 20000 значень. Це дозволяє проводити розрахунок фрактальних заходів та побудову фазового портрета системи протягом 2-3 хвилин. Також зазначимо, що для чистоти експерименту в нормальному режимі було розглянуто трафіки, захоплені в нічний, ранковий, денний та вечірній час. Це зроблено для того, щоб показати, що завантаженість каналу не призводить до аномальних змін значень фрактальних параметрів у нормальному режимі. Крім того, важливим є розгляд ситуації, коли у захопленому трафіку лише частина дискретного ряду відповідає часу проведення мережевої атаки. Як показано нижче, у разі за значеннями фрактальних заходів без аналізу фазового простору неможливо визначити наявність мережевої атаки. В результаті буде доведено, що розрахунку значень фрактальних заходів (показника Херста, кореляційної

розмірності) у загальному випадку недостатньо для визначення мережевої атаки. Таким чином, щоб судити про мережеву атаку тільки за показником Херста потрібно, щоб мережева атака протікала під час всього інтервалу захоплення трафіку. Іншими словами, використання лише показника Херста при створенні індикатора мережевої атаки не дає жодної гарантії її виявлення. Тільки за сукупним аналізом фрактальних заходів та виду фазового простору можна говорити про наявність чи відсутність мережевої атаки.

Було розглянуто 4 «знімки» телекомунікаційного трафіку за відсутності мережевої атаки, тобто в нормальному стані. Ці трафіки відповідають різному завантаженню каналу в різний час доби (день, ніч, ранок, вечір). Це дозволить отримати доказ того, що незалежно від завантаження каналу у нормальному стані значення фрактальних параметрів та вид фазового портрета телекомунікаційного трафіку приблизно збігаються між собою.

Трафік 1. Денний вхідний трафік у момент відсутності мережевої атаки (рис. 2.6).

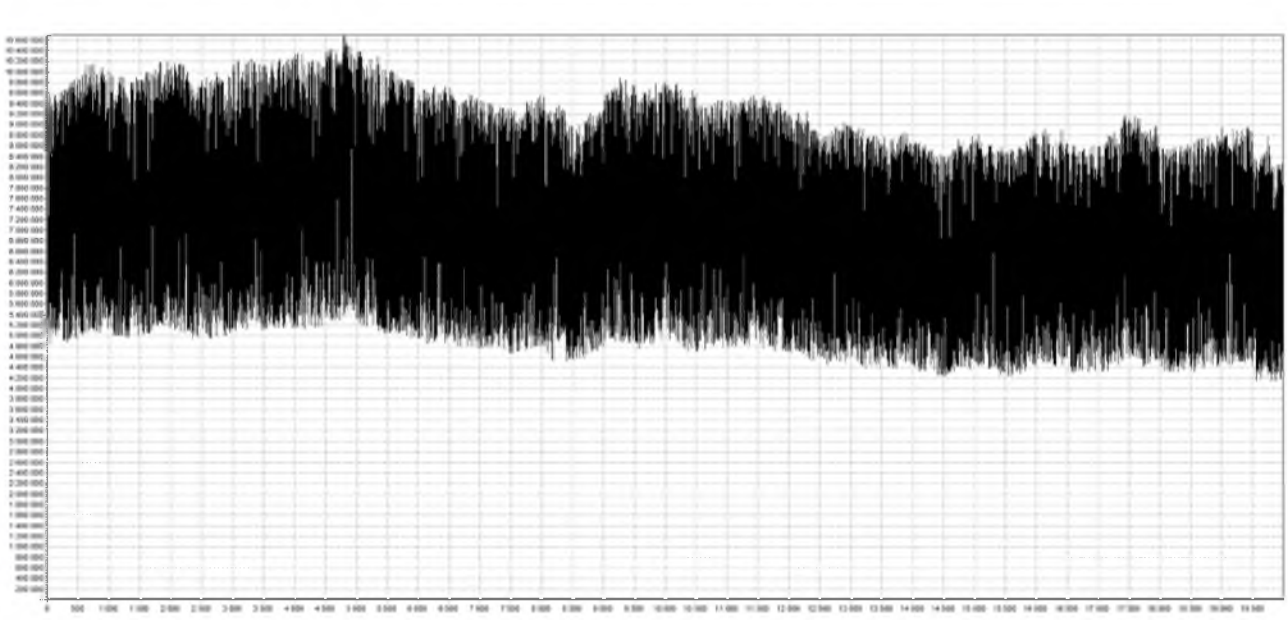

Рисунок 2.6 – Телекомунікаційний трафік 1

На рис. 2.7 показано залежністю R/S-параметра від запізнення N у подвійному логарифмічному масштабі, а також апроксимуюча пряма. Показник

Херста для трафіку 1 виявився рівним H=1.28, що говорить про його фрактальну природу.

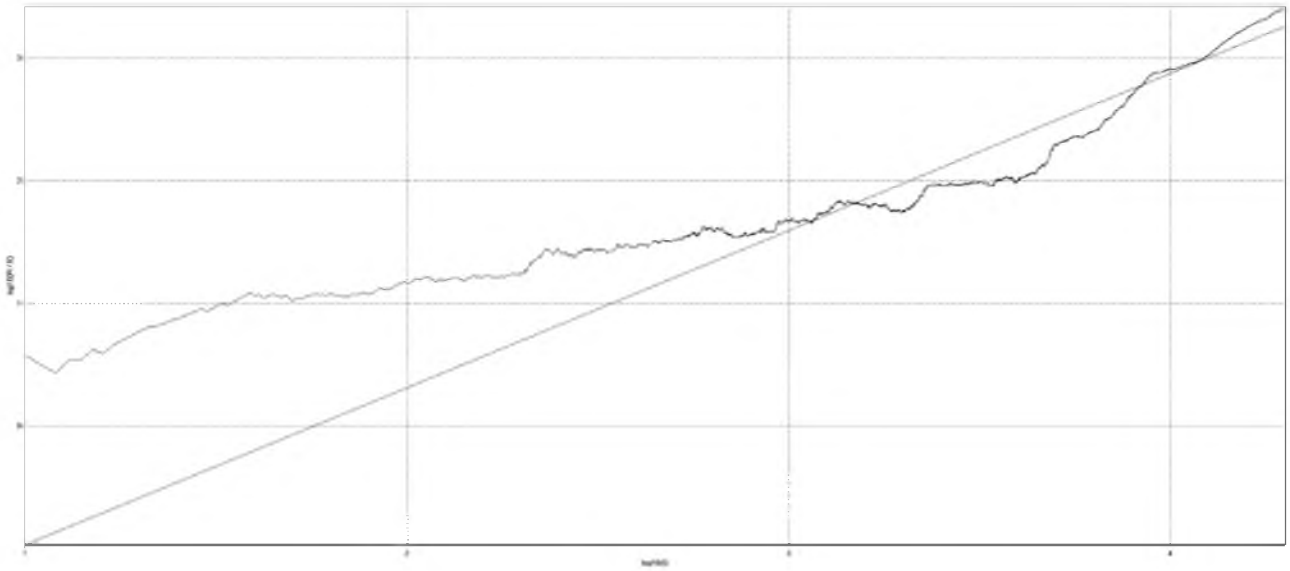

Рисунок 2.7 – Залежність R/S від запізнення N у подвійному логарифмічному масштабі для трафіку 1

На рис. 2.8 наведено залежність кореляційної розмірності D_C від розмірності простору вкладень, а також дотичну до графіка цієї функції. Кореляційна розмірність становила 11,39. Розмірність простору вкладень 17.

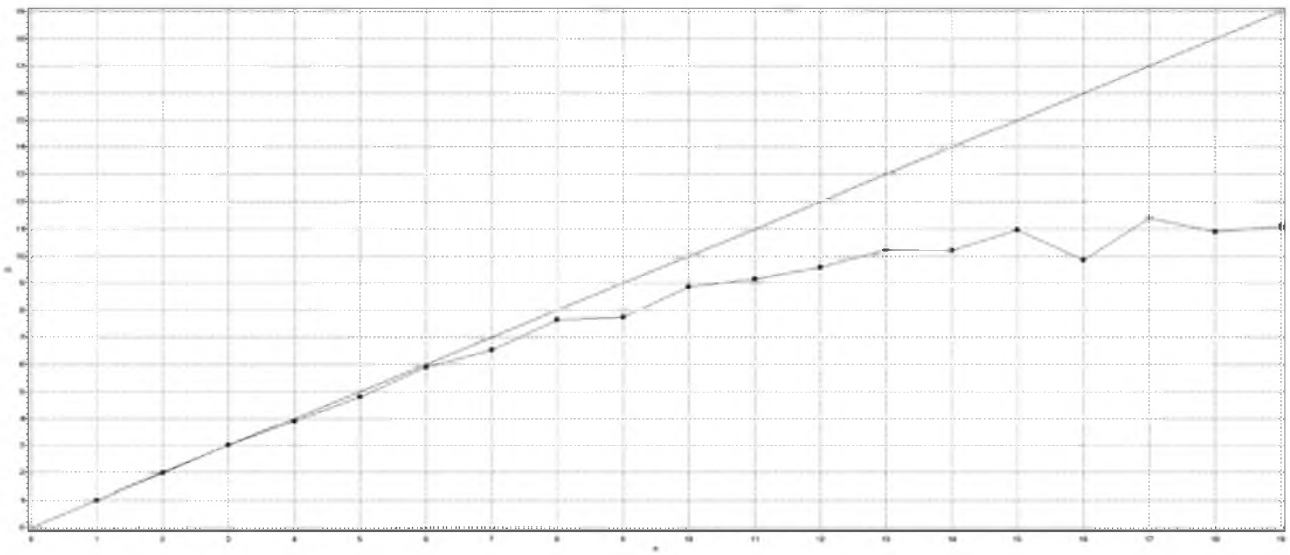

Рисунок 2.8 – Залежність кореляційної розмірності D_C від розмірності відновленого фазового простору для трафіку 1

На рис. 2.9 наведено вид фазового простору для трафіку 1.

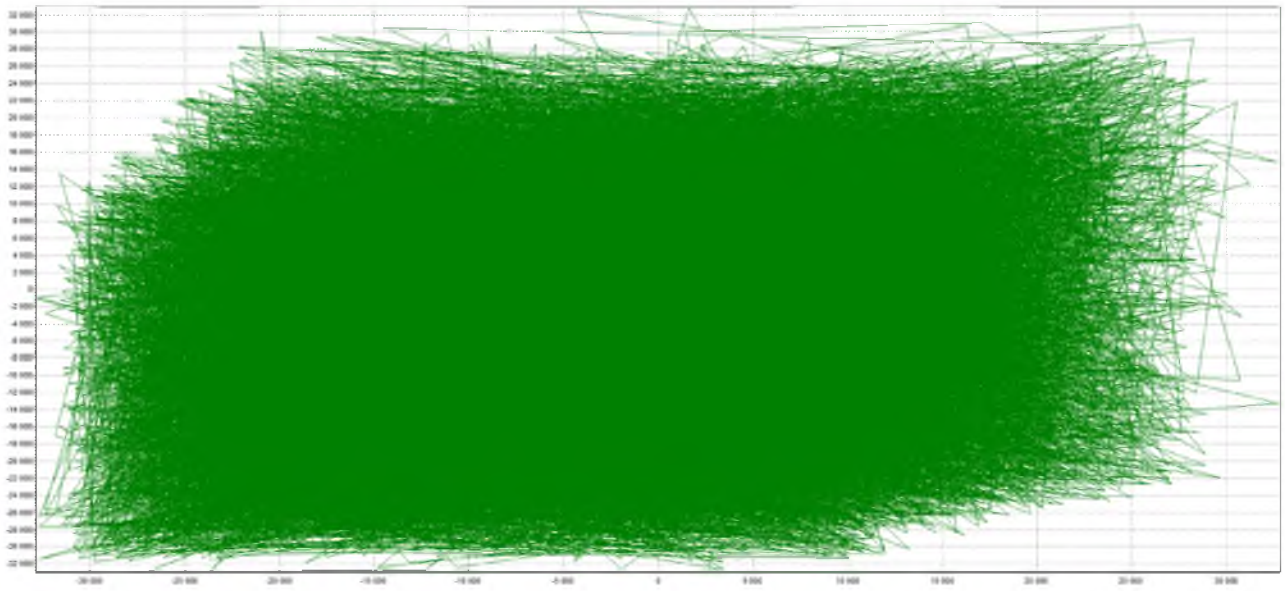

Рисунок 2.9 – Фазовий простір для трафіку 1

Трафік 2. Нічний вхідний трафік у момент відсутності мережевої атаки (рис. 2.10).

