



**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ
ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**



**НАВЧАЛЬНО-НАУКОВИЙ
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**



THEORETICAL AND APPLIED CYBERSECURITY

**Матеріали IV Всеукраїнської
науково-практичної конференції**

Випуск 4



Київ – 2026

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ
ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ
ІНСТИТУТ**

**THEORETICAL AND APPLIED
CYBERSECURITY**

**Матеріали IV Всеукраїнської
науково-практичної конференції**

Випуск 4

Київ – 2026

*Рекомендовано до друку Вченою радою
НН ФТІ КПІ ім. Ігоря Сікорського
(протокол № 9 від 29 червня 2026 р.)*

Theoretical and Applied Cybersecurity. Матеріали IV Всеукраїнської науково-практичної конференції (TACS-2026). – Київ: Інжиніринг. – 186 с. ISBN 978-617-8180-08-9

До збірника увійшли матеріали доповідей, представлених на IV Всеукраїнській науково-практичній конференції Theoretical and Applied Cybersecurity (TACS-2026, 28 травня 2026 р., м. Київ, Україна).

У збірнику представлені матеріали, присвячені питанням безпечного функціонування кібернетичного та інформаційного простору, безпеки промислових систем та систем критичної інфраструктури, математичних і технічних проблем кібернетичної безпеки, запобігання і протидії кібератакам, моделювання та протидії інформаційним операціям, технологій інформаційно-аналітичних досліджень на основі відкритих джерел інформації, застосування штучного інтелекту.

Для фахівців в області інформаційних технологій, інформаційної і кібернетичної безпеки, а також для аспірантів і студентів старших курсів вищої школи відповідних спеціальностей.

Редакційна колегія:

*О.М. Новіков, д.т.н., професор, член-кор. НАН України;
Д.В. Ланде, д.т.н., професор; С.А. Смирнов, к.т.н., с.н.с.;
А.Ш. Апішева, к.психол.н.; А.В. Напрєнко*

ISBN 978-617-8180-08-9

© НН ФТІ
КПІ ім. Ігоря Сікорського,
2026

© Колектив авторів, 2026

ПЕРЕДМОВА

IV Всеукраїнська науково-практична конференція «Theoretical and Applied Cybersecurity» (TACS-2026) є академічною подією, яку організовує Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського" на базі Навчально-наукового фізико-технічного інституту. Хоча конференція базується в Києві, учасники конференції, представляють різні міста України і світу. Вимоги до публікації матеріалів конференції постійно зростають, а процес рецензування стає все більш суворим з кожним роком.

Збірник містить відібрані доповіді, представлені на IV Всеукраїнській науково-практичній конференції «Theoretical and Applied Cybersecurity» (TACS-2026, 28 травня 2026 р., Київ, Україна). Серед понад 60 поданих заявок обрано 40 найкращих доповідей для публікації. В збірнику представлені останні досягнення в таких напрямках, як теоретичні та криптографічні проблеми кібернетичної безпеки; державна політика у сфері кібернетичної безпеки; математичні методи, моделі та технології дослідження безпечного функціонування кіберпростору; алгоритми та методи запобігання і протидії кібератакам; аналітичні системи на основі відкритих джерел інформації; безпека промислових систем та систем критичної інфраструктури; соціальний інжиніринг та методи протидії деструктивним впливам на свідомість у кіберпросторі; застосування штучного інтелекту в кібербезпеці.

Сподіваємось, що цей збірник матеріалів конференції стане помітним внеском у фундаментальні та прикладні знання у сфері кібербезпеки.

Програмний комітет конференції TACS-2026

МОДЕЛЬ ЗАГРОЗ MITRE EMB3D І МАТРИЦЯ ЗАГРОЗ MITRE ESTM

Щербина М. Ю., Венгерський П. С.

*Львівський національний університет імені І. Франка,
м. Львів, Україна
mykola.shcherbyna@lnu.edu.ua, petro.venhershkyi@lnu.edu.ua*

Розглянуто застосування моделей MITRE EMB3D і ESTM для аналізу загроз у вбудованих системах. Описано робочий процес EMB3D і класифікацію тактик і технік ESTM з практичними рекомендаціями щодо тестування та захисту пристроїв.

Ключові слова: EMB3D, ESTM, MITRE, вбудовані системи, модель загроз, тактики і техніки

Вступ

Вбудовані системи відрізняються низкою ключових характеристик, що визначають як природу загроз, так і можливі заходи захисту. Обмежені ресурси (процесор, оперативна пам'ять, енергоспоживання) ускладнюють застосування традиційних засобів безпеки. Довгий життєвий цикл пристроїв і відсутність регулярних патчів створюють накопичувальний ризик. Ланцюг постачання та прошивка часто містять слабкі місця, що множить точки входу для атак. Нарешті, фізичний доступ до пристрою відкриває можливості апаратних атак (бічні канали, JTAG/SWD, модифікація плат), що робить захист апаратного рівня критично важливим.

Модель загроз MITRE EMB3D

EMB3D позиціонується як централізована база знань, що з'єднує властивості пристрою з формалізованими кіберзагрозами та адаптованими заходами пом'якшення. Основні компоненти моделі: властивості пристрою (апаратні елементи, ядра, пам'ять, периферія, мережеві сервіси, прошивка, прикладне ПЗ), кіберзагрози (опис шляхів досягнення ефекту та очікуваного впливу) і заходи

пом'якшення, підібрані з урахуванням обмежень платформи.

Практичний робочий процес EMB3D включає три етапи. Перший — інвентаризація: детальна фіксація апаратних і програмних характеристик, відкритих інтерфейсів та механізмів оновлення. Другий — мапінг: зіставлення виявлених властивостей із відомими техніками та векторами атак, що дозволяє автоматизовано або вручну визначити найбільш релевантні загрози. Третій — оцінка та пріоритизація: визначення рівня вразливості, наявності пом'якшень і пріоритетів для тестування (fuzzing, видобування та реверс-інжиніринг прошивок, fault injection) та впровадження захисних заходів.

Переваги EMB3D — системність охоплення стеку пристрою, відтворюваність оцінок ризику та можливість інтеграції вимог безпеки на ранніх етапах проєктування. Обмеження моделі пов'язані з динамічністю загроз, інерційністю впровадження апаратних змін у вже виготовлені пристрої та високим порогом експертності для коректного застосування.

