УДК 004.728.5

О. В. Салієва
Д. О. Пінчук

МЕТОДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ ПРИХОВАНИМ КАНАЛАМ ВИТОКУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ НА ОСНОВІ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ ТА ПОВЕДІНКОВИХ МОДЕЛЕЙ

Вінницький національний технічний університет

Анотація

У роботі досліджено проблему функціонування прихованих каналів витоку інформації в комп'ютерних мережах, які дозволяють здійснювати несанкціоновану передачу даних шляхом використання легітимних мережевих протоколів. Проведено аналіз сучасних підходів до їх виявлення, зокрема статистичного аналізу мережевого трафіку та методів поведінкового моделювання. Запропоновано комплексний підхід до виявлення прихованих каналів із використанням методів машинного навчання, що дозволяє підвищити точність детектування та знизити рівень хибних спрацювань.

Ключові слова: приховані канали, комп'ютерні мережі, витік інформації, аналіз трафіку, ентропія, машинне навчання, кібербезпека.

Abstract

This paper investigates the issue of covert information leakage channels in computer networks, which enable unauthorised data transmission through the use of legitimate network protocols. An analysis of current approaches to their detection is carried out, in particular statistical analysis of network traffic and behavioural modelling methods. A comprehensive approach to detecting covert channels using machine learning methods is proposed, which allows for improved detection accuracy and a reduction in the false positive rate.

Keywords: covert channels, computer networks, data leakage, traffic analysis, entropy, machine learning, cybersecurity.

Вступ

У сучасних умовах стрімкого розвитку інформаційних технологій та глобалізації мережевої інфраструктури питання забезпечення кібербезпеки комп'ютерних мереж набуває особливої актуальності. Зростання обсягів передавання даних, використання розподілених систем і хмарних сервісів створює нові можливості для функціонування як легітимних сервісів, так і прихованих механізмів передачі інформації.

Однією з найбільш складних і водночас малодосліджених загроз є приховані канали витоку інформації (covert channels), які дозволяють здійснювати несанкціоновану передачу даних шляхом використання штатних мережевих протоколів та сервісів. Особливістю таких каналів є їх здатність маскуватися під нормальний мережевий трафік, що значно ускладнює їх виявлення традиційними засобами захисту інформації. Сучасні дослідження показують, що традиційні системи виявлення вторгнень не забезпечують достатнього рівня ефективності у протидії прихованим каналам, оскільки вони орієнтовані переважно на сигнатурний аналіз відомих загроз. У зв'язку з цим зростає необхідність розробки нових підходів до аналізу мережевого трафіку, які враховують поведінкові особливості функціонування мережі та дозволяють виявляти аномалії у її роботі.

Перспективним напрямом є використання статистичних методів аналізу та алгоритмів машинного навчання, які дозволяють здійснювати глибокий аналіз великих обсягів мережевих даних і виявляти приховані закономірності. Поєднання цих підходів відкриває можливості для створення ефективних систем виявлення прихованих каналів витоку інформації.

Метою даної роботи є аналіз методів виявлення та протидії прихованим каналам витоку інформації в комп'ютерних мережах, а також розробка комплексного підходу на основі аналізу мережевого трафіку та поведінкових моделей.

Результати дослідження

Приховані канали витоку інформації (covert channels) є специфічним класом загроз у комп'ютерних мережах, які дозволяють передавати інформацію у спосіб, що не передбачений політикою безпеки системи. На відміну від традиційних каналів передачі даних, вони використовують легітимні механізми функціонування системи, що робить їх малопомітними для стандартних засобів контролю та захисту інформації. Концепція прихованих каналів була вперше формалізована у роботах, присвячених проблемі ізоляції інформаційних потоків у багатокористувацьких системах [1].

Згідно з класичним підходом, приховані канали поділяються на два основні типи: канали зберігання (storage channels) та часові канали (timing channels). Канали зберігання реалізуються шляхом модифікації спільних ресурсів або структур даних, наприклад полів заголовків мережевих пакетів. У свою чергу, часові канали базуються на зміні часових характеристик обробки або передачі інформації, таких як затримки між пакетами або швидкість передачі даних. Така класифікація є базовою для розуміння механізмів функціонування прихованих каналів та їх подальшого аналізу. У комп'ютерних мережах приховані канали можуть реалізовуватись на різних рівнях мережевої взаємодії, включаючи мережевий, транспортний та прикладний рівні. При цьому різноманітність протоколів і механізмів передачі даних створює широкі можливості для прихованої передачі інформації, що значно ускладнює процес їх виявлення. Сучасні дослідження показують, що більшість відомих методів реалізації прихованих каналів можуть бути узагальнені у вигляді обмеженої кількості шаблонів, що повторюються в різних протоколах [2].

