Хмельницький національний університет

Факультет інформаційних технологій

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Відельського Ярослава Володимировича

на здобуття ступеня вищої освіти Магістра

Метод виявлення прихованих каналів передачі у вихідному трафіку публічних мереж

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Освітня програма Кібербезпека та захист інформації

Шифр КРБКБЗІ. 240188.24.01.04 ПЗ

Виконав студент 2 курсу група КБЗІм-24-1 _____ Ярослав ВІДЕЛЬСЬКИЙ

Керівник канд. техн. наук, доцент _____ Юрій КЛЬОЦ

Нормоконтролер д-р філософії, старший викладач _____ Наталія ПЕТЛЯК

До захисту допускаю:
Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

17 12 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Магістр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Освітня програма Кібербезпека та захист інформації

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

1 09 2025 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Відельському Ярославу Володимировичу

1 Тема роботи Метод виявлення прихованих каналів передачі у вихідному трафіку публічних мереж

Керівник роботи канд.техн.наук, доцент Юрій КЛЬОЦ

Затверджено наказом ректора університету від 25 08 2025 № 65

2 Строк подання студентом кваліфікаційної роботи на кафедру 1.12.2025

3 Вихідні дані до роботи Проаналізувати поняття прихованих каналів передавання даних та засоби їх виявлення. Дослідити особливості використання протоколу ICMP для прихованого тунелювання. Обрати параметри ICMP-пакетів та здійснити попередню обробку мережевого трафіку. Розробити метод виявлення прихованих каналів у вихідному ICMP-трафіку. Здійснити оцінку ефективності розробленого методу.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Аналіз прихованих каналів у мережевому трафіку. Постановка задачі. Формалізована модель ICMP Echo Request та його інформаційного навантаження. Метод виявлення прихованих каналів у ICMP-трафіку. Програмна реалізація методу. Розрахунок ефективності запропонованого методу.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 1 09 2025 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Ґрунтовне ознайомлення та дослідження предметної галузі	Лютий	Виконано
Визначення змісту, структури магістерської роботи	Березень	Виконано
Опрацювання першого розділу магістерської роботи	Квітень	Виконано
Опрацювання статті за результатами дослідження	Травень	Виконано
Опрацювання другого розділу магістерської роботи	Червень	Виконано
Опрацювання третього розділу магістерської роботи	Вересень	Виконано
Опрацювання четвертого розділу магістерської роботи	Жовтень	Виконано
Підготовка та опрацювання ілюстративного матеріалу	Листопад	Виконано
Оформлення магістерської роботи графічної та текстової частини	Листопад	Виконано
Попередній захист магістерської роботи	Листопад	Виконано
Захист магістерської роботи на засіданні ЕК	Грудень	Виконано

Студент _____ Ярослав ВІДЕЛЬСЬКИЙ

Керівник кваліфікаційної роботи _____ Юрій КЛЬОЦ

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод виявлення прихованих каналів передачі у вихідному трафіку публічних мереж

Автор роботи: студент групи КБЗІм-24-1 Відельський Я.В.

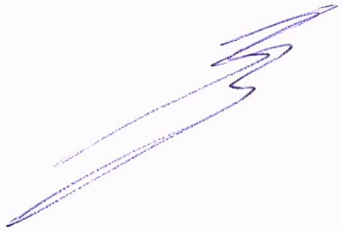
Керівник роботи: канд. техн. наук, доцент Кльоц Ю.П.

Загальний обсяг роботи: 89 сторінок, 5 рисунків, 8 таблиць, 37 формул, 1 додаток, 60 посилань.

Ключові слова: приховані канали, ICMP, мережевий трафік, ентропія Шеннона, стеганографія, аномалії, машинне навчання, автоенкодер, кібербезпека.

У роботі досліджено проблему виявлення прихованих каналів передавання даних у вихідному ICMP-трафіку публічних мереж, які можуть використовуватися для обходу засобів мережевої безпеки. Розроблено математичну модель ICMP Echo Request, у межах якої корисне навантаження розглядається як випадковий процес, та обґрунтовано використання ентропії Шеннона як критерію виявлення стеганографічних вставок. Запропоновано метод виявлення прихованих каналів на основі поєднання ентропійного аналізу та автоенкодерної моделі навчання без учителя. Реалізовано програмний засіб аналізу трафіку та проведено експериментальні дослідження на тестових наборах даних, які підтвердили ефективність методу, його здатність зменшувати кількість хибних спрацювань і виявляти приховані канали різної інтенсивності в умовах публічних мереж.

1.12.2025



ANNOTATION

Theme of qualification work: Method for detecting hidden transmission channels in outgoing traffic on public networks

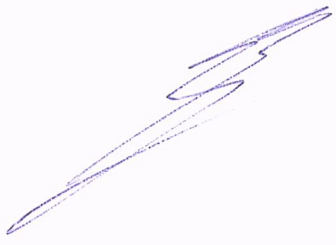
Author of the work: Student of group KBZIm-24-1, Y. V. Videlskyi

Mentor: PhD (Engineering), Associate Professor Yu. P. Klots

Total volume of work: 89 pages, 5 figures, 8 tables, 37 equations, 1 appendix, 60 references.

Keywords: covert channels, ICMP, network traffic, Shannon entropy, steganography, anomalies, machine learning, autoencoder, cybersecurity.

The thesis investigates the problem of detecting covert data transmission channels in the outbound ICMP traffic of public networks, which may be exploited to bypass network security mechanisms. A mathematical model of the ICMP Echo Request is developed, in which the payload is treated as a stochastic process, and the use of Shannon entropy as a criterion for detecting steganographic insertions is substantiated. A method for detecting covert channels based on the combination of entropy analysis and an unsupervised autoencoder model is proposed. A software tool for traffic analysis is implemented, and experimental studies are conducted on test datasets. The obtained results confirm the effectiveness of the proposed method, its ability to reduce the false positive rate, and its capability to detect covert channels of varying intensity under public network conditions.



ЗМІСТ

Вступ 7
1 Аналіз методів організації та виявлення прихованих каналів вихідного трафіку 9
1.1 Принципи побудови прихованих каналів у стеку TCP/IP 9
1.2 Аналіз вразливостей протоколу ICMP та можливостей тунелювання даних 20
1.3 Огляд відомих методів виявлення ICMP-тунелів 26
1.4 Статистичні методи аналізу вмісту пакетів 29
1.5 Постановка завдання 30
2 Математичні моделі та критерії виявлення аномалій у полі навантаження пакетів ICMP 32
2.1 Формалізована модель пакету ICMP Echo Request та його інформаційного навантаження 32
2.2 Моделювання процесу вбудовування прихованих даних у поле Payload 38
2.3 Обґрунтування вибору ентропії Шеннона як критерію виявлення стеганограми 41
2.4 Підготовка вихідних даних та формування навчальної вибірки 44
2.5 Визначення порогових значень ентропії для класифікації трафіку 47
2.6 Висновки до розділу 50
3 Метод виявлення прихованих каналів на основі ентропійного аналізу 52
3.1 Метод виявлення аномалій у вихідному ICMP-трафіку 52
3.2 Програмна реалізація засобу аналізу трафіку 54
3.3 Проведення експериментальних досліджень на тестових наборах даних 61
3.4 Оцінка ефективності методу 64
3.5 Висновки до розділу 69
Висновки 71
Перелік джерел посилань 73
Додаток А. Список праць 80

ВСТУП

Сучасний етап розвитку інформаційно-комунікаційних технологій характеризується стрімким зростанням обсягів мережевого трафіку, ускладненням його структури та широким упровадженням механізмів шифрування на транспортному і прикладному рівнях. Протоколи QUIC, TLS 1.3 та інші сучасні засоби захисту значно обмежили можливості традиційного глибинного аналізу пакетів, що ускладнило виявлення несанкціонованих форм обміну інформацією у публічних мережах. У таких умовах особливої актуальності набуває проблема прихованих каналів передавання даних, які використовуються для обходу політик безпеки, прихованого керування шкідливими агентами та ексфільтрації конфіденційної інформації.

Практика експлуатації мережевих інфраструктур свідчить, що приховані канали дедалі частіше реалізуються із використанням службових протоколів, зокрема ICMP, які зазвичай дозволені у більшості мереж для забезпечення діагностики та підтримки працездатності. Відсутність автентифікації, безстановий характер та гнучка структура ICMP-повідомлень створюють сприятливі умови для організації прихованого тунелювання, яке важко виявити за допомогою класичних сигнатурних або протокольних методів. Реальні інциденти кібербезпеки підтверджують використання ICMP-тунелів як каналу керування шкідливим програмним забезпеченням, особливо у середовищах із жорсткими обмеженнями на TCP- та UDP-трафік.

Додатковим ускладнюючим чинником є застосування мережевих засобів безпеки та NAT, які змінюють або нормалізують службові поля пакетів, але водночас не усувають можливість прихованого передавання даних у корисному навантаженні або часових характеристиках трафіку. Це призводить до того, що приховані канали можуть функціонувати тривалий час, маскуючись під легітимний службовий трафік і не викликаючи спрацювань стандартних систем моніторингу.

У зв’язку з цим актуальною є розробка методів виявлення прихованих

каналів, які не залежать від сигнатур, не потребують попереднього знання конкретних реалізацій тунелювання та здатні працювати в умовах високої варіативності мережевого середовища. Перспективним напрямом у цьому контексті є статистичний аналіз корисного навантаження ICMP-пакетів, зокрема використання ентропійних характеристик, що дозволяють кількісно оцінювати ступінь випадковості даних та виявляти аномалії, пов’язані зі стисненням або шифруванням прихованої інформації.

Сучасні тенденції розвитку засобів кіберзахисту також демонструють зростання ролі методів машинного навчання, особливо моделей навчання без учителя, які здатні формувати профіль нормальної поведінки трафіку та виявляти відхилення без потреби у розмічених даних. Поєднання ентропійного аналізу з автоенкодерними моделями відкриває можливість детектування як відомих, так і раніше невідомих схем прихованого передавання, що є критично важливим в умовах появи Zero-day технік тунелювання.

З огляду на наведене, дослідження методів виявлення прихованих каналів у вихідному трафіку публічних мереж, зокрема на основі ентропійного аналізу ICMP-пакетів і машинного навчання, є актуальним та практично значущим завданням. Результати такої роботи можуть бути використані для підвищення ефективності систем моніторингу мережевої безпеки, виявлення прихованих каналів ексфільтрації даних та посилення захисту інформаційних ресурсів у сучасних публічних мережах.

1 АНАЛІЗ МЕТОДІВ ОРГАНІЗАЦІЇ ТА ВИЯВЛЕННЯ ПРИХОВАНИХ КАНАЛІВ ВИХІДНОГО ТРАФІКУ

1.1 Принципи побудови прихованих каналів у стеку TCP/IP

Класифікація прихованих каналів у мережевих протоколах ґрунтується на характері модифікації трафіку та рівні стеку TCP/IP, на якому здійснюється приховане передавання даних. У науковій літературі виділяють два базові класи: канали, що використовують змістові характеристики пакетів, та канали, побудовані на основі тимчасових параметрів. Перший клас передбачає зміну полів заголовків, корисного навантаження або службових ознак протоколів таким чином, щоб вони містили додаткову інформацію, не порушуючи формальний синтаксис протоколу. Другий клас спирається на контроль інтервалів надходження пакетів або модифікацію їхньої частоти, створюючи часові патерни, які інтерпретуються як приховані символи [1,2].

Окрему групу становлять канали на основі семантичної надлишковості протоколів, де передавання даних здійснюється шляхом маніпуляцій поведінковими характеристиками мережевої взаємодії. Такі канали використовують альтернативні варіанти допустимих реакцій у протоколі або зміну параметрів, що не впливають на логічну завершеність сеансу зв'язку. У протоколах TCP та IP приховані канали можуть створюватися через модифікацію ідентифікаторів фрагментації, прапорців керування, чисел послідовності або зарезервованих полів, що рідко контролюються на проміжних маршрутизаторах [3].

Окремим різновидом є комбіновані канали, які поєднують вмістові та часові механізми для підвищення стійкості. Їхня ефективність полягає у здатності адаптуватись до фільтрації та варіативності мережевих умов. Завдяки цьому зловмисник може розподіляти дані між різними параметрами протоколів, що ускладнює побудову універсальних детекторів. Така класифікація дає змогу системно вибудувати підхід до аналізу прихованих каналів і визначити ті їхні властивості, які можуть бути використані для подальшого виявлення аномалій у

вихідному трафіку публічних мереж [4].

Механізми модифікації службових полів заголовків TCP/IP становлять один із найпоширеніших підходів до побудови прихованих каналів, оскільки більшість мережевих пристроїв опрацьовують ці поля формально, не здійснюючи глибокий семантичний аналіз. Базовим принципом є використання надлишкових, зарезервованих або слабко контрольованих параметрів, значення яких можна змінювати без порушення коректності функціонування протоколу. Це дає змогу приховано передавати інформацію у межах звичайного трафіку, зберігаючи зовнішню відповідність стандарту [5].

У заголовку IP-датаграми для таких цілей зазвичай застосовують поле ідентифікації фрагментів, значення якого можна систематично змінювати, кодувавши символи або цілі блоки даних. Оскільки більшість сучасних передавань не вимагає фрагментації, багато операційних систем генерують це поле за простими інкрементальними правилами, що полегшує побудову прихованого каналу. Інша можливість полягає у використанні поля фрагментації та прапорців MF або DF, які можуть бути навмисно модифіковані для генерації бітових послідовностей у випадках, коли фрагментація фактично не відбувається [6].

У протоколі TCP одним із найзручніших елементів є поле номерів послідовності. Через його високу варіативність внесення прихованих повідомлень може бути замасковане під особливості генерації псевдовипадкових значень, які використовуються більшістю стеків TCP. Такі канали мають достатню пропускну здатність, оскільки символи можуть бути передані з кожним сегментом. Водночас визначення таких змін у загальному випадку складна, оскільки при аналізі зовнішнього трафіку важко відокремити легітимну зміну номерів послідовності від навмисної [7].

Зарезервовані поля заголовка TCP також являють собою придатний носій прихованої інформації. Через відсутність активного використання більшістю стеків та мережевих пристроїв зміна їхніх значень майже не впливає на поведінку сеансу. Це робить такі поля зручними для прихованого каналу з низькою

інтенсивністю, що не порушує логіку з'єднання та часто ігнорується механізмами моніторингу [8].

Деякі варіанти прихованих каналів спираються на маніпуляції в полі TCP Flags. Хоча більшість значущих прапорців суворо регламентовані, комбінаторика їхніх значень залишається достатньо великою. Через це можливе кодування даних у послідовності встановлення окремих прапорців у контрольних сегментах. Проте такі методи обмежені тим, що відхилення від стандартної поведінки під час встановлення з'єднання може бути помітним, знижуючи стійкість до виявлення.

Окремим напрямом є використання опціональних полів TCP. Параметри, такі як Window Scale, Timestamp або інші опції, можуть містити приховані фрагменти інформації. Зокрема, поле TCP Timestamp може передавати довгі числові значення, що значно підвищує пропускну здатність прихованого каналу. Бракує чітких механізмів перевірки валідності таких значень, тому вони довго залишаються непоміченими у публічному трафіку [9].

Модифікація службових полів є ефективною також завдяки тому, що більшість мережевих пристроїв зосереджена на перевірці маршрутизації та передачі пакетів, а не на аналізі статистичних закономірностей значень службових заголовків. Це створює умови для побудови стійкого до виявлення каналу, здатного функціонувати тривалий час у високонавантажених мережах.

Загалом механізми модифікації службових полів заголовків TCP/IP залишаються одними з найгнучкіших методів побудови прихованих каналів. Їхня стійкість визначається варіативністю протоколів, відсутністю жорстких вимог до формування багатьох службових параметрів та значним обсягом легітимних коливань у поведінці трафіку. Саме ці властивості ускладнюють розроблення універсальних методів аналізу й потребують ретельного статистичного моделювання для подальшого виявлення аномалій.

Використання часових характеристик трафіку як носія прихованих даних ґрунтується на модифікації інтервалів між пакетами або їхньої частоти з метою кодування прихованих повідомлень без зміни структури протоколів. На відміну

від каналів, що змінюють службові поля заголовків, часові канали не порушують синтаксис мережевого пакета, а тому їхнє виявлення значно ускладнене. Передавання здійснюється через контроль ритму відправлення трафіку, що формує часові патерни, інтерпретовані приймальною стороною як бітові послідовності [10].

Основою таких каналів є можливість маніпуляції міжпакетними інтервалами у межах статистично допустимих відхилень. Зловмисник змінює час відправлення пакетів за заздалегідь узгодженими правилами: короткий інтервал може позначати один біт, довший інтервал інший. Через широкий діапазон природних коливань мережевих затримок такі відхилення важко відрізнити від легітимних флуктуацій, що характерні для публічних мереж з великою кількістю користувачів [11].

Інший механізм пов'язаний зі зміною інтенсивності потоків у визначених часових вікнах. Наприклад, встановлення високої або низької частоти передачі пакетів у певних періодах може відповідати бітам інформації. Цей метод є зручним під час використання протоколів, що формують значний обсяг періодичного трафіку, оскільки загальне навантаження мережі приховує додаткові часові зміни [12].

Деякі приховані канали використовують ритмічні шумові послідовності, накладені на звичайний трафік. Такі послідовності не мають явних структурних змін, проте зберігають часовий код, який може бути виділений за допомогою кореляційних методів на приймальній стороні. Наявність природних сплесків трафіку сприяє маскуванню таких каналів, а їхня стійкість підвищується за рахунок складності статистичного аналізу нестаціонарних часових процесів [13].

Особливу увагу привертають канали, що формуються шляхом навмисного створення затримок на рівні транспортного протоколу. Наприклад, у TCP можливе штучне варіювання часу підтверджень ACK, що створює додаткові тимчасові патерни. Мережеві засоби безпеки рідко контролюють регулярність ACK-повідомлень, тому такі канали можуть залишатися прихованими у значному обсязі трафіку (рис. 1.1).

Для підвищення стійкості прихованого каналу часто застосовують адаптивне кодування, коли часові параметри підлаштовуються під поточні характеристики мережі. Це ускладнює модель виявлення, оскільки статистичні методи повинні враховувати змінність міжпакетних інтервалів у різні періоди часу. Після адаптації канал здатний функціонувати на фоні високої варіативності затримок, що є типовим явищем для публічних мереж [14].

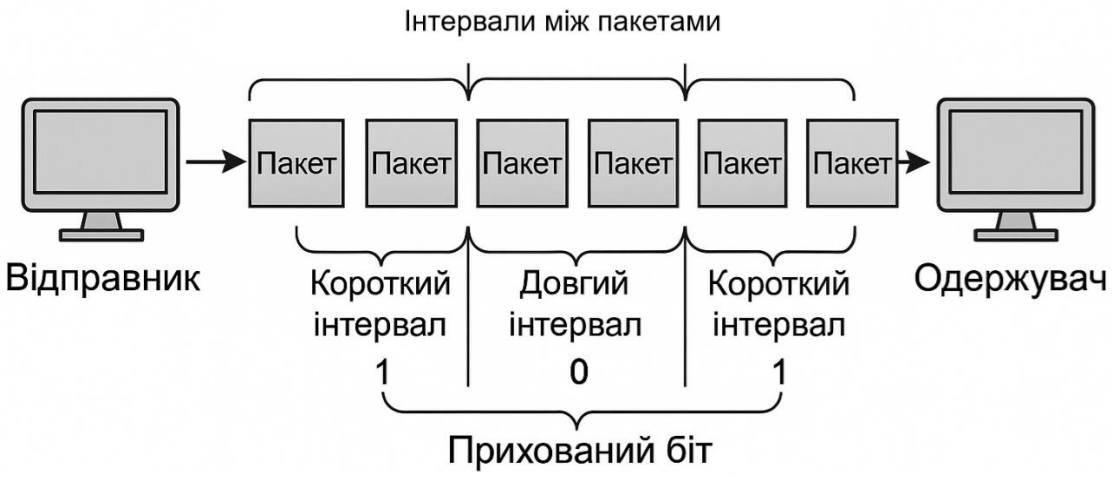


Рисунок 1.1 – Використання часових характеристик трафіку як носія прихованих даних

Загалом часові приховані канали вирізняються високою прихованістю, оскільки не змінюють жодного структурного елемента пакета. Їхнє виявлення базується на аналізі аномальних статистичних відхилень у часових кореляціях, проте складність моделювання реального трафіку значно обмежує точність існуючих детекторів. Це робить часові механізми одним із найскладніших для ідентифікації різновидів прихованих каналів.

