УДК 004.056.5:621.391 DOI: 10.31673/2786-8362.2026.012746

Шуклін Г.В., к.т.н.; **Шавловський Я.С.**

ДВОКОНТУРНИЙ АЛГОРИТМ ВИЯВЛЕННЯ І ПОДАВЛЕННЯ ПРИХОВАНИХ КАНАЛІВ В ЗАКРИТИХ МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Shuklin G.V., Shavlovsky Ya.S. A dual-loop algorithm for detecting and suppressing covert channels in closed special-purpose networks. This article addresses the problem of detecting and suppressing covert information transmission channels in closed special-purpose networks. It is shown that traditional methods of passive traffic monitoring have limited effectiveness under conditions of an adaptive attacker and the deterministic characteristics of closed networks. A two-loop algorithm is proposed, based on a combination of statistical analysis of network traffic parameters and adaptive control of data transmission characteristics. The outer loop of the algorithm ensures the detection and estimation of hidden channel parameters, while the inner loop actively suppresses them by introducing controlled stochastic distortions. A mathematical description of the algorithm for the intelligent detection and suppression of covert information exfiltration channels is presented; a formalization of the estimation of a covert channel's information capacity is carried out; and the results of simulation modeling are presented. It is shown that the proposed algorithm ensures a significant reduction in the throughput of covert channels with an acceptable impact on the quality of service for legitimate traffic. For the first time, a nonlinear model of covert communication channels has been constructed that accounts for adaptive control of countermeasures against information leakage, leading to a reduction in the probability of sustained APT exfiltration in special-purpose networks.

Keywords: covert channels, closed channels, exfiltration, special-purpose networks, adaptive countermeasures, DNS tunneling, dual-loop control, cybersecurity

Шуклін Г.В., Шавловський Я.С. Двоконтурний алгоритм виявлення і подавлення прихованих каналів в закритих мережах спеціального призначення. У статті розглядається проблема виявлення та придушення прихованих каналів передачі інформації в закритих мережах спеціального призначення. Запропоновано двоконтурний алгоритм, заснований на поєднанні статистичного аналізу параметрів мережевого трафіку та адаптивного керування характеристиками передачі даних. Представлено математичний опис алгоритму інтелектуального виявлення і подавлення прихованих каналів екс-фільтрації інформації, здійснено формалізацію оцінки інформаційної ємності прихованого каналу, представлено результати імітаційного моделювання. Показано, що запропонований алгоритм забезпечує значне зниження пропускної здатності прихованих каналів при допустимому впливі на якість обслуговування легітимного трафіку. Побудовано нелінійну модель прихованих каналів зв'язку в яких враховується адаптивне керування протидії витоку інформації, що призводить до зниження ймовірності стійкості APT екс-фільтрації в мережах спеціального призначення.

Ключові слова: приховані канали, закриті канали, екс-фільтрація, мережі спеціального призначення, адаптивна протидія, DNS-тунелювання, двоконтурне керування, кібербезпека

Вступ

Закриті мережі спеціального призначення (МСП) широко використовуються для передачі та обробки критично важливої інформації в державних, військових та промислових системах [1]. Характерними особливостями таких мереж є фізична та логічна ізоляція, обмежений набір використовуваних протоколів, передбачувані профілі трафіку та суворі вимоги до інформаційної безпеки. Незважаючи на високий рівень захищеності, закриті мережі залишаються вразливими до загроз, пов'язаних із використанням прихованих каналів передачі інформації. Приховані канали дають змогу зловмиснику передавати дані в обхід стандартних механізмів контролю доступу та виявлення вторгнень, використовуючи тимчасові, статистичні або структурні особливості мережевого трафіку. Особливу небезпеку становлять тимчасові та статистичні приховані канали, які маскуються під легітимну поведінку мережі та можуть адаптуватися до змін умов передачі. У зв'язку з цим актуальним є завдання розробки алгоритмів, що забезпечують не лише виявлення прихованих каналів, а й їхнє активне придушення в режимі реального часу. Сучасні загрози витоку інформації в МСП характеризуються переходом від прямих каналів виведення даних до прихованих і механізмів екс-фільтрації, які важко виявити. Найбільш небезпечними є канали, що маскуються під

легітимні сервісні протоколи: DNS, HTTPS, ICMP, службові API та міжсегментні системні обміни [2]. В умовах функціонування МСП приховані канали становлять особливу загрозу з таких причин:

- висока прихованість та низька інтенсивність передачі;
- тривале стійке функціонування в рамках APT-сценаріїв;
- можливість адаптації до політик безпеки;
- використання довірених системних сервісів.

