https://doi.org/10.31891/2219-9365-2026-86-31
УДК 004.056.5:004.75:519.7

ШАВЛОВСЬКИЙ Ярослав
Державний університет інформаційно-комунікаційних систем
https://orcid.org/0009-0006-2725-5996
shavlovskyyaroslav@gmail.com

# ІНТЕЛЕКТУАЛЬНА СИСТЕМА ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ВИБОРУ КОНТРЗАХОДІВ ПРОТИ ПРИХОВАНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ В МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

*У роботі розроблено інтелектуальну систему прийняття рішень щодо вибору оптимальних контрзаходів проти прихованих каналів екс-фільтрації інформації в мережах спеціального призначення (МСП). Особливу небезпеку становлять адаптивні сценарії екс-фільтрації, у яких порушник динамічно змінює параметри функціонування прихованого каналу залежно від реакції системи кіберзахисту.*

*Запропоновано математичну модель адаптивного вибору захисних заходів на основі інтегральної оцінки ризику прихованого каналу, показників якості обслуговування мережі та ймовірності зміни тактики зловмисника. Введено оптимізаційний функціонал, який забезпечує компроміс між мінімізацією витоку інформації та збереженням допустимого рівня функціонування критичної інформаційної інфраструктури. Розроблено дворівневу структуру інтелектуальної системи, у якій перший рівень реалізує аналіз аномалій мережевого трафіку та оцінювання ризику прихованого каналу, а другий рівень виконує адаптивний вибір контрзаходу за критерієм мінімізації сукупних втрат.*

*Розроблено механізм інтелектуального керування контрзаходами в умовах неповної інформації та динамічних змін роботи МСП за рахунок наявності мережевих аномалій, змін поведінки користувачів і можливості адаптації порушника до захисних механізмів. Отримано аналітичні умови стійкості системи прийняття рішень та доведено збіжність алгоритму вибору захисних заходів. Проведено чисельне моделювання роботи системи і показано, що запропонований підхід дозволяє знизити ризик витоку інформації без критичного погіршення параметрів функціонування МСП та забезпечує підвищення ефективності адаптивного кіберзахисту в умовах сучасних мережевих загроз.*

*Ключові слова: кібербезпека, приховані канали, витік інформації, інтелектуальне управління, прийняття рішень, адаптивні контрзаходи, мережі спеціального призначення, оптимізація ризиків.*

SHAVLOVSKYI Yaroslav
State University of Information and Communication Systems

# INTELLIGENT DECISION-MAKING SYSTEM FOR SELECTING COUNTERMEASURES AGAINST HIDDEN INFORMATION LEAKAGE CHANNELS IN SPECIAL-PURPOSE NETWORKS

*This paper presents an intelligent decision-making system for selecting optimal countermeasures against covert exfiltration channels in special-purpose networks (SPN). Adaptive exfiltration scenarios pose a particular danger, in which the attacker dynamically changes the operating parameters of the covert channel depending on the response of the cybersecurity system.*

*A mathematical model for the adaptive selection of protective measures is proposed, based on an integrated assessment of the risk of a covert channel, network service quality indicators, and the probability of changes in the attacker's tactics. An optimization objective function is introduced that strikes a balance between minimizing information leakage and maintaining an acceptable level of critical information infrastructure performance. A two-level structure for an intelligent system has been developed, in which the first level performs analysis of network traffic anomalies and assessment of the risk of a hidden channel, while the second level selects a countermeasure adaptively based on the criterion of minimizing total losses.*

*A mechanism has been developed for the intelligent control of countermeasures under conditions of incomplete information and dynamic changes in the operation of the SPN, due to network anomalies, changes in user behavior, and the attacker's ability to adapt to defense mechanisms. Analytical conditions for the stability of the decision-making system have been derived, and the convergence of the algorithm for selecting defense measures has been proven. Numerical simulations of the system's operation were conducted, demonstrating that the proposed approach reduces the risk of information leakage without significantly compromising the performance of the SPN and enhances the effectiveness of adaptive cybersecurity in the face of modern network threats.*

*Keywords: cybersecurity, covert channels, information leaks, intelligent management, decision-making, adaptive countermeasures, special-purpose networks, risk optimization.*

Стаття надійшла до редакції / Received 02.04.2026
Прийнята до друку / Accepted 28.04.2026
Опубліковано / Published 31.05.2026



## ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Сучасні МСП характеризуються високою критичністю інформації, що захищається, жорсткими вимогами до безперебійності функціонування та обмеженою допустимістю помилкових блокувань. У таких умовах застосування жорстких сигнатурних методів захисту виявляється недостатнім, оскільки приховані канали екс-фільтрації інформації використовують дозволені протоколи, легітимні сервіси та довірені

маршрути взаємодії. Особливу складність становлять APT-сценарії, в яких зловмисник динамічно змінює тактику екс-фільтрації: переходить між DNS tunneling, HTTPS covert channel, beaconing, low-rate exfiltration та timing-каналами. В результаті завдання протидії перетворюється не тільки на проблему виявлення, але й на проблему вибору оптимального захисного впливу.

Застосування надмірно жорстких контрзаходів може порушити функціонування МСП, а занадто м'які заходи не забезпечують достатнього рівня захисту. Отже, потрібна інтелектуальна система прийняття рішень, здатна в реальному часі обирати оптимальні контрзаходи з урахуванням:

- рівня ризику прихованого каналу;
- ймовірності адаптації зловмисника;
- вартості сервісних втрат;
- допустимого рівня залишкового витоку.