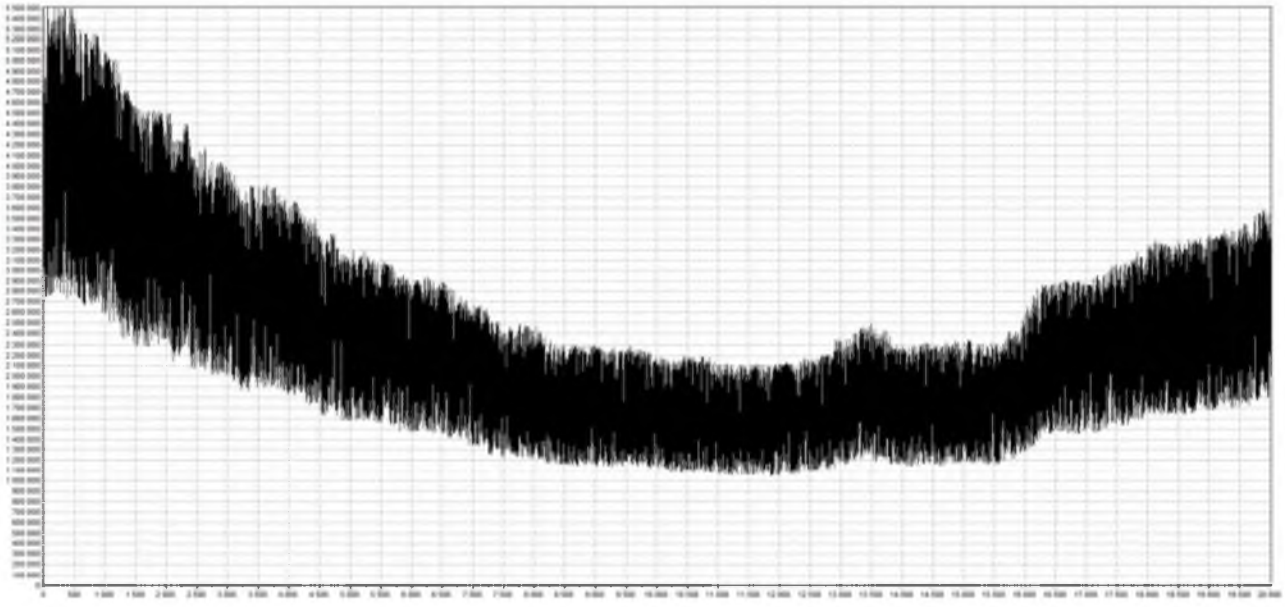

Рисунок 2.10 – Телекомунікаційний трафік 2

На рис. 2.11 показано залежністю R/S-параметра від запізнення N у подвійному логарифмічному масштабі, а також апроксимуюча пряма. Показник

Херста для трафіку 2 виявився рівним H=1.37, що говорить про його фрактальну природу.

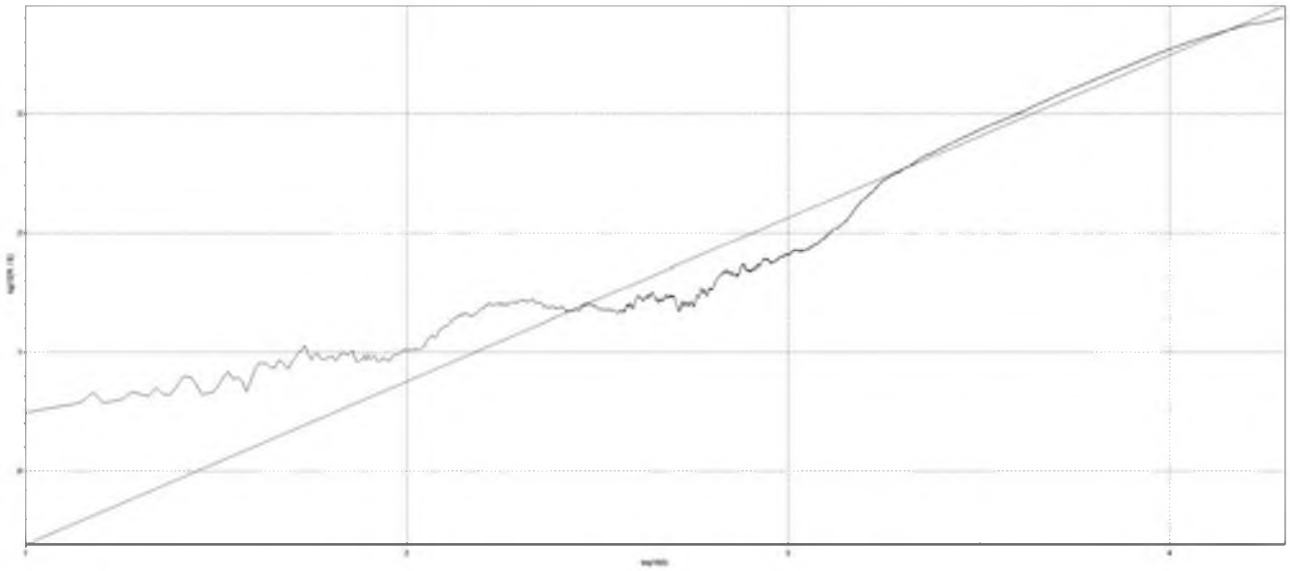

Рисунок 2.11 – Залежність R/S від запізнення N у подвійному логарифмічному масштабі для трафіку 2

На рис. 2.12 наведено залежність кореляційної розмірності D_C від розмірності простору вкладень, а також дотичну до графіка цієї функції. Кореляційна розмірність склала 9,41. Розмірність простору вкладень 14.

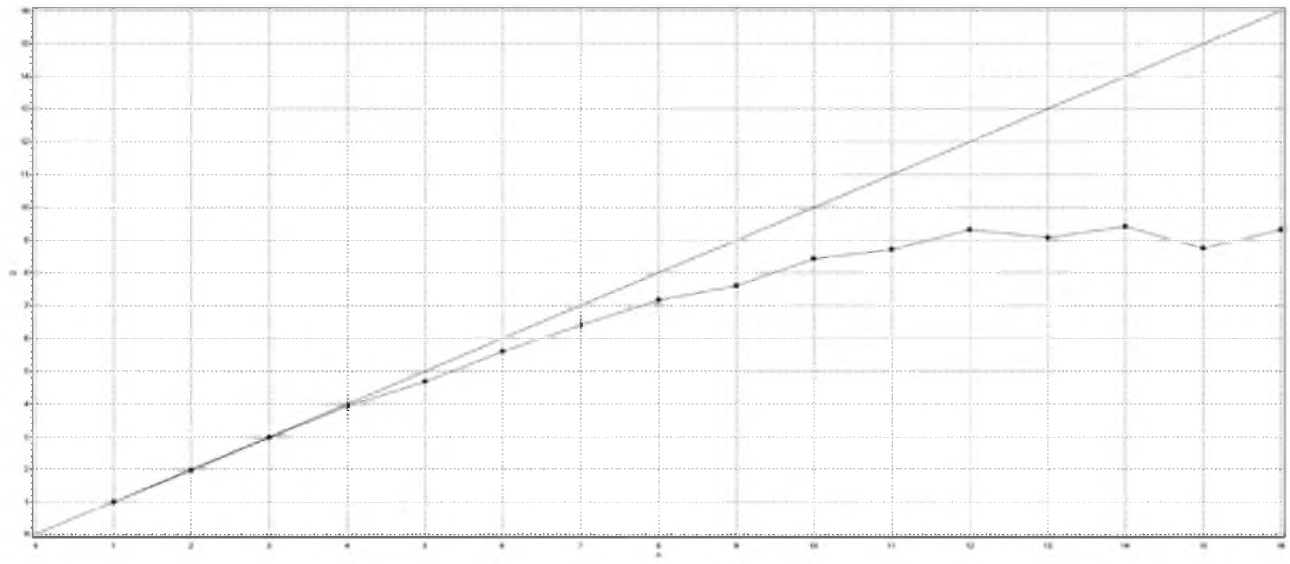

Рисунок 2.12 – Залежність кореляційної розмірності D_C від розмірності відновленого фазового простору для трафіку 2

На рис. 2.13 наведено вид фазового простору для трафіку 2.

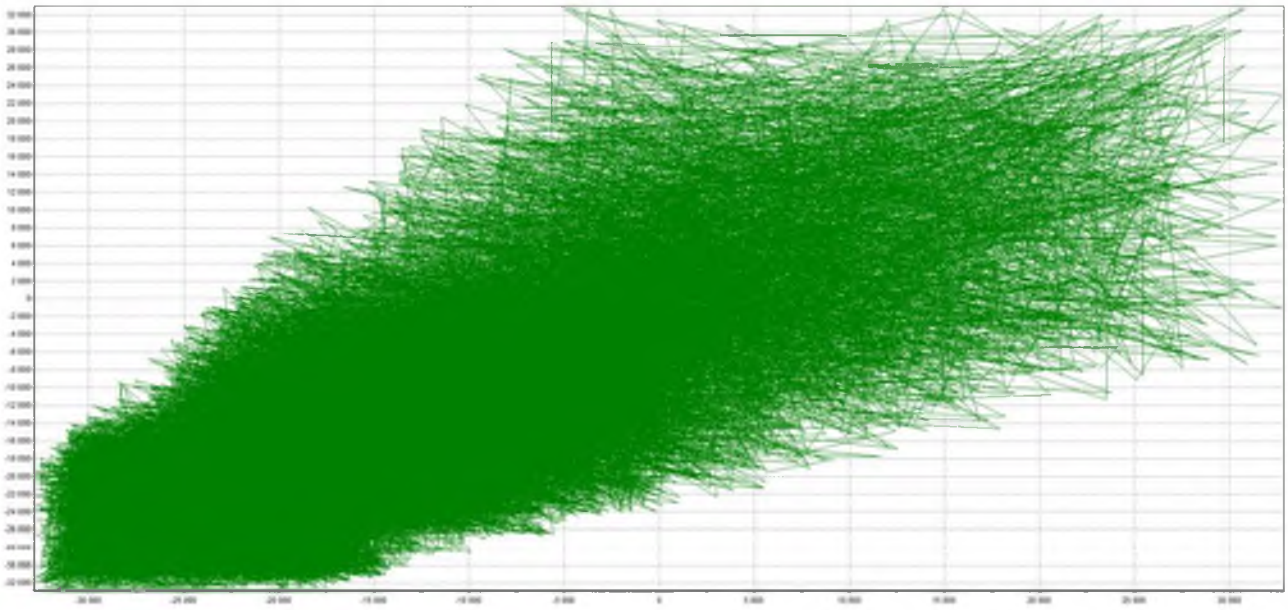

Рисунок 2.13 – Фазовий простір для трафіку 2

Трафік 3. Ранковий вхідний трафік у момент відсутності мережевої атаки (рис. 2.14).