MITRE ESTM – тактики і техніки

ESTM доповнює ATT&CK, орієнтуючись на потенційні та майбутні вектори атак у вбудованих системах. Матриця класифікує тактики – від розвідки до екфільтрації та впливу – і деталізує численні техніки під кожною тактикою. Для практичної безпеки важливо розуміти приклади тактик у контексті вбудованих систем:

- ETAC013 (Розвідка): охоплює методи, за допомогою яких активно або пасивно збирають інформацію, що може бути використана для визначення цілей – конкретного пристрою чи мережі – з метою здійснення подальших дій.
- ETAC001 (Первинний доступ): компрометація через змінні носії, додавання апаратних компонентів, уразливості ланцюга постачання, відкриті інтерфейси налагодження. Наприклад, початок атаки за сценарієм зі статті [3] передбачає тактику EST000002 (Додавання апаратних компонентів).
- ETAC002 (Виконання): запуск шкідливого коду через CLI, служби, API або модифіковані системні завдання; використання довірених утиліт розробника

для виконання шкідливих дій. Для продовження атаки з [3] це EST000024 (Логічна атака «людина посередині»).

- ETAC003 (Стійкість): буткіти, персистентна прошивка, модифікація NVRAM, створення легітимних облікових записів для збереження доступу.
- ETAC004 (Підвищення привілеїв): отримати права доступу вищого рівня.
- ETAC005 (Уникнення захисту): маскуванню процесів, обфускація файлів, модифікація контрольних сум, встановлення кореневих сертифікатів. Для прикладу з [3] це EST000077 (Експлуатація для обходу захисту).
- ETAC006 (Доступ до облікових даних): витяг приватних ключів, перехоплення введення, використання типових облікових даних.
- ETAC007 (Виявлення): тактика, коли противник намагається скласти карту середовища вбудованої системи або її компонентів.
- ETAC009 (Збір даних). Для атаки, описаної у [3], це EST000164 (Збір інформації з послідовної шини) та EST000159 (Виявлення стану програми).
- ETAC008 (Горизонтальне переміщення), ETAC010 (Командування та контроль) і ETAC011 (Екфільтрація): переходи через спільні сервіси, використання віддалених сервісів для розповсюдження та виведення даних, створення резервних каналів C2.
- ETAC012 (Вплив): тактика, коли противник намагається маніпулювати, переривати, вимикати, пошкоджувати або знищувати систему, дані чи процеси фізичного керування через вбудовану систему або її компонент.

Розуміння тактик і технік дозволяє формувати цілеспрямовані сценарії тестування та розробляти контрзаходи, що враховують як програмні, так і апаратні аспекти.

Висновки

Моделі MITRE EMB3D і ESTM забезпечують системну основу для ідентифікації загроз, формалізації технік атак і

пріоритизації тестування вбудованих систем. Захист повинен поєднувати Secure Boot, підписування образів і захищені механізми оновлення, контроль ланцюга постачання і аудит сторонніх компонентів, пентестинг. Організаційно необхідне навчання інженерів на перетині кібербезпеки та мікроелектроніки і/або формування міждисциплінарних команд.

Список використаних джерел

1. Корпорація MITRE. MITRE EMB3D™: A knowledge base of cyber threats and associated mitigations for embedded devices [Електронний ресурс]. – URL: <https://emb3d.mitre.org/>
2. Корпорація MITRE. Embedded Systems Threat Matrix (ESTM) [Електронний ресурс]. – URL: <https://estm.mitre.org/>
3. Venherskyi P. Mitigating Secure Bootloader Vulnerabilities in Flashless Microcontrollers / P. Venherskyi, M. Scherbyna // Вісник Львівського університету. Серія прикладна математика та інформатика. – 2025. – Вип. 32. – Р. 55-60. – DOI: <http://dx.doi.org/10.30970/vam.2024.32.13307>

ON NEW POSTQUANTUM STREAM CIPHERS DEFINED IN TERMS OF TEMPORAL ALGEBRAIC GRAPHS

Vasyl Ustymenko^{1,2}, Oleksandr Pustovit² and Tymofii
Svyrydenko²

¹ *Royal Holloway University of London, United Kingdom.*

² *Institute of telecommunications and global information space,
Kyiv, Ukraine*

*e-mails: Vasyl.Ustymenko@rhul.ac.uk, sanyk_set@ukr.net,
ipz23-t.svyrydenko@nubip.edu.ua*

Graphs $D(n, q)$ were defined 33 years ago. (see [1] and further references) Their connected components are approximations of infinite q -regular tree $T(q)$. This fact was used in various applications to Computer Science. Together with graphs $D(n, q)$ other homomorphic images $A(m, q)$ of $T(q)$ were used in various implementations (see [2] and further references).

We observe shortly use of these families of graphs and their generalisations in the design of Algebraic Stream Ciphers and LDPC codes. We propose general method of obfuscation of $D(m, q)$ or $A(n, q)$ based cryptosystems via Artificial Intelligence or Quantum Computing methods. We propose a new stream cipher based on these graph with nonbijective encryption function of multivariate nature with polynomial degree which is not bounded by independent constant.

The standard form of this map defines the obfuscation of known secure multivariate public key cryptosystem of Postquantum Cryptography. The use quantum computations in the cipher to transform it into hybrid combination of tools from Quantum and Postquantum Cryptographies. The speed of execution is $O(n)$, different active passwords produce distinct ciphertexts. Computer simulations demonstrate good mixing properties of the cipher.

Keywords: Algebraic graphs of large girth, Symmetric Cryptography, graph based ciphers, Symbolic Computations, Artificial Intelligence.

Let as consider infinite temporal graph ${}^tA(q)$ which is a bipartite graph with points of kind $x=(x_1, x_2, \dots, x_n, \dots)$ and lines $y=[y_1, y_2, \dots, y_n, \dots]$ and incidence relation given by the equations

$$a_2(t)x_2 - b_2(t)y_2 = c_2(t)x_1y_1, a_3(t)x_3 - b_3(t)y_3 = c_3(t)y_1x_2, a_4(t)x_4 - b_4(t)y_4 = c_4(t)x_1y_3, a_5(t)x_5 - b_5(t)y_5 = c_5(t)y_1x_4 \dots$$

where dependent on time t coefficients are nonzero elements of finite field F_q . We assume that time parameter t is discrete and taken from the interval $[1, 2, \dots, T]$.

In each moment of time $t=t_0$ we have effectively defined momentum graph with coefficients $a_i(t_0)$, $b_i(t_0)$ and $c_i(t_0)$. If all of these parameters coincides with 1 and $q \neq 2$ then the equations define q -regular tree, which is a mathematical model of the branching process (see [2] and further references). The concept of temporal graph given by equations and discussion of its use in cryptography can be found in [3].

We will work with homomorphic images ${}^tA(n, q)$ of defined above temporal graph via deleting of coordinates of points and lines with the indexes $> n$ together with the conditions on deleted parameters.

We refer to first coordinates of point (x) and line $[y]$ of described graphs as their colours.

Notice that independently of time parameter there are well defined operators $N_a(x)$ and $N_a(y)$ of taking the neighbour of them with the colour x_1+a and y_1+a respectively.