Таким чином, виникає науково-практична задача створення інтелектуальної системи прийняття рішень, здатної в умовах апріорної невизначеності та динамічної зміни поведінки порушника адаптивно обирати оптимальні контрзаходи проти прихованих каналів екс-фільтрації інформації. Така система повинна забезпечувати компроміс між мінімізацією ризику витоку інформації, збереженням стабільності функціонування мережі та урахуванням імовірності адаптації зловмисника до застосованих захисних заходів.

Актуальність даної задачі обумовлена необхідністю підвищення ефективності систем кіберзахисту МСП, створення адаптивних механізмів протидії прихованим каналам витоку інформації та забезпечення стійкого функціонування критичної інформаційної інфраструктури в умовах сучасних кіберзагроз.

## АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Проблематика протидії прихованим каналам витоку інформації в МСП є міждисциплінарною та охоплює напрями кібербезпеки, виявлення аномалій у мережевому трафіку, оцінювання ризиків, адаптивного управління контрзаходами та забезпечення стійкості критичної інформаційної інфраструктури.

У роботі [1] розглянуто методи приховування даних у комп'ютерних мережах – від класичних підходів до сучасних реалізацій в IoT- та AI-середовищах. Автори показують, що приховані канали можуть функціонувати на різних рівнях мережевої взаємодії та використовувати легітимні протоколи для маскування екс-фільтрації інформації. Акцентується увага на розроблення адаптивних механізмів протидії, здатних враховувати зміну тактики порушника. В [2] запропоновано використання нечіткої логіки для оцінювання ризиків багатостадійних кібератак на мережі критичної інфраструктури. Такий підхід є важливим для побудови інтелектуальних систем прийняття рішень, оскільки дозволяє працювати в умовах неповної, неточної або суперечливої інформації про стан мережі та поведінку порушника. В роботі [3] досліджено питання побудови криптографічних протоколів, вільних від клептографічних модифікацій. Описані приховані механізми витоку інформації та їх модифікації, що можуть створювати непомітні канали передачі секретних даних навіть у формально захищених криптографічних системах.

У роботах [4, 5] розглянуто можливості підвищення рівня безпеки хмарної інфраструктури за допомогою методів NLP та машинного навчання, а також методи виявлення шкідливих властивостей альтернативних прошивок маршрутизаторів. Застосування інтелектуального аналізу даних є перспективним для виявлення нетипових поведінкових патернів, прихованих ознак компрометації та аномалій, а також зміненій мережевій поведінці та можливості маскування шкідливої активності під легітимний трафік.

У роботах [6, 7] запропоновано метод виявлення DNS covert channel на основі LSTM-моделі та DNS tunneling. Автори показали використання рекурентних нейронних мереж, що дозволило враховувати часову залежність DNS-запитів, що є важливим для виявлення прихованих каналів та якості вибраних ознак, а також здатності моделі адаптуватися до нових сценаріїв атак.

У дослідженні [8] запропоновано поведінковий підхід до виявлення DNS covert channel із використанням машинного навчання. Основна перевага такого підходу полягає у можливості виявлення не лише відомих, але й модифікованих варіантів прихованих каналів, що особливо важливо для APT-сценаріїв, у яких порушник поступово змінює тактику екс-фільтрації. У роботі [9] представлено систему виявлення екс-фільтрації даних через DNS tunneling у реальному часі. Такий напрям є безпосередньо пов'язаним із темою даної статті, оскільки МСП потребують оперативного прийняття рішень щодо вибору контрзаходів без критичного погіршення якості функціонування мережі.

У статті [10] запропоновано модель адаптивних засобів безпеки на основі оцінювання ризику. Ця робота є однією з найбільш близьких до даної тематики дослідження, оскільки обґрунтовує необхідність автоматичного вибору захисних механізмів залежно від поточного рівня загрози, ризику та стану інформаційної системи.

У фундаментальному огляді [11] виконано класифікацію мережевих прихованих каналів на основі шаблонів їх побудови. Автори систематизували методи створення прихованих каналів, зокрема storage-based та timing-based підходи, що дозволяє глибше формалізувати модель загроз і визначати найбільш доцільні контрзаходи для кожного типу каналу. Продовженням є робота [12], де проведено огляд методів побудови та виявлення мережевих прихованих каналів. Особливу увагу приділено сучасним підходам до аналізу

мережевого трафіку та виявлення прихованої комунікації. Це підтверджує необхідність поєднання методів статистичного аналізу, машинного навчання та адаптивного вибору захисних дій.

У дослідженні [13] розглянуто виявлення DNS-тунелів за допомогою машинного навчання. Результати роботи підтверджують ефективність ML-підходів для класифікації DNS-трафіку, однак такі методи здебільшого орієнтовані саме на виявлення атаки, а не на вибір оптимального контрзаходу після її виявлення.

У роботі [14] розглянуто систему реалізації серверів з урахуванням аномалій у пакетах. Дане джерело є важливим для обґрунтування необхідності аналізу мережевих аномалій як одного з індикаторів прихованої активності. Підхід, пов'язаний з виявленням аномалій у пакетах, може бути інтегрований у перший рівень запропонованої інтелектуальної системи для формування інтегральної оцінки ризику.

