УДК 004.056.5:004.7

В. І. Кубіря
В. В. Гуменюк

МЕТОД ПРОГРАМНОГО ВИЯВЛЕННЯ МЕРЕЖЕВИХ ПРИХОВАНИХ КАНАЛІВ ДЛЯ ПРОТИДІЇ ВИТОКУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Вінницький національний технічний університет

Анотація

У тезах розглянуто мережеві приховані канали як механізм прихованого виведення даних, що маскується під штатний мережевий обмін. Проаналізовано storage-based і timing-based канали, визначено основні ознаки їх програмного виявлення та запропоновано підхід до виявлення на основі аналізу статистичних, часових, поведінкових і протокольних характеристик трафіку. Показано, що використання базового профілю нормальної мережевої активності та інтегральної оцінки аномальності дає змогу підвищити ефективність протидії витоку інформації з обмеженим доступом.

Ключові слова: мережеві приховані канали, програмне виявлення, ексфільтрація даних, аномалії трафіку, інформація з обмеженим доступом, кіберзахист.

Abstract

The thesis considers network covert channels as a mechanism of hidden data exfiltration disguised as legitimate network traffic. Storage-based and timing-based channels are analysed, the main indicators for their software detection are identified, and an approach to detection based on statistical, temporal, behavioural and protocol traffic features is proposed. It is shown that the use of a baseline profile of normal network activity and an integrated anomaly score can improve protection against the leakage of restricted information.

Keywords: network covert channels, software detection, data exfiltration, traffic anomalies, restricted information, cybersecurity.

Вступ

У сучасних інформаційно-комунікаційних системах одним із небезпечних сценаріїв порушення конфіденційності є приховане виведення даних через мережеві канали, що маскуються під штатний трафік. Для систем, у яких обробляється інформація з обмеженим доступом, така загроза є особливо критичною, оскільки відповідно до Закону України «Про інформацію» захист таких відомостей від несанкціонованого розкриття є обов'язковим [1]. У практиці кіберзахисту витік даних через альтернативні мережеві протоколи розглядаються як окрема техніка ексфільтрації, що передбачає використання нетипових каналів зв'язку для прихованого передавання інформації.

У науковій літературі мережеві приховані канали визначаються як спосіб непомітного передавання інформації через легітимні мережеві механізми. Сучасні дослідження поділяють такі канали на storage-based, що використовують службові поля мережевих протоколів для вбудовування даних, та timing-based, у яких передавання реалізується через модифікацію часових інтервалів між пакетами [2]. Метою роботи є розроблення методу програмного виявлення мережевих прихованих каналів для протидії витоку інформації з обмеженим доступом.

Результати дослідження

Проблема виявлення мережевих прихованих каналів полягає в тому, що їх активність часто не супроводжується очевидними сигнатурами шкідливого програмного забезпечення або різким порушенням мережевої взаємодії. Для техніки MITRE ATT&CK T1048 [3] (Exfiltration Over Alternative Protocol) характерним є використання нетипових мережевих протоколів для передавання даних, незвичні процеси-ініціатори, робота в нетиповий час, а також аномально великі або тривалі сеанси передавання. Це означає, що класичні сигнатурні засоби не забезпечують достатньої ефективності, а більш перспективним підходом є програмний аналіз поведінки мережевого трафіку.

Перспективним рішенням є застосування підходу виявлення аномалій поведінки системи, який ґрунтується на побудові профілю нормального трафіку та виявленні відхилень від нього. Згідно з NIST IR 8219 [4], такі системи можуть генерувати сповіщення за відхиленнями трафікових, об'ємних, поведінкових і протокольних параметрів. У поєднанні з результатами сучасних досліджень це дає підстави розглядати програмне виявлення мережевих прихованих каналів як задачу комплексного аналізу ознак, серед яких доцільно враховувати міжпакетні інтервали, статистику довжин пакетів, частоту звернень до окремих сервісів, нетипове використання службових полів протоколів, рівень ентропії корисного навантаження та відхилення від звичного профілю мережевої взаємодії.

У межах даної роботи пропонується метод, який передбачає збір і попередню обробку мережевого трафіку, формування базового профілю нормальної мережевої активності, виділення статистичних, часових та протокольних ознак, обчислення інтегральної оцінки аномальності та формування повідомлення про можливий прихований канал. Перевагою такого підходу є відсутність залежності від конкретної сигнатури шкідливого засобу та можливість адаптації до нових способів прихованої ексфільтрації.