Реалізація прихованих каналів у комп'ютерних мережах часто базується на модифікації службових полів мережевих протоколів. Зокрема, у протоколах IP та TCP можуть використовуватись резервні або мало контрольовані поля заголовків для вбудовування додаткової інформації. Наприклад, зміна ідентифікаторів пакетів, прапорців або порядкових номерів може використовуватись для передачі бітових послідовностей між відправником і отримувачем без порушення загальної логіки мережевої взаємодії [3].

Окрему категорію становлять часові приховані канали, в яких інформація передається шляхом варіювання інтервалів між передачею пакетів або зміни швидкості передачі даних. У таких каналах кожен часовий інтервал або його зміна може інтерпретуватися як біт інформації. Незважаючи на відсутність змін у структурі пакетів, подібні методи є ефективними, оскільки складно відрізнити навмисну модуляцію затримок від природних коливань мережевого трафіку. Також широкого поширення набули приховані канали, що використовують прикладні протоколи, зокрема DNS та HTTP. Одним із найбільш відомих прикладів є DNS-тунелювання, при якому дані кодуються у DNS-запитах і відповідях. Це дозволяє обходити мережеві екрани та системи фільтрації, оскільки DNS-трафік зазвичай дозволений у більшості мереж. Подібні підходи активно використовуються як у легітимних цілях (наприклад, для обходу обмежень), так і зловмисниками для ексфільтрації даних [4].

Крім того, приховані канали можуть комбінувати декілька методів одночасно, що значно підвищує їхню стійкість до виявлення. Наприклад, поєднання модифікації заголовків пакетів із часовою модуляцією дозволяє створювати більш складні та менш помітні канали передачі інформації. Такі гібридні підходи ускладнюють аналіз мережевого трафіку та вимагають застосування комплексних методів детектування [5].

У сучасних комп'ютерних мережах для виявлення загроз широко застосовуються системи виявлення та запобігання вторгненням (IDS/IPS), які реалізують переважно сигнатурний підхід. Сутність такого підходу полягає у порівнянні мережевого трафіку з базою відомих шаблонів атак. Хоча цей метод є ефективним для виявлення вже відомих загроз, він виявляється малоефективним щодо прихованих каналів, оскільки останні часто не мають чітко визначених сигнатур і можуть змінювати свою поведінку [6].

Альтернативою сигнатурному підходу є евристичні та методи виявлення аномалій, які базуються на виявленні відхилень від нормальної поведінки мережі. Однак ефективність таких методів значною мірою залежить від якості сформованих правил і профілів. У випадку прихованих каналів ці методи часто демонструють низьку точність через здатність таких каналів імітувати легітимний трафік, що призводить до високого рівня хибних результатів. Крім того, традиційні системи виявлення мають обмеження, пов'язані з припущенням про "закритий світ", у якому всі можливі типи атак відомі заздалегідь. У реальних умовах це припущення не виконується, оскільки зловмисники постійно

розробляють нові методи прихованої передачі інформації. Це робить класичні підходи недостатньо адаптивними до нових загроз [7].

Таким чином, аналіз традиційних методів виявлення показує їх обмежену ефективність у контексті протидії прихованим каналам витоку інформації, що обумовлює необхідність розробки більш гнучких та інтелектуальних підходів до аналізу мережевого трафіку [6].

Одним із ефективних підходів до виявлення прихованих каналів є статистичний аналіз мережевого трафіку, який базується на дослідженні характеристик переданих даних. До основних параметрів, що підлягають аналізу, належать розміри пакетів, інтервали між їх передачею, частота появи певних значень у заголовках, а також розподіл трафіку у часі. Виявлення відхилень цих параметрів від нормального профілю може свідчити про наявність прихованих каналів витоку інформації [8].

Важливим інструментом статистичного аналізу є використання ентропійних характеристик, зокрема ентропії Шеннона, яка дозволяє оцінити рівень невизначеності або випадковості даних у мережевому трафіку. Зміни ентропії можуть вказувати на аномальну поведінку, зокрема на наявність структурованих прихованих повідомлень у потоці даних, які зазвичай мають інші статистичні властивості порівняно з нормальним трафіком [9].