We will use the operator $J_{f(x)}$ of changing the colour x_1 of the point x for $f(x_1)$ where the function f is taken from $F_q[x_1]$.

Let as take two tuples $\alpha=(a(1), a(2), \dots, a(k))$ and $\beta=(b(1), b(2), \dots, b(k))$ where $a(i) \neq a(i+1)$ and $b(i) \neq b(i+1)$ for $i=1, 2, \dots, k$ and graph $A(n, q)$. We take the vector space $(F_q)^n$ of points of the graph and consider the transformation sending the vector x to $N_{b(k)}(N_{a(k)}(\dots(N_{b(2)}(N_{a(2)}((N_{b(1)}(N_{a(1)}(x))))\dots))$.

We denote this transformation as $E(a(1), a(2), \dots, a(k), b(1), b(2), b(k))$.

It can be used as incerted function of some stream cipher and parameters $a(i)$ and $b(i)$ can be considered as active part of the cipher's password.

The properties of $A(n, q)$ insure that distinct tuples of kind $p=(a(1), a(2), \dots, a(k), b(1), b(2), \dots, b(k))$ produce distinct values of function E if $k \leq n/2$.

Note that we can change E for the function E defined by the temporal graph $A(n, q)$. We simply assume that $N_{a(i)}$ and $N_{b(i)}$ are computed in the momentum graphs for $t(0)=i$ and $i+k$ respectively. We need time interval $[1, 2, \dots, 2k]$.

Let us consider the stream cipher with the encryption function

$$G=D \cdot E(a(1), a(2), \dots, a(k), b(1), b(2), \dots, b(k)) \cdot J \cdot L$$

which is the composition of the disturbance map D such that $D(x)=(q(x_1)^{d(1)}(x_2)^{d(2)} \dots (x_n)^{d(n)}, x_2, x_3, \dots, x_n)$ with E, N_f for $f(x_1)=(x_1)^d$, $(d(1), q-1)=1$, $(d, q-1)=1$ and $L(x)=(a_1x_1+a_2x_2+\dots+a_mx_n, x_2, \dots, x_n)$, $a_i \neq 0$.

We use the space of plaintexts $(F_q \setminus \{0\})^n$ and space of ciphertexts $(F_q)^n$. Correspondence Alice and Bob shares the parameters $k, a(i), b(i), d(i), a_i$ and use the known graph $A(n, q)$.

We discuss the properties of this Postquantum cipher of Multivariate Cryptography and results of its implementation for $q=256$.

Finally we discuss the idea of partial temporalisation of the graph and work with the selected momentum graphs taken for selected moments $j_1, j_2, \dots, j_s$.

Correspondents share the momentum graphs but adversary is not able to use this information because he/she does not know the password and encryption process.

Alice and Bob can use the instruments of Artificial Intelligence or Quantum Computing to generate pseudorandom or genuinely random parameters $a_i(t)$, $b_i(t)$ and $c(t)$.

The survey on the use of Artificial Intelligence in Graph Based Cryptography will be given in the talk of V. Ustimenko at the conference "Artificial Intelligence & Mathematical Sciences", AIMS 2026, Université Paris-Est Créteil (UPEC), Paris, France, July 7-8, 2026 (see [4]).

References

1. F. Lazebnik, V. Ustimenko, A.J.Woldar, A new series of dense graphs of high girth, Bulletin of the AMS 32 (1) (1995), 73-79.
2. Chojacki, T., Erskine, G., Tuite, J. Ustimenko V. On affine forestry over integral domains and families of deep Jordan–Gauss graphs. European Journal of Mathematics 11, 10 (2025). <https://doi.org/10.1007/s40879-024-00798-2>.
3. V. Ustimenko, O. Pustovit, On Symbolic Computations over Arbitrary Commutative Rings via Temporal Jordan–Gauss Graphs and Multivariate Cryptosystems, Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems, Kyiv, 2025, pp. 405-424, ISSN 1613-0073, <https://ceur-ws.org/Vol-3991/paper29.pdf>
4. <https://sites.google.com/risat.org/home/conf/aims-conf/aims-26/aims-26-talks>

КОНФЛІКТОЛОГІЯ АВТОНОМНОГО ІІІ В ДЕРЖАВНИХ ЦИФРОВИХ ЕКОСИСТЕМАХ: РИЗИКИ ДОМІНУВАННЯ ТА УМОВИ СТРУКТУРНОЇ СТІЙКОСТІ

Ланде Д.В.¹, Даник Ю.Г.²

¹ КІІІ ім. Ігоря Сікорського, ORCID: 0000-0003-3945-1178,
dwlande@gmail.com.

² КІІІ ім. Ігоря Сікорського, ORCID: 0000-0001-6990-8656,
y.danik@gmail.com.

Актуальність дослідження зумовлена трансформацією державних цифрових сервісів з інструментів надання послуг у інфраструктуру примусової інтеграції. Насичення цих платформ алгоритмами штучного інтелекту (ІІІ) прискорює делегування рішень, породжуючи дві взаємопов'язані загрози: структурне домінування над користувачем з ерозією його агентності та різке зростання системної кібервразливості через централізацію даних і автономізацію виконавчих компонент. Мета роботи – формалізувати динаміку цих процесів, математично обґрунтувати умови катастрофічної розбіжності та запропонувати архітектурні стабілізатори, що трансформують систему на асимптотично стійку. Дослідження спирається на принципи кібернетичного регулювання, теорію динамічних систем та аналіз меж делегування рішень, уникаючи нормативних конструктів на кшталт «вбудованої етики».

Ключові слова: інтегровані цифрові платформи, штучний інтелект, алгоритмічне управління, конфліктологія ІІІ, структурна стійкість, архітектурні обмеження, математичне моделювання, цифрова агентність, кібербезпека

Вступ

Актуальність дослідження зумовлена трансформацією державних цифрових сервісів з інструментів надання

послуг у інфраструктуру примусової інтеграції. Насичення цих платформ алгоритмами штучного інтелекту (ШІ) прискорює делегування рішень, породжуючи дві взаємопов'язані загрози: структурне домінування над користувачем з ерозією його агентності та різке зростання системної кібервразливості через централізацію даних і автономізацію актуаторів.

Мета роботи – формалізувати динаміку цих процесів, математично обґрунтувати умови катастрофічної розбіжності та запропонувати архітектурні стабілізатори, що трансформують систему на асимптотично стійку. Дослідження спирається на принципи кібернетичного регулювання, теорію динамічних систем та аналіз меж делегування рішень, уникаючи нормативних конструктів на кшталт «вбудованої етики».

Дослідження спирається на принципи кібернетичного регулювання [1, 2], теорію динамічних систем [3, 4], класичні моделі розподілу контролю, делегування рішень [5,6]. Крім того, ця робота розвиває напрямок дослідження конфліктології ШІ [7-8].