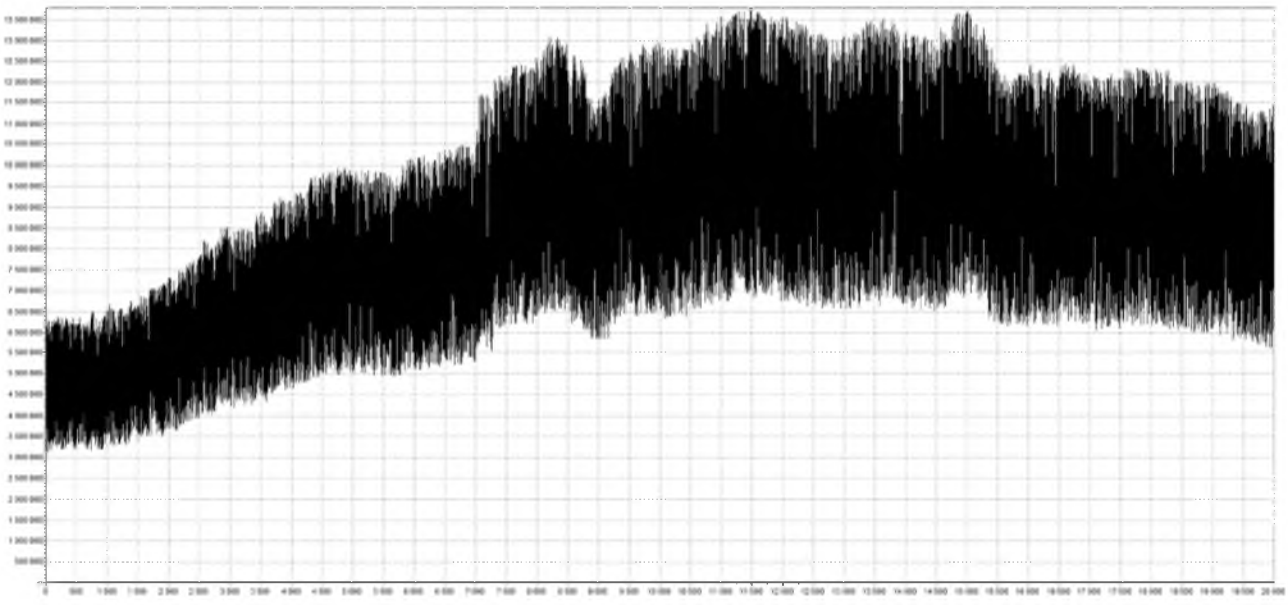

Рисунок 2.14 – Телекомунікаційний трафік 3

На рис. 2.15 показано залежністю R/S-параметра від запізнення N у подвійному логарифмічному масштабі, а також апроксимуюча пряма. Показник

Херста для трафіку 3 виявився рівним H=1.48, що говорить про його фрактальну природу.

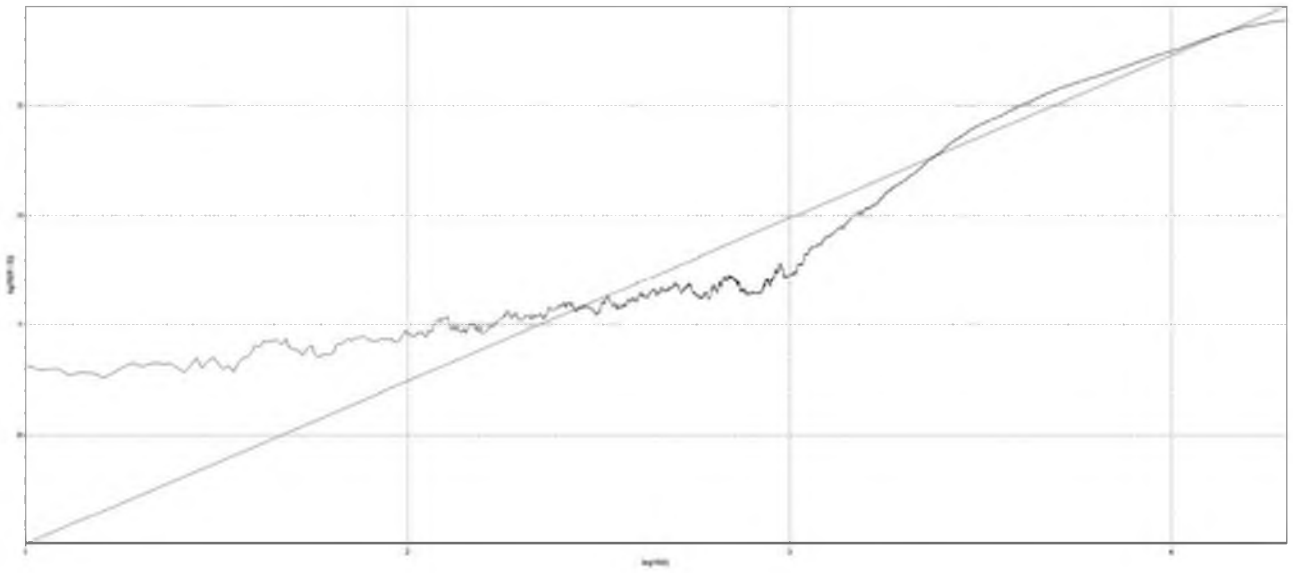

Рисунок 2.15 – Залежність R/S від запізнення N у подвійному логарифмічному масштабі для трафіку 3

На рис. 2.16 наведено залежність кореляційної розмірності D_C від розмірності простору вкладень, а також дотичну до графіка цієї функції. Кореляційна розмірність склала 9,68. Розмірність простору вкладень 13.

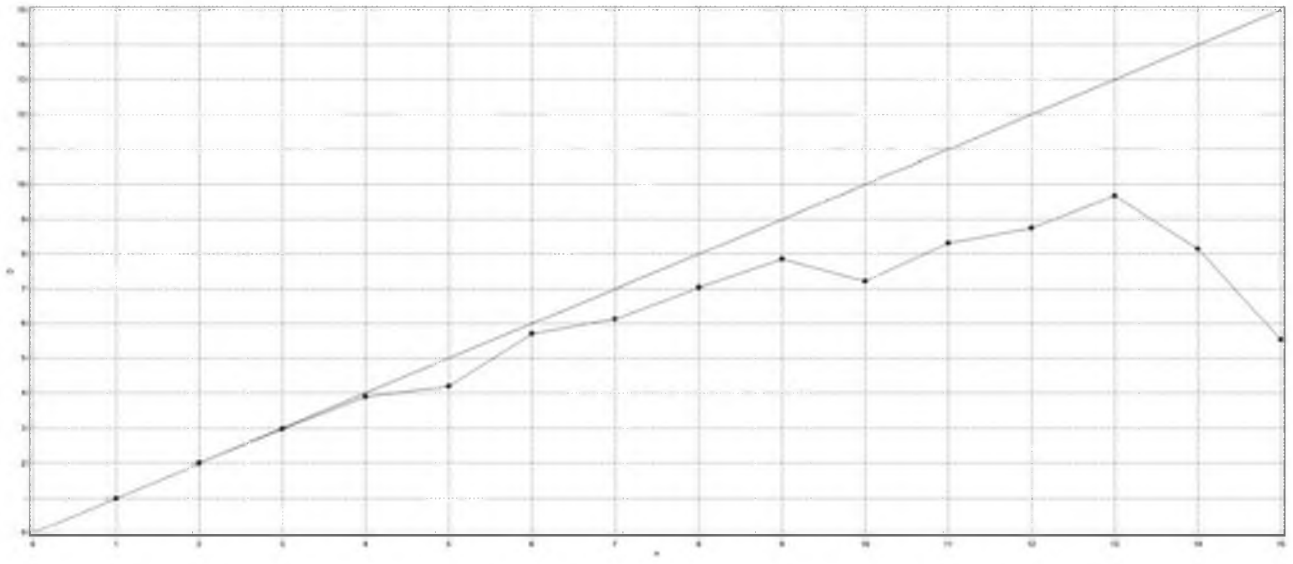

Рисунок 2.16 – Залежність кореляційної розмірності D_C від розмірності відновленого фазового простору для трафіку 3

На рис. 2.17 наведено вид фазового простору для трафіку 3.

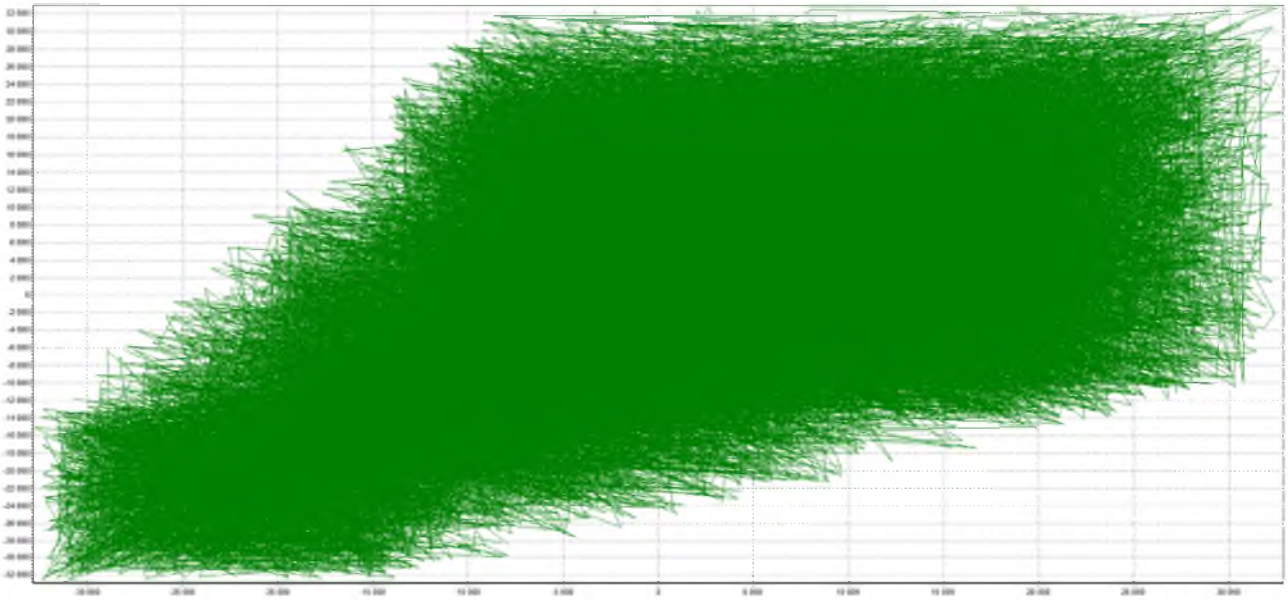

Рисунок 2.17 – Фазовий простір для трафіку 3

Трафік 4. Вечірній вхідний трафік у момент відсутності мережевої атаки (рис. 2.18).