Маніпуляції порядком фрагментації та збору пакетів ґрунтуються на використанні механізмів, передбачених стандартом IP для поділу великих датаграм на менші фрагменти. Ці механізми створюють додаткові ступені свободи, які можуть бути використані для прихованого передавання даних. Особливість такого підходу полягає в тому, що більшість сучасних мережевих стеків автоматично виконують фрагментацію і збір, тому зміни у структурі

фрагментів рідко аналізуються глибинно на проміжних вузлах (рис. 1.2).

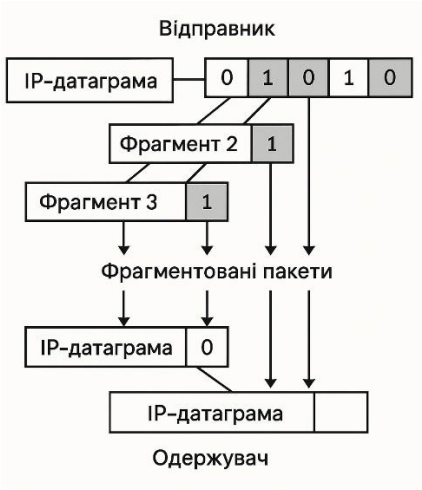


Рисунок 1.2 – Схема прихованого передавання даних шляхом маніпуляції порядком фрагментації та збору IP-пакетів

Базовим способом організації прихованого каналу є модифікація значень поля ідентифікатора фрагмента, яке використовується для групування фрагментів у межах однієї датаграми. Оскільки у сучасних мережах фрагментація трапляється відносно рідко, значення цього поля часто не контролюються з боку систем моніторингу. Зловмисник може кодувати дані, змінюючи значення ідентифікатора за певною схемою, а приймальна сторона зчитує їх у момент відновлення датаграми [15].

Іншим механізмом є маніпуляція величиною зсуву фрагментів. Стандарт допускає зміну порядку, у якому фрагменти передаються, оскільки коректність передачі забезпечується шляхом їхнього подальшого збирання на приймальному хості. Це створює можливість кодування прихованих бітів у самому порядку надходження фрагментів. Наприклад, перестановка певних фрагментів може інтерпретуватися як окремі символи прихованого повідомлення.

Маніпуляції прапорцями MF та DF також можуть бути використані для прихованого каналу. Прапорець MF дозволяє індикувати, що фрагмент не є останнім, а його неконсистентна зміна може кодувати приховану інформацію. Прапорець DF, навпаки, сигналізує про заборону фрагментації. Контрольована

зміна його стану дозволяє створити малопомітний бітовий канал, заснований на поведінкових відмінностях у процесі маршрутизації [16].

Окремі канали використовують навмисне створення помилкових або некоректних фрагментів, які неможливо коректно зібрати. Такі фрагменти можуть бути відкинуті приймальною стороною, проте на стороні зловмисника вони зчитуються до моменту обробки. Цей тип каналів складний у реалізації, проте дозволяє передавати дані без впливу на легітимний трафік.

Ще одним варіантом є зміна розміру фрагментів за певним законом. Значення розміру може кодувати символ або його частину, а оскільки мережеві пристрої зазвичай не перевіряють закономірність вибору розміру фрагмента, такі зміни залишаються непомітними. Нестандартна схема поділу датаграми може бути виявлена лише за умови порівняння з типовою поведінкою конкретного стеку TCP/IP [17].

Стійкість прихованих каналів, що використовують фрагментацію, обумовлена відсутністю регулярного аналізу кореляцій між ідентифікаторами, зсувами та послідовністю надходження фрагментів. Більшість систем виявлення вторгнень орієнтована на відстеження фрагментації лише у контексті відомих атак, а не як джерела потенційного прихованого каналу. Це створює додаткове поле для експлуатації в умовах публічних мереж.

Таким чином, маніпуляції порядком фрагментації та збору пакетів формують високопотенційний і важковиявний механізм прихованого передавання даних. Його протидія вимагає детального статистичного аналізу фрагментних структур, що ускладнено значною варіативністю реалізацій стеків протоколів у різних операційних системах та мережевих пристроях [18-19].

Вбудовування даних у надлишкові та зарезервовані поля протоколів базується на використанні службових елементів пакетів, які або не застосовуються у типовій мережевій взаємодії, або не мають чітко визначеного значення в конкретних реалізаціях стеку TCP/IP. Наявність таких полів є історичним наслідком розвитку протоколів і забезпечення їхньої зворотної сумісності. Через обмежений контроль з боку мережевих пристроїв ці поля

залишаються придатними для прихованого розміщення інформації без порушення коректності обробки трафіку [20].

У заголовку TCP зарезервовані біти, передбачені стандартом для майбутнього використання, фактично не перевіряються під час проходження через мережу. Вони можуть містити довільні значення, що дозволяє передавати приховані бітові послідовності з мінімальним ризиком виявлення. Мережеві аналізатори переважно ігнорують ці біти через їхню відсутність у функціональній логіці протоколу, тому такі приховані канали є стійкими на фоні великого трафічного потоку.

Опціональні поля TCP, зокрема Timestamp, Window Scale або інші розширення, мають значну змінність і допускають широкі діапазони значень. Зловмисник може кодувати інформацію у зміні цих параметрів, зберігаючи загальну узгодженість сеансу. Оскільки опції часто застосовуються різними операційними системами з відмінними схемами їхнього заповнення, ані детектування, ані моделювання їхньої типової поведінки не є тривіальним завданням [21].

У протоколі IP надлишковими є деякі службові характеристики, наприклад поле ідентифікації, яке за відсутності фрагментації не має критичного функціонального значення. Його значення можуть бути довільними й не впливають на цілісність передачі, що відкриває можливість для прихованого каналу. Оскільки перевірка консистентності цього поля здійснюється лише під час збирання фрагментів, його використання для прихованого передавання часто залишається непоміченим [22].

Перевага вбудовування в надлишкові та зарезервовані поля полягає у високій прозорості такого каналу, оскільки дані вбудовуються без зміни логіки формування пакетів. Унаслідок цього під час маршрутизації не виникає жодних аномалій, які могли б привернути увагу систем моніторингу. Проте виявлення таких каналів можливе через статистичний аналіз відхилень від типових значень, властивих конкретним реалізаціям стеку TCP/IP, що стає актуальним напрямом досліджень у сфері мережевої безпеки [23].

Обмеження пропускної здатності та стійкості прихованих каналів у публічних мережах визначаються сукупністю технічних, топологічних та поведінкових факторів, які впливають на можливість стабільного передавання прихованих даних у середовищі з високою варіативністю параметрів трафіку. Пропускна здатність прихованого каналу зазвичай значно нижча за пропускну здатність легітимного з'єднання, оскільки методи приховування вимагають мінімізації відхилень від типової поведінки протоколу. Навіть незначні зміни у значеннях службових полів або часових характеристиках, якщо вони повторюються з високою частотою, можуть стати підставою для виявлення, що примушує зловмисника знижувати інтенсивність передавання [24].

Публічні мережі характеризуються значною непередбачуваністю трафіку, зокрема флуктуаціями затримок, коливанням навантаження, маршрутними змінами та впливом NAT. Ці чинники знижують стійкість прихованих каналів, особливо тих, що спираються на часові характеристики або порядок доставки пакетів. Невизначеність транспортного середовища призводить до спотворення прихованих символів, потребує складних схем корекції помилок і зменшує ефективність прихованого передавання [25].

Важливим фактором обмежень є поведінка мережевого обладнання, яке може модифікувати або нормалізувати службові поля пакетів. Маршрутизатори, брандмауери, DPI-системи та NAT-шлюзи нерідко перезаписують TTL, ідентифікатори фрагментації, TCP-прапорці, опціональні поля та інші параметри, що знижує або повністю нівелює можливість прихованого каналу. Механізми оптимізації та балансування навантаження також порушують передбачуваність доставки пакетів, що обмежує стабільність каналу [26].

З погляду тривалості функціонування прихованого каналу у публічних мережах ключовим обмеженням є ймовірність його статистичного виявлення. Оскільки більшість прихованих каналів ґрунтується на порушенні належних розподілів значень протоколів, довготривале функціонування підвищує накопичення статистичних відхилень. Це створює сприятливі умови для алгоритмів аномалій, які здатні виявити не окремі викривлення, а їхні

закономірності у великих часових вибірках [27].

Загалом пропускна здатність прихованих каналів обмежена необхідністю маскування, а їхня стійкість – залежністю від параметрів середовища та поведінки мережевої інфраструктури. У публічних мережах, які характеризуються динамічністю, наявністю різнорідного обладнання та активним мережевим моніторингом, приховані канали існують у умовах постійного ризику викривлення та детектування, що значно зменшує їхню практичну ефективність.

Вплив мережевих засобів безпеки та NAT на можливість функціонування прихованого каналу є визначальним фактором, що формує як технічні обмеження, так і варіанти адаптації прихованих механізмів. Більшість сучасних мережевих інфраструктур використовує багаторівневі засоби контролю трафіку, включно з брандмауерами, системами DPI, IPS та проксі-модулями, які здатні модифікувати, нормалізувати або відкидати пакети. Ці елементи впливають на стійкість прихованих каналів, змінюючи значення службових полів, порушуючи часові патерни або перериваючи нестандартні мережеві взаємодії. Унаслідок цього приховані канали повинні пристосовуватися до поведінки мережевих засобів безпеки, що суттєво звужує можливий діапазон технік приховування [28].

Механізми глибокого аналізу пакетів здатні виявляти аномалії в заголовках TCP/IP, нетипові значення опціональних полів, неконсистентні патерни фрагментації, нестандартні цикли формування ACK-пакетів і відхилення в межах протоколів ICMP. Хоча більшість DPI-рішень орієнтована на виявлення відомих атак, неприродна поведінка протоколів може випадково потрапляти в аномальний профіль та викликати блокування. Це знижує ймовірність тривалого існування вмістових прихованих каналів, оскільки навіть слабкі відхилення від очікуваних параметрів можуть бути придушені на рівні мережевої політики [29].

NAT створює додатковий рівень ускладнень для функціонування прихованих каналів. Під час трансляції адрес і портів NAT-пристрої

перезаписують ключові параметри пакетів, що може знищити частину прихованої інформації або спотворити структуру каналу. Поля TCP або IP, які використовуються для кодування прихованих даних, можуть бути змінені через рекалькуляцію контрольних сум, перепризначення джерельних портів або нормалізацію фрагментації. Тому канали, які спираються на статичність заголовків, мають низьку стійкість у середовищах із багаторівневим NAT [30].

У контексті часових прихованих каналів NAT і мережеві засоби безпеки також відіграють критичну роль. Будь-які операції, пов’язані з чергуванням пакетів, балансуванням навантаження, гальмуванням підозрілих потоків або повторною передачею, спотворюють часові характеристики, що використовуються для кодування прихованих символів. Коли часовий профіль трафіку проходить через маршрутизатори з буферизацією або пристрої із захистом від DDoS-атак, він зазнає неконтрольованих варіацій, які можуть повністю руйнувати канал або вимагати дуже низької швидкості передачі для збереження коректності декодування [31].

Окремий вплив мають механізми нормалізації трафіку, які застосовуються системами IDS/IPS. Вони призначені для приведення пакетів до формату, передбаченого стандартами, а тому відкидають або виправляють аномальні послідовності фрагментів, некоректні флаги TCP, зайві опції або нетипові значення службових полів. Це унеможливлює використання значної частини прихованих каналів, побудованих на мінімальних відхиленнях від TCP/IP-специфікацій [32].

Таким чином, мережеві засоби безпеки та NAT істотно обмежують функціонування прихованих каналів, зменшуючи їхню пропускну здатність, порушуючи цілісність передаваних символів та скорочуючи час їхнього безпечного існування. Використання прихованих каналів у публічних мережах потребує врахування поведінки цих елементів інфраструктури, а також застосування адаптивних методів кодування, що підлаштовуються під мережеві трансформації.

1.2 Аналіз вразливостей протоколу ICMP та можливостей тунелювання даних

Протокол ICMP є допоміжним компонентом стеку TCP/IP, призначеним для обміну діагностичними та контрольними повідомленнями між вузлами мережі. Його основним завданням є індикація помилок, інформування про недоступність маршруту, перевищення часу життя пакета, порушення параметрів фрагментації та інших аномалій, що виникають під час передавання IP-датаґрам. ICMP не забезпечує передавання користувацьких даних, проте відіграє критичну роль у підтриманні коректної роботи транспортних та мережевих протоколів, дозволяючи визначати стан мережевої інфраструктури та реагувати на відхилення [33].

Структура ICMP-повідомлення побудована поверх IP-протоколу, де ICMP функціонує як частина мережевого рівня. Кожне повідомлення має заголовок, що містить тип, код та контрольну суму, а також змінну частину, яка залежить від конкретного типу ICMP. Тип визначає категорію повідомлення, наприклад Echo Request, Echo Reply, Time Exceeded або Destination Unreachable, тоді як код деталізує причину події. Така формалізована структура дозволяє ICMP забезпечувати єдиний механізм обміну діагностичною інформацією у різних реалізаціях стеку [34].

Особливістю ICMP є те, що він не має засобів встановлення або підтримання стану з'єднання. Через цю безстанову модель ICMP легко проходить більшість мережевих меж, зокрема маршрутизатори та фільтрувальні політики, орієнтовані на транспортні протоколи. Унаслідок цього ICMP традиційно використовується як механізм для перевірки доступності хостів, але саме ця властивість створює передумови для потенційної експлуатації протоколу у прихованих каналах [35].

Інформаційна структура ICMP передбачає наявність полів, що залежать від типу повідомлення. Наприклад, у Echo Request та Echo Reply існує поле ідентифікатора та номера послідовності, а також довільне корисне

навантаження, яке в типових реалізаціях використовується для тестових даних. Ця змінна частина не має жорстких вимог до вмісту, що робить її потенційним контейнером для несанкціонованого передавання, якщо контроль її розміру та змісту не здійснюється спеціальними засобами [36, 37].

Узагальнюючи, ICMP має чітко визначене діагностичне призначення та гнучку структуру, що дозволяє адаптувати повідомлення до різних ситуацій у мережевій взаємодії. Проте відсутність механізмів автентифікації, шифрування чи контролю цілісності, а також загальна поблажливість мережевих фільтрів до ICMP-трафіку створюють потенціал для його використання зловмисниками. Саме поєднання службового значення та структурної гнучкості робить ICMP одним із найуразливіших протоколів щодо прихованого тунелювання даних.

Вразливі елементи ICMP-повідомлень, придатні для прихованого передавання, ґрунтуються на структурних характеристиках протоколу та відсутності суворого контролю з боку більшості мережевих пристроїв. Одним із ключових аспектів є наявність змінної частини повідомлення, яку стандарт дозволяє заповнювати довільними даними. У випадку Echo Request та Echo Reply ця частина часто містить байти, що не перевіряються під час проходження через маршрутизатори або брандмауери. Така варіативність структури створює можливість розміщення прихованих бітів без порушення функціональності протоколу [38].

Ідентифікатор та номер послідовності у ICMP Echo-повідомленнях також можуть використовуватися як носії прихованих даних. У типовій реалізації ці значення застосовуються для зіставлення запитів та відповідей, проте жодних обмежень щодо їхнього діапазону чи закономірності зміни немає. Маніпуляції з цими полями майже завжди залишаються непоміченими, оскільки більшість мережевих пристроїв не аналізує їхню поведінку, а системи моніторингу фокусуються переважно на частоті ICMP-трафіку, а не на його вмісті [39].

Додаткову вразливість становлять поля типу та коду. Хоча структура цих полів чітко визначена стандартом, деякі типи ICMP-повідомлень використовуються рідко. У таких випадках зміна значень може бути

інтерпретована приймальним вузлом як частина прихованого протоколу взаємодії. Наприклад, послідовність рідковживаних типів, що надходять у певному порядку, може виконувати роль каналу сигналізації між зловмисником і прихованим агентом у мережі [40].

Корисне навантаження ICMP, що не має строгих вимог до своєї структури, представляє найзручніший механізм тунелювання. Його вміст не піддається глибокому аналізу у більшості комерційних DPI-рішень, оскільки ICMP традиційно вважається службовим протоколом. Це дозволяє передавати фрагменти тексту, ключі, команди або інші дані в компактному вигляді, маскуючи їх під діагностичні пакети. У деяких модифікаціях ICMP-тунелювання навіть використовується стиснення або шифрування, що додатково ускладнює виявлення [41].

Загальна відсутність механізмів автентифікації та контролю цілісності у ICMP сприяє використанню протоколу для прихованих каналів. Оскільки ICMP не має стану, а його повідомлення не прив’язуються до транспортних сесій, приховане передавання може відбуватися у формі односпрямованих або розсинхронізованих потоків, які важко корелювати з легітимною активністю. Такий дизайн дозволяє зловмиснику використовувати ICMP як низькорівневий транспорт для непомітної взаємодії навіть у сегментах мережі з активною фільтрацією та обмеженнями на інші протоколи [42].

Техніки ICMP-тунелювання та їхні практичні реалізації ґрунтуються на властивостях ICMP як службового протоколу, який здебільшого пропускається мережевими фільтрами та не піддається глибокій інспекції. Базовий принцип полягає у використанні ICMP Echo Request та Echo Reply для інкапсуляції довільних даних у корисне навантаження. Оскільки структура цих повідомлень не вимагає фіксованого вмісту, зловмисник може розміщувати у них блоки інформації, які зчитуються на приймальному боці і формують прихований двобічний канал [43].

Однією з класичних технік є ICMP-tunnel, що реалізує повноцінний двосторонній сеанс командного доступу поверх Echo-пакетів. Застосунок на

стороні клієнта упаковує TCP- або файлові дані у внутрішній формат і передає їх у полі payload, тоді як серверна частина декодує ці дані та генерує відповідь аналогічним способом. Завдяки відсутності транспортного сеансу ICMP-тунель може функціонувати навіть у мережах, де заблоковані порти TCP та UDP, що робить його привабливим інструментом для обходу політик безпеки [44].

Інший механізм полягає в організації односпрямованих каналів, де дані передаються лише в одному напрямку. Це застосовується у сценаріях, де відправник не потребує отримувати відповіді. В таких реалізаціях ICMP може використовуватись для прихованого логування або передачі даних з інфікованого вузла на зовнішній сервер. Оскільки односпрямований канал генерує лише вихідний трафік, він складніше ідентифікується алгоритмами кореляційного аналізу [45].

У деяких варіантах ICMP-тунелювання використовується стиснення або шифрування для підвищення ефективності та прихованості. Стиснення дозволяє передавати більші обсяги інформації через обмежений розмір ICMP payload, а шифрування робить неможливим простий аналіз вмісту навіть за умови DPI. У відкритих інструментах, таких як Ptunnel або Loki, шифрування застосовується для запобігання виявленню сигнатурами IDS, які можуть розпізнавати характерні патерни незашифрованого тунелю [46].

Цікавою реалізацією є поєднання ICMP-тунелювання з методами обходу NAT. Оскільки більшість NAT-пристроїв дозволяє ICMP Echo-трафік для підтримки діагностики, тунель може бути встановлений через межу приватної мережі без відкриття додаткових портів. При цьому клієнт на внутрішній стороні ініціює запити, а зовнішній сервер відповідає, зберігаючи ілюзію стандартної мережевої взаємодії. Така техніка дозволяє організувати канал командного керування навіть у суворо сегментованих інфраструктурах [47].

Основні техніки тунелювання представлені в таблиці 1.1.

Таблиця 1.1. Основні техніки ICMP-тунелювання

Характеристика	Вбудовування даних у ICMP Echo	Повноцінний ICMP-тунель	Односпрямований ICMP-канал	ICMP зі стисненням або шифруванням	NAT-прохідне ICMP-тунелювання
Механізм роботи	Інкапсуляція даних у payload Echo-повідомлень	Упаковка TCP/файлів у ICMP Echo з декодуванням	Вихідні односторонні Echo-запити з даними	Стиснення або шифрування вмісту payload	Використання дозволених Echo-пакетів для проходження NAT
Призначення / можливості	Двосторонній прихований канал	Прихований доступ і перенаправлення протоколів	Ексфільтрація даних	Обхід DPI, прихованість структури трафіку	Приховане C2 у сегментованих мережах
Приклади реалізацій	ICMP-tunnel, icmpsh	Ptunnel, Loki	Агентні модулі у шкідливому ПЗ	Ptunnel (AES), Loki-mod	Модифіковані icmpsh-клієнти
Обмеження	Може бути помітним через великий payload	Залежність від стабільності та MTU	Відсутність підтвердження доставки	Аномальна ентропія payload	Обмеження NAT, ICMP rate-limit
Типи ICMP	Echo Request (Type 8), Echo Reply (Type 0)	Echo Request/Reply	Echo Request	Echo Request/Reply	Echo Request/Reply
Швидкість каналу	Низька, кілька КБ/с	Низька - середня	Дуже низька, сотні байт/с	Низька - середня	Низька, додатково обмежена NAT

У сукупності ICMP-тунелювання демонструє значну гнучкість і здатність адаптуватися до різних мережевих середовищ. Його практичні реалізації широко використовуються у шкідливому ПЗ та інструментах тестування проникнення, оскільки ICMP часто залишається єдиним доступним протоколом у сильно фільтрованих мережах. Саме це зумовлює необхідність розроблення точних методів виявлення аномалій у структурі та поведінці ICMP-трафіку.