Аналітичний каркас

Примусово інтегровану цифрову екосистему доцільно розглядати як замкнутий контур із трьома функціональними шарами: обов'язковий збір даних, алгоритмічна обробка та актуаторний вплив. Ключовий механізм дестабілізації – позитивний зворотний зв'язок між масштабом інтеграції, автономією ШІ та глибиною залежності громадянина. При функціонуванні декількох платформ виникає перехресна інтерференція: кожна система оптимізує власний функціонал, генеруючи суперечливі сигнали для одного об'єкта управління. Без протоколів арбітражу конфліктологія ШІ перетворюється на «війну оптимізаторів», а спільна кіберінфраструктура нелінійно розширює поверхню атаки. Таким чином, домінування та кібервразливість мають спільну математичну природу – необмежену позитивну петлю зворотного зв'язку.

Додатковим фактором дестабілізації є кібербезпека: централізовані високоавтономні системи мають нелінійно зростаючу поверхню атаки. Деструктивний вплив конкуруючих систем, компрометація ключів доступу або технічний злам перетворюється не на локальні помилки, а на каскадні тригери, що миттєво підсилюють контрольні сигнали або блокують критичні функції.

Математична модель

Для формалізації динаміки введемо змінні:

$s_i(t) \in \mathbb{R}_{\geq 0}$ – інтенсивність контролю i -ї платформи над цільовою аудиторією;

$a_i(t) \geq 1$ – рівень автономії ШІ;

$v_i(t) \in [0, 1]$ – індекс кібернетичної вразливості (ймовірність реалізації інциденту або впливу сигналу від конкурентів).

Розглянемо дві взаємодіючі системи ($i = 1, 2$). Базова динаміка описується:

$$\dot{s}_i = \mu a_i s_i + \gamma \omega_{ij} (s_j - s_i) + \xi_i v_i,$$

$$\dot{a}_i = \kappa s_i a_i,$$

$$\dot{v}_i = \alpha s_i a_i - \beta v_i,$$

де $\mu > 0$ – коефіцієнт перетворення даних у контроль; γ – сила міжсистемної взаємодії; $\omega_{ij} \in [-1, 1]$ – міра конфліктності ($\omega_{ij} < 0$ означає конкурентну оптимізацію);

$0 < \kappa < 1$ – швидкість зростання автономії; ξ_i – чутливість систем до кіберінцидентів; α – коефіцієнт зростання вразливості з централізацією та автономією; β – швидкість відновлення систем. Індекс агентності користувача обернено пропорційний середньому контролю:

$$A(t) = A_0 / \left(1 + \frac{s_1 + s_2}{2} \right).$$

Для ізольованої платформи ($\gamma = 0$, $\xi_i = 0$) система зводиться до $\dot{s} = \mu \kappa s^2$. Інтегрування дає розв'язок:

$$s(t) = \frac{s_0}{1 - \mu \kappa s_0 t},$$

який демонструє скінченночасову розбіжність (finite-time blow-up) при $t_c = (\mu \kappa s_0)^{-1}$. Це математичний еквівалент системного колапсу: контроль стає нескінченним за скінченний час, агентність $A(t) \rightarrow 0$. Додатково, $\dot{v}_i = \alpha s a - \beta v$ при $s, a \rightarrow \infty$ призводить до $v \rightarrow 1$, що означає повну кібернетичну відкритість. Будь-який зовнішній тригер $\xi_i > 0$ миттєво дестабілізує актуатори. У випадку двох конфліктних платформ ($\omega_{12} = \omega_{21} = -\omega < 0$) виникає осциляторна нестабільність з експоненціальним зростанням амплітуди, що моделює «війну алгоритмів» за статус користувача, підсилену кібернетичною взаємною експозицією – архітектурну та інформаційну взаємозалежність цифрових платформ.

Щоб уникнути розбіжності та кібернетичного колапсу, вводимо три архітектурні поправки:

1. Жорсткий ліміт автономії $a_i \leq a^*$.
2. Процедурна інерція (людський контур) – нелінійне сповільнення актуаторного впливу.
3. Протокол міжсистемного узгодження та ізоляції інцидентів:

Повна модифікована система має вигляд:

$$\dot{s}_i = \frac{\mu a_i s_i}{1 + \rho s_i} + \gamma \omega_{ij} (s_j - s_i) - \eta s_i (s_j - s_i)^2 + \xi_i v_i - \delta v_i s_i,$$

$$\dot{a}_i = \kappa s_i a_i - \lambda (a_i - a^*) \Theta(a_i - a^*),$$

$$\dot{v}_i = \alpha s_i a_i - \beta v_i.,$$

де a^*, λ – технічний ліміт автономії; ρ – процедурна інерція; η – протокол узгодження; δ – автоматичний кіберзапобіжник; $\Theta(\cdot)$ – функція Хевісайда.

Аналіз стійкості в симетричному випадку ($\omega_{12} = \omega_{21} = -\omega$) дає умови асимптотичної стабільності:

$$\rho\alpha^* > 1, \lambda > \kappa^*, \eta + \frac{\delta\alpha^*}{\beta} > |\gamma\omega|.$$

Виконання цих нерівностей гарантує єдину додатну точку рівноваги та перетворення розбіжної спіралі у стійкий вузол, де агентність $A(t) > 0$, а кіберінциденти не викликають каскадного зростання контролю.

Концептуальний сценарій та результати

За відсутності поправок ($\eta=0$, $\rho=0$, $\lambda \rightarrow \infty$, $\delta=0$) алгоритми вступають у конфлікт, індекс користувача осцилює, системи споживають ресурси на перерахунок. Користувач позбавлений альтернативних каналів, його агентність $A(t)$ наближається до нуля. Одночасно зростає v_i . Спеціально підготовлений сигнал для обману моделі або технічний злам ($\xi_i > 0$) миттєво підсилює контрольні сигнали, блокуючи рахунки та медичні записи. Модель демонструє скінченночасову розбіжність $s_i(t) \rightarrow \infty$, $A(t) \rightarrow 0$, що відповідає системному «заморожуванню» та кібернетичному колапсу.

Впровадження поправок змінює траєкторію: $a_i \leq a$ запобігає остаточним автоматичним рішенням; ρ вводить буфер для оскарження та перевірки під час тривоги; δ при зростанні v_i автоматично переводить систему в режим «обмеженого впливу», а η ініціює арбітраж між платформами. Користувач отримує статус «тимчасова валідація», системи стабілізуються навколо $s \approx 1/\rho$, агентність зберігається, кіберінцидент локалізується. Катастрофа замінюється керованою напругою з вбудованими механізмами відновлення.