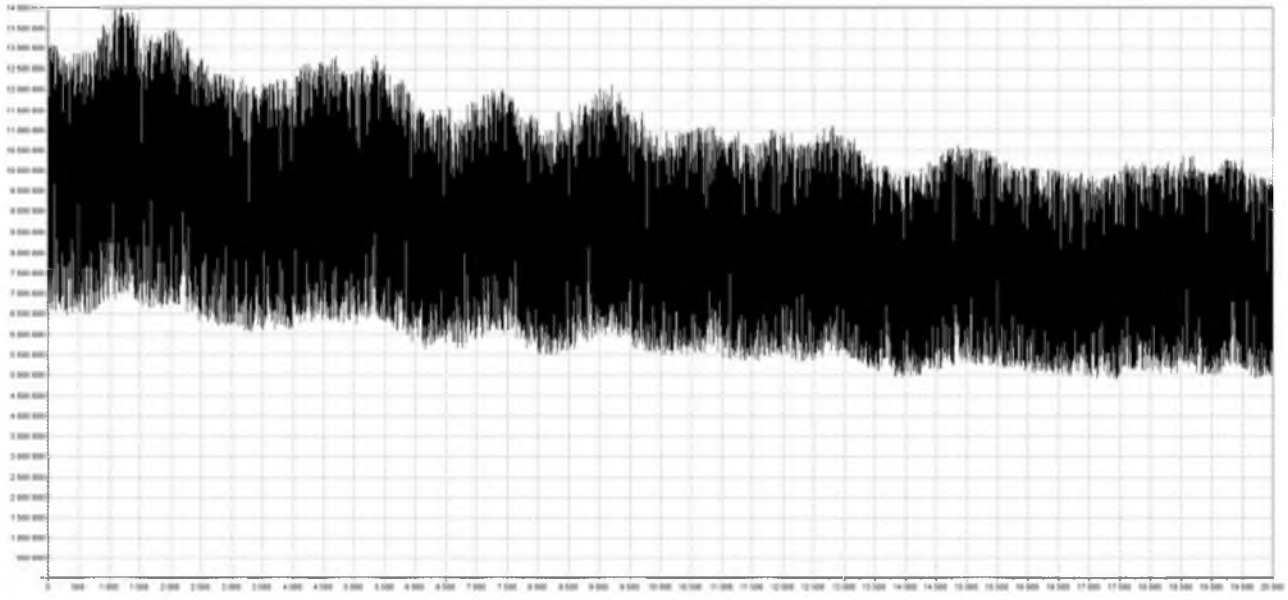

Рисунок 2.18 – Телекомунікаційний трафік 4

На рис. 2.19 показано залежністю R/S-параметра від запізнення N у подвійному логарифмічному масштабі, а також апроксимуюча пряма. Показник

Херста для трафіку 4 виявився рівним H=1.28, що говорить про його фрактальну природу.

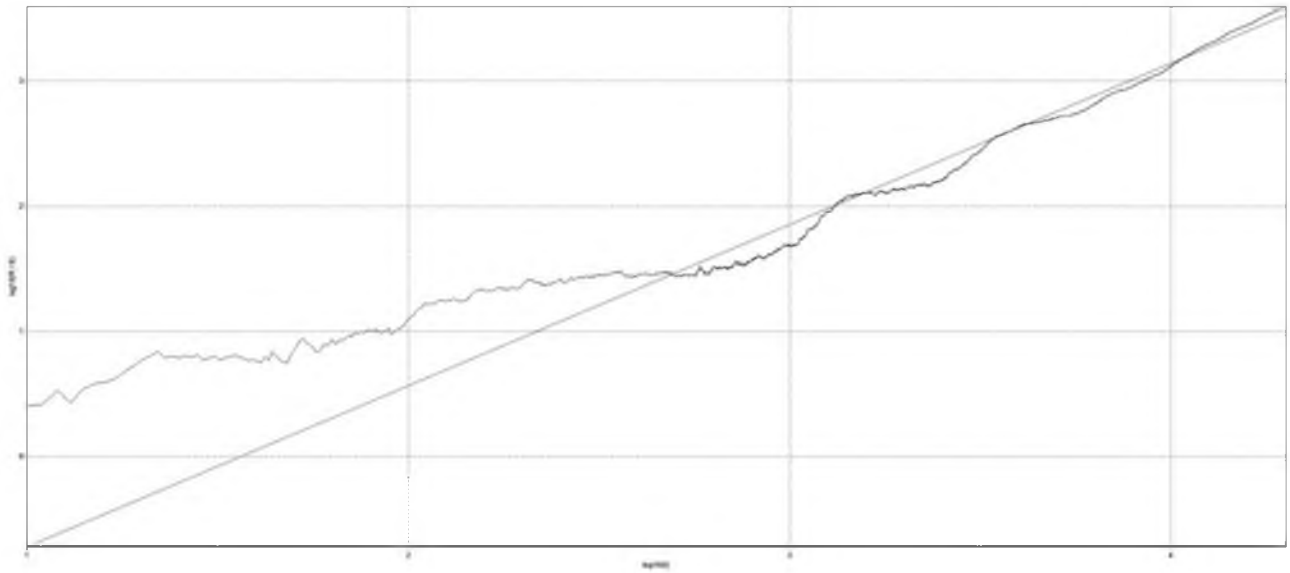

Рисунок 2.19 – Залежність R/S від запізнення N у подвійному логарифмічному масштабі для трафіку 4

На рис. 2.20 наведено залежність кореляційної розмірності D_C від розмірності простору вкладень, а також дотичну до графіка цієї функції. Кореляційна розмірність склала 11,06. Розмірність простору вкладень 15.

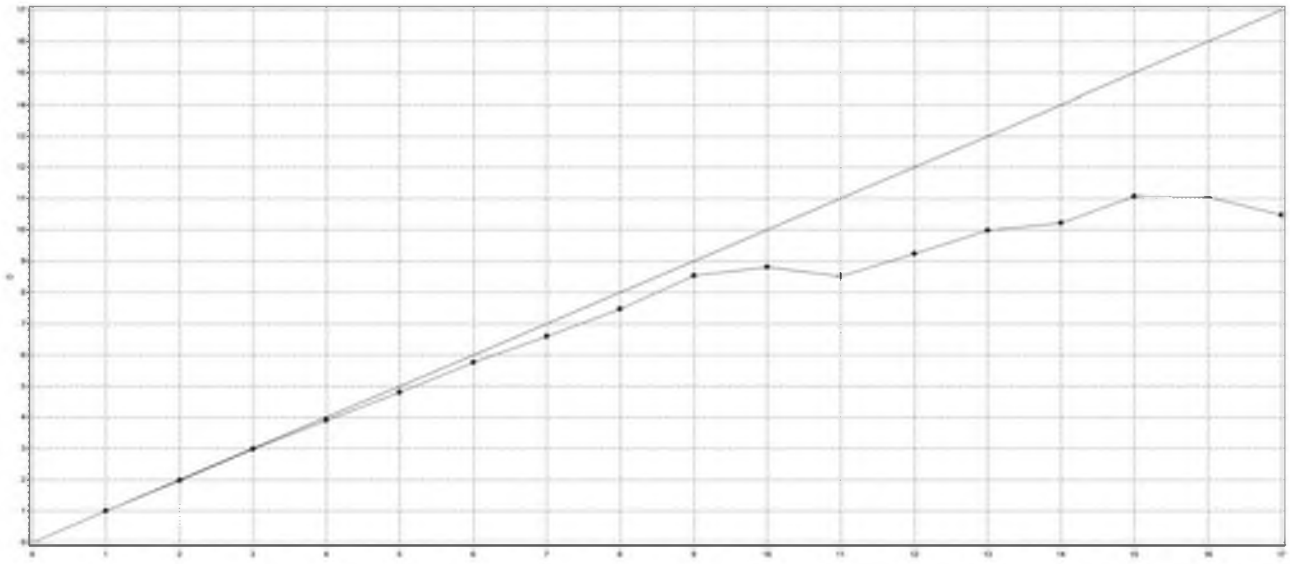

Рисунок 2.20 – Залежність кореляційної розмірності D_C від розмірності відновленого фазового простору для трафіку 4

На рис. 2.21 наведено вид фазового простору для трафіку 4.

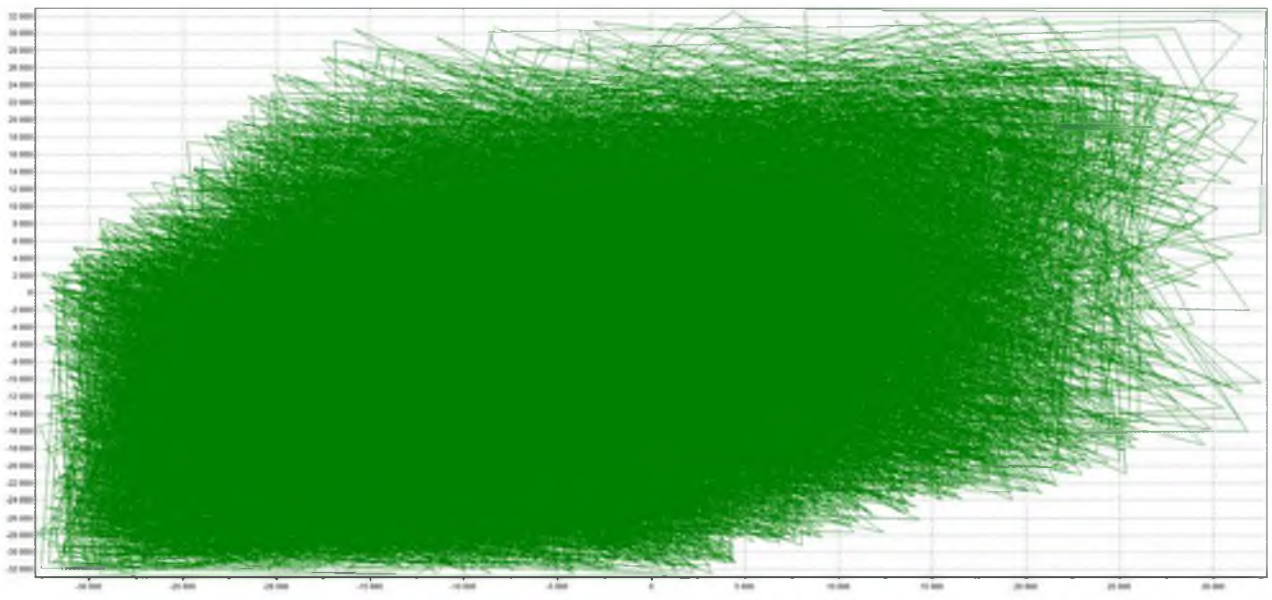

Рисунок 2.21 – Фазовий простір для трафіку 4

Розглянемо «знімки» телетрафіку за наявності мережевої атаки.

Трафік 5. Трафік за наявності DDoS-атаки на сайт, причому тривалість атаки не дорівнює усьому інтервалу дослідження (рис. 2.22). Спочатку мережа працювала в нормальному режимі, потім сталася DDoS-атака на деякий хост.