Таким чином, аналіз сучасних джерел показує, що більшість існуючих досліджень зосереджена на окремих аспектах проблеми: побудові прихованих каналів, виявленні DNS tunneling, класифікації мережевих аномалій, використанні машинного навчання, оцінюванні ризику або адаптивних засобах безпеки. Водночас недостатньо розробленими залишаються питання комплексного вибору контрзаходів після виявлення прихованого каналу з одночасним урахуванням ризику витоку інформації, якості функціонування мережі та ймовірності адаптації порушника. Саме це визначає актуальність розроблення інтелектуальної системи прийняття рішень щодо вибору оптимальних контрзаходів проти прихованих каналів екс-фільтрації інформації в мережах спеціального призначення.

## ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

**Метою статті** є розроблення інтелектуальної системи прийняття рішень щодо вибору оптимальних контрзаходів проти прихованих каналів витоку інформації в МСП на основі адаптивного оцінювання ризику, показників якості функціонування мережі та ймовірності зміни тактики порушника.

Для досягнення мети роботи необхідно:

1. Провести аналіз сучасних методів протидії прихованим каналам витоку інформації в МСП та визначити їх основні недоліки;
2. Розробити математичну модель стану захищеності МСП в умовах екс-фільтрації інформації через приховані канали;
3. Сформувати множину адаптивних контрзаходів та визначити їх функціональне призначення для протидії прихованим каналам витоку інформації;
4. Розробити дворівневу інтелектуальну систему прийняття рішень щодо вибору захисних заходів в умовах динамічної зміни стану мережі та поведінки порушника.
5. Провести чисельне моделювання роботи інтелектуальної системи та оцінити ефективність запропонованого підходу при різних сценаріях прихованої екс-фільтрації інформації.

## ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

МСП, яка знаходиться в стані захисту від екс-фільтрації в момент часу $t$, математично описується чотиривимірним вектором $S(t)$, який має наступний вид:

$$S(t) = \left\{ R_{int}(t), R_{fact}(t), p(t), q(t) \right\}, \tag{1}$$

де $R_{int}(t)$ – інтегральний ризик існування прихованого каналу; $R_{fact}(t)$ – ризик фактичного витоку інформації; $p(t)$ – ймовірність зміни дій порушника; $q(t)$ – показник якості обслуговування мережі.

Для забезпечення захисту МСП від витоку інформації необхідно здійснювати керування процесом захисту. Позначимо через $U$ множину керуючих параметрів, тобто множину контрзаходів, яка складається з шести елементів $u_i, i = \overline{1,6}$. В табл. 1 представлено позначення керуючих впливів і їх функціональне призначення.

Таблиця 1

**Керуючий вплив і його функціональне призначення**

| $u_i, i = \overline{1,6}$ | **Функціональне призначення** |
|---|---|
| $u_1$ | Керуючий вплив, який зменшує пропускну спроможність каналу передачі даних |
| $u_2$ | Інтелектуальне обмеження небезпечної DNS активності без повного відключення DNS сервісу |
| $u_3$ | Адаптивне стохастичне спотворення часової структури трафіку |
| $u_4$ | Введення порушника в оману шляхом створення хибного інформаційного середовища |
| $u_5$ | Ізоляція мережевого сегмента, вузла або підсистеми, пов'язаної з підозрілою активністю |
| $u_6$ | Примусове завершення активної мережевої сесії, пов'язаної з витоком даних |

Введемо три функції. Функція втрат від витоку інформації:

$$f(u,t) = R_{fact}(t) \cdot \left(1 - \frac{C_{u_i}}{C_0}\right), \tag{2}$$

де $C_0$ – ємність каналу до застосування контрзаходів; $C_{u_i}$ – ємність каналу після застосування контрзаходу $u_i, i = \overline{1,6}$, що представлені в табл. 1.

Функція (2) – це функція втрат якості функціонування мережі:

$$g(u,t) = \max\left\{0, q_{\min}(t) - q_{u_i}(t)\right\}, \tag{3}$$

де $q_{u_i}(t)$ – якість обслуговування мережі після здійснення контрзаходів.

Функція (3) являє собою функцією втрат від якості обслуговування:

$$\phi(u,t) = p(t) \cdot M_u, \tag{4}$$

де $M_u$ – міра негативних наслідків, що виникають через те, що порушник пристосовується до конкретного контрзаходу $u_i$.

Після введення функцій (2) – (4), введемо функціонал $J(u,t)$, який має наступне представлення:

$$J(u,t) = f(u,t) + \lambda_1 \cdot g(u,t) + \lambda_2 \cdot \phi(u,t), \tag{5}$$

де $\lambda_1$, $\lambda_2$ – вагові коефіцієнти управління, що визначають пріоритети інтелектуальної системи прийняття рішень.

Ці два коефіцієнти є ключовими параметрами компромісу, що представлено на рис. 1.