Математична реалізація запропонованого методу базується на безперервному моніторингу мережевих пакетів у межах ковзного часового вікна, що дозволяє системі динамічно оцінювати стан інформаційного обміну на об'єкті інформаційної діяльності (ОІД). Процес аналізу починається з формування вектора поточних ознак $X = \{x_1, x_2, \dots x_n\}$, де кожна компонента відповідає статистичному параметру мережевого обміну, зокрема рівень ентропії службових полів протоколів мережевого та транспортного рівнів. Наступним етапом є статистична стандартизація кожної ознаки за формулою:

$$z_i = \frac{|x_i - \mu_i|}{\sigma_i}$$

де x_i – поточне значення i -ї ознаки, обчислене у межах ковзного часового вікна; μ_i та σ_i – відповідно середнє значення та стандартне відхилення цієї ознаки, отримані на етапі формування базового профілю нормальної мережевої активності.

Використання модуля різниці дозволяє враховувати як позитивні, так і негативні відхилення від еталонного значення. Отримане значення z_i є нормалізованою оцінкою аномальності i -ї ознаки та використовується для подальшого обчислення інтегрального показника.

Застосування цієї моделі дозволяє перетворити абсолютні значення відхилень у відносні показники аномальності. У наведеній формулі чисельник визначає амплітуду відхилення параметра від норми, тоді як знаменник масштабує її відповідно до фонової варіативності, зафіксованої під час навчання системи у штатному режимі функціонування мережі. Такий підхід забезпечує приведення різнорідних метрик до безрозмірного вигляду, що робить їх математично порівнянними та дозволяє кількісно оцінювати рівень аномальності незалежно від специфіки ТКВІ.

Інтегральний показник аномальності S розраховується як зважена сума отриманих нормалізованих відхилень за формулою:

$$S = \sum_{i=1}^{n} w_i \cdot z_i \ .$$

де w_i – ваговий коефіцієнт i -ї ознаки, що відображає її інформативність у процесі виявлення прихованого каналу. Використання вагових коефіцієнтів дає змогу адаптувати програмний модуль до специфіки конкретного об'єкта інформаційної діяльності та надавати пріоритет найбільш значущим ознакам. Значення S використовується як інтегральна оцінка рівня аномальності мережевої активності: чим більшим воно є, тим вищою є ймовірність використання прихованого каналу для виведення інформації з обмеженим доступом за межі контрольованої зони. Практична цінність запропонованого методу полягає в можливості його реалізації як окремого програмного модуля моніторингу мережі або як підсистеми у складі системи виявлення вторгнень. Наукова новизна методу полягає у поєднанні статистичних, часових, поведінкових і протокольних ознак у межах єдиної інтегральної моделі оцінки аномальності мережевого трафіку.

Висновки

Мережеві приховані канали слід розглядати як реалістичний механізм витоку інформації з обмеженим доступом, що може використовувати легітимні мережеві сервіси та уникати простого

сигнатурного контролю. Запропонований метод програмного виявлення ґрунтується на інтегрованому аналізі статистичних, часових, поведінкових і протокольних ознак мережевого трафіку та дає змогу формувати кількісну оцінку аномальності мережевої активності. Подальші дослідження доцільно спрямувати на розроблення прототипу програмного засобу, його експериментальну перевірку на реальних наборах мережевого трафіку та оцінювання точності виявлення прихованих каналів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Закон України «Про інформацію» від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/go/2657-12 (дата звернення: 10.02.2026).

2. Kou X., Lei Y., Guo C. et al. A Survey of Network Covert Channel: Construction and Detection. 2025. URL: https://pure.bit.edu.cn/en/publications/a-survey-of-network-covert-channel-construction-and-detection/ (дата звернення: 20.02.2026).

3. MITRE ATT&CK. Exfiltration Over Alternative Protocol (T1048). URL: https://attack.mitre.org/techniques/T1048/ (дата звернення: 8.03.2026).

4. McCarthy J. et al. NIST IR 8219: Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection. 2020. URL: https://csrc.nist.gov/pubs/ir/8219/final (дата звернення: 20.03.2026).

Кубіря Варвара Іванівна - студентка, 1КІТС-23б, Вінницький національний технічний університет, м. Вінниця, e-mail: 07-23-250.stud@vntu.vn.ua.

Науковий керівник: Гуменюк Вячеслав Володимирович - асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: hvv@vntu.edu.ua.

Kubiria Varvara Ivanivna - student, Vinnytsia National Technical University, Vinnytsia, , e-mail: 07-23-250.stud@vntu.vn.ua.

Scientific supervisor: Humeniuk Viacheslav Volodymyrovych - Assistant of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: hvv@vntu.edu.ua.