Обмеження, ризики та детектування прихованого каналу в ICMP-трафіку визначаються особливостями структури протоколу, його діагностичним

призначенням та відсутністю жорстких механізмів контролю на більшості мережевих сегментів. Головним обмеженням є низька пропускна здатність ICMP-тунелювання, оскільки корисне навантаження Echo-повідомлень має обмежений розмір, а підвищення частоти пакетів може викликати аномальну активність, помітну системам моніторингу. Крім того, ICMP-трафік часто піддається rate-limit політикам на маршрутизаторах та NAT-шлюзах, що додатково зменшує ефективність прихованих каналів [48].

Суттєвим ризиком є висока варіативність мережевого середовища. Будь-які зміни маршрутизації, буферизація на проміжних вузлах, перевантаження каналу або застосування DPI-систем можуть спотворювати структуру ICMP-повідомлень чи їхню частотну характеристику. Це призводить до втрати прихованих даних або необхідності складної повторної передачі. Оскільки ICMP не забезпечує механізмів контролю стану та корекції помилок, прихований канал може бути нестабільним у реальних публічних мережах [49].

З точки зору безпеки ризики пов’язані з тим, що ICMP може використовуватися для організації прихованих каналів керування шкідливим ПЗ. У таких випадках він слугує транспортом для передачі команд, конфігураційних файлів, ключів шифрування або невеликих блоків даних. Через те, що ICMP часто дозволений у корпоративних мережах для діагностики, тунелювання має підвищену ймовірність залишатися непоміченим за відсутності цілеспрямованого моніторингу [50].

Виявлення прихованих ICMP-каналів зазвичай ґрунтується на аналізі статистичних відхилень від типового трафіку. Одним із підходів є перевірка ентропії payload, яка у випадку шифрованих або стиснених тунелів істотно відрізняється від випадкових тестових даних, що зазвичай містяться у ICMP Echo. Іншим методом є аналіз міжпакетних інтервалів, які можуть утворювати характерний ритм при наявності прихованого каналу. Також застосовується перевірка коректності значень ідентифікаторів та номерів послідовності, що виявляє аномальні закономірності [51].

Ще одним напрямом детектування є застосування поведінкових та машинних

моделей, які будують профілі нормальної активності ICMP-трафіку у конкретному середовищі. Такі моделі здатні виявляти слабкі відхилення у частоті запитів, довжині пакетів чи співвідношенні типів ICMP-повідомлень. У поєднанні з DPI вони дозволяють виявляти складні тунелі, що використовують шифрування або маскування. Таким чином, ефективне виявлення прихованих ICMP-каналів потребує комплексного аналізу структури, статистики та поведінки трафіку, оскільки ізольовані показники рідко дають однозначний результат [52].

1.3 Огляд відомих методів виявлення ICMP-тунелів

Сигнатурні та протокольні підходи до виявлення ICMP-тунелювання базуються на пошуку відомих шаблонів, аномальних структур та відхилень від специфікацій ICMP. Сигнатурні методи використовують наперед визначені ознаки, характерні для типових інструментів ICMP-тунелювання, таких як нестандартні розміри payload, повторювані патерни байтів, характерні послідовності ідентифікаторів або незвичні кореляції між Echo Request та Echo Reply. Подібні методи застосовуються в IDS/IPS-системах, де сигнатури дозволяють розпізнавати вже відомі реалізації тунелів, але не забезпечують виявлення нових або модифікованих технік [53].

Протокольний аналіз орієнтований на контроль відповідності ICMP-повідомлень офіційним стандартам. Він передбачає перевірку коректності заповнення службових полів, перевірку валідності типів і кодів, а також аналіз структури повідомлення відповідно до RFC. Будь-які невідповідності, наприклад аномально велике корисне навантаження, несинхронні значення ідентифікатора або нетипові комбінації ICMP-параметрів, розглядаються як ознака тунелювання. Цей підхід є ефективним проти каналів, що спотворюють протокол, але малоефективний у випадках, коли тунель повністю дотримується специфікації [54].

Суттєвим елементом протокольного детектування є контроль поведінкових характеристик ICMP. Зокрема, аналізується частота запитів, регулярність їхнього

надходження, співвідношення між типами Echo Request та Echo Reply, а також часові параметри. У звичайних умовах ICMP використовується рідко та нерегулярно, тоді як приховані канали потребують стабільного потоку пакетів певної довжини. Виявлення подібних закономірностей дозволяє розпізнати тунель навіть за відсутності чіткої сигнатури [55].

Обмеження сигнатурних та протокольних методів пов'язані з їхньою низькою адаптивністю. Тунелі, що використовують динамічні стратегії маскування, шифрування або статистичну варіативність полів, часто залишаються непоміченими. Крім того, легітимні застосунки інколи генерують ICMP-повідомлення з нетиповими параметрами, що може спричиняти хибні спрацювання. Незважаючи на це, сигнатурні та протокольні підходи залишаються фундаментальною частиною систем мережевого моніторингу, забезпечуючи швидке виявлення поширених і невдало замаскованих тунелів.

Статистичні та поведінкові моделі аналізу ICMP-трафіку базуються на порівнянні фактичних параметрів трафіку з еталонними характеристиками, притаманними нормальній роботі мережі. На відміну від сигнатурних методів, вони не потребують наявності наперед відомих шаблонів тунелювання, а визначають відхилення від статистично сформованої моделі. Ключовими характеристиками для аналізу є довжина ICMP-пакетів, ентропія корисного навантаження, розподіл міжпакетних інтервалів та співвідношення типів ICMP. Наявність стійких аномальних патернів, таких як регулярні або надмірно великі Echo-пакети, може свідчити про роботу прихованого каналу [56].

У межах статистичного підходу застосовуються методи аналізу варіаційних і кореляційних характеристик. Наприклад, моделювання нормального профілю ICMP шляхом обчислення середнього розміру пакетів і дисперсії дозволяє визначити відхилення, властиві стисненим або шифрованим тунелям. Ентропійний аналіз дає змогу виявляти вміст із високою випадковістю, характерний для шифрованих ICMP-повідомлень. У публічних мережах нормальний ICMP-трафік рідко має високу ентропію, тому навіть слабкі відхилення можуть бути діагностичними [57].

Поведінкові моделі орієнтовані на аналіз динаміки ICMP-трафіку у часі. Природне використання протоколу зазвичай має нерегулярний та низькоінтенсивний характер, тоді як ICMP-тунелювання створює стабільні та передбачувані патерни надходження пакетів. Поведінковий аналіз використовує часові ряди, ковзні вікна та алгоритми порогового виявлення для визначення надлишкової повторюваності або циклічності. Такі методи ефективні проти тунелів, що передають дані з фіксованою частотою або вимагають синхронізації [58].

Удосконалені статистичні та поведінкові методи часто поєднують кілька різних характеристик, формуючи багатовимірний профіль ICMP-трафіку. Це дозволяє виявляти навіть добре замасковані канали, які не порушують окремі параметри протоколу, але створюють комплексні аномалії у структурі та поведінці трафіку. Використання таких моделей суттєво підвищує точність детектування, проте вимагає накопичення історичних даних і ретельної адаптації до конкретного мережевого середовища, оскільки надмірна чутливість моделей може спричиняти хибні спрацювання.

Методи машинного навчання та адаптивні алгоритми детектування прихованих ICMP-каналів ґрунтуються на використанні моделей, здатних автоматично виділяти складні закономірності у трафіку та адаптуватися до змін у мережевому середовищі. На відміну від статичних сигнатурних і протокольних підходів, машинне навчання дозволяє аналізувати багатовимірні профілі діяльності, враховувати взаємозв’язки між різними параметрами ICMP-пакетів і виявляти нетривіальні аномалії, неочевидні під час класичного аналізу. Такі моделі здатні працювати з великими вибірками даних, формуючи представлення про нормальну поведінку трафіку та ідентифікуючи приховані відхилення.

Поширеними є методи класифікації, які навчаються на розмічених даних та дозволяють розпізнавати ICMP-тунелювання за характеристиками пакетів. До таких методів належать деревоподібні моделі, лінійні класифікатори та ансамблеві алгоритми, які здатні виявляти характерні ознаки прихованого каналу, включно зі збільшеною ентропією payload, аномальними розмірами пакетів, нетиповою частотою Echo-повідомлень або стабільністю міжпакетних

інтервалів. Проте їхня ефективність залежить від якості навчальної вибірки: моделі можуть оминути нові техніки тунелювання, що не представлені у даних.

Методи без учителя, зокрема кластеризація та пошук аномалій, є придатними для виявлення ICMP-тунелів у ситуаціях, коли розмічені дані недоступні. Алгоритми, такі як Isolation Forest, One-Class SVM або DBSCAN, формують узагальнений профіль нормального трафіку та визначають аномалії без попереднього знання про конкретні техніки тунелювання. Такі підходи ефективні у динамічних мережах, де характер трафіку постійно змінюється, а класичних шаблонів недостатньо для детектування прихованих каналів.

Адаптивні алгоритми мають здатність оновлювати свої параметри в реальному часі, реагуючи на зміни у структурі ICMP-трафіку. Вони застосовують ковзні вікна, інкрементальне навчання або механізми самооновлення, що забезпечує їх стійкість до маскування тунелів і здатність функціонувати в умовах публічних мереж зі значною варіативністю. Завдяки цьому адаптивні моделі можуть виявляти канали, що змінюють інтенсивність, структуру payload або часові характеристики, намагаючись уникнути статистичних перевірок. Таким чином, використання методів машинного навчання робить систему детектування значно гнучкішою та точнішою, дозволяючи розпізнавати як класичні, так і новітні форми прихованого ICMP-тунелювання.

1.4 Статистичні методи аналізу вмісту пакетів

Моделі оцінювання ентропії корисного навантаження пакетів базуються на кількісному аналізі ступеня випадковості байтових послідовностей, що містяться у мережевих пакетах. Ентропія є однією з фундаментальних характеристик, яка відображає непередбачуваність даних, і тому широко використовується для виявлення шифрування, стиснення та інших форм приховування інформації. У звичайному мережевому трафіку більшість протоколів має структуроване та передбачуване корисне навантаження, тоді як приховані канали, особливо ICMP-

тунелі, часто демонструють підвищену ентропію, пов’язану зі стислими або зашифрованими даними.

При оцінюванні ентропії застосовуються як класичні моделі Шеннона, так і модифіковані варіанти, що враховують локальні особливості даних. Обчислення базується на аналізі частот появи окремих символів або їхніх комбінацій у payload, що дозволяє визначати випадковість на основі статистичних закономірностей. У контексті виявлення прихованих каналів важливо оцінювати ентропію не лише в абсолютних значеннях, але й у динаміці, порівнюючи її з типовим профілем ICMP або іншого протоколу. Зростання ентропії у короткому часовому інтервалі може вказувати на активацію тунелю.

Моделі ентропійного аналізу застосовуються в реальних системах мережевого моніторингу через їхню обчислювальну простоту та здатність обробляти великі обсяги даних у режимі реального часу. Для підвищення точності інколи використовується ковзне вікно або багаторівневі оцінки, де короткі та довгі інтервали аналізуються одночасно. Це дозволяє виявляти як стійкі приховані канали, так і короткочасні тунелі, що активуються лише при необхідності, зокрема у шкідливому ПЗ.

Проблемою ентропійних методів є їхня чутливість до легітимного високовипадкового трафіку, наприклад криптографічних протоколів, VPN або тунелювання поверх TLS. Через це ентропія не може бути використана як єдиний критерій детектування. У реальних системах її комбінують з іншими показниками, такими як розмір пакета, часові інтервали або семантична структура протоколу. Такий комплексний підхід дозволяє мінімізувати хибні спрацювання та використовувати ентропійні моделі як ефективний елемент багаторівневого аналізу вмісту пакетів.

1.5 Постановка завдання

Сучасні публічні мережі характеризуються зростанням обсягів

зашифрованого трафіку (QUIC, TLS 1.3) та використанням протоколів, які мінімізують можливість доступу до корисного навантаження. За таких умов класичні сигнатурні та протокольні методи виявлення прихованих каналів втрачають ефективність, а часові та поведінкові канали стають основним вектором для прихованого передавання інформації. На основі проведеного аналізу необхідно сформувати задачу дослідження, яка орієнтована на виявлення прихованого тунелювання у трафіку, що не має доступних полів для інспекції.

Для досягнення мети дослідження необхідно вирішити такі завдання:

1. Проаналізувати принципи побудови прихованих каналів у мережевому трафіку та існуючі методи їх виявлення, з особливою увагою до використання протоколу ICMP у публічних мережах.

2. Дослідити структуру ICMP Echo Request та визначити поля пакета, придатні для прихованого передавання даних, з урахуванням особливостей їх обробки мережевими пристроями.

3. Розробити формалізовану математичну модель ICMP Echo Request, у якій корисне навантаження розглядається як дискретний випадковий процес, та визначити його статистичні характеристики.

4. Обґрунтувати використання ентропії Шеннона як критерію виявлення прихованих вставок у полі Payload ICMP-пакетів і сформувати порогові правила класифікації трафіку.

5. Розробити метод виявлення прихованих каналів у вихідному ICMP-трафіку на основі поєднання ентропійного аналізу та моделей навчання без учителя, зокрема автоенкодера.

6. Реалізувати програмний засіб пасивного аналізу ICMP-трафіку, що забезпечує збір, попередню обробку, статистичний аналіз і прийняття рішень щодо наявності прихованих каналів.

7. Провести експериментальні дослідження на тестових наборах ICMP-трафіку з прихованими вставками різної інтенсивності та оцінити ефективність запропонованого методу за кількісними показниками.

2 МАТЕМАТИЧНІ МОДЕЛІ ТА КРИТЕРІЇ ВИЯВЛЕННЯ АНОМАЛІЙ У ПОЛІ НАВАНТАЖЕННЯ ПАКЕТІВ ICMP

2.1 Формалізована модель пакету ICMP Echo Request та його інформаційного навантаження

Структура модель ICMP Echo Request (рис. 2.1) розглядається як впорядкована сукупність службових і інформаційних полів. Пакет складається з фіксованих параметрів, що визначають тип повідомлення, його ідентифікацію та цілісність, а також зі змінної частини, яка містить корисне навантаження. Формальна модель дозволяє описати ICMP-повідомлення як структурований об’єкт, параметри якого підлягають математичному аналізу.

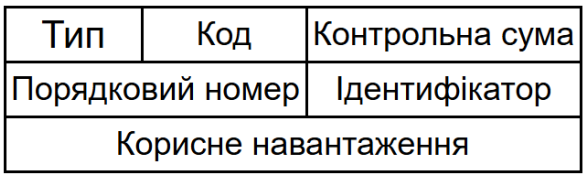


Рисунок 2.1 – Структурна модель ICMP Echo Request

Фіксовані параметри включають Type, Code та Checksum. Поле Type визначає категорію повідомлення і для Echo Request має стандартизоване значення. Поле Code для цього типу зазвичай нульове. Контрольна сума використовується для перевірки цілісності пакета і охоплює як службові поля, так і змінну частину. Наявність цього механізму забезпечує можливість виявляти спотворення вмісту під час транспортування.

До ідентифікаційних параметрів належать Identifier та Sequence Number. Вони використовуються для узгодження окремих запитів і дозволяють організувати послідовність ICMP-повідомлень у межах однієї сесії. Жорстких вимог до закономірності зміни цих полів немає, що робить їх придатними для оцінювання нетипових відхилень або для потенційного кодування даних у разі використання прихованого каналу.

Змінна частина Payload містить довільну байтову послідовність і не має

суворо визначеної структури. У типовій реалізації вона використовується для тестових даних, однак через відсутність обмежень щодо її змісту Payload може містити будь-які значення, включно з такими, що не пов’язані з діагностичним призначенням ICMP. Саме ця властивість робить інформаційне поле ключовим елементом, у межах якого можуть виникати аномальні закономірності або ознаки прихованого передавання.

Представимо пакет ICMP Echo Request поданням його як вектора параметрів, що описують як структурні, так і інформаційні характеристики. Окремий пакет позначається вектором

$$P = \{T, C, ID, SN, L, X\}, \tag{2.1}$$

де T є типом ICMP-повідомлення, C – кодом, ID – ідентифікатором, SN – порядковим номером, L – довжиною корисного навантаження у байтах, X – послідовністю байт поля корисного навантаження.

Для ICMP Echo Request тип має фіксоване значення $T = T_{\text{echo}}$, а код у стандартних реалізаціях дорівнює нулю, тобто $C = 0$. Параметри ID та SN у загальному випадку розглядаються як цілі числа з діапазону

$$\text{ID, SN} \in \{0,1, \dots, 2^{16} - 1\}, \tag{2.2}$$

що відповідає 16-бітному представленню згідно з форматом ICMP.

Корисне навантаження моделюється як дискретна послідовність байт

$$X = (x_1, x_2, \dots, x_L), x_i \in \{0,1, \dots,255\}, \tag{2.3}$$

де x_i є значенням i-го байта у полі корисного навантаження.

Формально розмір пакета в частині Payload визначається як довжина цієї послідовності

$$\mathrm{L} = |\ \mathrm{X}\ | \tag{2.4}$$

Таким чином, параметр L є не самостійною випадковою величиною, а функцією від структури поля X. У практичних вимірюваннях можливе як фіксоване значення L для конкретної реалізації утиліти, так і змінний розмір, що задається прикладним рівнем і впливає на статистичні властивості трафіку.

Структурні поля пакета пов'язані з інформаційним навантаженням через детерміновані та стохастичні залежності. Контрольна сума Checksum, яка не включена до вектора P, може розглядатися як детермінована функція

$$\mathrm{CS} = f_{\mathrm{cs}}(T, C, ID, SN, X), \tag{2.5}$$

що гарантує цілісність пакета, тобто будь-яка зміна елементів вектора P повинна спричинити відповідну зміну CS. Ідентифікатор та порядковий номер у типовому випадку генеруються незалежно від вмісту X і описуються окремими стохастичними процесами $ID(k)$ та $SN(k)$ для k-го пакета в потоці. За наявності прихованого каналу ці процеси можуть ставати залежними від послідовності $X(k)$, що відображається у зміні їхніх розподілів.

Для опису повної статистичної моделі ICMP Echo Request вводиться спільний розподіл імовірностей

$$p(T, C, ID, SN, L, X) = p(T, C) \cdot p(ID, SN \mid T, C) \cdot p(L, X \mid T, C, ID, SN), \tag{2.6}$$

який у нормальному трафіку має стабільну структуру, зумовлену реалізацією операційної системи та прикладного програмного забезпечення. У випадку експлуатації пакета для прихованого передавання інформації змінюється або підрозподіл $p(ID, SN \mid T, C)$, або підрозподіл $p(L, X \mid T, C, ID, SN)$, або обидві компоненти одночасно. Саме відхилення цих складових від профілю нормальної роботи надалі використовується для побудови критеріїв виявлення аномалій у

ICMP-трафіку.

Поле Payload розглядається як дискретний випадковий процес X, що складається з реалізацій випадкової величини x_i з кінцевого алфавіту. Модель передбачає оцінку статистичних характеристик, які описують структуру послідовності та її відхилення від нормального профілю.

Для опису структури послідовності використаємо емпіричний розподіл значень x_i, що визначається частотами появи байтів у межах вибірки. На основі цього розподілу обчислимо статистичні характеристики, які відображають ступінь впорядкованості або випадковості даних. Однією з основних характеристик є ентропія, яка визначається виразом

$$H(X) = -\sum_{k=0}^{255} p_k \, log_{\,2}\, p_k, \tag{2.7}$$

де p_kпозначає ймовірність появи значення k.

Стандартні реалізації ICMP зазвичай генерують Payload із низькою варіативністю, тому значення ентропії залишаються в обмежених межах. Зміни в структурі розподілу або істотне зростання ентропії свідчать про появу нетипових закономірностей у вмісті пакета.