Додатково застосовуються методи аналізу розподілів імовірностей та кореляційних залежностей між параметрами трафіку. Наприклад, аналіз автокореляції міжпакетних інтервалів дозволяє виявляти періодичні або штучно сформовані патерни, характерні для часових прихованих каналів. Такі методи дають змогу виявляти навіть слабко виражені аномалії у великих обсягах мережевих даних [10].

Водночас, статистичні методи мають певні обмеження, пов’язані з високою чутливістю до варіативності мережевого трафіку та складністю формування універсальних порогових значень для виявлення аномалій. Це зумовлює необхідність поєднання статистичних підходів із більш адаптивними методами, зокрема алгоритмами машинного навчання [8].

У зв’язку з обмеженнями традиційних та статистичних методів, все більшого поширення набувають підходи, засновані на використанні методів машинного навчання для аналізу мережевого трафіку. Основною перевагою таких методів є здатність автоматично виявляти складні залежності та приховані закономірності у великих обсягах даних без необхідності явного задання правил детектування. Серед найбільш поширених підходів використовуються алгоритми класифікації, такі як метод опорних векторів (SVM), дерева рішень та ансамблеві методи, зокрема Random Forest. Ці алгоритми дозволяють будувати моделі, які розрізняють нормальний та аномальний мережевий трафік на основі попередньо розмічених даних. Їх застосування демонструє високу ефективність при виявленні складних атак, у тому числі прихованих каналів витоку інформації [11].

Окрім цього, важливу роль відіграють методи неконтрольованого навчання, зокрема алгоритми кластеризації, які дозволяють виявляти аномалії без попереднього маркування даних. Такі підходи є особливо корисними в умовах, коли відсутні повні набори даних для навчання або коли необхідно виявляти нові, раніше невідомі типи прихованих каналів. Важливим напрямом є також використання гібридних моделей, які поєднують сигнатурні та підходи з виявленням аномалій. Такі системи дозволяють одночасно враховувати відомі шаблони атак і виявляти нові відхилення у поведінці мережі, що значно підвищує загальну ефективність виявлення загроз [12].

З урахуванням проаналізованих підходів доцільним є використання комплексного методу виявлення прихованих каналів витоку інформації, який поєднує статистичний аналіз мережевого трафіку та методи машинного навчання. Такий підхід дозволяє враховувати як кількісні характеристики трафіку, так і складні поведінкові залежності, що формуються у процесі функціонування мережі. Комбінування різних методів є одним із ключових напрямів розвитку сучасних систем виявлення аномалій [13].

Запропонований підхід передбачає формування базового профілю нормального мережевого трафіку на основі історичних даних. Для цього здійснюється збір мережевих параметрів, таких як міжпакетні інтервали, розміри пакетів, частота передачі та інші статистичні характеристики. Отримані дані використовуються для побудови моделі нормальної поведінки, яка надалі виступає еталоном для порівняння. Відхилення від цього профілю можуть інтерпретуватися як потенційні ознаки прихованих каналів [13].

На наступному етапі здійснюється витяг ознак (feature extraction) та їх аналіз із використанням статистичних методів, зокрема оцінки ентропії, дисперсії та кореляційних залежностей. Це дозволяє зменшити розмірність даних і виділити найбільш інформативні характеристики трафіку. Подібні підходи широко застосовуються в задачах виявлення аномалій, оскільки дозволяють підвищити

ефективність подальшого машинного аналізу. Далі отримані ознаки подаються на вхід алгоритмів машинного навчання, які здійснюють класифікацію або кластеризацію мережевого трафіку. У межах запропонованого підходу доцільно використовувати комбінацію контрольованих та неконтрольованих методів, що дозволяє одночасно виявляти як відомі, так і нові типи прихованих каналів. Такий гібридний підхід забезпечує більш високу адаптивність системи до змін у мережевому середовищі [12].

Узагальнено запропонований підхід може бути представлений у вигляді послідовності етапів: збір мережевого трафіку, попередня обробка даних, витяг ознак, статистичний аналіз, застосування алгоритмів машинного навчання та прийняття рішення щодо наявності аномалій. Така багаторівнева модель дозволяє підвищити точність виявлення прихованих каналів та зменшити кількість хибних спрацювань [13].