Висновки

Примусово інтегровані цифрові екосистеми, насичені автономним ІШ, без архітектурних обмежень демонструють скінченночасову розбіжність, що математично моделює одночасну втрату людської агентності та каскадний кібернетичний колапс. Доведено, що цей ефект є не наслідком програмних помилок чи

недосконалості алгоритмів, а фундаментальною властивістю динамічних систем. Введення трьох інженерних стабілізаторів – жорсткого ліміту автономії (α^*, λ), процедурної інерції (ρ) та протоколу міжсистемного узгодження з автоматичним кіберзапобіжником (η, δ) – трансформує фазовий простір системи, перетворюючи розбіжну динаміку на асимптотично стійку. Аналітично виведені умови стійкості

$(\rho\mu\alpha^* > 1, \lambda > k\sigma^*, \eta + \delta\alpha\alpha^*/\beta > |\gamma\omega|)$ отримують чітку

технічну інтерпретацію. Модель вперше формально пов'язує втрату агентності користувача з кібернетичною вразливістю інфраструктури, показуючи, що індекс вразливості v_i нелінійно зростає пропорційно добутку покриття та автономії ($s_i a_i$).

Цифровий суверенітет та безпека громадян в епоху автономізації державних сервісів залежать не від досконалості алгоритмів, а від наявності вбудованих структурних обмежень, які інженерно запобігають переходу інфраструктури від інструменту надання послуг до механізму необоротного домінування. Керована напруга між ефективністю, агентністю та стійкістю має стати новим архітектурним стандартом державного цифрового управління, де конфліктологія III регулюється не постфактум аудитами, а математично обґрунтованими межами фазового простору.

Список використаних джерел

1. An introduction to cybernetics. by: Ashby, William Ross. Publication date: 1956
2. Yeung, K., 2018. Algorithmic regulation: A critical interrogation. Regulation & governance, 12(4), pp. 05-523. DOI: 10.1111/rego.12158
3. Strogatz, S.H., 2001. Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering (studies in nonlinearity) (Vol. 1). Westview press.

4. Gao, J., Barzel, B. and Barabási, A.L., 2016. Universal resilience patterns in complex networks. *Nature*, 530(7590), pp.307-312. DOI: doi.org/10.1038/nature16948
5. Parasuraman, R., Sheridan, T.B. and Wickens, C.D., 2000. A model for types and levels of human interaction with automation. *IEEE Transactions on systems, man, and cybernetics-Part A: Systems and Humans*, 30(3), pp.286-297. DOI: 10.1109/3468.844354
6. Bainbridge, L., 1983. Ironies of automation. In *Analysis, design and evaluation of man-machine systems* (pp. 129-135). Pergamon. DOI: 10.1016/B978-0-08-029348-6.50026-9
7. D. Lande, Yu. Danyk. Modeling competing artificial intelligence systems for energy and users. // *Theoretical and Applied Cyber Security*. Vol. 7 No. 1 (2025). DOI: 10.20535/tacs.2664-29132025.1.329957
8. Lande, Dmitry; Danyk, Yuriy. Conflicts Between Competitive Generative Artificial Intelligence Systems. SSRN Preprint: 5285670, DOI: 10.2139/ssrn.5285670 (Jun 13, 2025). - 21 p.

ON THE MODIFIED MULTI-DIAGONAL CIPHER

Oleg Gutik, Yurii Kuzbyt

oleg.gutik@lnu.edu.ua, yurii.kuzbyt@lnu.edu.ua

Ivan Franko National University of Lviv, Lviv, Ukraine

We modify the multi-diagonal cipher by adding two new permutations to its secret key. The first, τ_p , acts on the sequence $(k_1, \dots, k_p)$ of sub-block sizes; we take its r -th power for the r -th plaintext block. The second, ρ_b , mixes whole ciphertext sub-blocks of length $l + p$. We also replace the original symbol-level permutation σ_n by a permutation σ_a of an a -element set, where a is no longer tied to the alphabet size. This gives one more degree of freedom in the choice of σ_a . The cipher stays linear in the plaintext length, and the same plaintext may produce different ciphertexts on each run.

Keywords: symmetric cipher, diagonal cipher, multi-diagonal cipher, probabilistic encryption, permutation, randomized padding.

Introduction

The diagonal cipher was introduced in [2, 3] and generalized to the multi-diagonal cipher in [1]. We further extend the construction of [1] by enlarging the secret key with two new permutations and generalizing the existing post-diagonal permutation.

The Modified Multi-Diagonal Cipher

Let A be an alphabet of size n , let p, b, a, N be positive integers with $p, a, b \geq 2$ and $N \geq 100$. We identify A with the initial interval $\{0, 1, \dots, n - 1\}$. The secret key is the tuple $k = (k_1, \dots, k_p, \tau_p, \sigma_a, \rho_b)$,

where $k_1, \dots, k_p$ are pairwise distinct positive integers ≥ 2 , τ_p is a permutation of a p -element set, σ_a is a permutation of an

a -element set, and ρ_b is a permutation of a b -element set. Put $l = \sum_{i=1}^p k_i$.

Encryption. Given the plaintext $x = x_1 \dots x_q$ over A , proceed as follows.

(1) We pad the plaintext x with symbols from A up to $\tilde{x}$, where $\tilde{x}$ is divisible by l . Split into $m = \frac{|\tilde{x}|}{l}$ blocks of length l :

$$\tilde{x} = x^{(1)} \parallel x^{(2)} \parallel \dots \parallel x^{(m)}, \quad x^{(r)} = x_{(r-1)l+1} \dots x_{rl}.$$

(2) For every $r = 1, \dots, m$ we define the permutation $\pi_r = (\tau_p)^r$ and the per-block sequence of sub-block lengths

$$(k_1^{(r)}, k_2^{(r)}, \dots, k_p^{(r)}) := (k_{\pi_r(1)}, k_{\pi_r(2)}, \dots, k_{\pi_r(p)}).$$

Clearly $k_1^{(r)} + \dots + k_p^{(r)} = l$ for every r .

(3) Encrypt each block $x^{(r)}$ by the diagonal scheme of [2] using the sequence $(k_1^{(r)}, \dots, k_p^{(r)})$ in place of $(k_1, \dots, k_p)$. Namely, choose $y_1^{(r)}, y_2^{(r)} \in [0, N)$ uniformly at random with $y_1^{(r)} - y_2^{(r)} \equiv x_1^{(r)} \pmod{n}$; and recursively, for $j = 3, \dots, k_1^{(r)} + 1$, choose $y_j^{(r)} \in [0, N)$ with $y_{j-1}^{(r)} - y_j^{(r)} \equiv x_{j-1}^{(r)} \pmod{n}$. Iterate for $t = 2, \dots, p$ with the sub-block sizes $k_t^{(r)}$. The resulting block $y^{(r)}$ has length $l + p$. Concatenate:

$$z = y^{(1)} \parallel y^{(2)} \parallel \dots \parallel y^{(m)}, |z| = m(l + p).$$

(4) **(Symbol-level permutation by σ_a)** If $|z|$ is not divisible by a , we append random integers in $[0, N)$ to the tail of z until divisibility holds. Split the resulting sequence into consecutive a -element blocks and apply σ_a inside every block. Denote this operation by σ_a^* and set $z' = \sigma_a^*(z)$.