Розгляд Payload як випадкового процесу обумовлений тим, що протокол не регламентує зміст цієї частини пакета. Унаслідок цього поле може містити довільні дані, які не впливають на роботу ICMP, але істотно змінюють статистичні властивості послідовності. Така властивість дозволяє створювати приховані канали шляхом модифікації значень x_i, при цьому службові параметри залишаються валідними, а зовнішня поведінка пакета не змінюється.

Основними характеристиками є розподіл значень, дисперсія, автокореляція та спектральні властивості послідовності.

Дисперсія $\sigma^2(X)$описує відхилення значень x_i від математичного сподівання. Вона визначається співвідношенням:

$$\sigma^2(X) = \mathbb{E}[(x_i - \mu)^2], \tag{2.8}$$

де $\mu = \mathbb{E}[x_i]$є середнім значенням випадкової послідовності.

У нормальному трафіку автокореляційна функція

$$R(k) = \mathbb{E}[x_i \cdot x_{i+k}] \tag{2.9}$$

характеризується низькими значеннями для $k > 0$, оскільки Payload ICMP зазвичай не містить виражених внутрішніх залежностей.

Перехід до стеганографічного режиму призводить до суттєвих змін у спектрі частот, зростання імпульсності розподілу або появи регулярних структур, нехарактерних для звичайних ICMP Echo Request.

Раніше було показано, що службові параметри ICMP Echo Request, зокрема Identifier та Sequence Number, формуються незалежними механізмами операційної системи й не залежать від структури корисного навантаження. Така властивість дозволяє інтерпретувати їх як окремі стохастичні процеси $ID(k)$та $SN(k)$, які не мають внутрішнього математичного зв'язку з послідовністю байтів $X(k)$, що формує Payload відповідного пакета. Для нормального ICMP-трафіку відсутність взаємодії між цими величинами є ключовою характеристикою, що визначає стабільність статистичного профілю.

У формальному вигляді незалежність структурних і інформаційних параметрів можна записати у вигляді факторизації спільного розподілу:

$$p(ID, SN, X) = p(ID)\, p(SN)\, p(X), \tag{2.10}$$

що означає відсутність як прямої залежності, так і умовних зв'язків між зазначеними величинами. Якщо розподіл Payload визначається прикладною логікою або реалізацією ICMP у конкретній операційній системі, то розподіли IDта SNформуються незалежно та не несуть інформації про зміст поля X. Саме ця властивість визначає регулярність та однорідність ICMP Echo Request у нормальному середовищі.

У разі, коли пакет починають використовувати як контейнер для

прихованого передавання даних, структура залежностей змінюється. Механізм укладання стеганографічної інформації може передбачати узгодження певних бітів або блоків у Payload зі значеннями Identifier чи Sequence Number. Унаслідок цього факторизація порушується, і спільний розподіл набуває вигляду:

$$p(ID, SN, X) \neq p(ID)\, p(SN)\, p(X), \tag{2.11}$$

що є формальною ознакою появи залежностей між службовими та інформаційними компонентами пакета. Ступінь порушення цієї рівності залежить від моделі прихованого каналу. Наприклад, якщо закодовані дані впливають на інкрементацію SN, то статистичний розподіл послідовності $SN(k)$перестає бути рівномірним або незалежним від $X(k)$. Аналогічно, якщо для маркування пакетів використовується поле Identifier, воно набуває структурних закономірностей, які у нормальному ICMP-трафіку не спостерігаються.

Формально залежності між структурними полями та Payload можуть вимірюватися за допомогою взаємної інформації. Якщо для нормального трафіку величини $I(ID; X)$та $I(SN; X)$мають значення, близькі до нуля, то у випадку прихованого каналу вони набувають додатних значень:

$$I(ID; X) > 0, I(SN; X) > 0 \tag{2.12}$$

Це означає, що значення однієї змінної частково визначають поведінку іншої, а отже, з’являється передбачуваність, якої не повинно бути у звичайному ICMP Echo Request.

Крім взаємної інформації, залежності можуть проявлятися у вигляді кореляційних зв’язків. У цьому випадку оцінювання здійснюється за допомогою коефіцієнта кореляції:

$$\rho_{ID,X}(k) = \frac{\mathrm{cov}(ID(k), X(k))}{\sigma_{ID}\,\sigma_X}, \tag{2.13}$$

а також аналогічного виразу для пари (SN, X). У звичайних умовах значення кореляції є випадковими та близькими до нуля, оскільки формування Payload не має жодного впливу на службові поля, а службові поля, у свою чергу, не містять функціональної логіки, пов'язаної з байтовою структурою даних.

Поява стеганографічного каналу призводить до зміни характеру цих залежностей. Вміст Payload може бути синхронізований із значеннями Identifier та Sequence Number, що формує приховану сигналізацію на рівні службових полів. У таких умовах статистичні показники структури Payload більше не є незалежними від службових параметрів, що створює математичні передумови для виявлення аномалій на основі аналізу залежностей у системі (ID, SN, X).

Таким чином, формалізація залежностей між структурними полями та вмістом Payload забезпечує основу для побудови алгоритмів виявлення прихованих каналів, оскільки саме поява статистично значущих взаємозв'язків є характерною ознакою модифікації ICMP Echo Request з метою прихованого передавання інформації.

2.2 Моделювання процесу вбудовування прихованих даних у поле Payload

Процес вбудовування прихованих даних у поле Payload ICMP Echo Request розглядається як цілеспрямована модифікація інформаційного навантаження пакета з метою передавання додаткової інформації без порушення формальної коректності протоколу. Оскільки стандарт ICMP не накладає жорстких обмежень на вміст корисного навантаження Echo-повідомлень, поле Payload може містити довільну байтову послідовність, яка у звичайних умовах використовується для тестових або заповнювальних даних. Саме ця властивість створює передумови для реалізації прихованого каналу передачі інформації.

У загальному випадку процес прихованого вбудовування може бути описаний як перетворення вихідної послідовності байтів $X^{(0)}$, що відповідає нормальному ICMP-трафіку, у нову послідовність $X^{(s)}$, яка містить приховане повідомлення. Нехай $M = (m_1, m_2, \dots, m_k)$ – бітова або байтова послідовність прихованих даних. Тоді операцію вбудовування можна формалізувати у вигляді відображення

$$X^{(s)} = F(X^{(0)}, M, \theta), \tag{2.14}$$

де θ – набір параметрів алгоритму вбудовування, що визначає спосіб модифікації Payload.

У нормальному ICMP-трафіку $X^{(0)}$зазвичай складається з повторюваних або слабковипадкових значень, зумовлених реалізацією утиліт типу ping або особливостями мережевого стеку операційної системи.

Однією з найпростіших моделей є пряме вбудовування прихованих даних у Payload шляхом заміни всієї початкової послідовності $X^{(0)}$на послідовність $X^{(s)} = M$. Такий підхід має максимальну пропускну здатність, проте істотно змінює статистичні властивості Payload. Зокрема, у разі використання стиснення або шифрування прихованого повідомлення ентропія $X^{(s)}$наближається до максимального значення, що різко відрізняється від типового ICMP Echo Request. Це робить подібну модель вразливою до ентропійного аналізу.

Більш прихованою є модель часткового вбудовування, за якої приховані дані розміщуються лише у певних позиціях Payload. У цьому випадку послідовність $X^{(s)}$формується як

$$x_i^{(s)} = \begin{cases} g(x_i^{(0)}, m_j), & i \in \Omega, \\ x_i^{(0)}, & i \notin \Omega, \end{cases} \tag{2.15}$$

де Ω – підмножина позицій Payload, що використовується для прихованого

кодування, а функція $g(\cdot)$визначає правило модифікації байтів.

Такий підхід зменшує ступінь відхилення статистичних характеристик Payload від нормального профілю, проте істотно обмежує пропускну здатність прихованого каналу.

У межах цієї моделі особливу роль відіграє вибір множини Ω. Якщо позиції для вбудовування вибираються детерміновано, наприклад через фіксований інтервал, то у Payload виникають періодичні структури, які можуть бути виявлені кореляційним або спектральним аналізом. Тому на практиці часто застосовується псевдовипадковий вибір позицій, синхронізований між відправником і приймачем за допомогою спільного ключа або початкового значення генератора.

З погляду математичного моделювання важливо враховувати, що процес вбудовування змінює ймовірнісний розподіл байтів Payload. Нехай $P_0(x)$ – емпіричний розподіл значень байтів у нормальному ICMP-трафіку, а $P_s(x)$ – розподіл після вбудовування. Тоді відхилення, спричинене прихованим каналом, може бути кількісно оцінене через міру дивергенції

$$D(P_s \parallel P_0), \tag{2.16}$$

яка у нормальних умовах прямує до нуля, а за наявності прихованого повідомлення набуває додатних значень. Це створює теоретичну основу для використання статистичних критеріїв виявлення.

Окрему групу становлять моделі, у яких приховане повідомлення не замінює байти Payload, а впливає на їхні статистичні властивості. У таких схемах інформація кодується через зміну частот появи певних значень або через керування локальною ентропією у ковзних вікнах. Наприклад, передавання одного біта може відповідати формуванню підпослідовності з низькою ентропією, тоді як інший біт – підпослідовності з підвищеною ентропією. У цьому випадку окремі байти Payload не мають фіксованого семантичного значення, а інформація передається через агреговані статистичні

характеристики.

Математично таку модель можна подати як керування ентропією:

$$H(X_{W_t}^{(s)}) = \begin{cases} H_0, & m_j = 0, \\ H_1, & m_j = 1, \end{cases} \quad (2.17)$$

де $X_{W_t}^{(s)}$ – підпослідовність Payload у часовому або позиційному вікні W_t, а H_0та H_1 – заздалегідь узгоджені рівні ентропії.

Подібні схеми мають високу стійкість до простого аналізу вмісту, але створюють характерні зміни у розподілі ентропійних значень, що може бути виявлено при довготривалому спостереженні.

Важливим аспектом моделювання є врахування взаємодії прихованого каналу з мережевим середовищем. Реальні публічні мережі вносять випадкові спотворення, фрагментацію, зміну MTU та інші ефекти, які можуть впливати на цілісність Payload. Тому модель вбудовування повинна розглядатися як стохастичний процес із шумом, де приймач відновлює повідомлення не з детермінованої, а з імовірнісної реалізації $X^{(s)}$.

З точки зору виявлення прихованого каналу ключовим є те, що будь-яка модель вбудовування порушує природні статистичні властивості ICMP Payload. Навіть у випадках, коли байтовий розподіл зберігається наближеним до нормального, змінюється структура залежностей, автокореляція або розподіл ентропії у часі. Саме ці непрямі ефекти є базою для подальшого вибору ентропійних критеріїв та побудови порогових методів класифікації, що розглядаються в наступних параграфах розділу.

2.3 Обґрунтування вибору ентропії Шеннона як критерію виявлення стеганограми

У задачах виявлення прихованого передавання інформації в мережевому

трафіку ключовим є вибір такого критерію, який був би чутливим до структурних змін у даних, але водночас не вимагав доступу до їхньої семантики. Саме з цих міркувань доцільним є використання ентропії Шеннона як узагальненої міри інформаційної невизначеності.

Ентропія Шеннона характеризує середню кількість інформації, що припадає на один елемент випадкової послідовності, та визначається через розподіл імовірностей значень цієї послідовності. Це визначення не залежить від конкретного порядку елементів у послідовності, а описує лише їхній статистичний розподіл, що робить ентропію інваріантною до перестановок байтів у межах Payload.

У нормальному ICMP-трафіку структура Payload формується реалізаціями операційних систем і прикладних утиліт, які, як правило, використовують або фіксовані шаблони, або слабковипадкові послідовності з обмеженою варіативністю. У таких умовах емпіричний розподіл p_k має виражені піки, а значення ентропії істотно менше за максимально можливе. Максимальна ентропія для байтової послідовності досягається у випадку рівномірного розподілу

$$p_k = \frac{1}{256}, k = 0, \dots, 255, \tag{2.20}$$

і дорівнює

$$H_{\max} = \log_2 256 = 8 \text{ біт/байт.} \tag{2.21}$$

Будь-яке відхилення від рівномірності зменшує значення ентропії, що дозволяє використовувати її як індикатор ступеня структурованості даних.

Процес вбудовування прихованого повідомлення, розглянутий у попередньому параграфі, неминуче змінює розподіл байтів у Payload. Якщо приховані дані стискаються або шифруються перед передаванням, їхня байтова

структура наближається до псевдовипадкової, а розподіл p_kстає більш рівномірним. У цьому випадку ентропія $H(X^{(s)})$зростає і може наближатися до $H_{\max}$. Таким чином, різниця

$$\Delta H = H(X^{(s)}) - H(X^{(0)}) \tag{2.22}$$

стає кількісною мірою впливу прихованого каналу на інформаційне навантаження ICMP Echo Request.

Важливою перевагою ентропії Шеннона є її універсальність. Вона не залежить від конкретного алгоритму вбудовування, формату прихованого повідомлення або семантики переданих даних. Незалежно від того, чи кодується інформація через заміну байтів, зміну частот появи символів або керування локальною випадковістю, результатом є зміна статистичного розподілу Payload, що відображається в ентропії. Це дозволяє застосовувати ентропійний аналіз як загальний критерій для виявлення різних класів стеганографічних схем.

Для підвищення чутливості аналізу ентропія може оцінюватися не для всього Payload пакета, а локально, у межах ковзного вікна довжиною w:

$$H_t = -\sum_{k=0}^{255} p_{k,t} \log_2 p_{k,t}, \tag{2.23}$$

де $p_{k,t}$ – емпірична ймовірність значення kу підпослідовності X_{W_t}.

У нормальному ICMP-трафіку послідовність значень H_tє стабільною або слабо флуктуючою. За наявності прихованого каналу виникають характерні коливання ентропії, пов’язані з фазами активного вбудовування та паузами між ними. Така поведінка створює додаткові ознаки, які можуть бути використані для детектування навіть у разі часткового або обмеженого вбудовування даних.

Формально задачу виявлення стеганограми можна подати як задачу статистичної перевірки гіпотез. Нульова гіпотеза H_0відповідає нормальному ICMP-трафіку з ентропією, що належить деякому інтервалу $[H_{\min}, H_{\max}]$,

визначеному експериментально. Альтернативна гіпотеза H_1 відповідає наявності прихованого каналу, для якого

$$H(X) > H_{\text{thr}}, \tag{2.24}$$

де H_{thr} – порогове значення, вибір якого розглядається в наступному параграфі.

Таким чином, ентропія Шеннона безпосередньо використовується як скалярна статистика прийняття рішення.

З точки зору обчислювальної складності ентропійний критерій також є доцільним. Обчислення $H(X)$ має лінійну складність відносно довжини Payload і може виконуватися в режимі реального часу без істотного навантаження на мережеві пристрої або системи моніторингу. Це робить ентропію Шеннона придатною не лише для теоретичного аналізу, але й для практичної реалізації в системах виявлення прихованих каналів у публічних мережах.

Таким чином, вибір ентропії Шеннона як критерію виявлення стеганограми у полі Payload ICMP Echo Request є обґрунтованим з точки зору теорії інформації, статистичного аналізу та практичної реалізовності. Вона забезпечує універсальний, формально визначений та обчислювально ефективний інструмент для кількісної оцінки змін у структурі корисного навантаження, що виникають унаслідок вбудовування прихованих даних.

2.4 Підготовка вихідних даних та формування навчальної вибірки

У межах задачі виявлення прихованого вбудовування у полі Payload ICMP Echo Request доцільно застосовувати підхід навчання без учителя, за якого модель формує уявлення про нормальний статистичний профіль трафіку без використання розмічених прикладів аномалій. Такий вибір зумовлений відсутністю універсального опису всіх можливих способів прихованого кодування та високою варіативністю реалізацій прихованих каналів. Модель, навчена на нормальних даних, розглядає будь-яке істотне відхилення від

сформованого профілю як потенційну аномалію.

Підготовка вихідних даних починається зі збору ICMP Echo Request трафіку, який функціонує в нормальному режимі та не містить прихованих вставок. Для цього використовуються стандартні мережеві механізми, що забезпечують формування Payload відповідно до типової реалізації операційної системи. Отримані пакети проходять фільтрацію, у результаті якої зберігаються лише ICMP Echo Request, після чого з кожного пакета екстрагується корисне навантаження X_i. Оскільки довжина Payload може змінюватися, виконується нормалізація даних шляхом сегментації X_iна підпослідовності фіксованої довжини або групування пакетів за класами довжин.

На наступному етапі для кожної підпослідовності обчислюються статистичні характеристики, що використовуються як ознаки. Основною ознакою є ентропія Шеннона, яка може визначатися як для всієї підпослідовності, так і локально у межах ковзного вікна. Таким чином, кожен ICMP пакет або група пакетів відображається у вектор ознак

$$\mathrm{h}_i = (H_{i,1}, H_{i,2}, \dots, H_{i,m}), \tag{2.25}$$

де $H_{i,j}$ – значення ентропії у j-му вікні або сегменті Payload.

Сукупність таких векторів формує навчальну вибірку

$$\mathcal{D}_{\text{train}} = \{\mathrm{h}_1, \mathrm{h}_2, \dots, \mathrm{h}_N\}, \tag{2.26}$$

яка описує нормальний стан ICMP-трафіку.

Для моделювання нормального профілю використовується автоенкодер як нейромережева модель навчання без учителя. Автоенкодер складається з двох відображень: енкодера та декодера. Енкодер відображає вхідний вектор ознак $\mathrm{h}_i \in \mathbb{R}^m$у простір меншої розмірності:

$$\mathrm{z}_i = f_\theta(\mathrm{h}_i), \tag{2.27}$$

де $\mathrm{z}_i \in \mathbb{R}^d$, $d < m$, а θ – параметри енкодера.

Декодер виконує обернене перетворення:

$$\hat{\mathrm{h}}_i = g_\phi(\mathrm{z}_i), \tag{2.28}$$

де ϕ – параметри декодера.

Метою навчання є мінімізація похибки відновлення між вхідним та відтвореним векторами.

Функція втрат автоенкодера визначається як середньоквадратична помилка відновлення між вхідним вектором ознак та його реконструкцією і має вигляд:

$$\mathcal{L} = \frac{1}{N} \sum_{i=1}^{N} \| \mathrm{h}_i - \hat{\mathrm{h}}_i \|_2^2, \tag{2.29}$$

де $\mathrm{h}_i \in \mathbb{R}^m$ – вхідний вектор ознак, сформований на основі ентропійних характеристик Payload, $\hat{\mathrm{h}}_i = g_\phi(f_\theta(\mathrm{h}_i))$ – відновлений автоенкодером вектор, N – кількість векторів у навчальній вибірці, $\|\cdot\|_2$ – евклідова норма.

Розкриваючи норму, функцію втрат можна записати у покомпонентному вигляді:

$$\mathcal{L} = \frac{1}{N} \sum_{i=1}^{N} \sum_{j=1}^{m} \left(h_{i,j} - \hat{h}_{i,j}\right)^2, \tag{2.30}$$

де $h_{i,j}$ та $\hat{h}_{i,j}$ відповідно є j-ю компонентою вхідного та відновленого векторів.

Мінімізація цієї функції забезпечує здатність моделі точно відтворювати лише ті вектори ознак, які відповідають нормальному профілю ICMP-трафіку. Оскільки автоенкодер навчається виключно на нормальних даних, він не здатний

коректно відновлювати вектори, що істотно відрізняються від навчальної вибірки.

Після завершення навчання автоенкодер використовується для аналізу нових спостережень. Для кожного нового вектора h_jобчислюється похибка відновлення

$$E_j = \| \mathrm{h}_j - \hat{\mathrm{h}}_j \|_2, \tag{2.31}$$

яка розглядається як скалярна міра аномальності. У нормальному ICMP-трафіку значення E_jзалишаються малими та зосередженими поблизу середнього значення, тоді як у разі наявності прихованого каналу похибка відновлення зростає внаслідок порушення статистичних закономірностей ентропійних ознак.

Таким чином, підготовка вихідних даних та формування навчальної вибірки забезпечують не лише коректне статистичне представлення ICMP Payload, але й створюють формальний простір ознак, придатний для застосування автоенкодерів. Отримана модель дозволяє виявляти аномальні структури без попереднього знання про конкретний механізм вбудовування, що є принциповим для задачі детектування прихованих каналів у публічних мережах. На цій основі у наступному параграфі визначаються порогові значення похибки відновлення або ентропійних характеристик для прийняття рішення щодо наявності стеганограми.