Висновки

У результаті проведеного дослідження встановлено, що приховані канали витоку інформації становлять одну з найбільш складних і небезпечних загроз для безпеки комп'ютерних мереж, оскільки дозволяють здійснювати передачу даних у спосіб, який не контролюється традиційними засобами захисту. Їх використання базується на експлуатації легітимних механізмів мережевих протоколів, що суттєво ускладнює процес виявлення.

Проаналізовано основні методи реалізації прихованих каналів, зокрема модифікацію полів заголовків мережевих пакетів, використання часових характеристик трафіку та застосування прикладних протоколів. Встановлено, що традиційні сигнатурні та евристичні підходи до виявлення загроз є недостатньо ефективними в умовах динамічного розвитку методів прихованої передачі інформації.

Показано, що статистичний аналіз мережевого трафіку, зокрема із використанням ентропійних характеристик, дозволяє виявляти аномалії у поведінці мережі, однак має обмеження, пов'язані з варіативністю трафіку та складністю визначення порогових значень. У зв'язку з цим обґрунтовано доцільність застосування методів машинного навчання, які забезпечують більш гнучкий та адаптивний аналіз мережевих даних. Запропоновано комплексний підхід до виявлення прихованих каналів витоку інформації, що поєднує статистичні методи аналізу та алгоритми машинного навчання. Такий підхід дозволяє підвищити точність виявлення, зменшити кількість хибних спрацювань та забезпечити адаптацію до нових типів загроз. Отримані результати можуть бути використані при розробці сучасних систем захисту інформації та вдосконаленні засобів моніторингу безпеки комп'ютерних мереж.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cabuk S. CERIAS : CERIAS - Purdue University. URL: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2006-53.pdf (дата звернення: 19.03.2026).
2. Zander S. Covert channels and countermeasures in computer network protocols. ResearchGate. URL: https://www.researchgate.net/publication/3200183_Covert_channels_and_countermeasures_in_computer_network_protocols_Reprinted_from_IEEE_Communications_Surveys_and_Tutorials (дата звернення: 19.03.2026).
3. Shirey R. RFC 4949: Internet Security Glossary, Version 2. IETF Datatracker. URL: https://datatracker.ietf.org/doc/html/rfc4949 (дата звернення: 19.03.2026).
4. Rezaei A. Rejuvenating High Available Virtualized Systems. IEEExplore. URL: https://ieeexplore.ieee.org/document/5438079 (дата звернення: 19.03.2026).
5. Schmidbauer T., Wendzel S. SoK: A Survey Of Indirect Network-level Covert Channels. Zenodo. URL: https://zenodo.org/records/6349088 (дата звернення: 20.03.2026).
6. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Technical Series Publications. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf (дата звернення: 20.03.2026).

7. Sommer R. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Xplore. URL: https://ieeexplore.ieee.org/document/5504793 (дата звернення: 20.03.2026).
8. Liang H. Cooperative data dissemination via roadside WLANs. IEEE Xplore. URL: https://ieeexplore.ieee.org/document/6178836 (дата звернення: 20.03.2026).
9. SHANNON C. E. The Bell System Technical Journal. Harvard Mathematics Department : Home page. URL: https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf (дата звернення: 20.03.2026).
10. Osterlind F. Cross-Level Sensor Network Simulation with COOJA. IEEE Xplore. URL: https://ieeexplore.ieee.org/document/4116633 (дата звернення: 20.03.2026).
11. Buczak A. L. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Xplore. URL: https://ieeexplore.ieee.org/document/7307098 (дата звернення: 20.03.2026).
12. Ring M. A survey of network-based intrusion detection data sets. Science Direct. URL: https://www.sciencedirect.com/science/article/abs/pii/S016740481930118X (дата звернення: 20.03.2026).
13. Chandola, Varun. Anomaly Detection: A Survey. University of Minnesota. URL: https://conservancy.umn.edu/items/9dbaeaa6-e0fc-4089-b3e0-82df90129904 (дата звернення: 20.03.2026).

Пінчук Дар'я Олександрівна **–** студентка групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: dashapinchukschool@gmail.com

Науковий керівник: ***Салієва Ольга Володимирівна*** – доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@vntu.edu.ua

Pinchuk Daria O. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: dashapinchukschool@gmail.com

Supervisor: **Saliieva Olha V**. – Doctor of Philosophy (PhD) in specialty 125 "Cybersecurity", Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, email: salieva8257@ vntu.edu.ua