Виходячи з наведених причин, виявлення та інтелектуальне придушення прихованих каналів екс-фільтрації інформації в МСП є актуальною задачею сьогодення.

Аналіз останніх досліджень. У дослідженнях [2] значну увагу приділено саме DNS-тунелюванню як одному з найбільш поширених способів організації прихованих каналів. У роботі [3] узагальнено підходи до виявлення DNS-тунелів із використанням методів машинного навчання. Автори показують, що DNS є привабливим середовищем для прихованої передачі даних через його критичну роль у функціонуванні мереж та відносно слабке блокування такого трафіку в корпоративних середовищах. Подібний напрям розвинуто у праці [4], де запропоновано метод виявлення DNS-прихованих каналів на основі моделі LSTM. Перевагою такого підходу є можливість автоматичного виявлення складних часових і послідовнісних закономірностей без ручного формування ознак.

Окремий напрям становлять дослідження часових прихованих каналів, у яких інформація кодується не у змісті пакетів, а в інтервалах між ними [5]. Автори розглядають методи виявлення часових прихованих каналів, наголошуючи, що саме міжпакетні інтервали можуть бути використані зловмисником для кодування прихованої інформації.

Важливими для даного дослідження є роботи, присвячені не лише виявленню, а й активному придушенню прихованих каналів. У праці [6] представлено систему NetWarden, яка після виявлення підозрілих з'єднань застосовує механізми буферизації та зміни часових характеристик передавання для руйнування прихованого каналу. Автори підкреслюють, що для часових каналів ефективним є внесення контрольованих змін у часову структуру трафіку.

У сучасних роботах також розглядаються методи аналізу та протидії прихованим каналам у спеціалізованих і промислових мережах [7, 8]. Автори досліджують продуктивність і можливість реалізації часових прихованих каналів у мережах IEEE 802.15.4, зокрема для IoT та критичних систем, і підкреслюють необхідність розроблення ефективних механізмів пом'якшення впливу таких каналів. Крім того, вони розглядають методи побудови, виявлення та зменшення впливу мережевих часових прихованих каналів, що є важливим теоретичним підґрунтям для формалізації задачі оцінювання їхньої пропускної спроможності.

Останні дослідження також демонструють, що приховані канали стають дедалі складнішими й адаптивнішими. Зокрема, у роботі [9] розглянуто формування багатовимірних ознак трафіку для прихованих каналів, де підкреслюється проблема балансу між непомітністю, стійкістю та пропускною здатністю прихованої передачі. Це підтверджує необхідність розроблення не лише пасивних засобів моніторингу, а й адаптивних алгоритмів активного впливу на параметри прихованого каналу.

Водночас вітчизняні автори активно досліджують засоби інтелектуального виявлення мережевих атак. У роботі [2] запропоновано програмний прототип системи виявлення мережевих атак на основі методів інтелектуального аналізу даних і нейромережевих структур; результати експериментів підтверджують ефективність такого підходу для захисту інформаційних мереж. Подібні ідеї розвиваються у роботі [10], де запропоновано інтелектуальну систему моніторингу й аналізу трафіку для виявлення атак у програмно-конфігурованих мережах. Особлива увага приділяється DPI-аналізу, евристичним методам і потребі виконання аналізу трафіку на швидкості каналу передавання даних.

Таким чином, аналіз останніх досліджень свідчить, що наявні підходи до виявлення прихованих каналів можна умовно поділити на кілька груп: статистичні методи аналізу мережевого трафіку, методи машинного та глибокого навчання, DPI-аналіз, евристичні методи, а також активні методи придушення шляхом зміни часових характеристик трафіку.

Водночас більшість існуючих рішень орієнтована або на виявлення прихованого каналу, або на його часткове обмеження. Недостатньо дослідженим залишається питання побудови єдиного адаптивного механізму, який поєднує статистичне виявлення прихованого каналу з активним керованим зниженням його пропускної спроможності за умови збереження допустимої якості обслуговування легітимного трафіку.

Постановка завдання. Незважаючи на широке застосування засобів моніторингу мережевого трафіку, систем виявлення вторгнень та механізмів контролю доступу, проблема своєчасного виявлення прихованих каналів екс-фільтрації інформації в закритих МСП залишається недостатньо вирішеною. Особливу складність становлять тимчасові та статистичні приховані канали, які не порушують формальну структуру протоколів, маскуються під легітимний трафік і можуть адаптувати параметри передачі до поточного стану мережі.