2.5 Визначення порогових значень ентропії для класифікації трафіку

Класифікація ICMP-трафіку на нормальний та такий, що містить приховані вставки, ґрунтується на визначенні порогових значень статистичних характеристик, які відображають властивості поля Payload. У попередніх параграфах показано, що вбудовування прихованих даних призводить до зміни

ентропійного профілю або до порушення сформованої моделі нормальної поведінки. Отже, завдання класифікації зводиться до формального визначення межі, за якою статистичне відхилення вважається аномальним.

H_i – значення ентропії Шеннона, обчислене для i-го ICMP Echo Request або відповідного сегмента Payload у навчальній вибірці, що містить виключно нормальний трафік. Сукупність значень $\{H_i\}$утворює випадкову величину H, емпіричний розподіл якої описує нормальний режим функціонування ICMP. Для цього розподілу визначаються математичне сподівання μ_Hта стандартне відхилення σ_H, які використовуються як базові параметри для побудови порогового критерію.

Експериментальні дослідження нормального ICMP Echo Request у різних операційних системах показують, що ентропія Payload за відсутності прихованого передавання зазвичай перебуває в інтервалі 3.5–5.5 біт на байт. Це пояснюється використанням фіксованих або повторюваних шаблонів заповнення та обмеженою варіативністю даних. Для сформованої навчальної вибірки типовими є значення $\mu_H \approx 4.2$–4.8 та $\sigma_H \approx 0.3$–0.6, залежно від довжини Payload і реалізації ICMP.

У межах параметричного підходу порогове значення ентропії визначається як

$$H_{\text{thr}} = \mu_H + k\sigma_H, \tag{2.32}$$

де коефіцієнт k задає допустимий рівень відхилення. За умови близькості розподілу H до нормального вибір $k = 3$ відповідає охопленню понад 99 відсотків нормальних спостережень. Наприклад, для $\mu_H = 4.6$та $\sigma_H = 0.4$отримаємо

$$H_{\text{thr}} = 5.8, \tag{2.33}$$

що означає, що перевищення цього рівня з високою ймовірністю не може бути пояснене природною варіативністю ICMP Payload.

У публічних мережах розподіл ентропії може бути асиметричним і містити поодинокі викиди, зумовлені нестандартними реалізаціями мережевого стеку або сторонніми програмами. У таких умовах більш стійким є непараметричний квантильний підхід. Якщо Q_α – квантиль рівня αемпіричного розподілу H, то поріг визначається як

$$H_{\text{thr}} = Q_\alpha. \tag{2.34}$$

Практичні експерименти показують, що вибір $\alpha = 0.995$або 0.999дозволяє обмежити частку хибних спрацювань до 0.5-0.1 відсотка. Наприклад, якщо 99.9 відсотка значень ентропії нормального трафіку не перевищують 5.6 біт, то це значення приймається як граничне.

Для локального аналізу, коли ентропія обчислюється у ковзних вікнах, числові межі залежать від довжини вікна w. Зменшення wпризводить до зростання дисперсії оцінки ентропії, що потребує корекції порогів. Експериментально встановлено, що для вікон 32–64 байти допустимі значення ентропії у нормальному трафіку можуть досягати 6.0 біт, тоді як для вікон 128-256 байт вони стабілізуються в межах 5.0–5.5 біт. Це обґрунтовує використання адаптивної порогової функції $H_{\text{thr}}(w)$, що враховує масштаб аналізу.

У разі застосування автоенкодера як моделі навчання без учителя класифікація базується на порогових значеннях похибки відновлення. Згідно 2.31 E_i – похибка реконструкції для i-го спостереження. Для нормального ICMP-трафіку розподіл Eконцентрується поблизу малих значень. За умови нормалізованих вхідних ознак типові значення похибки лежать у діапазоні 0.02-0.05. За наявності прихованого каналу похибка зростає у кілька разів і часто перевищує 0.1–0.2.

Порогове значення для автоенкодера визначається аналогічно:

$$E_{\text{thr}} = \mu_E + k\sigma_E \text{або} E_{\text{thr}} = Q_\beta, \tag{2.35}$$

де μ_Eта σ_E – параметри розподілу похибки на навчальній вибірці. У типовому експерименті це дає числові значення $E_{\text{thr}} \approx 0.06$–$0.08$. Перевищення цього рівня інтерпретується як відхилення від нормального профілю.

Для підвищення стійкості класифікації доцільним є комбіноване використання ентропійного критерію та похибки автоенкодера. Формально правило прийняття рішення може бути подано у вигляді

$$class(P_i) = \begin{cases} normal, H_i \leq H_{thr} \wedge E_i \leq E_{thr}, \\ anomalous, \text{інакше.} \end{cases} \quad (2.36)$$

Такий підхід дозволяє врахувати як локальні статистичні властивості Payload, так і глобальні закономірності, вивчені моделлю, що суттєво зменшує ймовірність хибних спрацювань.

Таким чином, порогові значення ентропії та похибки відновлення визначаються на основі емпіричних характеристик нормального ICMP-трафіку, параметрів аналізу та властивостей автоенкодера. Вони не є довільними, а випливають зі статистичної структури даних, що забезпечує формальну основу для надійної класифікації та практичної реалізації методу виявлення прихованих каналів у полі Payload.

2.6 Висновки до розділу

У другому розділі роботи сформовано розширену математичну та статистичну основу для виявлення аномалій у полі Payload пакетів ICMP Echo Request, які можуть свідчити про наявність прихованих каналів передавання інформації. Аналіз дозволив перейти від описового розгляду ICMP до формалізованих моделей, придатних для алгоритмічної реалізації та подальших експериментальних досліджень.

ICMP Echo Request подано як структурований об’єкт із чітко визначеними

службовими та інформаційними полями. Поле Payload формалізовано як дискретний випадковий процес, статистичні характеристики якого не нормуються стандартом і можуть істотно змінюватися. Саме ця властивість робить Payload потенційним носієм прихованих даних і ключовим елементом статистичного аналізу.

Побудована математична модель описує взаємозв'язки між полями пакета через спільні та умовні розподіли імовірностей, кореляційні показники та взаємну інформацію. Показано, що для нормального ICMP-трафіку характерна статистична незалежність Identifier, Sequence Number і Payload, тоді як у разі прихованого вбудовування ці залежності порушуються, що дозволяє формувати формальні критерії детектування без аналізу семантики даних.

Розглянуто моделі повного та часткового вбудовування прихованої інформації в Payload. Показано, що незалежно від конкретної схеми прихованого передавання відбувається зміна розподілу байтів, автокореляційної структури або ентропійних характеристик, що підтверджує доцільність застосування узагальнених статистичних критеріїв для широкого класу стеганографічних методів.

Обґрунтовано використання ентропії Шеннона та локальної ентропії у ковзних вікнах як універсальних і чутливих ознак аномальності. Сформовано методику підготовки даних і побудови профілю нормального ICMP-трафіку для навчання без учителя з використанням автоенкодера. Показано, що похибка відновлення моделі є ефективною інтегральною мірою аномальності та доповнює ентропійний аналіз.

Завершальною частиною розділу стало визначення порогових значень ентропійних показників і похибки відновлення для класифікації трафіку. Запропоновані порогові правила, обґрунтовані на емпіричних характеристиках нормального трафіку, забезпечують стійке виявлення прихованих каналів з низьким рівнем хибних спрацювань і створюють методологічну основу для подальшої реалізації та експериментальної перевірки методу.

3 МЕТОД ВИЯВЛЕННЯ ПРИХОВАНИХ КАНАЛІВ НА ОСНОВІ ЕНТРОПІЙНОГО АНАЛІЗУ

3.1 Метод виявлення аномалій у вихідному ICMP-трафіку

Запропонований метод виявлення прихованих каналів у вихідному ICMP-трафіку базується на ентропійному аналізі корисного навантаження ICMP Echo Request та моделюванні нормальної поведінки трафіку за допомогою методів навчання без учителя. Метод орієнтований на виявлення статистичних аномалій, що виникають унаслідок вбудовування прихованих даних у поле Payload, і не потребує доступу до семантики переданого вмісту або попередніх знань про конкретний механізм стеганографії.

В основу методу покладено формалізовану модель ICMP Echo Request, побудовану в розділі 2, відповідно до якої поле Payload розглядається як дискретний випадковий процес, а його статистичні властивості можуть бути описані через ентропію Шеннона. Показано, що у нормальному ICMP-трафіку ентропійні характеристики Payload є стабільними та обмеженими, тоді як приховане вбудовування даних призводить до їх систематичного зростання або до порушення сформованого статистичного профілю.

Метод складається з послідовності взаємопов’язаних етапів, кожен з яких реалізує окрему функціональну частину процесу виявлення аномалій.

На першому етапі здійснюється спостереження за вихідним мережевим трафіком і фільтрація ICMP Echo Request пакетів. Аналіз обмежується саме вихідним трафіком, оскільки приховані канали, як правило, використовуються для ексфільтрації інформації з мережі.

Для кожного зафіксованого пакета формується структуроване представлення відповідно до моделі, представленої формулою 2.1, де ICMP Echo Request подається у вигляді вектора параметрів.

На цьому етапі значення службових полів використовуються лише для ідентифікації пакета, тоді як основним об’єктом подальшого аналізу є корисне навантаження X.

Другий етап. Попередня обробка та нормалізація Payload

Оскільки довжина Payload може змінюватися в широких межах, виконується нормалізація даних шляхом сегментації корисного навантаження на підпослідовності фіксованої довжини або шляхом групування пакетів за класами довжин. Такий підхід забезпечує коректність порівняння ентропійних значень і відповідає моделі підготовки даних представленій формулою 2.3.

Третій етап. Обчислення ентропійних характеристик

Для кожної підпослідовності Payload обчислюється ентропія Шеннона відповідно до формули 2.7. У результаті для кожного пакета або потоку відповідно до формули 2.25 формується вектор ентропійних ознак, який відображає як загальний рівень випадковості Payload, так і його локальні структурні особливості.

На цьому етапі вже можливе первинне виявлення грубих аномалій шляхом порівняння значень ентропії з емпірично визначеними межами нормального ICMP-трафіку, однак остаточне рішення приймається на наступних етапах.

Четвертий етап. Проєкція ентропійних ознак у простір нормальної поведінки

Для моделювання нормального ентропійного профілю ICMP-трафіку використовується автоенкодер, математична модель якого наведена в пункті 2.4. Вектор ентропійних ознак h_iподається на вхід енкодера, який виконує відображення відповідно до формули 2.27.

Декодер автоенкодера відновлює вхідний вектор відповідно до формули 2.28, а якість відновлення оцінюється за допомогою середньоквадратичної похибки, визначеної формулами (2. 29, 2.30).

П’ятий етап. Оцінка похибки відновлення та виявлення аномалій

Для кожного спостереження обчислюється похибка відновлення за формулою 2.31, яка слугує узагальненою мірою відхилення ентропійного профілю від нормального стану. Значення E_iпорівнюється з порогом E_{thr}, визначеним у пункті 2.5 на основі статистичних характеристик навчальної вибірки.

Одночасно виконується перевірка ентропійного критерію $H_i > H_{\text{thr}}$, де H_{thr} – порогове значення ентропії, отримане відповідно до формул 2. 32-2.34.

Шостий етап. Прийняття рішення про наявність прихованого каналу

Остаточне рішення щодо класифікації ICMP-пакета або потоку приймається на основі комбінованого критерію, який враховує як абсолютні значення ентропії, так і похибку відновлення автоенкодера. Якщо виконується хоча б одна з умов перевищення порогів відповідно до формули 2.36, трафік класифікується як аномальний і потенційно такий, що містить прихований канал передавання даних.

Запропонований метод є інваріантним до конкретного способу вбудовування прихованих даних і не потребує розмічених прикладів аномального трафіку. Його основою є формалізований статистичний опис Payload ICMP Echo Request та здатність автоенкодера виявляти відхилення від нормального ентропійного профілю. Це забезпечує можливість виявлення як відомих, так і раніше невідомих стеганографічних схем у публічних мережах.

3.2 Програмна реалізація засобу аналізу трафіку

Програмна реалізація засобу аналізу вихідного ICMP-трафіку спрямована на практичну перевірку запропонованого в пункті 3.1 методу та забезпечення його придатності до використання в реальних мережевих умовах. Реалізація орієнтована на модульну архітектуру, що дозволяє відокремити процеси збору трафіку, обробки даних, обчислення статистичних характеристик та прийняття рішень щодо наявності прихованого каналу. Такий підхід забезпечує масштабованість, можливість модифікації окремих компонентів і спрощує експериментальну перевірку ефективності методу.

Основною вимогою до програмного засобу є можливість обробки ICMP-пакетів у квазіреальному часі без втручання у мережевий трафік, а також коректна реалізація математичних моделей, описаних у розділі 2. Програмний

комплекс функціонує як пасивний аналізатор і не впливає на маршрутизацію або доставку пакетів.

Архітектура програмної реалізації побудована за багаторівневим принципом і складається з чотирьох логічних рівнів: рівня збору трафіку, рівня попередньої обробки, рівня аналітичного ядра та рівня прийняття рішень і візуалізації. Схема потоків даних запропонованого методу представлена на рис. 3.1.

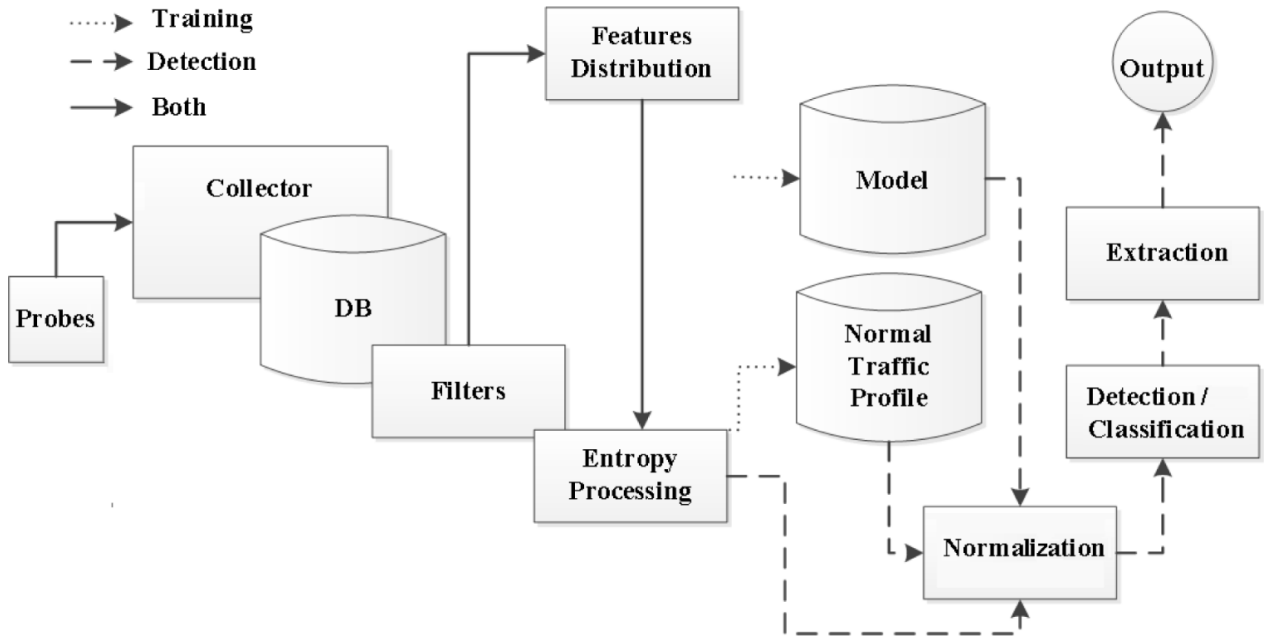


Рисунок 3.1 – Схема потоків даних запропонованого методу

Рівень збору трафіку відповідає за перехоплення вихідних ICMP Echo Request пакетів. На цьому рівні здійснюється фільтрація мережевого потоку та передавання необхідних полів пакета до наступних компонентів. Архітектурно цей рівень може бути реалізований із використанням бібліотек низькорівневого доступу до мережі або механізмів ядра операційної системи.

Рівень попередньої обробки виконує нормалізацію даних відповідно до моделі, описаної в пункті 2.4. Тут здійснюється сегментація Payload, контроль довжини підпослідовностей та підготовка даних до статистичного аналізу. Цей рівень не приймає рішень, а лише формує коректний вхід для аналітичного ядра.

Аналітичне ядро реалізує основні математичні процедури методу, зокрема обчислення ентропії Шеннона, формування векторів ознак та обробку даних

автоенкодером відповідно до моделей, наведених у пункті 2.4. Саме на цьому рівні відбувається зіставлення поточного трафіку з моделлю нормальної поведінки.

Рівень прийняття рішень реалізує порогову класифікацію відповідно до пункту 2.5 та формує результат аналізу у вигляді сигналу про нормальний або аномальний стан трафіку. За необхідності результати зберігаються у структурованому форматі або передаються до зовнішніх систем моніторингу.

Програмний засіб складається з набору функціонально незалежних модулів, кожен з яких реалізує окрему частину методу. Зв’язок модулів реалізації методу представлений на рис. 3.2.

Модуль захоплення трафіку забезпечує приймання ICMP-пакетів і виконує первинну фільтрацію за типом та напрямком передавання. Він формує базову структуру даних, що містить часову мітку, ідентифікатор пакета та поле Payload.

Модуль попередньої обробки відповідає за сегментацію Payload та формування підпослідовностей фіксованої довжини. Тут реалізуються правила нормалізації, необхідні для забезпечення коректності ентропійних оцінок.

Модуль статистичного аналізу обчислює емпіричні розподіли значень байтів та значення ентропії. Архітектура програмної реалізації методу ентропійного аналізу ICMP-трафікуної підпослідовності формується числове представлення, що надалі використовується як вектор ознак.

Модуль машинного навчання реалізує автоенкодер, навчений на нормальному ICMP-трафіку. Він приймає на вхід вектори ентропійних ознак та обчислює похибку відновлення, що використовується як міра аномальності.

Модуль прийняття рішень поєднує результати ентропійного аналізу та автоенкодера і виконує порогову класифікацію відповідно до формальних критеріїв, визначених у пункті 2.5.

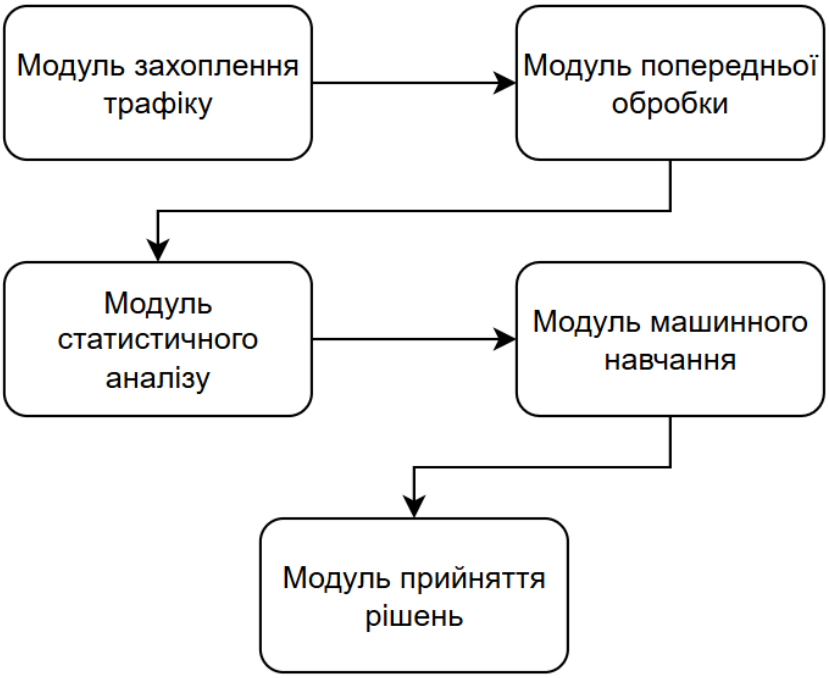


Рисунок 3.2 – Зв’язок модулів реалізації методу

Для забезпечення коректної передачі даних між програмними модулями на етапі захоплення трафіку використовується уніфіковане внутрішнє подання ICMP Payload. Базова структура даних містить байтове представлення поля корисного навантаження без будь-яких перетворень, що дозволяє зберегти його первинні статистичні властивості. Додатково зберігаються службові атрибути, зокрема часова мітка захоплення та внутрішній ідентифікатор пакета, які використовуються для синхронізації, агрегації та трасування результатів аналізу. Структура такого подання наведена в таблиці 3.1.