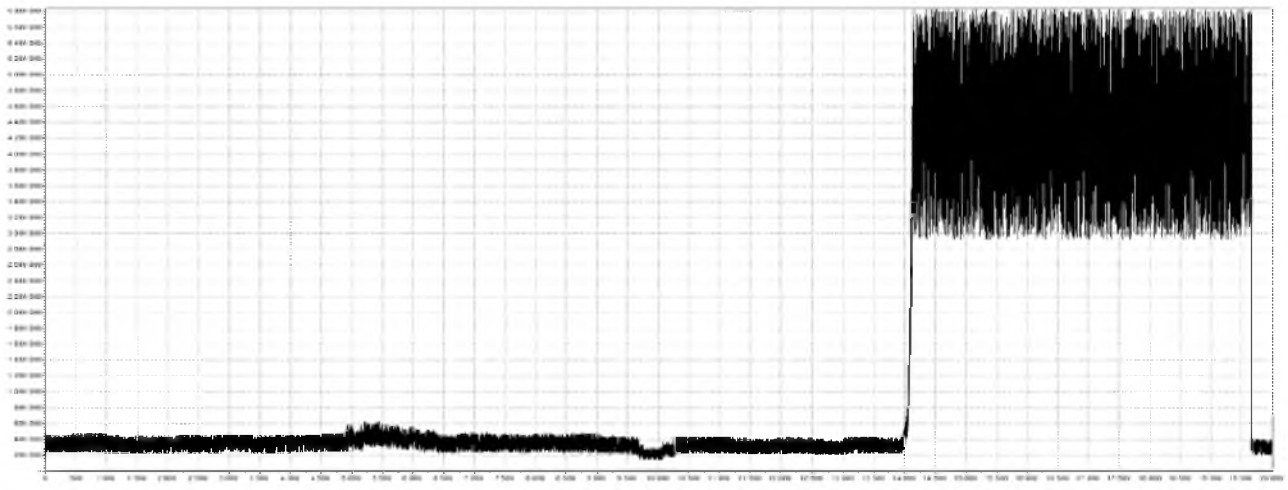

Рисунок 2.22 – Телекомунікаційний трафік 5

На рис. 2.23 показано залежністю R/S-параметра від запізнення N у подвійному логарифмічному масштабі, а також апроксимуюча пряма. Показник

Херста для трафіку 5 виявився рівним H=1.46, що говорить про його фрактальну природу.

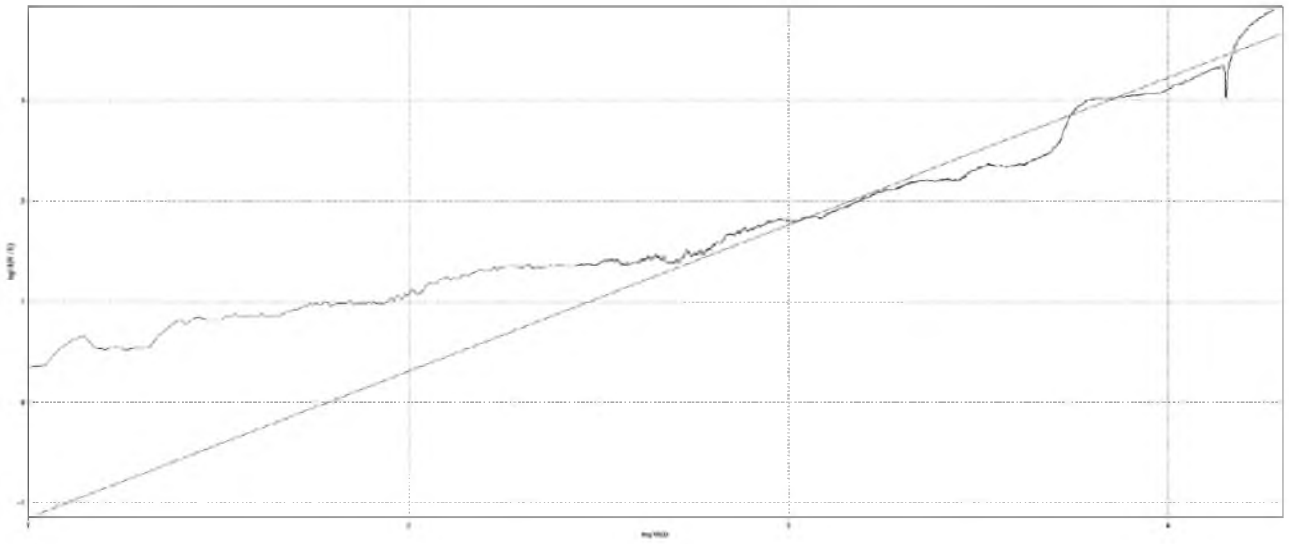

Рисунок 2.23 – Залежність R/S від запізнення N у подвійному логарифмічному масштабі для трафіку 5

На рис. 2.24 наведено залежність кореляційної розмірності D_C від розмірності простору вкладень, а також дотичну до графіка цієї функції. Кореляційна розмірність склала 10,15. Розмірність простору вкладень 15.

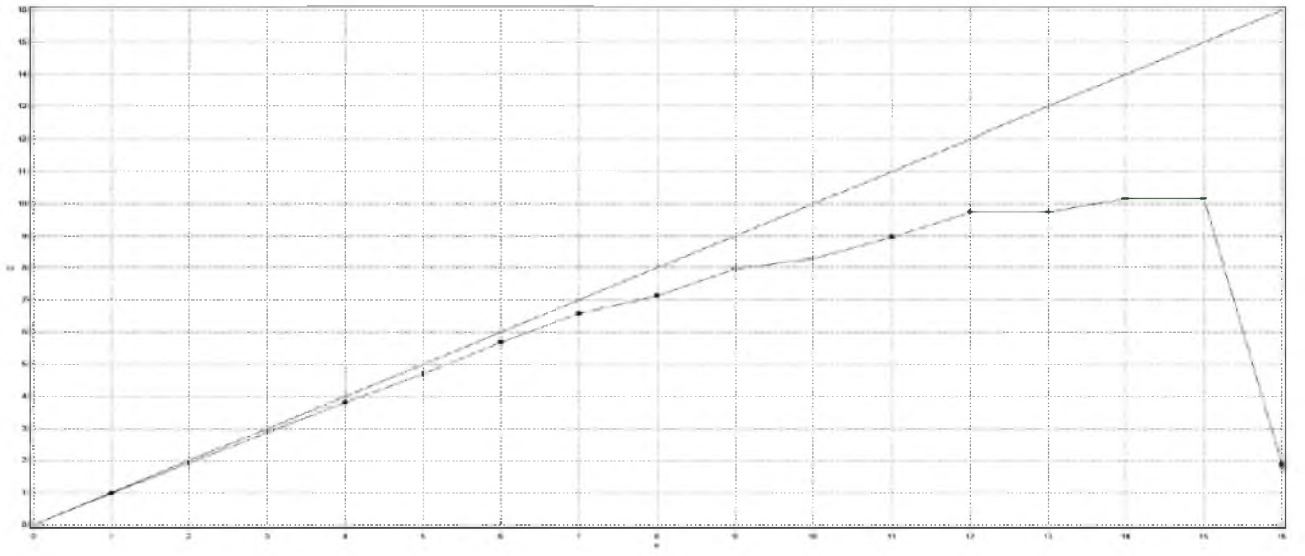

Рисунок 2.24 – Залежність кореляційної розмірності D_C від розмірності відновленого фазового простору для трафіку 5

На рис. 2.25 наведено вид фазового простору для трафіку 5.

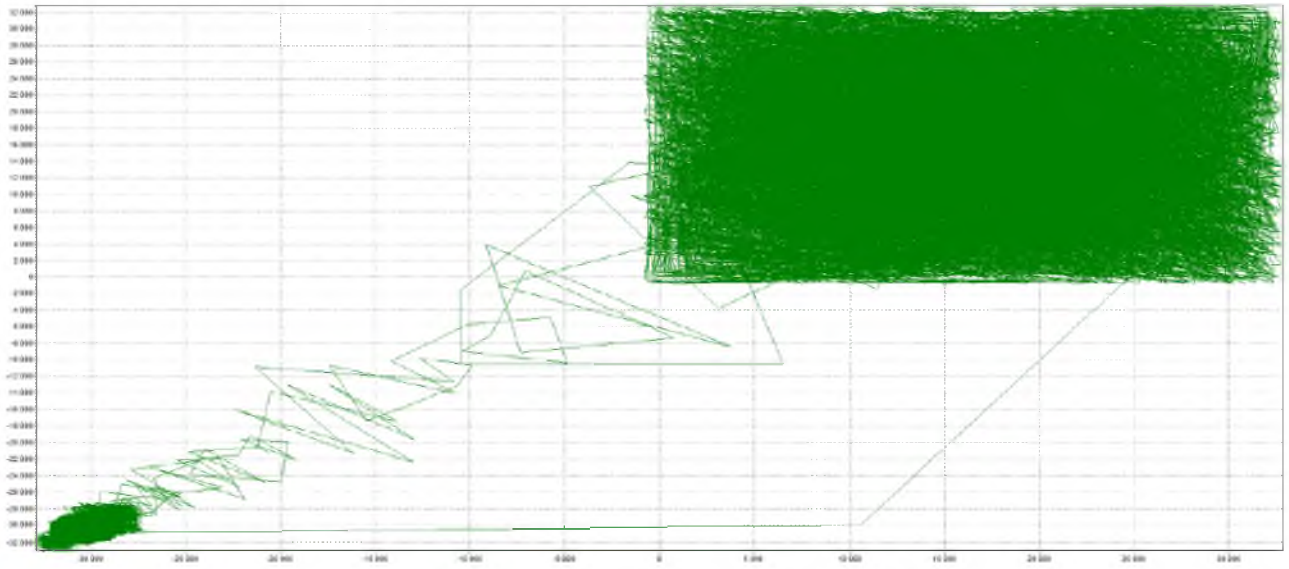

Рисунок 2.25 – Фазовий простір для трафіку 5

Трафік 6. Трафік за наявності DDoS-атаки на сайт, причому тривалість атаки дорівнює тривалості усього інтервалу дослідження (рис. 2.26).