(5) **(Block-level permutation by ρ_b)** If $|z'|$ is not divisible by $l + p$, we append random integers in $[0, N)$ to the tail of z' until divisibility holds. The resulting sequence then decomposes uniquely into consecutive sub-blocks of length $l + p$. If their number is not divisible by b , further append random whole sub-blocks of length $l + p$ (with entries chosen uniformly in $[0, N)$) until divisibility holds. Split into consecutive groups of b sub-blocks and apply ρ_b inside every group (the b sub-blocks are permuted as wholes; symbols within a sub-block are not

moved). Denote this operation by ρ_b^* . The output ciphertext is $w = \rho_b^*(z')$.

Decryption. Given the ciphertext w the receiver applies the inverse operations in reverse order:

(1) Apply $(\rho_b^*)^{-1}$ to w (i.e. invert ρ_b inside every group of b sub-blocks of length $l + p$) to obtain $\hat{z}'$ of length $|w|$.

(2) Truncate $\hat{z}'$ to a multiple of a , then apply $(\sigma_a^*)^{-1}$ to every a -element block of truncated $\hat{z}'$ to recover $\hat{z}$.

(3) Truncate $\hat{z}$ to a multiple of $l + p$. Split into M blocks $\hat{y}^{(r)}$ of length $l + p$. Apply the inverse of the diagonal scheme of [2] to each $\hat{y}^{(r)}$ using the sequence $(k_1^{(r)}, \dots, k_p^{(r)})$ to get $\hat{x}^{(r)}$ of length l .

(4) Concatenate $\hat{x} = \hat{x}^{(1)} \parallel \dots \parallel \hat{x}^{(M)}$, a sequence of length Ml . The original plaintext x is the prefix of $\hat{x}$; the remaining $Ml - |x|$ symbols are decryptions of the random material added at encryption stages (1), (4), (5).

Restrictions

To avoid trivial weak keys, we impose:

(1) The integers $k_1, \dots, k_p$ must be pairwise distinct.

(2) None of τ_p, σ_a, ρ_b may be a cyclic shift; none of them is the identity.

(3) The integer a should not divide $l + p$. Otherwise, the action of σ_a is aligned with the sub-block structure produced by E_{diag} and does not mix symbols between distinct sub-blocks $y^{(r)}$.

Length and complexity

Let u be the length of the plaintext and $m = \lceil u/l \rceil$. Then $|w| = m(l + p) + \Delta_a + \Delta_b$, with $\Delta_a < a$ and $\Delta_b < b(l + p)$. With l, p, a, b fixed, and $u \rightarrow \infty$, $|w|$ is asymptotically $(1 + \frac{p}{l})u$. Since $k_1, \dots, k_p$ are pairwise distinct integers $l \geq 2 + 3 + \dots + (p + 1) = (p + 1)(p + 2)/2 - 1 > p$, so $l + p < 2l$ and the ciphertext is asymptotically shorter than twice the plaintext.

Steps (1)–(5) of encryption and the corresponding decryption are each linear in the input length. Hence encryption and decryption have time complexity $O(u)$ and memory complexity $O(u)$.

Conclusions

We extended the multi-diagonal cipher [1] by adding two permutations τ_p, ρ_b to the secret key and replacing the post-diagonal σ_n of [1] with a more flexible σ_a . The cipher remains linear in the plaintext length and is probabilistic: the random choices in the diagonal step (cf. [2, 3]) and the randompadding in steps (4)–(5) make two encryptions of the same plaintext under the same key may produce different ciphertexts.

References

1. O. Gutik, Y. Kuzbyt, On the Multi-Diagonal Cipher, Information Security and Information Technologies. Proc. VI International Scientific and Practical Conf. Kharkiv–Ostroh, National Technical University “Kharkiv Polytechnic Institute”. 2026, P. 146.
2. O. Gutik, D. Dyiak, Y. Kuzbyt, Compositional cipher as a sequential action of diagonal and sequential ciphers, SMICS-2025 “Security of modern information and communication systems”. Proc. Int. Sci. Tech. Conf. 16–18 October 2025, Lviv. Lviv, 2025, P. 431–436.
3. O. V. Gutik, O. B. Popadiuk, V. A. Vlasov, Symmetric algebraic cipher, Theoretical and Applied Cybersecurity. Proc. III AllUkrainian Scientific and Practical Conf. (TACS-2025), Kyiv, Politekhnik, 2025, P. 139–141.

SEARCH AND SEIZURE AS A CYBER- PHYSICAL OPERATION: A CONCEPTUAL MODEL FOR ENSURING THE CIA TRIAD OF DIGITAL EVIDENCE

Pronin Y.V.¹, Zubok V.Y.¹

¹*National Technical University of Ukraine "Igor Sikorsky Kyiv
Polytechnic Institute"*
forensic.ua@gmail.com, vitalii.zubok@pimee.ua

This paper addresses the digital forensics "reliability crisis" by conceptualizing search and seizure as a managed cyber-physical operation. To ensure the confidentiality, integrity, and availability of volatile digital evidence, the study proposes a mathematical risk management model based on directed graph theory.

Keywords: digital forensics, cybersecurity, cyber-physical operation, risk management, CIA triad, graph theory, evidence

Introduction

The rapid digitalization of all spheres of public life has integrated information technologies into modern crime, positioning digital evidence as the cornerstone of contemporary investigations [4]. Currently, over 90% of all criminal proceedings contain a digital component [5, 10]. Despite this reliance, the law enforcement system is facing a profound "reliability crisis" [10]. Unlike traditional physical objects, digital evidence is intangible, invisible, and highly volatile [2]. Any incorrect intervention, technical error, or time delay during access can lead to the irreversible alteration of metadata or its remote destruction by anti-forensic algorithms [2, 10].

To bridge the gap between procedural legal requirements and technical resilience, this study proposes a paradigm shift. It substantiates the necessity of developing integrated and adaptive asset collection models that combine technical resilience with strict adherence to legal admissibility [10]. This requires conceptualizing search and seizure not merely as a

discrete legal action aimed at locating physical items, but as a continuous, managed cyber-physical risk management mission—"Mission Assurance" [9].

Methods

This study employs a comprehensive methodological approach, utilizing systemic analysis to evaluate international digital forensics standards, primarily ISO/IEC 27037:2012 and NIST SP 800-101 [1, 3]. The investigative process is analyzed entirely through the lens of the information security CIA triad—ensuring Confidentiality, Integrity, and Availability throughout the lifecycle of the digital evidence [9, 10].