У закритих МСП трафік, як правило, має відносно стабільні статистичні характеристики, що створює передумови для виявлення аномалій на основі аналізу міжпакетних інтервалів. Водночас застосування лише пасивного моніторингу не забезпечує гарантованого припинення прихованої передачі даних, оскільки після виявлення каналу зловмисник може змінювати інтенсивність, часові зсуви або інші параметри екс-фільтрації. Тому актуальним є завдання розробки алгоритму, який поєднує виявлення прихованого каналу з активним адаптивним впливом на його пропускну спроможність.

Завдання дослідження полягає у розробленні двоконтурного алгоритму виявлення та придушення прихованих каналів у закритих МСП, який забезпечував би статистичне виявлення ознак прихованої передачі даних за параметрами міжпакетних інтервалів та подальше зниження пропускної спроможності прихованого каналу шляхом введення керованих випадкових затримок із контролем допустимого впливу на якість обслуговування легітимного трафіку.

Для досягнення поставленої мети сформулюємо основні завдання:

1. Проаналізувати особливості функціонування прихованих каналів екс-фільтрації інформації в закритих МСП;
2. Побудувати математичну модель мережевого трафіку на основі статистичного опису міжпакетних інтервалів у нормальному режимі та за наявності прихованого каналу;
3. Сформувати статистичний критерій виявлення прихованого каналу з урахуванням порогового значення та допустимого рівня хибної тривоги;
4. Розробити зовнішній контур алгоритму, призначений для збору телеметрії, адаптивної оцінки параметрів трафіку та прийняття рішення про наявність прихованого каналу;
5. Розробити внутрішній контур алгоритму, призначений для активного придушення прихованого каналу шляхом введення керованих випадкових затримок;
6. Формалізувати оцінку інформаційної пропускної спроможності прихованого каналу до та після застосування механізмів придушення;
7. Провести чисельне моделювання роботи запропонованого алгоритму та оцінити ефективність зниження пропускної спроможності прихованого каналу за умови збереження прийнятної якості обслуговування легітимного трафіку.

Метою роботи є розробка та дослідження двоконтурного алгоритму виявлення та придушення прихованих каналів у закритих МСП.

Виклад основного матеріалу дослідження

Особливості прихованих каналів в закритих мережах. У закритих МСП приховані канали, як правило, реалізуються без зміни формальної структури протоколів і не призводять до порушення правил маршрутизації. Найпоширенішими є тимчасові приховані канали, в яких інформація кодується за рахунок зміни між-пакетних інтервалів або затримок передачі. Відмінною рисою закритих мереж є низька варіативність параметрів трафіку, що, з одного боку, спрощує виявлення аномалій, а з іншого – підвищує вимоги до точності алгоритмів, оскільки помилкові спрацьовування можуть призвести до погіршення роботи критично важливих сервісів.

У рамках даної роботи передбачається модель зловмисника, який має доступ до одного або декількох вузлів мережі та використовує тимчасові приховані канали з адаптацією параметрів передачі до спостережуваних характеристик мережі.

Архітектура двоконтурного алгоритму. Запропонований алгоритм побудований за принципом двоконтурного керування та включає зовнішній і внутрішній контури.

Перший крок алгоритму є зовнішній контур за допомогою якого здійснюється виявлення прихованого каналу та оцінки його параметрів. Для цього відбувається збір телеметрії мережевого трафіку, обчислення статистичних характеристик між-пакетних інтервалів та порівняння їх з еталонними значеннями, характерними для нормального режиму роботи мережі.

Другий крок алгоритму – це внутрішній контур, який призначено для активного придушення виявленого прихованого каналу. Придушення здійснюється шляхом введення керованих випадкових затримок у процес передачі пакетів, що призводить до руйнування структури прихованого каналу та зниження його пропускної здатності.

Математична модель виявлення прихованих каналів. Розглянемо потік пакетів, що характеризується послідовністю між-пакетних інтервалів τ_i, де $i = \overline{1,n}$. Якщо мережа працює в режимі, коли відсутній зовнішній деструктивний вплив, то закон розподілу випадкового значення τ_i описуються нормальним розподілом, який має наступне представлення:

$$f(\tau_i) = \frac{1}{\sigma_0\sqrt{2\pi}} e^{-\frac{(\tau_i - a_0)^2}{2\sigma_0^2}}, \quad (1)$$

де a_0 – середнє значення між-пакетного інтервалу; σ_0 – середнє квадратичне відхилення значення між-пакетного інтервалу.

Якщо в мережі існує прихований канал, то параметри нормального закону розподілу (1) мають інші значення. Тобто, будемо вважати, що при наявності прихованого каналу, закон розподілу випадкового значення τ_i має наступний вид:

$$f(\tau_i) = \frac{1}{\sigma_1\sqrt{2\pi}} e^{-\frac{(\tau_i - a_1)^2}{2\sigma_1^2}}, \quad (2)$$

де a_1 – середнє значення між-пакетного інтервалу при наявності прихованого каналу i при $a_1 \neq a_0$; σ_1 – середнє квадратичне відхилення значення між-пакетного інтервалу при наявності прихованого каналу.