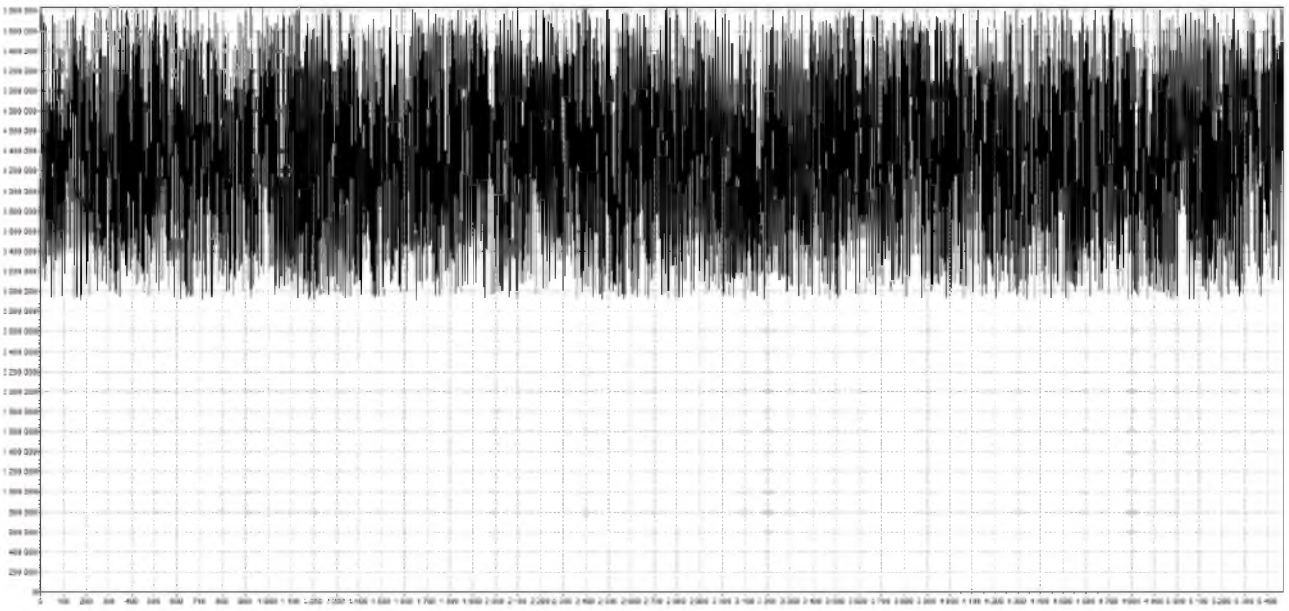

Рисунок 2.26 – Телекомунікаційний трафік 6

На рис. 2.27 показано залежністю R/S-параметра від запізнення N у подвійному логарифмічному масштабі, а також апроксимуюча пряма. Показник

Херста для трафіку 6 виявився рівним H=0.4, що говорить про його фрактальну природу.

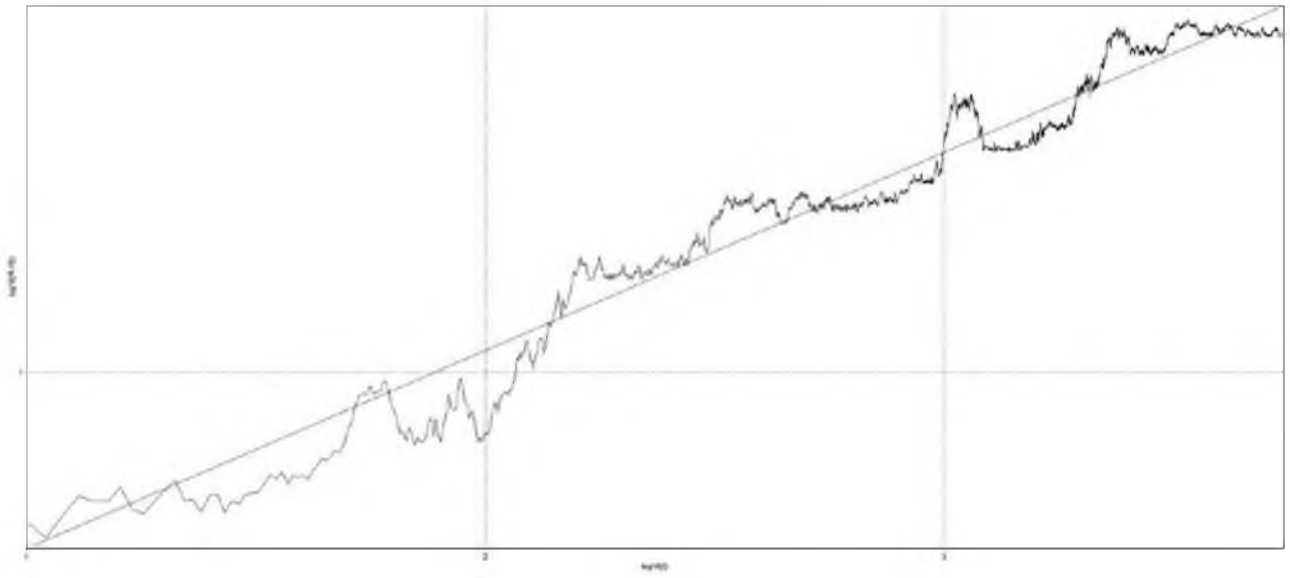

Рисунок 2.27 – Залежність R/S від запізнення N у подвійному логарифмічному масштабі для трафіку 8

На рис. 2.28 наведено залежність кореляційної розмірності D_C від розмірності простору вкладень, а також дотичну до графіка цієї функції. Кореляційна розмірність склала 8,86. Розмірність простору вкладень 11.

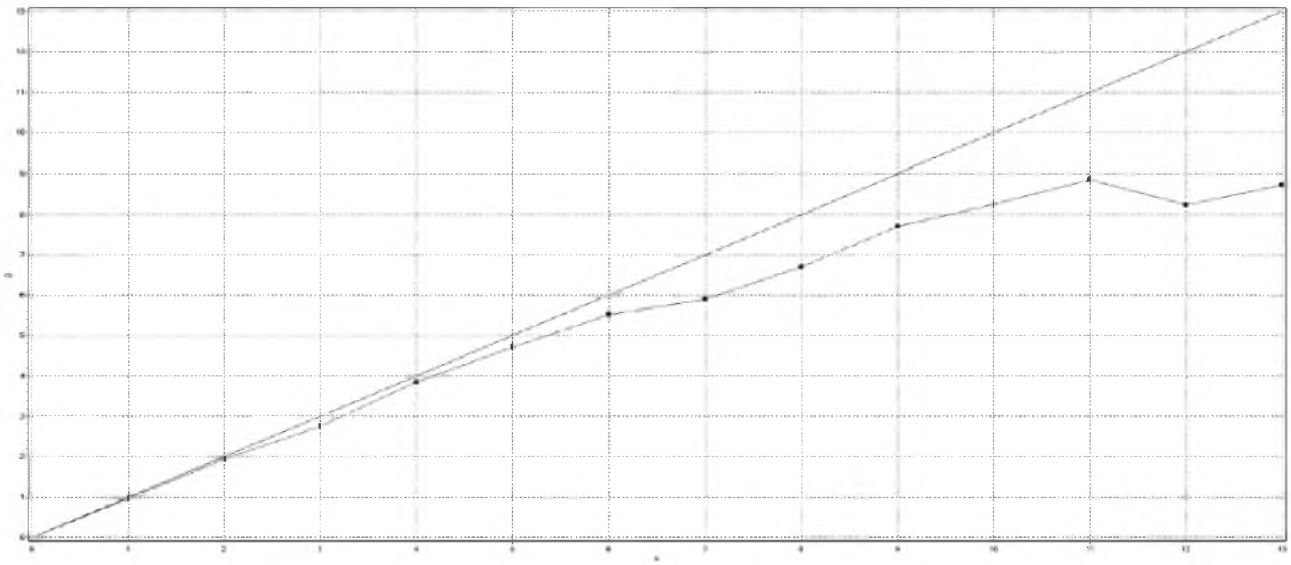

Рисунок 2.28 – Залежність кореляційної розмірності D_C від розмірності відновленого фазового простору для трафіку 6

На рис. 2.29 наведено вид фазового простору для трафіку 6.

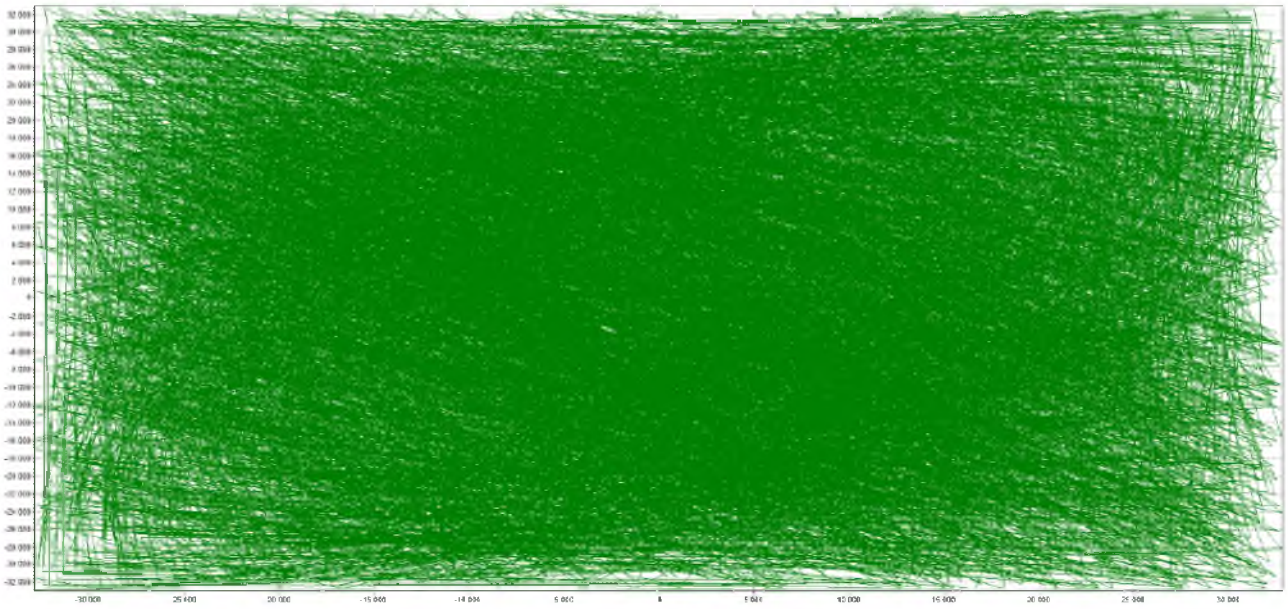

Рисунок 2.29 – Фазовий простір для трафіку 6

Слід зазначити, що форма фазового атрактора не залежить від того, що було спочатку – мережева атака або нормальний режим (у випадку трафіку 5). В обох випадках фазовий атрактор буде зосереджений у правому верхньому куті фазового простору. Тому приклад такого трафіку і його характеристик в роботі не приводиться.

Для проведення аналізу відобразимо значення отриманих фрактальних параметрів та заповненості фазових траєкторій у таблиці 2.1.

Розглянемо загальні принципи фрактального індикатора трафіку, який можна створити на основі проведених досліджень.

1. Якщо показник Херста менший за 0.5, це свідчить, що на всьому часовому інтервалі дослідження відбувається мережева атака.

2. Якщо кореляційна розмірність менша за 9, це свідчить, що на всьому часовому інтервалі дослідження відбувається мережева атака.

3. Коли мережева атака відбувається не на всьому часовому інтервалі дослідження, показник Херста та кореляційна розмірність не несуть жодної інформації.

Таблиця 2.1 – Зведені результати моделювання

Показник	Нормальний режим, трафік				Часткова мережева атака	Повна мережева атака
	1	2	3	4	5	6
Показник Херста	1.28	1.37	1.48	1.28	1.46	0.4
Кореляційна розмірність	11.39	9.41	9.68	11.06	10.15	8,86
Розмірність простору вкладень	17	14	13	15	15	11
Вид фазового простору	Атрактор по центру	Атрактор по центру	Атрактор по центру	Атрактор по центру	Атрактор у верхньому куті	Атрактор у всьому просторі

4. Коли мережева атака відбувається не на усьому часовому інтервалі дослідження, то її наявність можна судити лише по вигляду фазового простору. Як показали дослідження, атрактор динамічної системи в даному випадку прагне зайняти найбільш далеку позицію від центру системи координат (зміщується в правий верхній кут простору).