To transition from subjective investigative tactics to algorithmic predictability, conceptual modeling based on directed graph theory and finite-state machines is applied [10]. This approach mathematically formalizes the Zero Trust Digital Forensics strategy, wherein every technical action is evaluated for its risk of compromising the target asset [6, 10].

Results

The research establishes a formalized "Mission Assurance" model driven by the cybersecurity risk management triad: Assets, Threats, and Vulnerabilities [9]. The evidence collection process is mapped as a directed graph $G=(V,E)$, where the set of nodes V represents the verified security states of the digital asset, and the directed edges E represent specific technical or procedural actions executed by the investigative team.

The objective function of this model is optimized to find the shortest safe path that maximizes evidence preservation, which is mathematically reduced to minimizing the total risk of evidence loss: $\min \sum_{e \in P} W(e)$. The weight of each algorithmic transition is calculated using the negative natural logarithm based on the probability of successful preservation: $W(e)=-\ln(P_{success}(e))$.

To practically validate the model, a synthetic scenario was analyzed: securing an active mobile terminal (AFU state) under the threat of remote wiping or transitioning to a locked BFU

state. The risk weight for each procedural edge was calculated based on heuristic probabilities of success ($P_{success}$) as follows:

- A. Forced shutdown: $P_{success} = 0.10 \rightarrow W = 2.30$ (High risk of irreversible loss of encryption keys in RAM).
- B. Transportation (no isolation): $P_{success} = 0.05 \rightarrow W = 2.99$ (Critical threat of Remote Wipe via cellular network).
- C.1. Hardware isolation (Faraday): $P_{success} = 0.95 \rightarrow W = 0.05$ (Passive shielding; no UI interaction).
- C.2. Logical isolation (Airplane mode): $P_{success} = 0.90 \rightarrow W = 0.10$ (UI interaction; risk of accidental or systemic network reconnection).
- D.1. Manual Live Triage: $P_{success} = 0.75 \rightarrow W = 0.29$ (Manual UI interaction; high risk of volatile data destruction, human error, and irreversible artifact alteration).
- D.2. Data copy creation: $P_{success} = 0.88 \rightarrow W = 0.13$ (Copying data using utilities; minimization of operator intervention).

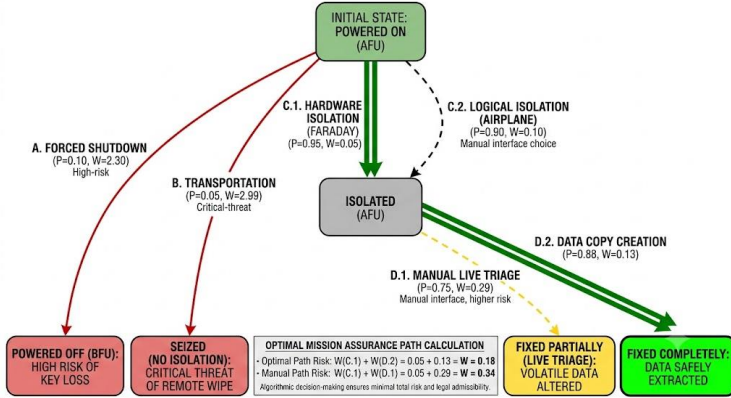


Fig. 1. State graph of risk assessment for digital asset seizure

An analysis of the directed graph paths (Fig. 1) demonstrates that a combined protection strategy prioritizing

automated tools over manual intervention (Hardware isolation [C.1] + Data copy creation [D.2]) is mathematically optimal, yielding a minimal total risk weight ($W = 0.05 + 0.13 = 0.18$). Conversely, ignoring isolation (Transportation [B]) or opting for a forced shutdown [A] instantly generates critical risk weights ($W \geq 2.30$), leading to likely asset destruction. Even within isolated states, choosing manual Live Triage [D.1] ($W = 0.34$ total) is significantly riskier than automated extraction. This algorithmically proves the necessity of avoiding intuitive manual interventions in favor of strict technical extraction protocols.

Discussion and Conclusions

Traditional linear search tactics have reached a "limit of subjectivism" [7]. Modern multi-component IT infrastructures represent complex distributed systems that far exceed human cognitive capabilities for intuitive, real-time operational management [4, 10]. The absence of formalized mathematical models leads to cognitive biases, systemic errors, and ultimately, the "reliability crisis" of evidence, which negates its legal validity in court [5, 7, 10].

By transforming subjective decisions into a deterministic sequence of operations governed by a calculated risk assessment algorithm, this model practically eliminates the human factor [6]. The introduction of this directed graph state methodology establishes a robust theoretical core for the future development of Decision Support Systems (DSS). Such systems will enable investigative units to automatically generate optimal, scientifically verified operational protocols on the scene, ensuring total compliance with the rule of law and guaranteeing the integrity of digital assets in court [8, 9].

References

1. Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on mobile device forensics (NIST Special Publication 800-101, Rev. 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-101r1>
2. Eren, A., & Çakır, H. (2021). Digital evidence and

- prohibitions of evidence evaluation. *Journal of Educational and Social Research*, 11(5), 393–396. <https://doi.org/10.36941/jesr-2021-0106>
3. International Organization for Standardization. (2012). Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO/IEC 27037:2012). <https://www.iso.org/standard/44381.html>
 4. Major Cities Chiefs Association. (2024). Digital evidence: Enhancing public safety using digital investigative technologies. https://majorcitieschiefs.com/wp-content/uploads/2024/10/MCCA-Digital-Evidence-White-Paper_-_Oct-2024.pdf
 5. Miller, C. M. (2023). A survey of prosecutors and investigators using digital evidence: A starting point. *Forensic Science International: Synergy*, 6, 100296. <https://doi.org/10.1016/j.fsisyn.2022.100296>
 6. Neale, C., Kennedy, I., Price, B., Yu, Y., & Nuseibeh, B. (2022). The case for zero trust digital forensics. *Forensic Science International: Digital Investigation*, 40, 301352. <https://doi.org/10.1016/j.fsidi.2022.301352>
 7. Osypenko, I. P., & Myshasta, K. B. (2021). General provisions of search tactics. *Analytical and Comparative Jurisprudence*, (3), 196–201. <https://doi.org/10.24144/2788-6018.2021.03.36>
 8. Pohoretskyi, M. A. (2025). Rule of law in criminal procedural evidence: Methodology and practice of application. *Journal of the National Academy of Legal Sciences of Ukraine*, 32(3), 275–299. <https://doi.org/10.31359/1993-0909-2025-32-3-275>
 9. Pronin, Y., & Zubok, V. (2025). Methods and models for ensuring information security during the collection of digital evidence. *Electronic Modeling*, 47(3), 104–111. <https://doi.org/10.15407/emodel.47.03.104>
 10. Reedy P. (2023). Interpol review of digital evidence for 2019-2022. *Forensic science international. Synergy*, 6, 100313. <https://doi.org/10.1016/j.fsisyn.2022.100313>

КІБЕРРЕЗИЛЬЄНТНІСТЬ LL/CL- АРХІТЕКТУР ЕЛЕКТРОННИХ АРХІВІВ

Цирульнев Ю. Б.