Нехай $\tilde{a}$ – оцінка математичного сподівання міжпакетних інтервалів у поточному вікні спостереження. Введемо величину d, яка характеризує, наскільки поточне значення $\tilde{a}$ відрізняється від a_0 і яке будемо визначати наступним чином:

$$d = \frac{\left|\tilde{a} - a_0\right|}{\sigma_0}.$$

Виходячи з представлень (1) і (2) будемо розглядати дві гіпотези: H_0 – прихований канал відсутній і H_1 – прихований канал присутній. Введемо величину γ, яка є критичним значенням статистичного тесту, який розділяє дві гіпотези. Тоді, критерієм виявлення прихованого каналу буде виконання наступної нерівності

$$d > \gamma.$$

Порогове значення γ обирається відповідно допустимим рівнем хибної тривоги. Якщо p_{fa} – ймовірність хибної тривоги, то:

$$p_{fa} = p_{H_0}(d > \gamma),$$

де $p_{H_0}(d > \gamma)$ – умовна ймовірність події $d > \gamma$ при умові відсутності прихованого каналу – подія H_0.

Математична модель придушення прихованого каналу зі зниженням його пропускної спроможності. Інформаційну пропускну спроможність C прихованого каналу можна представити наступним чином:

$$C = \frac{I(B, \tau_i)}{T}, \tag{3}$$

де B – це сигнал, тобто інтервал, що кодується і передається; $I(B, \tau_i)$ – між інтервалом, що кодується і міжпакетним інтервалом, який спостерігається; T – середній інтервал часу передачі бітової послідовності.

При наявності прихованого каналу значення τ_i – міжпакетних інтервалів змінюються і біт $b_i \in \{0,1\}$ кодується зі зсувом середнього, тобто представлення (2) буде мати наступний вид:

$$f(\tau_i) = \frac{1}{\sigma_{noise}\sqrt{2\pi}} e^{-\frac{(\tau_i - (a_0 + b_i\Delta))^2}{2\sigma_{noise}^2}},$$

де Δ – значення часового зсуву при передачі інформації; σ_{noise} – середнє квадратичне відхилення фонового шуму.

Таким чином, якщо $\Delta \neq 0$, то це свідчить про наявність прихованого каналу. Спостережувана величина τ_i є міжпакетний інтервал, що вимірюється на стороні системи моніторингу, і є результатом накладення вихідного сигналу B, що формується джерелом трафіку, та випадкових спотворень, зумовлених мережевими умовами та механізмами придушення. Саме величина τ_i використовується для оцінки статистичних характеристик трафіку, виявлення прихованих каналів екс-фільтрації та аналізу його пропускної спроможності.

Придушення прихованого каналу здійснюється за рахунок випадкової величини $\Delta_{\max}$, яка являє собою час затримки в мс і середнє значення якої визначається наступним чином:

$$\overline{\Delta(\Delta t)} = \frac{\Delta_{mzx}}{2}. \tag{4}$$

Представлення (4) дає спроможне явно керувати середньою величиною спотворень, які присутні в трафіку.

Для величини Δ розглядаємо різницеве рівняння, яке має наступне представлення:

$$\Delta_{\max}(k+1) = \begin{cases} \Delta_{\max}(k) + \beta \cdot D_k, D_k > \gamma, \\ \max\{\Delta_{\min}, \Delta_{\max}(k-\beta), D_k \leq \gamma\} \end{cases}. \tag{5}$$

Представлення (5) показує, що якщо аномалія зростає, то придушення прихованого каналу стає більш активним, а якщо аномалія зникає, то придушення зменшується до мінімально доступного рівня.

Адаптивна оцінка параметрів трафіку. В процесі функціонування МСП, математичне сподівання міжпакетних інтервалів являє собою деяку послідовність $\tilde{\tilde{a}}$, тобто $\tilde{\tilde{a}} \in \left\{ \overset{\neq}{a_k} \right\}$. Тоді, для вікна спостереження оцінка математичного сподівання міжпакетних інтервалів підпорядковується наступному різницевому рівнянню:

$$\tilde{\tilde{a}}_{k+1} = (1-\alpha) \cdot \tilde{\tilde{a}}_k + \alpha \cdot \tau_i, \tag{6}$$

де α – параметр адаптації при $\alpha \in [0,1]$.