5. Коли мережева атака відбувається на всьому часовому інтервалі дослідження, атрактор заповнює максимально можливу частину фазового простору.

6. Різний рівень навантаження мережі не призводить до великого впливу на значення фрактальних параметрів.

7. У нормальному стані мережі атрактор представляє витягнуту фігуру, спрямовану від центру системи координат у правий верхній кут.

Таким чином, у загальному випадку показник Херста та кореляційна розмірність є первинними індикаторами наявності мережевої атаки і за їх значеннями однозначний висновок можна зробити лише тоді, коли мережева атака почалася і продовжується до теперішнього часу. Єдиним достовірним показником наявності мережевої атаки є форма фазового атрактора, його розташування. Цей факт є основним для створення фрактального індикатора стану мережі.

Розглянемо алгоритм роботи фрактального індикатора.

1. На вхід програми надходить одновимірний часовий дискретний ряд зі значеннями завантаження каналу деякої тривалості.

2. Обчислюється показник Херста. Якщо його значення менше 0.5, це означає, що з початку запису трафіку і до поточного моменту спостерігається DDoS-атака на певний хост. Для підтвердження наявності мережевої атаки можуть бути використані кореляційна розмірність та розмірність простору вкладення.

3. Якщо значення показника Херста більше 0,5, значення кореляційної розмірності більше 9 та розмірність простору вкладень більше 12, то ситуація може відповідати як нормальному режиму роботи, так і ситуації, що має місце DDoS-атака з якогось конкретного (не початкового) моменту записаного трафіку. І тут необхідно розрахувати фазовий портрет динамічної системи. Якщо атрактор йде на фазовому просторі у правий верхній кут, це однозначно свідчить про наявність мережевої атаки, якщо він витягнутий від центру системи координат у правий верхній кут, це відповідає звичайному режиму роботи мережі.

Отже, було доведено, що для виявлення наявності мережевих атак необхідно спільне використання фрактальних параметрів (показника Херста, кореляційної розмірності, розмірності простору вкладень) та фазового портрета системи.

2.4 Висновки

У цьому розділі було розглянуто питання своєчасного визначення мережевих атак за допомогою фрактальних методів оцінки мережевого трафіку, що ґрунтуються на ознаках його самоподібності.

1. Розглянуто відомі методи розрахунку фрактальних параметрів (показника Херста, кореляційної розмірності, розмірності простору вкладень) стосовно телекомунікаційного трафіку.

2. Проведено розрахунок фрактальних параметрів телекомунікаційного трафіку у різному стані мережі: нормальному; за наявності мережевої атаки у всьому інтервалі дослідження та за наявності мережевої атаки на деякому часовому проміжку фіксованої тривалості.

3. Доведено, що за значеннями показника Херста та кореляційної розмірності не можна однозначно судити про наявність мережевої атаки.

4. Показано, що показник Херста є індикатором мережевої атаки лише у випадку, коли DDoS-атака відбувається на всьому часовому інтервалі дослідження.

5. Доведено, що за будь-яких ситуаціях про наявність мережевої атаки можна судити за формою фазового атрактора системи.

6. Визначено вид фазового атрактора телекомунікаційного трафіку у різному стані мережі: нормальному; за наявності мережевої атаки у всьому інтервалі дослідження та за наявності мережевої атаки на деякому часовому проміжку фіксованої тривалості.

7. Доведено, що в стані мережевої атаки показник Херста менший за 0,5, тобто відбувається втрата самоподібності трафіку, проте це має місце лише в тому випадку, коли мережева атака триває на всьому часовому інтервалі дослідження.

8. Доведено, що в стані мережевої атаки кореляційна розмірність менша за 9, проте це має місце лише у тому випадку, коли мережева атака триває на всьому часовому інтервалі дослідження.

9. Доведено, що різний рівень навантаження мережі у нормальному стані (без мережної атаки) не призводить до великого впливу на значення фрактальних параметрів.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою даного розділу є обґрунтування економічної доцільності фрактального аналіз трафіку в інформаційно-комунікаційних мережах для систем виявлення атак. Досягнення цієї мети потребує здійснення визначення величини капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення; річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування; річного економічного ефекту від впровадження запропонованих заходів; показників економічної ефективності впровадження системи захисту на підприємстві.

3.1 Розрахунок (фіксованих) капітальних витрат

До капітальних витрат належать витрати на розробку заходів із забезпечення інформаційної безпеки, а також витрати на придбання матеріальних та нематеріальних активів.

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

Визначення трудомісткості розробки підходу щодо фрактального аналіз трафіку в інформаційно-комунікаційних мережах для систем виявлення атак

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

де $t_{тз}$ – тривалість складання технічного завдання на розробку підходу щодо фрактального аналіз трафіку в інформаційно-комунікаційних мережах для систем виявлення атак, $t_{тз}$=15;

$t_в$ – тривалість аналізу існуючих інформаційних потоків організації, вивчення ТЗ, літературних джерел за темою тощо, $t_в$=*30*;

$t_а$ – тривалість аналізу існуючих загроз безпеки інформації, $t_а$=*40*;

$t_р$ – тривалість розробки підходу щодо фрактального аналіз трафіку в інформаційно-комунікаційних мережах для систем виявлення атак, $t_м$=*46*;

$t_д$ – тривалість підготовки технічної документації, $t_д$=*10*.

Отже,

$$t = t_{тз} + t_в + t_а + t_р + t_д = 15+30+40+46+10 = 141 \text{ години.}$$

Розрахунок витрат на розробку підходу щодо фрактального аналіз трафіку в інформаційно-комунікаційних мережах для систем виявлення атак

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

$$К_{рп} = З_{зп} + З_{мч}.$$

$$К_{рп} = З_{зп} + З_{мч} = 34200+2096{,}08 = 36296{,}08 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 141*200 = 28200 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

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

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

$$З_{мч} = t*С_{мч} = 141*13{,}79 = 2096{,}08 \text{ грн.}$$

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

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = 0{,}7 \cdot 4 \cdot 1{,}68 + \frac{10800 \cdot 0.2}{1920} + \frac{6400 \cdot 0.4}{1920} = 13{,}79 \text{ грн.}$$

Виявлення мережевих атак здійснювалася за допомогою спеціалізованого програмного забезпечення через моніторингу мережевого трафіку між клієнтською системою, на яку здійснюватиметься атака та системою зловмисника (атакуюча система), а також аналізі підозрілого трафіку мережі, з подальшою оцінкою атаки, ризиків її здійснення, збитків та механізмів протидії атакуючій системі. За допомогою відомих програм для запису трафіку у режимі

онлайн проводилося протоколювання телекомунікаційного трафіку (навантаження мережі) залежно від часу. Отже, додаткові капітальні витрати не виникають.

Додаткові витрати виникають у разі залучення зовнішніх консультантів і складають 8000 грн,

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

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} = 36296,08 + 8000 = 44296,08 \text{ грн.}$$

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

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

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

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

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

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \text{ грн.}$$

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в} = 0$);

$С_{к}$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки.

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

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

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються сукупною величиною витрат на організаційні заходи, яка складає 10000 грн.

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

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

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

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 25000 грн. Додаткова заробітна плата – 5% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,2 ставки. Отже,

$$С_з = (25000*12 + 25000*12*0,05)*0,2= 63000 \text{ грн.}$$

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

$$С_{єв} = 63000*0,22 = 13860 \text{ грн.}$$

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

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

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,9 кВт);

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

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

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

$$С_{ел} = 0,9*5*1920*1,68 = 14512,2 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат – 1% ($С_{тос}$ = 44296,08*0,01=442,96 грн).

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

$$С_к = 10000+63000+13860 +14512,2+442,96 = 101815,16 \text{ грн.}$$

Витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) можна орієнтовно визначити, виходячи з величини капітальних витрат та середньостатистичних даних щодо активності користувачів. За статистичними даними активність користувачів складає 20%. Тому:

$$С_{ак} = 44296,08*0,2=8859,22 \text{ грн.}$$

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

$$С = 101815,16 + 8859,22 = 110674,38 \text{ грн.}$$

3.2 Оцінка можливого збитку

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

Оцінка можливого збитку від атаки на вузол або сегмент мережі.

Необхідні *вихідні дані* для розрахунку:

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

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

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

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

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 17000 грн./міс.;

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

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

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

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

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 44.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

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

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

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

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

$$П_п = \frac{\sum З_с}{F} t_п = \frac{17000 * 5}{176} * 2 = 965{,}91 \text{ грн},$$

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

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

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

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

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

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

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

$$П_{ви} = \frac{\sum З_с}{F} t_{ви} = \frac{17000*5}{176} * 2 = 965{,}91 \text{ грн.}$$

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

$$П_{пв} = \frac{\sum З_р}{F} t_в = \frac{25000*1}{176} * 3 = 426{,}14 \text{ грн.}$$

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

$$П_в = 965{,}91+426{,}14 = 1392{,}04 \text{ грн.}$$

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

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

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

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

$$U = 965{,}91+1392{,}04+1682{,}69 = 4040{,}64 \text{ грн.}$$

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

$$B = \sum_i \sum_n U = \sum_1 \sum_{44} 4040{,}64 = 177788{,}16 \text{ грн.}$$

3.2.1 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C \text{ грн.},$$

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

R – вірогідність успішної реалізації загрози (84%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$$E = 177788{,}16 * 0{,}84 - 110674{,}38 = 38667{,}67 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

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

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

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

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

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{38667{,}674}{44296{,}08} = 0{,}87 \text{ частки одиниці,}$$

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

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (6%);

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

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,87 > (6 - 5)/100 = 0,87 > 0,01.$$

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

$$T_o = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{0,87} = 1,15 \text{ роки.}$$

3.4 Висновок

Отже, фрактальний аналіз трафіку в інформаційно-комунікаційних мережах для систем виявлення атак може вважатися економічно доцільним, оскільки кожна вкладена у капітальні витрати гривня приноситиме 0,87 грн. економічного ефекту (у разі здійснення 44 атак на рік з вірогідністю їх реалізації 84%, часу простою вузла або сегмента корпоративної мережі внаслідок атаки, який дорівнює 2 годинам; часу відновлення після атаки персоналом, що обслуговує корпоративну мережу, який дорівнює 3 годинам; часу повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, який дорівнює 2 годинам). Капітальні витрати складатимуть 44296,08 грн. Період окупності складатиме 1,15 років.

ВИСНОВКИ

Основні результати кваліфікаційної роботи полягають у наступному:

1. Вибір СВА повинен ґрунтуватись на вимогах, що висуваються до системи захисту інформації в кожному конкретному випадку. Проведене дослідження та порівняльний аналіз сучасних систем виявлення атак та запобігання вторгненням показав, що при вдосконаленні існуючих та проектуванні нових систем необхідно враховувати визначені властивості, зважаючи на особливості реалізації та функціонування інформаційної системи, які підлягають захисту.