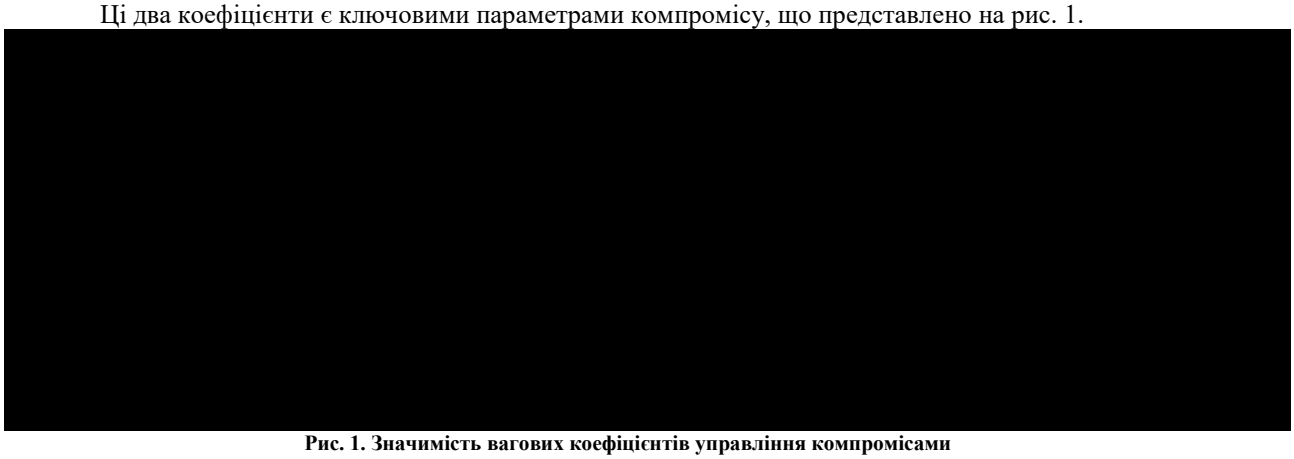

**Рис. 1. Значимість вагових коефіцієнтів управління компромісами**

Коефіцієнт $\lambda_1$ є коефіцієнтом важливості якості функціонування мережі, що характеризує затримку передачі інформації, варіативність часових характеристик, втрати пакетів, пропускну здатність та доступність сервісів. У контексті протидії прихованим каналам екс-фільтрації, цей коефіцієнт виступає обмеженням на застосування захисних заходів і використовується для забезпечення балансу між ефективністю захисту та стійкістю функціонування МСП.

Зростання значень коефіцієнта $\lambda_1$, що входить в представлення (5) показує, що стійкість системи захисту МСП порушується при затримках, при втраті доступу і при знижені якості сервісів. В цьому випадку необхідно обирати м'які контрзаходи, здійснювати адаптивне придушення і вводити порушника в оману. Якщо ж значення $\lambda_1$ зменшуються, то це свідчить про те, що параметри, які характеризують якість функціонування МСП стає менш важливими і при цьому допускаються жорсткі міри захисту і заради безпеки необхідно змінювати або модернізувати топологію мережі, а значить і відповідні апаратно-програмні засоби.

Коефіцієнт $\lambda_2$ характеризує важливість ймовірності адаптації порушника. Якщо значення цього коефіцієнту зростають, то інтелектуальна система враховує не лише поточну атаку, а й реакцію адаптивного зловмисника, тобто система сприймає як динамічний конфлікт між зловмисником, який намагається адаптуватись, і системою інформаційного захисту. Крім того, це зростання показує, що зловмисник намагається змінити канал ескалації. В цьому випадку необхідно уникати жорсткого блокування і надавати переваги таким діям, як вводити атакуючого в оману, здійснювати випадкові затримки і здійснювати заходи проти стеження. Якщо ж значення $\lambda_2$ зменшуються, то це означає, що інтелектуальна система не враховує

адаптацію зловмисника. В цьому випадку необхідно здійснювати жорстке блокування роботи мережі або припинити її роботу.

Після введення представлень (2) – (5) задача інтелектуальної системи прийняття рішень сформулюється наступним чином: необхідно знайти таку функцію $u_i^*(t) \in U$ адаптивного керування, щоб виконувалась умова:

$$u_i^*(t) = \arg\min_{u_j \in U} J(u,t), \qquad j = \overline{1,6} \tag{6}$$

при обмеженні

$$q_{u_i}(t) \geq q_{критичне}. \tag{7}$$

Рівність (6) показує, що система приймає такий контрзахід в момент часу $t$, при якому функціонал (5) приймає найменше значення. Тобто, із набору, що представлені в табл. 1, інтелектуальна система повинна обрати найбільш раціональний захід. Нерівність (7) показує, що після застосування контрзаходу $u_i(t)$ якість $q_{u_i}(t)$ функціонування мережі має залишатися не нижчою за критично допустимий рівень $q_{критичне}$.

**Основні результати.** На основі сформульованої постановки задачі представимо інтелектуальну систему, яка складається з двох рівнів. На першому рівні здійснюється оцінка стану захищеності МСП в момент часу $t$, а на другому рівні обирається контрзахід, який визначається за правилом (6) з урахуванням обмеження (7).

**Рівень 1. Оцінка стану захищеності МСП.** На цьому рівні формується інтегральний ризик існування прихованого каналу, який уявляє собою адитивну функцію, яка складається з чотирьох ознак і яка має наступне представлення:

$$R_{int}(t) = w_1 St(t) + w_2 H(t) + w_3 B(t) + w_4 A(t), \tag{8}$$

де $St(t)$ – статистика виявлення, яка показує наскільки режим роботи трафіку в момент часу $t$ відхилився від нормального режиму, тобто, наскільки змінились часові характеристики трафіку в поточний момент часу; $H(t)$ – ентропія трафіку, тобто вимір, який показує наскільки трафік схожий на випадково закодовані дані; $B(t)$ – показує, чи є періодична активність в мережевій активності; $A(t)$ – інтегральна оцінка аномальності DNS трафіку; $w_i, i = \overline{1,4}$ – вагові коефіцієнти адаптації.

На основі емпіричних спостережень було зроблено висновок для діапазонів значень інтегрального ризику. Якщо $R_{int}(t) \in [0, 0.3)$, то це означає що МСП працює в нормальному режимі, при $R_{int}(t) \in [0.3, 0.7)$ є підозра атаки на мережу і при $R_{int}(t) \in [0.7, 1]$ на МСП здійснюється атака.