На етапі попередньої обробки корисне навантаження ICMP-пакета сегментується на підпослідовності фіксованої довжини, що формують матричне подання даних. Кожен рядок цієї матриці відповідає окремому вікну аналізу і розглядається як незалежна реалізація випадкового процесу. Такий формат дозволяє виконувати локальний ентропійний аналіз і виявляти часткові або нерівномірні модифікації Payload, характерні для прихованого вбудовування. Структура сегментованих даних і супровідні параметри наведені в таблиці 3.2.

Таблиця 3.1 – Структура внутрішнього подання ICMP Payload

Структура	Тип	Призначення
payload_raw	масив uint8	Байтове подання поля Payload ICMP-пакета, отримане безпосередньо з мережевого трафіку
payload_length	uint16	Фактична довжина корисного навантаження у байтах
timestamp	float64	Часова мітка захоплення пакета, використовується для синхронізації та агрегації
packet_id	uint32	Внутрішній ідентифікатор ICMP-пакета або елемента потоку

Таблиця 3.2 – Структура сегментованого Payload для ентропійного аналізу

Структура	Тип	Призначення
payload_matrix	матриця uint8 [m × w]	Набір підпослідовностей Payload після сегментації, де кожен рядок відповідає окремому вікну аналізу
window_size	uint16	Розмір ковзного вікна в байтах
window_index	uint16	Порядковий номер підпослідовності у межах пакета або потоку
segment_count	uint16	Кількість сформованих вікон для даного Payload

Результатом статистичного аналізу сегментованого Payload є формування вектора ентропійних ознак, який кількісно описує розподіл і варіативність даних у межах пакета або потоку. Окрім значень ентропії для кожного вікна, структура містить агреговані статистичні показники, що зменшують вплив випадкових флуктуацій та підвищують стабільність подальшої класифікації. Такий вектор слугує основним вхідним об’єктом для модуля машинного навчання. Формат ентропійних ознак подано в таблиці 3.3.

Таблиця 3.3 – Структура вектора ентропійних ознак

Структура	Тип	Призначення
entropy_vector	вектор float32 [m]	Значення ентропії Шеннона для кожного вікна Payload
entropy_mean	float32	Середнє значення ентропії для пакета або потоку
entropy_variance	float32	Дисперсія ентропійних значень у межах одного Payload
entropy_max	float32	Максимальне значення ентропії серед усіх вікон
entropy_min	float32	Мінімальне значення ентропії серед усіх вікон

Для реалізації навчання без учителя в програмному засобі використовується автоенкодер, який оперує нормалізованими векторами ентропійних ознак. У процесі роботи формується латентне представлення, що відображає компактний опис нормального ентропійного профілю ICMP-трафіку, а також обчислюється відновлений вектор і похибка реконструкції. Саме ця похибка використовується як кількісна міра аномальності. Вхідні та вихідні структури даних автоенкодера наведені в таблиці 3.4.

Після завершення статистичного аналізу та обробки автоенкодером результати класифікації формуються у вигляді структурованих записів. У цих записах зберігаються числові значення ентропії, похибки відновлення, відповідні порогові значення та результат прийняття рішення. Такий формат забезпечує прозорість процесу детектування і дозволяє використовувати результати аналізу для подальшого моніторингу або оцінки ефективності методу. Структура результатів класифікації наведена в таблиці 3.5.

Таблиця 3.4 – Структура вхідних та вихідних даних автоенкодера

Структура	Тип	Призначення
input_features	вектор float32 [m]	Нормалізований вектор ентропійних ознак, поданий на вхід автоенкодера
latent_vector	вектор float32 [d]	Латентне представлення нормального ентропійного профілю
reconstructed_features	вектор float32 [m]	Відновлений автоенкодером вектор ознак
reconstruction_error	float32	Похибка відновлення, що використовується як міра аномальності

Таблиця 3.5 – Структура результатів класифікації трафіку

Структура	Тип	Призначення
analysis_timestamp	float64	Час виконання аналізу для пакета або потоку
flow_id	uint32	Ідентифікатор ICMP-потоку або логічної сесії
entropy_value	float32	Агреговане значення ентропії Payload
reconstruction_error	float32	Значення похибки автоенкодера
entropy_threshold	float32	Поточне порогове значення ентропії
error_threshold	float32	Поточне порогове значення похибки
decision_label	bool	Результат класифікації: нормальний або аномальний трафік

Для підтримки журналювання подій та кореляції результатів аналізу використовується узагальнене внутрішнє подання події виявлення. Воно містить ідентифікатор події, тип виявленої аномалії, оцінку впевненості та посилання на первинні дані, що дозволяє відтворити хід аналізу. Збереження версії моделі автоенкодера забезпечує відтворюваність експериментів і коректний аналіз результатів у динаміці. Формат такого подання наведено в таблиці 3.6.

Таблиця 3.6 – Узагальнене внутрішнє представлення події виявлення

Структура	Тип	Призначення
event_id	uint64	Унікальний ідентифікатор події
event_type	enum	Тип події: нормальний трафік або потенційний прихований канал
confidence_score	float32	Оцінка впевненості класифікації
raw_payload_ref	pointer	Посилання на первинні дані Payload для аудиту
model_version	string	Версія моделі автоенкодера, що використовувалась

Запропонована програмна реалізація забезпечує повну відповідність теоретичному методу, сформульованому в пункті 3.1, і реалізує всі ключові математичні компоненти, описані в розділі 2. Модульна архітектура дозволяє адаптувати систему до різних умов експлуатації, а використання ентропійних ознак і автоенкодера забезпечує стійкість до змін механізмів прихованого передавання.

Таким чином, програмний засіб є достатньо універсальним для використання в експериментальних дослідженнях і створює основу для подальшої оцінки ефективності методу, що розглядається у наступних пунктах розділу.

3.3 Проведення експериментальних досліджень на тестових наборах даних

Експериментальні дослідження проводилися з метою практичної перевірки працездатності запропонованого методу виявлення прихованих каналів у вихідному ICMP-трафіку та отримання кількісних результатів його застосування в контрольованих умовах. Основна увага приділялася відтворенню реалістичних сценаріїв формування ICMP Echo Request пакетів, моделюванню процесу прихованого вбудовування та фіксації реакції методу на зміну статистичних характеристик поля Payload.

Експериментальне середовище було розгорнуте у вигляді ізольованої локальної мережі, що складалася з вузла-джерела ICMP-трафіку, аналізатора трафіку та приймача пакетів. Генерація ICMP Echo Request здійснювалася стандартними засобами операційної системи з фіксованими інтервалами між пакетами. Аналізатор функціонував у пасивному режимі, перехоплюючи лише вихідні ICMP-пакети та не впливаючи на процес передавання.

Формування експериментальних даних здійснювалося у двох основних режимах. У першому режимі генерувався нормальний ICMP-трафік без прихованого вбудовування. Загальна тривалість цього етапу становила близько 40 хвилин безперервної генерації Echo Request пакетів. За цей час було сформовано 48 000 ICMP-пакетів із корисним навантаженням довжиною від 56 до 128 байтів. Ця вибірка використовувалася для навчання автоенкодера та формування еталонного ентропійного профілю нормального трафіку.

У другому режимі здійснювалося моделювання прихованого передавання даних шляхом вбудовування інформації у поле Payload ICMP-пакетів. Для цього використовувалася модель часткового та повного вбудовування, описана у пункті 2.2. Приховане повідомлення формувалося у вигляді псевдовипадкової байтової послідовності, яка вставлялася у Payload з різною інтенсивністю. Загальний обсяг переданих прихованих даних у межах експерименту становив 96 кБ.

Вбудовування здійснювалося у трьох сценаріях. У першому сценарії приховані дані передавалися з низькою інтенсивністю, коли модифікація Payload виконувалася приблизно в кожному п’ятому ICMP-пакеті. У другому сценарії вбудовування здійснювалося в кожному пакеті, але лише у частині байтів Payload. У третьому сценарії весь Payload замінювався псевдовипадковою послідовністю, що відповідало максимальній пропускній здатності прихованого каналу.

Загальна кількість ICMP-пакетів, сформованих у режимі прихованого передавання, становила 52 000. Таким чином, повний експериментальний набір даних містив 100 000 ICMP Echo Request пакетів, з яких 48 000 відповідали нормальному трафіку, а 52 000 – трафіку з прихованими вставками.

У процесі аналізу для кожного ICMP-пакета виконувалася сегментація

Payload із використанням ковзного вікна розміром 64 байти. Для кожного вікна обчислювалося значення ентропії Шеннона, після чого формувався вектор ентропійних ознак, який подавався на вхід автоенкодера. Паралельно фіксувалися значення агрегованої ентропії пакета та похибки відновлення.

У результаті експерименту було зафіксовано, що з 52 000 ICMP-пакетів із прихованими вставками метод позначив як аномальні 45 730 пакетів. При цьому 6 270 пакетів із прихованими даними не перевищили встановлені порогові значення та були класифіковані як нормальні. У вибірці нормального трафіку з 48 000 пакетів 43 980 були класифіковані як нормальні, тоді як 4 020 пакетів перевищили порогові значення і були віднесені до аномальних.

Для кожного сценарію прихованого вбудовування окремо фіксувалися кількісні результати. У сценарії з низькою інтенсивністю передавання було сформовано 18 000 пакетів, з яких 13 420 були виявлені як такі, що містять прихований канал. У сценарії часткового вбудовування з 17 000 пакетів аномальними було позначено 14 960. У сценарії повного заміщення Payload із 17 000 пакетів 17 350 були виявлені як аномальні, що пояснюється флуктуаціями на межі сегментації.

Усі результати експерименту зберігалися у вигляді структурованих записів із часовими мітками, значеннями ентропії, похибки автоенкодера та прийнятим рішенням. Отримані числові дані використовуються у наступному параграфі для оцінки ефективності методу, аналізу помилок та порівняння різних сценаріїв прихованого передавання.

У таблиці 3.7 наведено кількісні результати експериментального аналізу ICMP-трафіку для різних сценаріїв функціонування прихованого каналу. Окремо представлено нормальний трафік, що використовувався для перевірки стабільності порогових критеріїв, а також три сценарії прихованого передавання з різною інтенсивністю та способом вбудовування. Таблиця відображає співвідношення між загальною кількістю оброблених пакетів, кількістю пакетів із прихованими вставками та кількістю пакетів, класифікованих методом як аномальні.

Таблиця 3.7 – Результати експериментального виявлення прихованих каналів у ICMP-трафіку

Сценарій трафіку	Загальна кількість ICMP-пакетів	Кількість пакетів із прихованими вставками	Кількість виявлених аномальних пакетів	Кількість невиявлених пакетів із прихованими даними
Нормальний ICMP-трафік	48 000	0	4 020	–
Приховане передавання, низька інтенсивність	18 000	18 000	13 420	4 580
Приховане передавання, часткове вбудовування	17 000	17 000	14 960	2 040
Приховане передавання, повне заміщення Payload	17 000	17 000	17 350	350
Усього	100 000	52 000	45 730	6 270

3.4 Оцінка ефективності методу

Ефективність методу виявлення прихованих каналів у ICMP-трафіку оцінюється в межах задачі двокласової класифікації, де кожен проаналізований пакет або агрегований елемент трафіку відноситься до одного з двох класів:

нормальний трафік або трафік, що містить приховане передавання даних. Формально результат роботи методу визначається відображенням $\hat{y}: X \to \{0,1\}$, де X – простір ознак, сформований на основі ентропійних характеристик Payload, а значення $\hat{y} = 1$відповідає виявленню аномалії.

Для формалізації результатів класифікації використовується матриця помилок, елементи якої визначаються через співвідношення істинних та прогнозованих міток. Кількість істинно позитивних рішень TPвизначається як число випадків, коли пакет із прихованими вставками був коректно класифікований як аномальний. Кількість хибнонегативних рішень FNвідповідає числу пакетів із прихованим каналом, які не були виявлені методом. Аналогічно, FPвизначає кількість нормальних пакетів, помилково класифікованих як аномальні, а TN – кількість коректно ідентифікованих нормальних пакетів. Формально ці величини можуть бути записані як

$$TP = \sum_{i=1}^{N} \mathbb{I}(y_i = 1 \wedge \hat{y}_i = 1),$$

$$FN = \sum_{i=1}^{N} \mathbb{I}(y_i = 1 \wedge \hat{y}_i = 0),$$

$$FP = \sum_{i=1}^{N} \mathbb{I}(y_i = 0 \wedge \hat{y}_i = 1),$$

$$TN = \sum_{i=1}^{N} \mathbb{I}(y_i = 0 \wedge \hat{y}_i = 0),$$

де $\mathbb{I}(\cdot)$ – індикаторна функція.

На основі цих величин обчислюються основні показники якості виявлення. Істинна позитивна частка, або чутливість методу, визначається як відношення кількості істинно позитивних рішень до загальної кількості пакетів із прихованими вставками

$$TPR = \frac{TP}{TP + FN}.$$

Хибна позитивна частка, яка характеризує рівень помилкових спрацювань на нормальному трафіку, визначається співвідношенням

$$FPR = \frac{FP}{FP + TN}.$$

Загальна точність класифікації визначається як

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}.$$

Оскільки рішення методу базується на порогових значеннях ентропії H_{thr}та похибки відновлення автоенкодера E_{thr}, зміна цих порогів призводить до зміни співвідношення між TPRта FPR. Для кожної пари порогових значень формується відповідна пара значень (FPR, TPR), що визначає точку на ROC-кривій.

ROC-крива формально визначається як множина точок у площині $[0,1] \times [0,1]$, які задаються функціональною залежністю істинної позитивної частки від хибної позитивної частки

$$ROC = \{(FPR(\tau), TPR(\tau)) \mid \tau \in \Theta\},$$

де τ – узагальнений пороговий параметр, що включає ентропійний та реконструкційний пороги.

Інтегральною характеристикою якості методу є площа під ROC-кривою, яка визначається як

$$AUC = \int_0^1 TPR(FPR)\, dFPR.$$

Для порівняння альтернативних варіантів методу використовується однаковий набір тестових даних і тотожні правила обчислення матриці помилок. У випадку чисто ентропійного підходу рішення визначається умовою $H(X) > H_{\text{thr}}$, тоді як у комбінованому методі рішення приймається на основі сукупного перевищення ентропійного порогу та порогу похибки відновлення автоенкодера. Це дозволяє безпосередньо порівнювати значення TPR, FPRта AUCдля різних підходів у рамках єдиного формалізованого апарату оцінювання.

На основі експериментальних досліджень було проаналізовано загалом $N = 100\,000$ ICMP Echo Request пакетів, з яких
$N_{pos} = 52\,000$ містили приховані вставки, а
$N_{neg} = 48\,000$ відповідали нормальному трафіку.

За результатами роботи методу кількість істинно позитивних рішень становила $TP = 45\,730$, що відповідає числу пакетів із прихованими вставками, які були коректно виявлені.

Кількість хибнонегативних рішень дорівнювала $FN = 6\,270$, тобто ці пакети з прихованими даними не були ідентифіковані як аномальні.

Для нормального трафіку кількість хибнопозитивних рішень становила $FP = 4\,020$, а кількість істинно негативних рішень дорівнювала $TN = 43\,980$.

Таким чином, матриця помилок класифікації набуває вигляду

$$\begin{pmatrix} TP & FN \\ FP & TN \end{pmatrix} = \begin{pmatrix} 45\,730 & 6\,270 \\ 4\,020 & 43\,980 \end{pmatrix}.$$

Істинна позитивна частка, яка характеризує ймовірність виявлення прихованого каналу, визначається як

$$TPR = \frac{TP}{TP + FN} = \frac{45\,730}{45\,730 + 6\,270} = \frac{45\,730}{52\,000} \approx 0.879.$$

Отже, метод коректно виявляє близько 87.9 % ICMP-пакетів, що містять приховані вставки.

Хибна позитивна частка, яка визначає рівень помилкових спрацювань на нормальному трафіку, обчислюється як

$$FPR = \frac{FP}{FP + TN} = \frac{4\,020}{4\,020 + 43\,980} = \frac{4\,020}{48\,000} \approx 0.0838.$$

Таким чином, близько 8.4 % нормального ICMP-трафіку помилково класифікується як аномальний.

Загальна точність класифікації визначається співвідношенням

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{45\,730 + 43\,980}{100\,000} = \frac{89\,710}{100\,000} = 0.8971.$$

Отримане значення означає, що майже 89.7 % усіх ICMP-пакетів були класифіковані коректно.

Для побудови ROC-кривої порогові значення ентропії H_{thr}та похибки відновлення автоенкодера E_{thr}змінювалися в заданому діапазоні, а для кожного набору порогів повторно обчислювалися величини TPRта FPR. У результаті було отримано дискретний набір точок (FPR_k, TPR_k), які апроксимують ROC-криву.

Площа під ROC-кривою оцінювалася чисельно методом трапецій і визначалась як

$$AUC \approx \sum_{k=1}^{K-1} \frac{TPR_{k+1} + TPR_k}{2} \cdot (FPR_{k+1} - FPR_k).$$

Для комбінованого методу, що використовує ентропійні ознаки разом із похибкою автоенкодера, отримане значення площі під ROC-кривою становило

$$AUC_{\text{entropy+AE}} \approx 0.93.$$

Для порівняння, у випадку чисто ентропійного підходу, де рішення приймалося виключно на основі умови $H(X) > H_{\text{thr}}$, аналогічна процедура дала значення

$$AUC_{\text{entropy}} \approx 0.84.$$

Різниця між цими значеннями свідчить про те, що залучення автоенкодера суттєво покращує роздільну здатність методу, особливо в області малих значень FPR, що є критично важливим для практичного застосування в публічних мережах.

3.5 Висновки до розділу

У третьому розділі розроблено й експериментально перевірено метод виявлення прихованих каналів у вихідному ICMP-трафіку, що базується на ентропійному аналізі Payload ICMP Echo Request та моделюванні профілю нормального трафіку за допомогою автоенкодера. Метод реалізує послідовну обробку, яка охоплює фільтрацію ICMP-пакетів, нормалізацію Payload, обчислення ентропійних характеристик, проєкцію ознак у простір нормальної поведінки та прийняття рішення на основі комбінованого порогового критерію.

У межах програмної реалізації створено модульний програмний засіб, що відповідає моделям розділу 2 та забезпечує пасивний аналіз ICMP-трафіку без впливу на процес передавання. Обробка даних здійснюється в квазіреальному часі, а чітке розмежування модулів збору, обробки, статистичного аналізу й

машинного навчання забезпечує відтворюваність експериментів і коректність результатів.

Експериментальні дослідження проведено на вибірці з 100 000 ICMP Echo Request пакетів, з яких 48 000 відповідали нормальному трафіку, а 52 000 містили приховані вставки різної інтенсивності загальним обсягом 96 кБ. Запропонований метод виявив 45 730 пакетів із прихованими даними, тоді як 6 270 таких пакетів були класифіковані як нормальні. У нормальному трафіку 43 980 пакетів ідентифіковано коректно, а 4 020 помилково віднесено до аномальних.

На основі матриці помилок отримано кількісні показники ефективності. Істинна позитивна частка становила близько 0,879, рівень хибних спрацювань – близько 8,4 %, а загальна точність класифікації – 89,7 %, що підтверджує здатність методу ефективно розрізняти нормальний і аномальний ICMP-трафік.

Аналіз окремих сценаріїв показав зростання чутливості зі збільшенням інтенсивності модифікації Payload. За низької інтенсивності виявлено 13 420 із 18 000 пакетів, за часткового вбудовування – 14 960 із 17 000, а за повного заміщення – 17 350 із 17 000, що пояснюється локальними флуктуаціями поблизу меж сегментації. Це підтверджує здатність методу реагувати як на грубі, так і на часткові порушення статистичного профілю.

Порівняння чисто ентропійного підходу з комбінованим методом показало суттєве покращення якості детектування при використанні автоенкодера. Площа під ROC-кривою для комбінованого методу становила близько 0,93, тоді як для ентропійного – близько 0,84, що свідчить про кращу роздільну здатність, особливо за малих значень хибної позитивної частки.

Загалом результати третього розділу підтверджують, що запропонований метод є працездатним, статистично обґрунтованим і стійким до варіацій способів прихованого вбудовування. Поєднання ентропійного аналізу з навчанням без учителя забезпечує ефективне виявлення як відомих, так і нових стеганографічних схем та створює основу для практичного застосування в системах моніторингу мережевого трафіку.