Цей параметр є параметром керування динамікою, стійкістю і чутливістю МСП. Математично, представлення (4) – це експоненціальне згладжування.

Для середньо квадратичного відхилення фонового шуму різницеве рівняння має вид:

$$\sigma^2_{noise}(k+1) = (1-\alpha)\cdot\sigma^2_{noise}(k) + \alpha\cdot\left(\tau_k - \tilde{\tilde{a}}_k\right)^2.$$

Параметр адаптації α є ключовим параметром, який можна інтерпретувати як коефіцієнт довіри до нових даних. Якщо α наближається до 1, то це означає що система довіряє новим даним, а якщо α наближається до 0, то це означає що система довіряє минулим даним. Інакше кажучи, коефіцієнт адаптації α визначає швидкість оновлення статистичних оцінок параметрів трафіку і фактично задає динамічні властивості алгоритму виявлення. Він реалізує експоненціальне зважування спостережень, забезпечуючи компроміс між чутливістю до змін і стійкістю до шуму. Вибір α має істотний вплив на ймовірність виявлення прихованих каналів та рівень помилкових тривог. Він є параметром не просто параметром згладжування, а механізмом керування динамікою виявлення, що дозволяє переводити систему зі стабільного режиму в режим швидкого реагування при появі ознак прихованого каналу.

Для виявлення прихованого каналу введемо статистику:

$$D_k = \frac{\left|\tilde{\tilde{a}}_k - a_0\right|}{\sigma_0}. \qquad (7)$$

Якщо $\alpha \to 1$, то значення (6) швидко зростає і система швидко здійснює реакцію на зовнішній вплив. Якщо ж $\alpha \to 0$, то система стійка до хибних тривог. Величина τ_i має наступне представлення:

$$\tau_i = B + \varepsilon + \Delta,$$

де ε – істотний мережевий шум; Δ – затримка (придушення).

Зловмисник керує величиною B, тобто виконується умова:

$$B = \begin{cases} a_0, b_i = 0 \\ a_0 + \Delta, b_i = 1 \end{cases},$$

де $b_i \in \{0,1\}$ – біт таємної інформації, який зловмисник передає через мережу, використовуючи зміну часу між пакетами.

Задача придушення прихованого каналу полягає в мінімізації представлення (3), тобто $C \to \min C$.

Числовий приклад роботи запропонованого алгоритму. Розглянемо МСП, в якій в нормальному режимі міжпакетні інтервали описуються законом розподілу:

$$f(\tau_i) = \frac{1}{0{,}8\sqrt{2\pi}} e^{-\frac{(\tau_i - 10)^2}{1.28}},$$

причому $a_0 = 10$ мс, $\sigma_0 = 0{,}8$ мс.

При наявності прихованого каналу зловмисник кодує біти з зсувом середнього на $\Delta = 4$ мс, тобто, маємо:

$$f(\tau_i) = \frac{1}{0{,}8\sqrt{2\pi}} e^{-\frac{(\tau_i - (10+4b_i))^2}{1.28}}.$$

Нехай в поточному вікні ймовірність появи значення $b_i = 1$ дорівнює $p = 0{,}6$. Тоді, середнє значення трафіку в атакуючому вікні має наступне значення:

$$\tilde{\tilde{a}}_1 = a_0 + p\cdot\Delta = 10 + 0{,}6\cdot 4 = 12{,}4 \text{ мс}.$$

Покладемо $\alpha = 0{,}2$, $\gamma = 2{,}5$ і $\beta = 1{,}5$. Тоді, середній інтервал для оцінки пропускної спроможності каналу, має числове значення $T = \frac{a_0}{1000} = \frac{10}{1000} = 0{,}01$ с.

Зовнішній контур – виявлення прихованого каналу. Припустимо, що до кібератаки система функціонувала в нормальному стані, тобто $\tilde{a}_1 = a_0 = 10$ мс. Після появи прихованого каналу, вікно, яке спостерігається, виявило середній час $\bar{\tau}$ міжпакетними інтервалами, який дорівнює 12,4 мс. Тоді, згідно представленню (4), з урахуванням того, що $\tau_k = \bar{\tau} = 12,4$ мс, маємо $\tilde{a}_1 = 10 + 0,2 \cdot (12,4 - 10) = 10,48$ мс. На наступних кроках отримуємо: $\tilde{a}_2 = 10,864$ мс, $\tilde{a}_3 = 11,712$ мс, $\tilde{a}_4 = 11,41696$ мс, $\tilde{a}_5 = 11,613568$ мс. Використовуючи формулу (6), маємо:

$$D_1 = \frac{|10,48 - 10|}{0,8} = 0,6; \qquad D_2 = \frac{|10,864 - 10|}{0,8} = 1,08;$$

$$D_3 = \frac{|11,1712 - 10|}{0,8} = 1,464; \qquad D_4 = \frac{|11,41696 - 10|}{0,8} = 1,7712; \qquad D_5 = \frac{|11,613568 - 10|}{0,8} = 2,01696$$

.