**Рівень 2. Вибір контрзаходу.** Контрзахід обирається за правилом (5) і адаптивним розрахунком коефіцієнтів $\lambda_1$ та $\lambda_2$ за наступним правилом:

$$\lambda_i(t+1) = \lambda_i(t) + \eta \cdot \Delta_i(t), \qquad i = \overline{1,2}, \tag{9}$$

де $\eta$ – коефіцієнт навчання інтелектуальної системи; $\Delta_i$ – помилка керування якості функціонування мережі, що характеризує затримку передачі інформації, варіативність часових характеристик, втрати пакетів, пропускну здатність та доступність сервісів.

Ще важливою умовою функціонування інтелектуальної системи прийняття рішень є асимптотична збіжність до стійкості локального мінімуму функціонала (5). Тобто, послідовність здійснення контрзаходів в кінцевому етапі повинна прямувати до оптимального. Математично це твердження записується наступною умовою:

$$\lim_{t \to \infty} u_i^* = u_i^{opt} \tag{10}$$

і при цьому повинна постійно виконуватись умова:

$$J\left(u(t+1), t\right) \leq J\left(u(t), t\right). \tag{11}$$

Нерівність (11) показує, що сукупні втрати системи монотонно зменшуються з часом. Представлення (10) і (11) показують, що якщо система змінює контрзаходи досить «обережно» і не робить надто різких кроків, то з часом вона починає обирати дедалі ефективніші захисні дії та стабілізується навколо найкращого рішення. Інакше кажучи, запропонована інтелектуальна система вибору контрзаходів має властивість асимптотичної збіжності до стійкого локального мінімуму функціоналу втрат за умови дотримання вимог опуклості та обмеженості кроку адаптації. Це гарантує передбачуваність поведінки системи, відсутність нестійких коливань захисних впливів та стійке зниження сукупного ризику витоку інформації в МСП.

Для оцінки ефективності розробленої дворівневої інтелектуальної системи було створено експериментальну модель інформаційно-телекомунікаційної МСП, що функціонує в умовах прихованого витоку інформації. В табл. 2 представлено результати відповідних розрахунків.

Таблиця 2

**Числовий приклад функціонування інтелектуальної системи прийняття рішень щодо вибору контрзаходів в МСП**

| $u_i$ | $\left(1-\frac{C_{u_i}}{C_0}\right)$ | $q_{u_i}(t)$ | $f(u,t)$ | $g(u,t)$ | $\phi(u,t)$ | $J(u,t)$ | Важливість якості функціонування МСП |
|---|---|---|---|---|---|---|---|
| $u_1$ | 0.62 | 0.9 | 0.3192 | 0 | 0.138 | 0.3882 | так |
| $u_2$ | 0.84 | 0.8 | 0.1344 | 0 | 0.3128 | 0.2908 | так |
| $u_3$ | 0.71 | 0.86 | 0.2436 | 0 | 0.1012 | 0.2942 | так |
| $u_4$ | 0.55 | 0.93 | 0.378 | 0 | 0.552 | 0.4056 | так |
| $u_5$ | 0.94 | 0.6 | 0.0504 | 0.2 | 0.3588 | 0.3698 | ні |
| $u_6$ | 0.98 | 0.42 | 0.0168 | 0.38 | 0.4232 | 0.4944 | ні |

На основі даних (табл. 2) на рис. 2 та рис. 3 представлено реалізацію рівнів 1 і 2 інтелектуальної системи прийняття рішень.

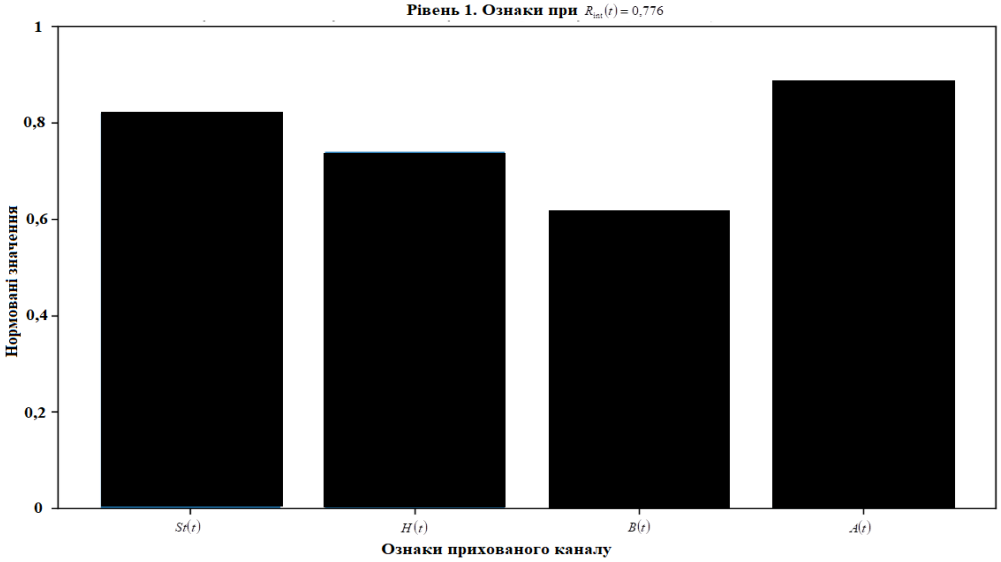


**Рис. 2 – Перший рівень дворівневої інтелектуальної системи прийняття рішень щодо протидії прихованим каналам витоку інформації в мережі спеціального призначення**

На рис. 2 наведено нормовані значення чотирьох ключових ознак ризику, які входять в представлення (8) для визначення $R_{int}(t)$. З рис. 2 видно, що $R_{int}(t) > 0.7$. Це означає, що інтелектуальна система вважає ймовірність існування прихованого каналу високою, тобто здійснюється атака.