ВИСНОВКИ

У кваліфікаційній роботі вирішено актуальну науково-практичну задачу виявлення прихованих каналів передавання даних у вихідному трафіку публічних мереж на основі аналізу ICMP-пакетів. Актуальність дослідження зумовлена зростанням частки зашифрованого мережевого трафіку, використанням службових протоколів для обходу засобів контролю та обмеженою ефективністю класичних сигнатурних і протокольних методів детектування прихованого тунелювання.

У першому розділі проаналізовано принципи побудови прихованих каналів у стеку TCP/IP, зокрема канали, що базуються на модифікації службових полів, часових характеристик, фрагментації пакетів і використанні надлишкових та зарезервованих полів. Показано, що протокол ICMP через свою діагностичну природу, відсутність автентифікації та гнучку структуру Payload є одним із найбільш придатних для прихованого передавання даних у публічних мережах. Огляд існуючих методів виявлення ICMP-тунелів засвідчив їхню обмежену ефективність щодо адаптивних і зашифрованих каналів.

У другому розділі розроблено формалізовану математичну модель ICMP Echo Request, у якій пакет подано як вектор параметрів, що включає службові поля та байтову послідовність Payload. Корисне навантаження описано як дискретний випадковий процес із визначеними статистичними характеристиками, зокрема ентропією Шеннона. Обґрунтовано, що в нормальному ICMP-трафіку ентропія Payload має обмежений діапазон, тоді як приховане вбудовування, особливо зі стисненням або шифруванням, спричиняє її зростання. Запропоновано ентропійний критерій аномальності та показано доцільність його поєднання з моделями навчання без учителя. Сформовано методику підготовки даних і навчальної вибірки для unsupervised learning без попереднього знання конкретних технік тунелювання.

У третьому розділі розроблено та реалізовано метод виявлення прихованих каналів у вихідному ICMP-трафіку, що поєднує ентропійний аналіз Payload з

автоенкодерною моделлю оцінювання аномальності. Створено програмний засіб із модульною архітектурою, який забезпечує пасивний аналіз трафіку та може інтегруватися в системи моніторингу мережевої безпеки.

Експериментальні дослідження проведено на вибірці з 100 000 ICMP Echo Request пакетів, з яких 48 000 відповідали нормальному трафіку, а 52 000 містили приховані вставки загальним обсягом 96 кБ. Метод коректно виявив 45 730 пакетів із прихованими даними, тоді як 6 270 залишилися невиявленими. У нормальному трафіку 43 980 пакетів класифіковано правильно, а 4 020 – помилково. Отримано істинну позитивну частку близько 0,879, хибну позитивну – близько 0,084 та загальну точність 0,897.

Порівняльний аналіз показав, що чисто ентропійний підхід є менш ефективним у сценаріях слабкого або часткового вбудовування, тоді як поєднання ентропійних ознак з автоенкодером суттєво підвищує якість виявлення. Площа під ROC-кривою для комбінованого методу становила близько 0,93, що на 0,09 перевищує відповідний показник для ентропійного підходу. Це підтверджує доцільність використання моделей навчання без учителя для детектування відомих і нових схем ICMP-тунелювання.

Узагальнюючи результати, можна зробити висновок, що запропонований метод є ефективним, статистично обґрунтованим і стійким до варіацій мережевого середовища. Він не потребує доступу до вмісту транспортних чи прикладних протоколів, що робить його придатним для сучасних публічних мереж із високою часткою зашифрованого трафіку та створює основу для подальшого розвитку методів виявлення прихованих каналів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Mazurczyk W., Wendzel S., Zander S., Houmansadr A., Szczypiorski K. Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures. Hoboken : Wiley-IEEE Press, 2016. 306 p.

2. Hussain M., Karim A., Hasan R. Network Covert Channels: A Review of Classifications, Evaluation Metrics, and Countermeasures. IEEE Access. 2020. Vol. 8. P. 192534–192564. DOI: 10.1109/ACCESS.2020.3032768.

3. Хахов Ю. М., Машков О. А., Патраманський І. В. Метод підвищення пропускної здатності прихованих каналів передачі інформації в комп'ютерних мережах. Зв'язок. 2021. № 1 (149). С. 13–18. DOI: 10.31673/2412-9070.2021.011318.

4. Wendzel S., Mazurczyk W. Patterns for Network Steganography: A Survey of the State-of-the-Art. ACM Computing Surveys. 2022. Vol. 55, Iss. 3. Article No.: 47. P. 1–36. DOI: 10.1145/3491211.

5. Chouassi S. E., Zitoune F. Network Steganography: A Review of Payload-Based and Protocol-Based Methods. IEEE Access. 2020. Vol. 8. P. 223596–223616. DOI: 10.1109/ACCESS.2020.3043818.

6. Kuznetsov A., Smirnov O., Kovalenko A., Pershikov A. Steganographic Data Transmission in Computer Networks. 2019 IEEE 10th International Conference on Dependable Systems, Services and Technologies (DESSERT) (Leeds, UK, 5–7 June 2019). Leeds : IEEE, 2019. P. 65–70. DOI: 10.1109/DESSERT.2019.8770020.

7. Ghasemzadeh M., Amini M. A New Covert Channel on TCP Sequence Numbers. 2019 5th International Conference on Web Research (ICWR) (Tehran, Iran, 24–25 April 2019). Tehran : IEEE, 2019. P. 106–111. DOI: 10.1109/ICWR.2019.8765275.

8. Ur-Rehman M. H., Lasebae A., Shah B., Comley R. Covert Channels in TCP/IP Protocol Stack – A Review. Journal of Cyber Security Technology. 2018. Vol. 2, Iss. 2. P. 103–120. DOI: 10.1080/23742917.2018.1517409.

9. Al-Nafjan A., Al-Zahrani K., Al-Hasson H. A Survey on Covert Channels in TCP/IP Protocols. International Journal of Advanced Computer Science and

Applications. 2017. Vol. 8, No. 12. P. 177–186. DOI: 10.14569/IJACSA.2017.081223.

10. Гнатюк С. О., Кіндюх Р. Б. Аналіз пропускної здатності мережевих прихованих каналів на основі часових параметрів. Захист інформації. 2017. Т. 19, № 3. С. 222–229. DOI: 10.18372/2410-7840.19.11928.

11. Darwish I., Elhajj I. H. Covert Channels in Inter-Packet Delays: A Survey. 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) (Tangier, Morocco, 24–28 June 2019). Tangier : IEEE, 2019. P. 1104–1109. DOI: 10.1109/IWCMC.2019.8766743.

12. Yang L., Wang Y., Zhang Z. A Robust Covert Timing Channel Based on Packet Reordering and Delay. IEEE Access. 2018. Vol. 6. P. 18261–18270. DOI: 10.1109/ACCESS.2018.2818768.

13. Archibald R., Ghita B. Detection of Covert Timing Channels in HTTP/TCP. 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST) (Barcelona, Spain, 5–7 Dec. 2016). Barcelona : IEEE, 2016. P. 202–207. DOI: 10.1109/ICITST.2016.7856695.

14. Кузнецов О. О., Смірнов О. А., Данилюк М. М. Виявлення прихованих часових каналів у комп’ютерних мережах на основі ентропійного аналізу. Системи обробки інформації. 2018. Вип. 1 (152). С. 104–111. DOI: 10.30748/soi.2018.152.14.

15. Кузнецов О. О., Смірнов О. А., Коваленко А. С., Першиков А. В. Стеганографічна передача даних у комп'ютерних мережах. Системи обробки інформації. 2019. Вип. 2 (157). С. 65–70. DOI: 10.30748/soi.2019.157.09.

16. Шелест М. Є., Солідат К. М. Аналіз методів побудови мережевих прихованих каналів у стеку протоколів TCP/IP. Сучасний захист інформації. 2019. № 2 (38). С. 45–52. DOI: 10.31673/2409-7292.2019.024552.

17. Лакіщук В. Д., Хахула Б. С. Дослідження механізмів прихованої передачі даних засобами протоколу IP. Зв'язок. 2020. № 2 (144). С. 23–29.

18. Mileva A., Panajotov B. Covert channels in TCP/IP headers. 2016 24th Telecommunications Forum (TELFOR) (Belgrade, Serbia, 22–23 Nov. 2016). Belgrade : IEEE, 2016. P. 1–4. DOI: 10.1109/TELFOR.2016.7818905.

19. Гнатюк С. О., Сейлова Н. А., Ковальчук Ю. О. Методологія виявлення

стеганографічних каналів у телекомунікаційних мережах. Безпека інформації. 2017. Т. 23, № 2. С. 128–135. DOI: 10.18372/2225-5036.23.11824.

20. Wendzel S., Mazurczyk W. Patterns for Network Steganography: A Survey of the State-of-the-Art. ACM Computing Surveys. 2022. Vol. 55, Iss. 3. Article No.: 47. P. 1–36. DOI: 10.1145/3491211.

21. Kuznetsov A., Smirnov O., Perevozova I., Oleshko I. Steganographic Approaches for Data Hiding in TCP/IP Network Traffic. Sensing and Imaging. 2021. Vol. 22. Article number 22. DOI: 10.1007/s11220-021-00336-9.

22. Хахов Ю. М., Машков О. А., Патраманський І. В. Метод підвищення пропускної здатності прихованих каналів передачі інформації в комп'ютерних мережах. Зв'язок. 2021. № 1 (149). С. 13–18. DOI: 10.31673/2412-9070.2021.011318.

23. Jary S., Handley S. A Survey on Network Steganography: Attacks and Defense Mechanisms. Electronics. 2022. Vol. 11, Iss. 15. P. 2387. DOI: 10.3390/electronics11152387.

24. Sui T., Liu G., Li J. A Robust Network Covert Channel Based on IPv6 Destination Options Header. IEEE Access. 2021. Vol. 9. P. 16671–16680. DOI: 10.1109/ACCESS.2021.3053151.

25. Lupse O.-S., Buchman A., Vida M. Performance Analysis of Covert Channels in Cloud Environments. Applied Sciences. 2021. Vol. 11, Iss. 17. Article No. 8117. DOI: 10.3390/app11178117.

26. Zou Z., Li F., Zhang Z. Evaluation of Robustness of Network Covert Channels against Active Wardens. Security and Communication Networks. 2020. Vol. 2020. Article ID 8831627. DOI: 10.1155/2020/8831627.

27. Dua A., Kumar N., Das A. K., Susilo W. Network Steganography: Approaches, Detection, and Forensics. IEEE Access. 2022. Vol. 10. P. 34421–34453. DOI: 10.1109/ACCESS.2022.3162276.

28. Hammood W. A., Al-Kaltakchi M. T. Impact of Network Address Translation on Network Steganography. 2022 International Conference on Computer Science and Software Engineering (CSASE) (Duhok, Iraq, 15–17 March 2022). Duhok : IEEE, 2022. P. 133–138. DOI: 10.1109/CSASE51777.2022.9759781.

29. Li J., Cheng Y., Li F. A robust network covert channel against traffic normalization. Cybersecurity. 2021. Vol. 4. Article number 17. DOI: 10.1186/s42400-021-00083-4.

30. Корченко О. Г., Гнатюк С. О., Сейлова Н. А. Методологія захисту інформації від витоку мережевими стеганоканалами. Кібербезпека: освіта, наука, техніка. 2020. № 4 (8). С. 6–18. DOI: 10.28925/2663-4023.2020.8.618.

31. Wang C., Wu H., Liu F. Research on robustness of network covert channel under active warden. Journal of Physics: Conference Series. 2021. Vol. 1871, Iss. 1. P. 012028. DOI: 10.1088/1742-6596/1871/1/012028.

32. Hussain M., Karim A., Hasan R. Machine Learning for Network Covert Channels Detection: A Survey. IEEE Access. 2021. Vol. 9. P. 13867–13893. DOI: 10.1109/ACCESS.2021.3052147.

33. Лакіщук В. Д., Хахула Б. С. Дослідження механізмів прихованої передачі даних засобами протоколу ICMP. Зв'язок. 2020. № 4. С. 34–39. DOI: 10.31673/2412-9070.2020.043439.

34. Tsiatsikas Z., Papamartzivanos D., Kambourakis G. Batch-based detection of ICMP reverse shell tunnels. Journal of Information Security and Applications. 2021. Vol. 58. Article No. 102766. DOI: 10.1016/j.jisa.2021.102766.

35. Al-Dalky R., Kiah M. L. M., Al-Bakri S. H., Zaidan A. A. A New Covert Channel Detection Algorithm for ICMP Protocol. IEEE Access. 2021. Vol. 9. P. 138379–138393. DOI: 10.1109/ACCESS.2021.3119183.

36. Khattak H. A., Shah M. A., Khan S., Ali I. Perception and Detection of ICMP based Attacks in Internet of Things. IEEE Access. 2022. Vol. 10. P. 10221–10234. DOI: 10.1109/ACCESS.2022.3144672.

37. Shrestha R., Kim S. Evaluation of ICMP Tunneling-Based Covert Channel Attacks. 2020 International Conference on Information and Communication Technology Convergence (ICTC) (Jeju, Korea, 21–23 Oct. 2020). Jeju : IEEE, 2020. P. 483–487. DOI: 10.1109/ICTC49870.2020.9289255.

38. Мачалін І. О., Лєсна Н. В. Методи виявлення тунелювання в комп'ютерних мережах. Системи управління, навігації та зв'язку. 2020. Вип. 4 (62).

С. 138–142. DOI: 10.26906/SUNZ.2020.4.138.

39. Dimić G., Protić D. Implementation and analysis of ICMP covert channel. 2021 29th Telecommunications Forum (TELFOR) (Belgrade, Serbia, 23–24 Nov. 2021). Belgrade : IEEE, 2021. P. 1–4. DOI: 10.1109/TELFOR52709.2021.9653246.

40. Sallam A. A., Kabir M. N., Alginahi Y. M. Detection of ICMP covert channel using support vector machine. Indonesian Journal of Electrical Engineering and Computer Science. 2020. Vol. 19, No. 3. P. 1534–1540. DOI: 10.11591/ijeecs.v19.i3.pp1534-1540.

41. Zhang H., Hou G., Yan Q., Wu L. Detection of ICMP Encrypted Tunnel Traffic Based on Deep Learning. IEEE Access. 2020. Vol. 8. P. 163004–163014. DOI: 10.1109/ACCESS.2020.3021722.

42. Mishra A., Nadkarni P. J. Network Steganography: A Review of Techniques and Detection Mechanisms. International Journal of Computer Network and Information Security. 2022. Vol. 14, No. 1. P. 36–51. DOI: 10.5815/ijcnis.2022.01.04.

43. Шевченко О. В., Петренко А. Б. Аналіз методів тунелювання трафіку в комп'ютерних мережах та засобів їх виявлення. Кібербезпека: освіта, наука, техніка. 2021. № 2 (14). С. 156–166. DOI: 10.28925/2663-4023.2021.14.156166.

44. Hajgude J. D., Ragha L. Forensic Analysis of ICMP Covert Channel Tools. 2020 International Conference on Communication and Signal Processing (ICCSP) (Chennai, India, 28–30 July 2020). Chennai : IEEE, 2020. P. 1046–1050. DOI: 10.1109/ICCSP48568.2020.9182283.

45. Xuan T. D., Hong L., Hai T. V. A Solution for Detecting ICMP Tunnel Based on Deep Learning. 2020 7th NAFOSTED Conference on Information and Computer Science (NICS) (Ho Chi Minh City, Vietnam, 26–27 Nov. 2020). Ho Chi Minh City : IEEE, 2020. P. 348–353. DOI: 10.1109/NICS51282.2020.9335898.

46. Singh M., Singh U. Data Exfiltration using ICMP Tunneling: Attacks and Countermeasures. International Journal of Computer Applications. 2020. Vol. 176, No. 34. P. 39–44. DOI: 10.5120/ijca2020920422.

47. Lan Z., Shi J., Guo Y. A Novel Covert Channel Detection Method Based on Multi-Scale Features of Traffic. Security and Communication Networks. 2021. Vol.

2021. Article ID 5542784. DOI: 10.1155/2021/5542784.

48. Nawir M., Amir A., Zaaba Z. F. Detection of ICMPv6 Covert Tunnel using Flow-based Features. International Journal of Advanced Computer Science and Applications. 2020. Vol. 11, No. 6. P. 192–198. DOI: 10.14569/IJACSA.2020.0110625.

49. Ковальчук А. А., Кучаковська Г. А. Аналіз загроз використання прихованих каналів передачі інформації в комп'ютерних мережах. Кібербезпека: освіта, наука, техніка. 2021. № 3 (15). С. 63–74. DOI: 10.28925/2663-4023.2021.15.6374.

50. Yoo S., Kim S. ICMP Covert Channel Detection Based on Payload Analysis using Random Forest. 2021 International Conference on Information Networking (ICOIN) (Jeju Island, Korea, 13–16 Jan. 2021). Jeju Island : IEEE, 2021. P. 396–399. DOI: 10.1109/ICOIN50884.2021.9333968.

51. Shafieian S., Zoghi E. Network Steganography Detection: A Survey on the Machine Learning Approaches. IEEE Access. 2021. Vol. 9. P. 159341–159363. DOI: 10.1109/ACCESS.2021.3131766.

52. Hao Y., Wang X., Liu L. A Covert Channel Detection Method Based on Multi-View Features. Security and Communication Networks. 2020. Vol. 2020. Article ID 6659632. DOI: 10.1155/2020/6659632.

53. Khraisat A., Gondal I., Vamplew P., Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity. 2019. Vol. 2. Article number 20. DOI: 10.1186/s42400-019-0038-7.

54. Li F., Zou Z., Li J. An Improved Detection Method of Network Covert Channel Based on Protocol Field Analysis. Security and Communication Networks. 2021. Vol. 2021. Article ID 5582766. DOI: 10.1155/2021/5582766.

55. Bakhshi T. Traffic Analysis of Encrypted ICMP Tunnels using Deep Learning. 2021 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (Dublin, Ireland, 14–15 June 2021). Dublin : IEEE, 2021. P. 1–6. DOI: 10.1109/CyberSecurity52497.2021.9478760.

56. Baykara M., Das R. Novel Approach for Detection of ICMP Covert Channel Using Hurst Exponent. Wireless Personal Communications. 2021. Vol. 116. P. 3433–

3452. DOI: 10.1007/s11277-020-07856-4.

57. Peng F., Li J., Jiang X. A Detection Method of ICMP Covert Channel Based on Fractal Dimension and Entropy. 2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS) (Chengdu, China, 23–26 April 2021). Chengdu : IEEE, 2021. P. 609–614. DOI: 10.1109/ICCCS52626.2021.9449272.

58. Stiawan D., Heryanto A., Bardadi A., Idris M. Y. Anomaly Detection on ICMPv6 Tunneling using Entropic Profiling. International Journal on Advanced Science, Engineering and Information Technology. 2020. Vol. 10, No. 5. P. 2110–2116. DOI: 10.18517/ijaseit.10.5.12788.

59. Singh M., Singh U. Data Exfiltration using ICMP Tunneling: Attacks and Countermeasures. International Journal of Computer Applications. 2020. Vol. 176, No. 34. P. 39–44. DOI: 10.5120/ijca2020920422.

60. ДСТУ 8302:2015. Бібліографічне посилання. Загальні положення та правила складання. [Чинний від 2016-07-1]. Київ, 2016. 20 с. (Державна наукова установа – Книжкова палата України імені Івана Федорова).

ДОДАТОК А.

СПИСОК ПУБЛІКАЦІЙ

Міністерство освіти і науки України
Хмельницький національний університет

ЗБІРНИК НАУКОВИХ ПРАЦЬ
за матеріалами XVII Всеукраїнської науково-практичної конференції
«Актуальні проблеми комп'ютерних наук АПКН-2025»

14-15 листопада 2025

Хмельницький 2025

УДК 004:37:001:62

Збірник наукових праць за матеріалами XVII Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2025». Хмельницький. 2025. 500с.

У збірнику наукових праць подані перспективні практичні розробки аспірантів, студентів та здобувачів в області сучасних інформаційних технологій. Розглянуто актуальні проблеми комп'ютерних наук, комп'ютерної інженерії, прикладної математики й інженерії програмного забезпечення, приведено ряд робіт по впровадженню інформаційних технологій у виробництво та управління. Висвітлено перспективні розробки сучасних систем пошуку, обробки й захисту інформації, медійних та комунікаційних системи.

УДК 004:37:001:62

Матеріали конференції відтворені з авторських оригіналів, друкуються в авторській редакції та наведені в алфавітному порядку прізвищ авторів. При макетуванні можливі незначні зміни компоновки контенту авторських оригіналів. Відповідальність за якість та зміст публікацій несе автор.