2. Наразі актуальним завданням є захист від мережевих атак, заснованих на використанні протоколів транспортного та мережевого рівнів стека TCP/IP. Існуючі засоби захисту не завжди справляються з новими видами таких атак, тому важливим напрямком досліджень та розробок є створення систем захисту, здатних захищати не від конкретних атак, а від цілих класів атак. Складність процесів виявлення та блокування атак суттєво збільшується внаслідок сучасних тенденцій розвитку інформаційно-телекомунікаційних технологій, у тому числі пов'язаних із зростанням розмірів та продуктивності мереж, ускладненням їхньої топології, зростанням обсягу «швидкого трафіку», обумовленого функціонуванням peer-to-peer додатків, VoIP-трафіком, роботою сканерів безпеки тощо.

3. Встановлено, що багато з сучасних способів виявлення атак у мережі недостатньо надійні, що, у першу чергу, пов'язано з недостовірним визначенням часу початку атаки. Дослідження фрактальних методів аналізу спрямовано на виявлення не властивих для звичайного трафіку структурних особливостей, викликаних аномальними змінами, що, у свою чергу, дозволить потім своєчасно блокувати атаку відомими методами.

4. Телекомунікаційний трафік, що є по суті часовим дискретним рядом, має фрактальні властивості. Телекомунікаційний трафік, має фрактальну природу, тому що його кореляційна розмірність не є цілим числом. Для оцінки

фрактальності того чи іншого фізичного процесу може бути використаний показник Херста, що дозволяє визначити рівень детермінованого хаосу в досліджуваній системі. Однак використання єдиного фрактального параметра для опису телекомунікаційного трафіку за наявності мережевих атак є недостатнім і не завжди повністю інформативним.

5. Розглянуто питання своєчасного визначення мережевих атак за допомогою фрактальних методів оцінки мережевого трафіку, що ґрунтуються на ознаках його самоподібності. Розглянуто відомі методи розрахунку фрактальних параметрів (показника Херста, кореляційної розмірності, розмірності простору вкладень) стосовно телекомунікаційного трафіку.

6. При моделюванні проведено розрахунок фрактальних параметрів телекомунікаційного трафіку у різному стані мережі: нормальному; за наявності мережевої атаки у всьому інтервалі дослідження та за наявності мережевої атаки на деякому часовому проміжку фіксованої тривалості. Встановлено наступне:

6.1.За значеннями показника Херста та кореляційної розмірності не можна однозначно судити про наявність мережевої атаки.

6.2. Показник Херста є індикатором мережевої атаки лише у випадку, коли DDoS-атака відбувається на всьому часовому інтервалі дослідження.

6.3. За будь-яких ситуаціях про наявність мережевої атаки можна судити за формою фазового атрактора системи.

6.4. В стані мережевої атаки показник Херста менший за 0,5, тобто відбувається втрата самоподібності трафіку, проте це має місце лише в тому випадку, коли мережева атака триває на всьому часовому інтервалі дослідження.

6.5. В стані мережевої атаки кореляційна розмірність менша за 9, проте це має місце лише у тому випадку, коли мережева атака триває на всьому часовому інтервалі дослідження.

6.6. Різний рівень навантаження мережі у нормальному стані (без атаки) не призводить до великого впливу на значення фрактальних параметрів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Браницкий А.А. Анализ и классификация методов обнаружения сетевых атак / А.А. Браницкий, И.В. Котенко // Труды СПИИРАН. – 2016. – Вып. 2(45). – С. 207-244.

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

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

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

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

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

7. Радівілова Т.А., Кіріченко Л.О., Тавалбех М.Х., Ільков А.А. Виявлення аномалій в телекомунікаційному трафіку статистичними методами // Кібербезпека: освіта, наука, техніка. – 2021. – № 3 (11). – С. 183-194.

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

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

10. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин – М.: ДМК Пресс, 2010 – 544 с.

11. Ленков С.В. Методы и средства защиты информации: в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко – К.: Арий, 2008 – Т.2: Информационная безопасность, 2008 – 344 с.

12. Обзор механизмов реализации и обнаружения атак [Электронный ресурс]. – Режим доступа: http://comp-bez.ru/?p=778

13. Радченко М.М. Аналіз системи виявлення вторгнень та комп'ютерних атак / М.М. Радченко, О.І. Іванов, С.І. Прохорський, К.К. Мужеський // Междисциплинарные исследования в науке и образовании, 2013. – 379 с.

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

15. Лукацкий А.В. Обнаружение атак / А.В. Лукацкий // СПб.: БХВ-Петербург. – 2003. – 608 с.

16. Kumar S., Spafford E.H. A Pattern Matching Model for Misuse Intrusion Detection // Proceedings of the 17th National Computer Security Conference, 1994. – P. 11-21.

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

18. Jyothsna V., Prasad V.V.R. A Review of Anomaly Based Intrusion Detection Systems // International Journal of Computer Applications. – 2011. – Vol. 28, no. 7. – pp. 26–35.

19. Baddar S.A.-H., Merlo A., Migliardi M. Anomaly Detection in Computer Networks: A State-of-the-Art Review // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. – 2014. – Vol. 5. no. 4. – P. 29–64.

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

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

22. Wu S.X., Banzhaf W. The Use of Computational Intelligence in Intrusion Detection Systems: A Review // Applied Soft Computing. – 2010. – Vol. 10, Issue 1. – P. 1-35.

23. Kabiri P. Research on Intrusion Detection and Response: A Survey / P. Kabiri, A.A. Ghorbani // International Journal of Network Security. – 2005. – Vol. 1, no. 2. – P. 84-102.

24. Debar H. Towards a taxonomy of intrusion-detection systems / H. Debar, M. Dacier, A. Wespi // Computer Networks. – 1999. – Vol. 31. Issue 8. – P. 805-822.

25. Barford P., Kline J., Plonka D., Ron A. A signal analysis of network traffic anomalies // Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement. – 2002. – P. 71-82.

26. Denning D.E. An Intrusion-Detection Model // IEEE Transactions on software engineering, 1987. – Vol. SE-13, Issue 2. – P. 222-232.

27. Lee W., Xiang D. Information-theoretic measures for anomaly detection // Security and Privacy. – 2001. – P. 130-143.

28. Krylov V.V., Samokhvalova V.V. Teoriya teletrafika i ee prilozheniya [Teletraffic Theory and Its Applications]. // SPb.: BHV-Petersburg. – 2005. – 288 p.

29. Mazurek M., Dymora P. Network anomaly detection based on the statistical self-similarity factor for HTTP protocol. // Przeglad elektrotechniczny. – 2014. – P. 127-130.

30. Lee K., Kim J., Kwon K.H., Han Y., Kim S. DDoS attack detection method using cluster analysis. // Expert Systems with Applications. – 2008. – Vol. 34. – Issue 3. – P. 1659-1665.

31. Ершов В.А. способы организации и методы противодействия DoS/DDoS-атакам / В.А. Ершов, У.В. Михайлова // Безопасность информационного 159 пространства: Сборник трудов XIII Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных, 2015. – С. 73-79.

32. Aleksander M. Features of Denial of Service Attacks in Information Systems / M. Aleksander // Computer and mathematical methods in modeling. – 2012. – Vol. 2. – № 2. – 129-133 с.

33. Karpinski M.P. Modeling network traffic computer network in implementation attacks such as DOS/DDOS. / M.P. Karpinski // Information Security, American Psychological Association. Ethical standards of psychologists. Washington, DC: American Psychological Association. – 2011. – №1 (5). – P. 143-146.

34. Шелухин О.И. Самоподобие и фракталы. Телекоммуникационные приложения / О.И. Шелухин, А.В. Осин, С.М. Смольский. – М.: ФИЗМАЛИТ, 2008. – 368 с. – ISBN 978-5- 9221-0949-9.

35. Кучук Г.А. Аналіз та моделі самоподібного трафіка / Г.А. Кучук, О.О. Можаев, О.В. Воробьев // Авиационно-космическая техника и технология. – 2006. – № 9 (35). – С. 173-180.

36. Leland W. On the selfsimilar nature of IP-trafic / W. Leland, M. Taqqu, W. Willinger // IEEE/ACM Transactions on Networking. – 1997. – № 3. – P. 423-431.

37. Гетьман А.И. Анализ сетевого трафика в режиме реального времени: обзор прикладных задач, подходов и решений / А.И. Гетьман, Ю.В. Маркин, Е.Ф. Евстропов, Обыденков Д.О. – Труды ИСП РАН, 2017. – Т.29(3). – С.117-150.

38. Кучук, Г.А. Фрактальный анализ процессов, структур и сигналов / Г.А. Кучук, А.А. Можаев, К.М. Руккас // Коллективная монография под ред. Р.Е. Пащенко – Х.: ЭкоПерспектива, 2006. – 360 с.

39. Шелухин О.И. Анализ изменений фрактальных свойств телекоммуникационного трафика вызванных аномальными вторжениями / О.И.

Шелухин, А.А. Антонян // T-Comm: Телекоммуникации и транспорт. – 2014. – Т. 8. – № 6. – С. 61-64.

40. Xia Z. Enhancing DDoS Flood Attack Detection via Intelligent Fuzzy Logic / Z. Xia, S. Lu, J. Li., J. Tang // Informatica. – 2010. – N. 34. – PP. 497–507.

41. Molnar S., Vidacs A. Fractal Characterization of Network Traffic from Parameter Estimation to Application. – Ph. D. dissertation. – Budapest Univ. of Technology and Economics, Dept. of Telecommunications and Telematics. – Budapest, 2000.

42. Paxon V. Wide-area Traffic: The Failure of Poisson Modelling / V. Paxon, S. Floyd // IEEE/ACM Transactions on Networking. – 1995. – Vol. 3. – P. 226-244.

43. Kihong Park. The protocol stack and its modulating effect on self-similar traffic / Park Kihong, Kim Gitae, M.E. Crovella // Self-Similar Network Traffic Analysis and Performance Evaluation. – Wiley-Interscience, 1991.

44. Астахов А. Актуальные вопросы выявления сетевых атак [Електронний ресурс]. – URL: http://www.infosecurity.ru/_gazeta/content /030211/article07.html#art6.

45. Сычев В. Фрактальный анализ. Программа Fractan 4.4. – http:// impb.ru/~sychyov/.

46. Архів трафіку – URL: http://ita.ee.lbl.gov.

47. Takens F. Detecting Strange Attracto R/S in Turbulence // Dynamical Systems and Turbulence. - Lecture Notes in Mathematics. – Berlin: Springer – Verlag. – 1981. – Vol. 898. – P. 366-381.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	**Формат**	**Найменування**	**Кількість листів**	**Примітки**
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	28	
6	А4	Спеціальна частина	29	
7	А4	Економічний розділ	9	
8	А4	Висновки	2	
9	А4	Перелік посилань	5	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація Шляхов.ppt

2 Диплом Шляхов.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ Пілова Д.П.

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125м-20-1 Шляхова В.І. на тему: «Фрактальний аналіз трафіку в інформаційно-комунікаційних мережах для систем виявлення атак»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 87 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на визначення мережевих атак за допомогою фрактальних методів оцінки мережевого трафіку, що ґрунтуються на ознаках його самоподібності.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі дослідження систем виявлення атак та методів аналізу мережевого трафіку, а також його фрактальних властивостей в ній сформульовані задачі, вирішенню яких присвячений спеціальний розділ. У ньому було запропоновано підхід до визначення аномалій телекомунікаційного трафіку, що базується на розрахунку фрактальних параметрів та визначення фазового портрета та шляхом моделювання оцінено його ефективність.

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

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

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

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