На рис. 3 представлено значення функціоналу втрат $J(u,t)$ для різних контрзаходів.

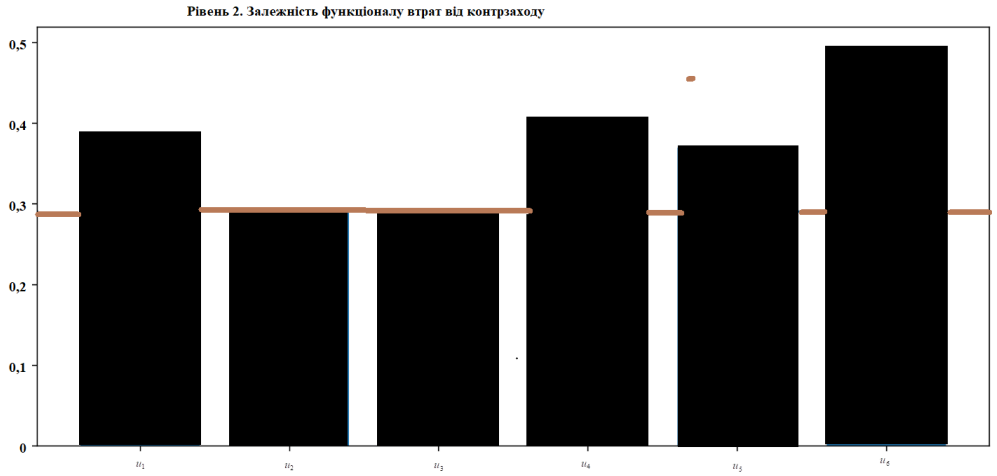


**Рис. 3 – Другий рівень дворівневої інтелектуальної системи прийняття рішень щодо протидії прихованим каналам витоку інформації в мережі спеціального призначення**

На рис. 3 представлено другий рівень дворівневої інтелектуальної системи прийняття рішень щодо протидії прихованим каналам витоку інформації в МСП. Рис. 3 ілюструє залежність значення функціоналу втрат $J(u_i,t)$ від вибору конкретного контрзаходу $u_i$, який застосовується для локалізації або придушення прихованого каналу екс-фільтрації інформації.

Висота прямокутника показує наскільки «дорого» системі застосовувати відповідний контрзахід. З даного рисунку видно, що мінімальне значення функціонал $J(u,t)$ приймає при $u_2$. Це означає, що для розглянутого сценарію витоку даних через DNS цей контрзахід забезпечує найкращий баланс між безпекою та стабільністю мережі.

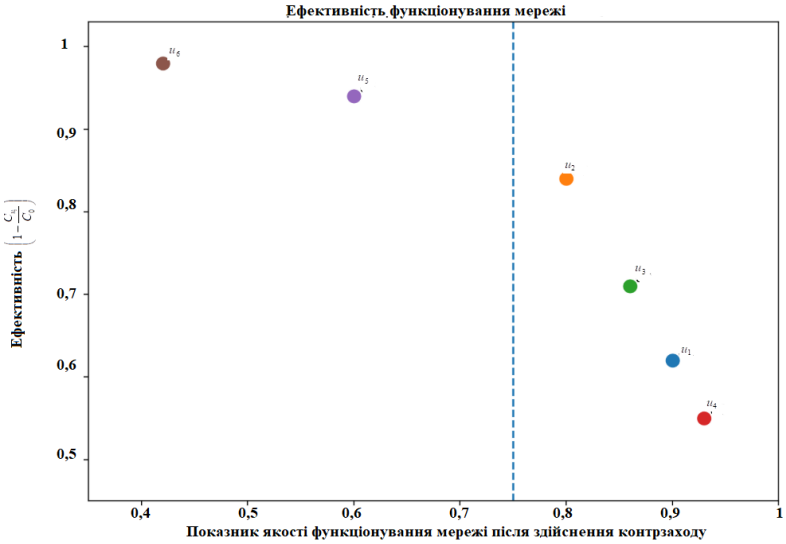


**Рис. 4 – Взаємозв'язок між ефективністю контрзаходу і якістю функціональності мережі після застосування контрзаходу**

На рис. 4 показано компроміс між ефективністю контрзаходів $\left(1-\frac{C_{u_i}}{C_0}\right)$ та якістю $q_{u_i}(t)$ обслуговування мережі. З рис. 4 видно, що підвищення ефективності придушення прихованого каналу супроводжується погіршенням параметрів функціонування МСП. Пунктирна лінія відповідає критично допустимому рівню показника якості функціонування мережі, нижче якого застосування контрзаходів вважається неприпустимим. Отримані результати підтверджують необхідність інтелектуального вибору захисних заходів на основі багатокритеріальної оптимізації.

Рис. 5 демонструє як інтелектуальна система прийняття рішення обирає контрзахід на основі балансу між ефективністю захисту, стійкістю мережі та мінімізацією ймовірності ескалації з боку зловмисника.