Система захисту не здійснює спрацьовування при виконанні нерівності $\Delta_5 < \gamma = 2,5$, однак при цьому аномалія набирає обороти. В табл. 1 представлено розрахункові значення для пар $\left(\tilde{a}_k; D_k\right)$ при $k = \overline{6,9}$ згідно (6) та (7).

Таблиця 1

Значення середнього і відповідної статистики

$\tilde{a}_{k+1}$	D_k
$\tilde{a}_6 = 11,7708544$	$D_6 = 2,213568$
$\tilde{a}_7 = 11,89668352$	$D_7 = 2,3708544$
$\tilde{a}_8 = 11,997346816$	$D_8 = 2,49668352$
$\tilde{a}_9 = 12,0778774528$	$D_9 = 2,597346816$

Внутрішній контур – адаптоване придушення. Після того, як було виявлено прихований канал, застосовуємо представлення (5). На дев'ятому кроці виявлення прихованого каналу, маємо $\Delta_{\max}(10) = 1 + 1,5 \cdot 2,597346816 \approx 4,9$ мс. Згідно (5), додаємо додаткову затримку Δt, яка рівномірно розподілена на інтервалі $(0, \Delta_{\max})$.

Тоді, дисперсія рівномірного шуму має вид $\sigma_{noise}(\Delta t) = \frac{D_{\max}^2}{12} = 1,997568$. Базова дисперсія $\sigma_B^2 = 0,8^2 = 0,64$. Тоді, згідно (5), маємо $\sigma_{\tau_i}^2 = 2,637568$. Для зниження пропускної спроможності прихованого каналу, застосовуємо представлення (3). Маємо: $C_0 = \frac{I_0}{T} = 50$ біт/с, де $\sigma_{noise}^2 = 0,64$; $I_0 = 0,5$ біт.

Побудуємо алгоритм виявлення та придушення прихованих каналів (рис. 1). Після придушення прихованого каналу:

$$\sigma_{noise}^2 = 2,637568; \qquad I_1 = 0,1565 \text{ біт}; \qquad C_1 = \frac{I_1}{T} = 15,65 \text{ біт/с}.$$

Отже, абсолютне значення пропускної спроможності прихованого каналу $\Delta C = C_0 - C_1 = 34,35$ біт/с, а відносне зниження пропускної спроможності прихованого каналу, складає $\frac{34,35}{50} \cdot 100\% = 68,7\%$. Таким чином, пропускна спроможність прихованого каналу знижена на 68,7%. На рис. 2 показана ефективність зростання статистики виявлення прихованого каналу в МСП.