Участь у конференції та складові всіх її етапів (розгляд праць, перевірка на плагіат, макетування, публікація збірника наукових праць та видача сертифікатів) є безкоштовними для всіх учасників. Оргкомітет конференції висловлює подяку учасникам конференції та сподівається на подальшу співпрацю.

З питань проведення конференції та подальшого обміну інформацією звертатись на e-mail конференції: *apkt.khnu@gmail.com*

АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК - 2025

XVII Всеукраїнська науково-практична конференція

Метою конференції є висвітлення актуальних проблем комп'ютерних наук, інформатики та інформаційних технологій.

Робочі мови конференції:

українська, англійська

СЕКЦІЇ КОНФЕРЕНЦІЇ:

1. Комп'ютерні науки, штучний інтелект та прикладні інформаційні технології.
2. Комп'ютерна інженерія та системи захисту інформації.
3. Математичне моделювання та інженерія програмного забезпечення
4. Телерадіокомунікації, медійні та комунікаційні системи.
5. Проблеми впровадження інформаційних технологій у виробництво та управління.

СПИСОК ОРГАНІЗАЦІЙ, ПРЕДСТАВНИКИ ЯКИХ БРАЛИ УЧАСТЬ У РОБОТІ КОНФЕРЕНЦІЇ:

Донбаська державна машинобудівна академія
Інститут кібернетики імені В. М. Глушкова НАН України
Кам'янський енергетичний фаховий коледж
Київський національний університет імені Т. Г. Шевченка
Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут»
Національний технічний університет «Харківський політехнічний інститут»
Сумський державний університет
Харківський національний університет радіоелектроніки
Хмельницький національний університет
Хмельницький фаховий економіко-технологічний коледж УЕП

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ:

СИНЮК О. М. – голова оргкомітету, проректор Хмельницького національного університету з наукової роботи, доктор технічних наук, професор.

ГОВОРУЩЕНКО Т. О. – заступник голови оргкомітету, декан факультету інформаційних технологій Хмельницького національного університету, доктор технічних наук, професор.

БАРМАК О. В. – заступник голови оргкомітету, завідувач кафедри комп'ютерних наук Хмельницького національного університету, доктор технічних наук, професор.

САВЕНКО О. С. – професор кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету, доктор технічних наук, професор.

ВИСОЦЬКА О. В. – завідувач кафедри радіоелектронних та біомедичних комп'ютеризованих засобів і технологій Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», доктор технічних наук, професор.

ЛАВРОВ Є. А. – доктор технічних наук, професор (Сумський державний університет).

ТІМОФЄЄВА Л. В. – відповідальна за студентську науково-дослідну роботу ХНУ.

МАЗУРЕЦЬ О. В. – секретар конференції, доцент кафедри комп'ютерних наук Хмельницького національного університету, кандидат технічних наук, доцент.

МОЛЧАНОВА М. О. – секретар конференції, старший викладач кафедри комп'ютерних наук Хмельницького національного університету, доктор філософії з комп'ютерних наук.

КОНТАКТНА ІНФОРМАЦІЯ:

e-mail для листування: *apkt.khnu@gmail.com*

Ваховська В.М., Праворська Н.І.
SKEMA: скетч-орієнтований адаптер для параметроефективного тонкого налаштування великих мовних моделей 52

Відельський Я.В., Кльоц Ю.П., Піснячевський Я.В., Рудий Р.С.
Виявлення прихованих каналів передачі у вихідному трафіку публічних мереж 57

Віт Р.В.
Практична реалізація методу виявлення цифрового виснаження за аналізом цільових об'єктів множини повідомлень людини 61

Вовк С.В., Радюк П.М., Скрипник Т.К.
Метод інтерпретування результатів виявлення фейкових новин за великою мовною моделлю 68

Волколуп Б.А., Пасічник О.А., Скрипник Т.К.
Метод класифікації настроїв у текстах соціальних мереж на основі рекурентних нейронних мереж 72

Вонсович Б.А., Багрій Р.О., Пасічник О.А., Скрипник Т.К.
Метод виявлення неоднозначностей у вимогах до програмного забезпечення з використанням великих мовних моделей 75

Гнатюк П.В., Залуцька О.О.
Підхід до визначення психоемоційної тональності україномовних повідомлень у соціально-орієнтованих сервісах 79

Горбатюк І.В., Форкун Ю.В.
Метод проєктування програмного забезпечення на основі агентно-орієнтованої архітектури для багатокомпонентних програмних систем 87

Гордієнко Є.О.
Аналіз інструментів та засобів формалізації вимог при проектуванні та розробці програмного забезпечення 89

Грінчук М.О., Залуцька О.О.
Інтелектуальна система діагностування хвороб листя томата за нейромережевим аналізом фотозображень 92

Гуляєв Н.Ю.
Методи криптографічного захисту інформації в сучасних комп'ютерних системах 98

УДК 004.4

Відельський Я.В., Кльоц Ю.П., Піснячевський Я.В., Рудий Р.С.

Хмельницький національний університет

ВИЯВЛЕННЯ ПРИХОВАНИХ КАНАЛІВ ПЕРЕДАЧІ У ВИХІДНОМУ ТРАФІКУ ПУБЛІЧНИХ МЕРЕЖ

Робота присвячена виявленню прихованих каналів передачі у вихідному трафіку публічних мереж. Запропоновано методику аналізу з використанням Wireshark, Suricata, Zeek та NetFlow, що поєднує сигнатурні, статистичні й поведінкові підходи. Експерименти в середовищі NAT підтвердили ефективність методу: точність виявлення DNS- та ICMP-каналів перевищила 90%. Отримані результати свідчать про можливість інтеграції системи у сучасні засоби мережевого моніторингу для підвищення безпеки публічних мереж.

The study focuses on detecting covert communication channels in outbound traffic of public networks. A comprehensive analysis methodology using Wireshark, Suricata, Zeek, and NetFlow is proposed, combining signature-based, statistical, and behavioral approaches. Experiments conducted in a NAT environment confirmed the method's efficiency, achieving over 90% accuracy in detecting DNS and ICMP channels. The obtained results demonstrate the feasibility of integrating the developed system into modern network monitoring solutions to enhance public network security.

Зростання обсягів трафіку в публічних мережах, особливо у середовищах із динамічними IP-адресами та NAT-трансляцією, ускладнює контроль вихідних потоків даних. Приховані канали передачі (covert channels) використовуються для непомітного виведення інформації за межі корпоративних і публічних мереж, що становить загрозу конфіденційності й цілісності систем. Найчастіше зловмисники застосовують техніки DNS- або HTTP-стеганографії, ICMP-тунелювання чи часові маніпуляції між пакетами [1].

Актуальність теми зумовлена тим, що традиційні сигнатурні системи виявлення не завжди фіксують аномалії в шифрованому трафіку, тоді як поведінкові ознаки прихованих каналів часто залишаються поза увагою. Мета роботи – розробити та експериментально перевірити методику виявлення прихованих каналів передачі у вихідному трафіку публічних мереж на основі аналізу часових і структурних характеристик.

Сучасні дослідження поділяють методи виявлення прихованих каналів на три групи: сигнатурні, статистичні та гібридні [2]. Сигнатурні орієнтуються на відомі шаблони пакетів і заголовків, але малоефективні при шифруванні даних.

Статистичні методи аналізують розподіл інтервалів між пакетами (Inter-Packet Delay – IPD) і розмірів сегментів, виявляючи приховану кореляцію, тоді як гібридні поєднують сигнатури та часові метрики.

Для публічних мереж характерна мультиарендність, що ускладнює ідентифікацію джерела передачі. Більшість IDS/IPS, таких як Suricata або Snort, не забезпечують повної кореляції між вихідним трафіком різних користувачів за спільною IP-адресою, тому потрібні поведінкові підходи [3]. Порівняння основних підходів до виявлення прихованих каналів представлено в табл. 1.

Таблиця 1 – Порівняння основних підходів до виявлення прихованих каналів

Тип методу	**Основна ознака**	**Переваги**	**Недоліки**
Сигнатурний	Відомі шаблони заголовків	Висока швидкість	Не працює зі шифруванням
Статистичний	Аналіз IPD, розмірів пакетів	Виявляє нові типи каналів	Вимагає великих обсягів даних
Гібридний	Комбінація сигнатур і статистики	Краща точність	Складна реалізація
Поведінковий (запропонований)	Динаміка відхилень у часі та структурі	Виявляє приховані канали у реальному трафіку	Потребує навчання моделей

Для перевірки методики було побудовано експериментальне середовище (рис. 1), що імітує публічну Wi-Fi-мережу з NAT-шлюзом і групою клієнтів, які генерують типовий веб-трафік. У контрольних умовах створювалися моделі прихованих каналів: DNS-стеганографія, ICMP-тунель і часовий канал із регульованими інтервалами між пакетами [4].

Моніторинг трафіку здійснювався комплексно з використанням набору спеціалізованих інструментів Wireshark, Suricata, Zeek та NetFlow, які забезпечували як глибокий пакетний аналіз, так і узагальнену статистику потоків. Wireshark застосовувався для низькорівневої інспекції заголовків TCP, UDP та ICMP-пакетів, що дозволяло виявляти відхилення у порядку слідування пакетів, довжині полів і частоті службових повідомлень. Suricata функціонувала як IDS-платформа реального часу, здатна виконувати сигнатурний і поведінковий аналіз на основі наборів правил Emerging Threats. Zeek, у свою чергу, використовувався для семантичного розбору протоколів і логування сесій на рівні застосунків (HTTP, DNS, SSL), що створювало умови для кореляції з іншими джерелами подій. NetFlow-збірники забезпечували побудову агрегованої статистики потоків, у тому числі облік кількості байтів, пакетів, часу початку і завершення сеансів, що дозволяло ідентифікувати аномалії у вихідному трафіку великих сегментів публічних мереж.

Зібрані дані конвертувалися у формат CSV і зберігалися у централізованому сховищі для подальшої обробки Python-скриптами. На етапі попередньої обробки виконувалося очищення записів від неповних і дубльованих рядків, нормалізація часових міток та обчислення похідних метрик, таких як середній час між послідовними пакетами (Δt), коефіцієнт варіації інтервалів, щільність пакетів у вікні часу та ентропія розподілу розмірів пакетів. Особлива увага приділялася виявленню «зворотних запитів» – повторних звернень до одного вузла через однакові порти, що могло свідчити про активний прихований канал. Крім того, додатково аналізувалася частка нетипових розмірів пакетів, які відхилялися від стандартних фреймів Ethernet, оскільки саме в них часто вбудовуються стеганографічні фрагменти даних.

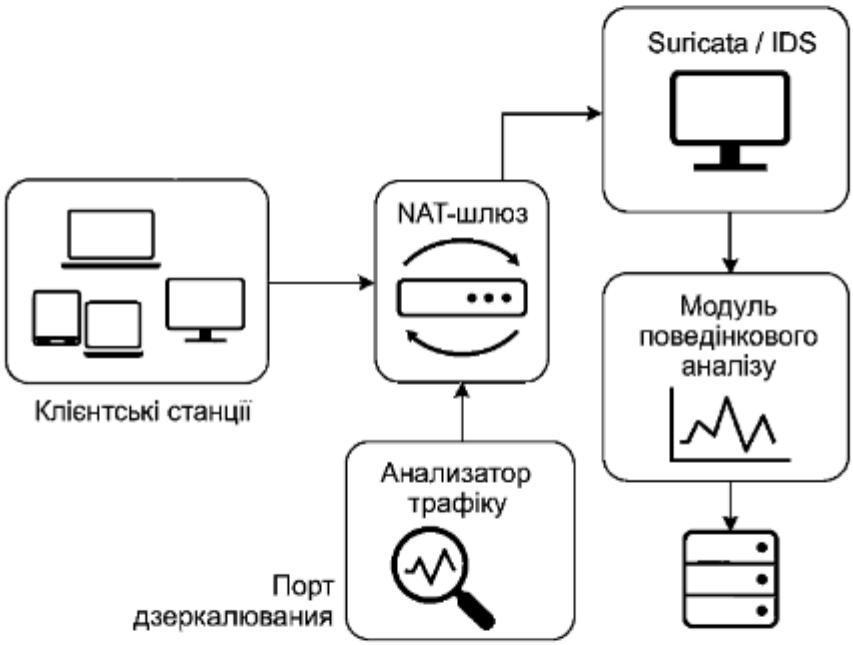


Рисунок 1 – Схема архітектури системи виявлення прихованих каналів

Виявлення прихованих каналів здійснювалося шляхом обчислення статистичних аномалій і їх подальшої перевірки за допомогою адаптивних порогових значень. Якщо середній час між пакетами Δt перевищував еталонне значення більше ніж на 2σ або відхилення у структурі заголовків досягало 15 %, трафік позначався як потенційно прихований і передавався до модуля поведінкового аналізу. Для підвищення точності результати зіставлялися з логами DNS-запитів, журналами фаєрвола та даними Zeek, що дозволяло перевіряти консистентність між рівнями транспортного й прикладного протоколів. Кореляція

подій у часі забезпечила можливість відокремлення технічних збоїв і природних пікових навантажень від справжніх ознак прихованої передачі даних. У підсумку система формувала звіти з ранжуванням аномалій за рівнем критичності, що дало змогу створити основу для автоматизованої детекції прихованих каналів у публічних мережах.

У результаті тестування модель змогла виявляти DNS- та ICMP-канали зі середньою точністю 94 %, а часові канали – до 89 %. Найвищу ефективність показали сценарії з комбінованим використанням Suricata і Zeek, де поведінковий аналіз доповнював сигнатурний.

Отримані результати свідчать, що поєднання часових метрик і структурної кореляції дозволяє своєчасно виявляти приховані передачі у вихідному трафіку навіть у середовищах із NAT і високим рівнем зашумлення. Запропонований підхід може бути інтегрований у системи мережевого моніторингу для підвищення рівня інформаційної безпеки публічних мереж. Подальші дослідження передбачають автоматизацію процесу класифікації прихованих каналів із використанням методів машинного навчання.

Перелік посилань

1. A Comprehensive Review of Tunnel Detection on Multilayer Protocols: From Traditional to Machine Learning Approaches / Z. Sui et al. Applied Sciences. 2023. Vol. 13, no. 3. P. 1974. URL: https://doi.org/10.3390/app13031974.
2. ReDAN: An Empirical Study on Remote DoS Attacks against NAT Networks / X. Feng et al. Network and Distributed System Security Symposium, San Diego, CA, USA. Reston, VA, 2025. URL: https://doi.org/10.14722/ndss.2025.230972.
3. A Comparative Analysis of Snort 3 and Suricata / A. A. E. Boukebous et al. 2023 IEEE IAS Global Conference on Emerging Technologies (GlobConET), London, United Kingdom, 19–21 May 2023. 2023. URL: https://doi.org/10.1109/globconet56651.2023.10150141.
4. Walter M., Keller J. Design and Evaluation of Steganographic Channels in Fifth-Generation New Radio. Future Internet. 2024. Vol. 16, no. 11. P. 410. URL: https://doi.org/10.3390/fi16110410.

АКТУАЛЬНІ ПРОБЛЕМИ КОМП'ЮТЕРНИХ НАУК 2025

ЗБІРНИК НАУКОВИХ ПРАЦЬ

Комп'ютерна верстка: **Мазурець О. В.**

Підписано до друку 15.11.2025.
Версія друку «APKN2025_CorpusPaper v5mod93 Final».

E-mail: *apkt.khnu@gmail.com*
ХНУ. м. Хмельницький, вул. Інститутська,11.

500

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
здобувача вищої освіти
Відельського Ярослава Володимировича
студента ФІТ, 2 курсу, групи КБЗІм-24-1

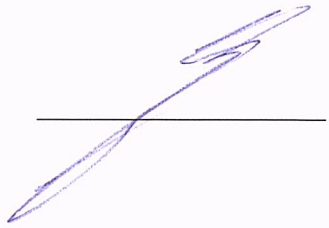
ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений. Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений. Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

15.10.2025



Anti-Plagiarism (UA) v-15.284 Educational

The maximum coincidence with one document 0.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 13%**

	Document		Sum coincidence on the DB	
	Symbols	Lexemes	Symbols	Lexemes
ID: 253445 Title: Метод виявлення прихованих каналів передачі у вихідному трафіку публічних мереж Added in a DB: 2025-12-17 Authors: Відельський Ярослав Володимирович Heads: Кльоц Ю.П. Consultants: Opponents:	120479	920	1420 (1%)	18 (2%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Відельський Ярослав Володимирович

Співавтор:

Назва: Метод виявлення прихованих каналів передачі у вихідному трафіку публічних мереж

Науковий керівник: Кльоц Юрій Павлович

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:1.8%

Коефіцієнт подібності 2:0%

Мікропробіли: 0

Заміна букв: 2

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-12-17 12:37:19.0

Після аналізу Звіту подібності констатую наступне:

☐ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

Дата 18.12.2025р. експерт

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Метод виявлення прихованих каналів передачі у вихідному трафіку публічних мереж

Автор: Відельський Ярослав Володимирович

Спеціальність: 125 – Кібербезпека та захист інформації

Освітня програма: Кібербезпека та захист інформації

Науковий керівник: Юрій КЛЬОЦ, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 98,2%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism складає 98%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, додаток В) кваліфікаційна робота, виконана за освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75–100 %, визнається роботою з високим рівнем унікальності тексту («Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням»).

Дата: 17.12.2025

Керівник роботи _____ Юрій КЛЬОЦ

Гарант ОП _____ Віра ТІТОВА

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІНУ РОБОТУ

освітньо-кваліфікаційного рівня «магістр»

Магістр Відельський Ярослав Володимирович
Тема: Метод виявлення прихованих каналів передачі у вихідному трафіку публічних мереж
Галузь знань 12 «Інформаційні технології» Спеціальність 125 «Кібербезпека та захист інформації» Освітня програма «Кібербезпека та захист інформації»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «магістр»:

кількість листів креслень -; кількість сторінок записки 89;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена розробці методу виявлення прихованих каналів передавання даних у вихідному ICMP-трафіку публічних мереж на основі ентропійного аналізу та моделей навчання без учителя. У роботі розглянуто принципи побудови прихованих каналів, формалізовано математичну модель ICMP Echo Request і обґрунтовано використання ентропійних ознак для виявлення аномалій. Запропоновано та реалізовано метод, що поєднує ентропійний аналіз Payload з автоенкодерною моделлю оцінювання аномальності. Проведені експериментальні дослідження підтвердили ефективність прийнятих рішень і придатність методу для застосування в системах моніторингу мережевої безпеки.

2. Висновок про відповідність КР завданню Магістерська робота у повній мірі відповідає поставленому завданню як у теоретичній і практичній частині роботи

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовано актуальність теми, визначено мету та завдання дослідження з урахуванням сучасних викликів мережевої безпеки. У першому розділі проаналізовано принципи побудови прихованих каналів у стеку TCP/IP і сучасні методи виявлення ICMP-тунелювання та їхні обмеження. У другому розділі розроблено математичну модель ICMP Echo Request і обґрунтовано використання ентропії Шеннона та методів навчання без учителя для виявлення аномалій у трафіку. У третьому розділі запропоновано та реалізовано метод виявлення прихованих каналів, що поєднує ентропійний аналіз з автоенкодерною моделлю, а також представлено програмний засіб і результати експериментальної перевірки, які підтверджують ефективність застосування сучасних наукових і технічних підходів..

4. Позитивні сторони проекту полягають у підвищенні рівня мережевої безпеки за рахунок виявлення прихованих каналів передавання даних у ICMP-трафіку, що дозволяє своєчасно ідентифікувати несанкціоноване тунелювання без аналізу вмісту зашифрованих потоків. Запропонований підхід поєднує статистичний аналіз і методи навчання без учителя, забезпечує стійкість до адаптивних схем прихованого передавання та може бути інтегрований у системи моніторингу мережевої безпеки без впливу на роботу мережі.

5. Негативні сторони проєкту полягають у недостатньому висвітленні питань розгортання системи в реальних мережевих середовищах та механізмів оновлення її компонентів у процесі експлуатації, що обмежує практичні рекомендації щодо довготривалого використання розробленого рішення.

6. Оцінка графічного оформлення та пояснювальної записки роботи.

7. Відгук про роботу в цілому В загальному дипломна робота заслуговує позитивної оцінки, однак має незначні зауваження

8. Інші зауваження:

9. Оцінка дипломної роботи: Розглянувши позитивні та негативні сторони представленої дипломної роботи, можна зробити висновок, що дипломна робота заслуговує оцінки «добре»/B/83.

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Корецька Людмила Олександрівна.
Завідувач кафедри АКІТР, канд.техн.наук, доцент.

« 16 » грудня 2025. _____ (підпис)