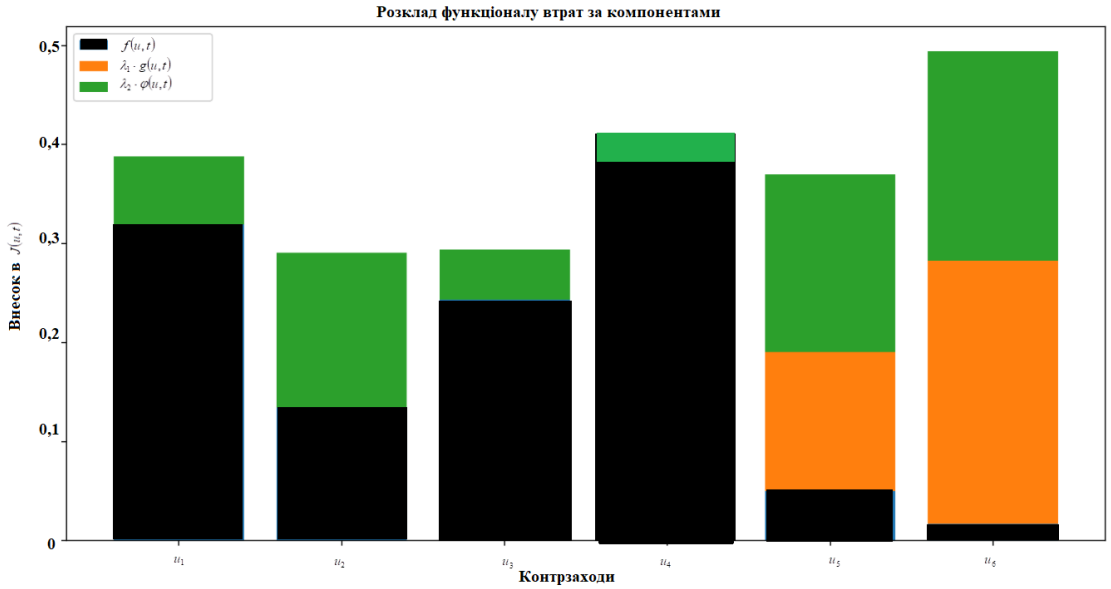


**Рис. 5. Структура функціонала втрат $J(u,t)$, який розраховується в другому рівні інтелектуальної системи прийняття рішень щодо протидії прихованим каналам екс-фільтрації в МСП**

На рис. 5 представлено структуру функціоналу втрат $J(u_i,t)$, який використовується у другому рівні інтелектуальної системи прийняття рішень щодо вибору контрзаходів проти прихованих каналів екс-фільтрації інформації в МСП.

## ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Вперше розроблено інтелектуальну систему прийняття рішень щодо вибору контрзаходів проти прихованих каналів витоку інформації в МСП, яка базується на математичній моделі адаптивного управління захисними заходами на основі інтегральної оцінки ризику та оптимізації сукупного функціоналу втрат і забезпечує підвищення ефективності протидії прихованим каналам у МСП завдяки динамічному вибору оптимальних захисних заходів при збереженні прийнятного рівня якості обслуговування та стабільності функціонування критичної інфраструктури. Отримано умови стійкості алгоритму та доведено його збіжність. Чисельні результати підтверджують, що інтелектуальний вибір контрзаходів забезпечує вищу ефективність захисту порівняно з локально-оптимальними рішеннями, орієнтованими лише на максимальне придушення каналу.

Перспективи подальших досліджень полягають у подальшому:

- розширенні моделі на багаторівневі розподілені МСП;
- інтегрувати методи машинного навчання та штучних нейронних мереж для прогнозування поведінки порушника;
- дослідженні прихованих каналів у хмарних та програмно-конфігурованих мережах;
- розробленні механізмів автоматичного синтезу контрзаходів у режимі реального часу;

Отримані результати можуть бути використані під час побудови перспективних систем кіберзахисту, комплексів моніторингу мережевого трафіку, систем виявлення прихованих каналів витоку інформації та адаптивних платформ забезпечення інформаційної безпеки МСП.

### Література

1. Shelest M., et al. (2025) Methods of Hiding Data in Computer Networks: from Classics to IoT and AI. Computer Systems and Information Technologies. No. 4. 27–34. https://doi.org/10.31891/csit-2025-4-3

2. Nakonechna Yu., et al. (2024) Fuzzy Logic in Risk Assessment of Multi-Stage Cyber Attacks on Critical Infrastructure Networks. Theoretical and Applied Cybersecurity. Vol. 6. 53–65. https://doi.org/10.20535/tacs.2664-29132024.2.318023

3. Коваленко Б.А. (2019) Побудова криптографічних протоколів, вільних від клептографічних модифікацій. Ukrainian Scientific Journal of Information Security. Vol. 25. Issue 2. 88–95. https://doi.org/10.18372/2225-5036.25.13840

4. Абібулаєв А.Р., Піскозуб А.З. (2025) Аналіз можливостей покращення стану безпеки хмарної інфраструктури за допомогою NLP та ML. Сучасний захист інформації. №2(62). 124–140. https://doi.org/10.31673/2409-7292.2025.026884

5. Прокопович-Ткаченко Д.І., Зубченко Н.С., Черкаський О.В., Черкаський Д.О., Тихоненко І.М. (2025) Методи виявлення шкідливих властивостей альтернативних прошивок маршрутизаторів у контексті сучасних мережевих загроз. Сучасний захист інформації. №4(64). 140–154. https://doi.org/10.31673/2409-7292.2025.041215

6. Chen S., et al. (2021) DNS Covert Channel Detection Method Using the LSTM Model. Computers & Security. Vol. 104. 102095. https://doi.org/10.1016/j.cose.2020.102095