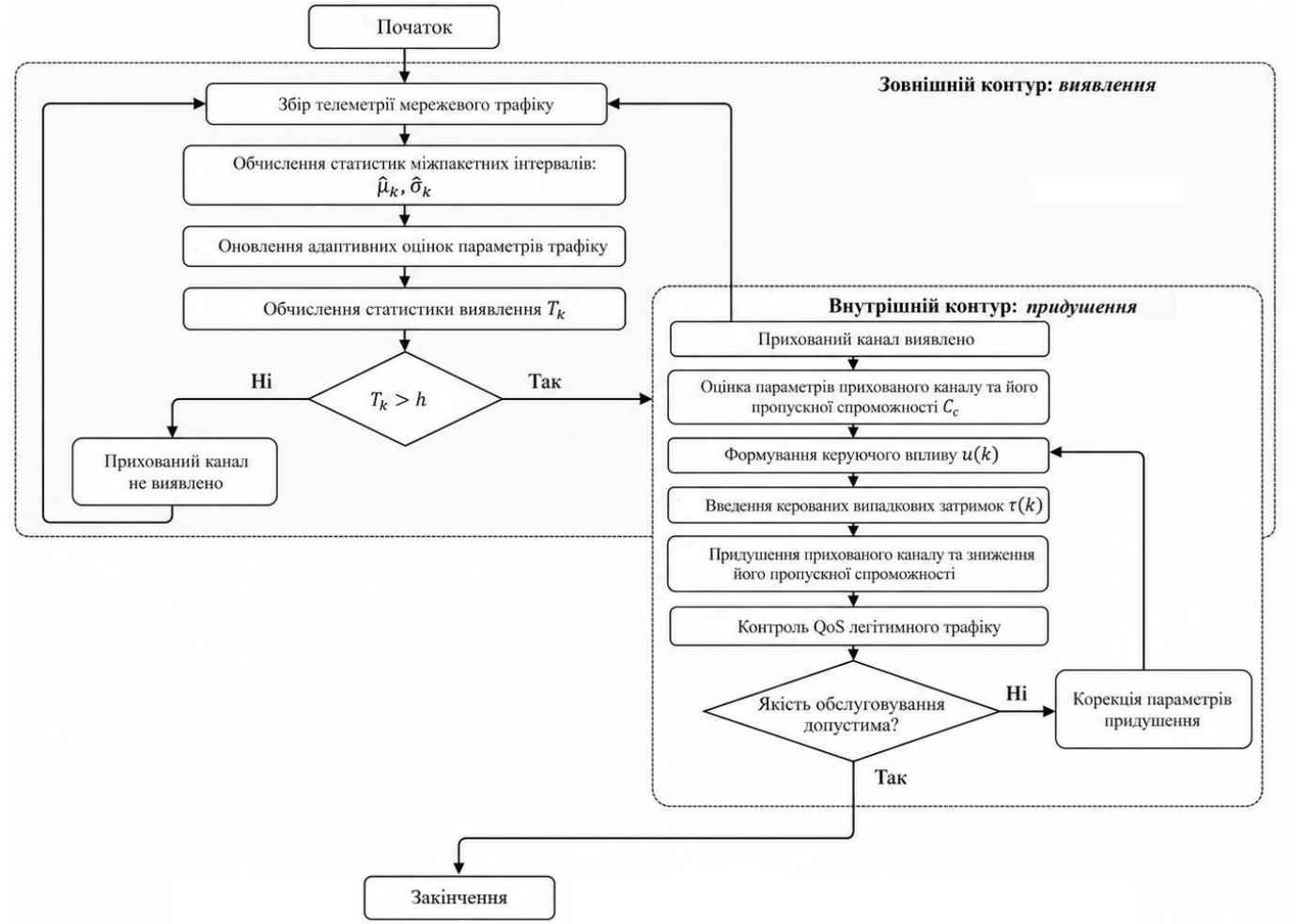

Рис. 1. Алгоритм виявлення та придушення прихованих каналів в МСП

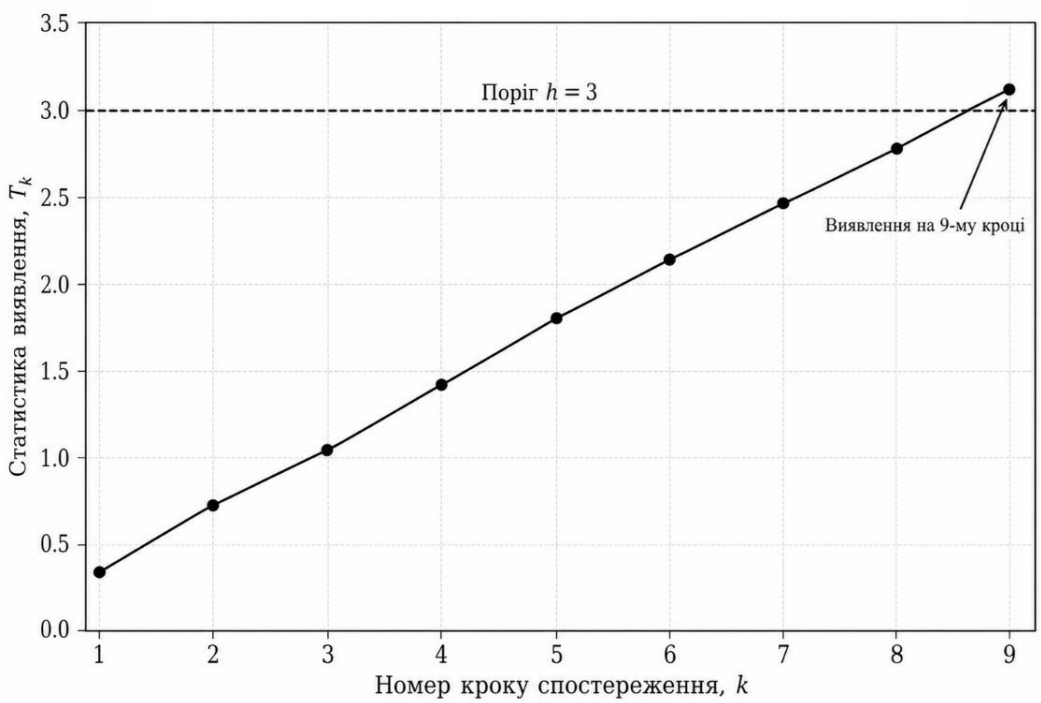

Рис. 2. Ефективність зростання статистики виявлення прихованого каналу в МСП

Як видно з рис. 2 виявлення має позитивний ефект на 9 кроці, але на 8 кроці ще не достатньо ефективно працює адаптивний алгоритм.