7. Aiello M., et al. (2015) DNS Tunneling Detection Through Statistical Fingerprints of Protocol Messages and Machine Learning. International Journal of Communication Systems. Vol. 28. Issue 14. 1987–2002. https://doi.org/10.1002/dac.2836

8. Saeli S., et al. (2020) DNS Covert Channel Detection via Behavioral Analysis: a Machine Learning Approach. https://doi.org/arXiv:2010.01582

9. Abualghanam O., et al. (2023) Real-Time Detection System for Data Exfiltration over DNS Tunneling Using Machine Learning. Electronics. No. 12(6). 1467. https://doi.org/10.3390/electronics12061467

10. Calvo M., et al. (2022) A Model for Risk-Based Adaptive Security Controls. Computers & Security. Vol. 115. 102612. https://doi.org/10.1016/j.cose.2022.102612

11. Wendzel S., et al. (2015) A Pattern-Based Survey and Categorization of Network Covert Channel Techniques. ACM Computing Surveys. Vol. 47. Issue 3. 50. https://doi.org/10.1145/2684195

12. Kou X., et al. (2025) A Survey of Network Covert Channel: Construction and Detection. Security and Communication Networks. IEEE 11th Conference on Big Data Security on Cloud (BigDataSecurity). 145–153. https://doi.org/10.1109/BigDataSecurity66063.2025.00026

13. Bykov N., Chernyshov Y. (2024) Detecting DNS Tunnels Using Machine Learning. IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology. IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). 92–94. https://doi.org/10.1109/USBEREIT61901.2024.10584043

14. Поночовний П.М., Пепа Ю.В. (2024) Система реалізації серверів з урахуванням аномалій в пакетах. Ukrainian Scientific Journal of Information Security. Vol. 26. Issue 2. 270–277. https://doi.org/10.18372/2410-7840.26.20018

## References

1. Shelest M., et al. (2025) Methods of Hiding Data in Computer Networks: from Classics to IoT and AI. Computer Systems and Information Technologies. No. 4. 27–34. https://doi.org/10.31891/csit-2025-4-3

2. Nakonechna Yu., et al. (2024) Fuzzy Logic in Risk Assessment of Multi-Stage Cyber Attacks on Critical Infrastructure Networks. Theoretical and Applied Cybersecurity. Vol. 6. 53–65. https://doi.org/10.20535/tacs.2664-29132024.2.318023

3. Kovalenko B.A. (2019) Pobudova kryptohrafichnykh protokoliv, vilnykh vid kleptohrafichnykh modyfikatsii. Ukrainian Scientific Journal of Information Security. Vol. 25. Issue 2. 88–95. https://doi.org/10.18372/2225-5036.25.13840

4. Abibulaiev A.R., Piskozub A.Z. (2025) Analiz mozhlyvostei pokrashchennia stanu bezpeky khmarnoi infrastruktury za dopomohoiu NLP ta ML. *Suchasnyi zakhyst informatsii*. No. 2(62). 124–140. https://doi.org/10.31673/2409-7292.2025.026884

5. Prokopovych-Tkachenko D.I., Zubchenko N.S., Cherkaskyi O.V., Cherkaskyi D.O., Tykhonenko I.M. (2025) Metody vyiavlennia shkidlyvykh vlastyvostei alternatyvnykh proshyvok marshrutyzatoriv u konteksti suchasnykh merezhevykh zahroz. *Suchasnyi zakhyst informatsii*. No. 4(64). 140–154. https://doi.org/10.31673/2409-7292.2025.041215

6. Chen S., et al. (2021) DNS Covert Channel Detection Method Using the LSTM Model. Computers & Security. Vol. 104. 102095. https://doi.org/10.1016/j.cose.2020.102095

7. Aiello M., et al. (2015) DNS Tunneling Detection Through Statistical Fingerprints of Protocol Messages and Machine Learning. International Journal of Communication Systems. Vol. 28. Issue 14. 1987–2002. https://doi.org/10.1002/dac.2836

8. Saeli S., et al. (2020) DNS Covert Channel Detection via Behavioral Analysis: a Machine Learning Approach. https://doi.org/arXiv:2010.01582

9. Abualghanam O., et al. (2023) Real-Time Detection System for Data Exfiltration over DNS Tunneling Using Machine Learning. Electronics. No. 12(6). 1467. https://doi.org/10.3390/electronics12061467

10. Calvo M., et al. (2022) A Model for Risk-Based Adaptive Security Controls. Computers & Security. Vol. 115. 102612. https://doi.org/10.1016/j.cose.2022.102612

11. Wendzel S., et al. (2015) A Pattern-Based Survey and Categorization of Network Covert Channel Techniques. ACM Computing Surveys. Vol. 47. Issue 3. 50. https://doi.org/10.1145/2684195

12. Kou X., et al. (2025) A Survey of Network Covert Channel: Construction and Detection. Security and Communication Networks. IEEE 11th Conference on Big Data Security on Cloud (BigDataSecurity). 145–153. https://doi.org/10.1109/BigDataSecurity66063.2025.00026

13. Bykov N., Chernyshov Y. (2024) Detecting DNS Tunnels Using Machine Learning. IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology. IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). 92–94. https://doi.org/10.1109/USBEREIT61901.2024.10584043

14. Ponochovnyi P.M., Pepa Yu.V. (2024) Systema realizatsii serveriv z urakhuvanniam anomalii v paketakh. Ukrainian Scientific Journal of Information Security. Vol. 26. Issue 2. 270–277. https://doi.org/10.18372/2410-7840.26.20018