Висновки

Чисельне моделювання двоконтурного алгоритму виявлення та придушення прихованого каналу показало, що статистика виявлення D_k заснована на нормованому відхиленні середнього міжпакетного інтервалу, забезпечує виявлення прихованого каналу при досягненні значення $D_9 = 2{,}597 > \gamma = 2{,}5$. Після виявлення зовнішній контур адаптивно підвищує максимальну випадкову затримку до $\Delta_{\max} = 4{,}896$ мс, що призводить до зростання дисперсії спостережуваного сигналу з 0,64 до 2,638 та зменшення інформаційної пропускної спроможності прихованого каналу з 50 біт/с до 15,65 біт/с.

Таким чином, запропонований двоконтурний алгоритм забезпечує зниження пропускної спроможності прихованого каналу на 68,7% при помірному збільшенні середньої затримки передачі.

Список використаної літератури:

1. Хорошко В., Лаптєв О., Хохлачова Ю., Аль-Далваш А., Пепа Ю. (2024) Особливості проектування захищених інформаційних мереж. Наукоємні технології. Том 62. №2. 154–163. https://doi.org/10.18372/2310-5461.62.18709.

2. Толюпа С., Плющ О., Пархоменко І. (2020) Побудова систем виявлення атак в інформаційних мережах на нейромережевих структурах. Кібербезпека: освіта, наука, техніка. Т. 2. № 10. 169–183. https://doi.org/10.28925/2663-4023.2020.10.169183.

3. Zander S., Armitage G., Branch P. (2007) A Survey of Covert Channels and Countermeasures in Computer Network Protocols. IEEE Communications Surveys & Tutorials. Vol. 9. No. 3. 44–57. https://doi.org/10.1109/COMST.2007.4317620.

4. Chen S., Lang B., Liu H., Li D., Gao C. (2021) DNS Covert Channel Detection Method Using the LSTM Model. Computers & Security. Vol. 104. 90–95. https://doi.org/10.1016/j.cose.2020.102095.

5. Han J., Huang C., Shi F., Liu J. (2020) Covert Timing Channel Detection Method Based on Time Interval and Payload Length Analysis. Computers & Security. Vol. 97. 101–110. https://doi.org/10.1016/j.cose.2020.101952.

6. Severino R., Rodrigues J., Alves J., Ferreira L.L. (2023) Performance Assessment and Mitigation of Timing Covert Channels over the IEEE 802.15.4. Journal of Sensor and Actuator Networks. Vol. 12, No. 4. 60–68. https://doi.org/10.3390/jsan12040060.

7. Belozubova A., Epishkina A., Kogos K. (2021) On/Off Covert Channel Capacity Limitation by Adding Extra Delays. IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering «ElCon». 2318–2322. https://doi.org/10.1109/ElConRus51938.2021.9396545.

8. Zhao H., Shi Y.-Q. (2013) Detecting Covert Channels in Computer Networks Based on Chaos Theory. IEEE Transactions on Information Forensics and Security. 35–42. https://doi.org/10.1109/TIFS.2012.2231861.

9. Zhang X., Guo L., Xue Y., Jiang H., Liu L., Zhang Q. (2019) A Hybrid Covert Channel with Feedback over Mobile Networks. In: Security and Privacy in Social Networks and Big Data. 87–94. https://doi.org/10.1007/978-981-15-0758-8_7.

10. Beshley M., Pryslupskyi A., Medvetskyi M., Beshley H. (2022) Intelligent Traffic Monitoring and Analysis System to Detect Attacks in Software-Defined Networks. Information and Communication Technologies, Electronic Engineering. Vol. 2. No. 1. 1–11. https://doi.org/10.23939/ictee2022.01.

Автори статті

Шуклін Герман – кандидат технічних наук, доцент, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна.

ORCID: 0000-0003-2507-384X

Шавловський Ярослав – аспірант, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0006-2725-5996

Authors of the article

Shuklin Herman – Candidate of Sciences (technical), Associate Professor, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine.

ORCID: 0000-0003-2507-384X

Shavlovsky Yaroslav – postgraduate, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0009-0006-2725-5996

Надійшла до редакції: 26.04.2026
Прийнята до друку: 27.04.2026
Опубліковано: 25.05.2026