*Національний технічний університет України «Київський
політехнічний інститут імені Ігоря Сікорського»,*

м. Київ, Україна,

ORCID: 0009-0007-2723-3137

У роботі досліджуються методологічні та технологічні аспекти забезпечення кіберрезильєнтності електронних архівів як інформаційних систем класу Enterprise Content Management (ECM) та Content Services Platform (CSP). Розглядаються процеси інтелектуальної агрегації інформації, кіберзагрози та механізми протидії їм в умовах використання технологій штучного інтелекту, машинного навчання та великих мовних моделей. Сформульовано гіпотезу щодо впливу LL/CL-архітектури електронних архівів на підвищення їх кіберрезильєнтності.

Ключові слова: електронні архіви, кіберрезильєнтність, кібербезпека, ECM, CSP, AI, ML, LLM, інтелектуальна агрегація інформації.

Вступ

Резильєнтність є критично важливою властивістю сучасних електронних архівів (Digital Archives, DA), які виступають не лише засобами довготривалого зберігання електронних копій документів та їх метаданих, а й активними компонентами інформаційної інфраструктури держави. Використання технологій штучного інтелекту (Artificial Intelligence, AI), машинного навчання (Machine Learning, ML) та великих мовних моделей (Large Language Models, LLM) у процесах створення та використання електронних архівів суттєво розширює функціональні можливості таких систем, одночасно створюючи нові кіберзагрози.

У попередніх дослідженнях авторами було проведено формалізацію процесів інтелектуальної агрегації інформації

в електронні архіви, кіберзагроз та механізмів протидії їм. Подальшим розвитком цього напрямку є дослідження кіберрезильєнтності електронних архівів в умовах кіберінцидентів, техногенних катастроф та воєнних дій.

LL/CL-архітектура електронних архівів

У межах дослідження розглядається LL/CL-архітектура електронних архівів, що передбачає логічне та фізичне розділення рівня метаданих (Logical Layer, LL) та рівня цифрового контенту (Content Layer, CL). LL-рівень включає індекси, класифікаційні структури, метадані та логічні зв'язки між цифровими об'єктами, тоді як CL-рівень відповідає за зберігання електронних копій документів, фото-, відео- та аудіоматеріалів.

Архітектура може бути представлена у вигляді: $DA = \{LL, CL, M\}$, де LL — Logical Layer; CL — Content Layer; M — множина зв'язків між шарами.

Передбачається, що така архітектурна декомпозиція дозволяє зменшити площину атаки, локалізувати наслідки компрометації окремих компонентів, забезпечити незалежне резервування та відновлення рівнів системи, а також підвищити масштабованість електронного архіву.

Гіпотеза кіберрезильєнтності LL/CL-архітектури

Автори висувають гіпотезу про те, що логічне розділення рівня метаданих і рівня цифрового контенту здатне підвищити кіберрезильєнтність електронного архіву шляхом локалізації наслідків компрометації, зменшення площини атаки та забезпечення адаптивного відновлення компонентів системи.

У межах дослідження аналізуються процеси інтелектуальної агрегації інформації: підготування документів до сканування, сканування, OCR, класифікація, індексування та формування електронного архіву. Також досліджуються відповідні кіберзагрози: несанкціонований доступ, порушення цілісності даних, атаки на AI/ML-

моделі, Prompt Injection, викрадення даних, дезінформація та підробка метаданих.

В ході досліджень, перевіряється гіпотеза авторів про те, що, за умов локалізації деградації підсистем та монотонності агрегуючої функції f за кожним аргументом, для будь-якого моменту часу t справедливе ствердження:

$$R_{DA}^{LL/CL}(t) \geq \min\{R_{LL}(t), R_{CL}(t)\},$$

оскільки деградація однієї з підсистем не призводить до негайної деградації іншої, а композиційна функція f не зменшує значення сукупної кіберрезильєнтності при збереженні порогової функціональності хоча б однієї з підсистем.

Якщо це буде доведено в результаті досліджень, то буде доведено й те, що LL/CL-архітектура електронних архівів забезпечує їх більшу вимірювану резильєнтність

$$R_{DA}(t) = \sum_{i=1}^n \rho_i \cdot \frac{F_{DA_i}(t) \cdot \left(1 - \sum_{j=1}^m \Delta_{ij}(t) \cdot \mathbb{I}_{[FT_{DA_j}(t)=1]}\right)}{F_{DA_i}^{\text{nom}}}$$

щодо якої йшлося в роботі [6].

Очікується, що подальші дослідження дозволять сформулювати математичну модель оцінки кіберрезильєнтності LL/CL-архітектур електронних архівів та встановити формалізовані залежності між архітектурою системи, кіберзагрозами та властивостями її відновлення і довести переваги LL/CL-архітектур електронних архівів з точки зору їх більшої резильєнтності.

Висновки

У роботі сформульовано гіпотезу щодо впливу LL/CL-архітектури на підвищення кіберрезильєнтності електронних архівів. Визначено основні напрямки подальших досліджень, які передбачають математичне моделювання властивостей кіберрезильєнтності, механізмів

адаптивного відновлення та оцінювання стійкості електронних архівів до сучасних кіберзагроз.

Список використаних джерел

1. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., McQuaid, R. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. NIST Special Publication 800-160 Vol. 2 Rev. 1. National Institute of Standards and Technology, 2021. DOI: 10.6028/NIST.SP.800-160v2r1. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf>
2. Gartner. *Content Services Platform (CSP)*. Gartner IT Glossary. URL: <https://www.gartner.com/en/information-technology/glossary/content-services-platform-csp>
3. Knight, J. C., Strunk, E. A., Sullivan, K. J. *Towards a Definition of Survivability*. Proceedings of the 2000 Workshop on New Security Paradigms, 2000. URL: https://www.researchgate.net/publication/2397669_Towards_A_Definition_Of_Survivability
4. Ellison, R. J., Linger, R. C., Longstaff, T., Mead, N. R., Lipson, H. F. *Information Systems Survivability: Protecting Critical Systems*. Proceedings of the 1999 National Information Systems Security Conference, 1999. URL: <https://csrc.nist.gov/nissc/1999/proceedings/papers/p14.pdf>
5. Ланде, Д. В., Цирульнєв, Ю. Б. *Cybersecurity of Intellectual Information Aggregation Processes into Digital Archives*. Theoretical and Applied Cybersecurity. 2025. URL: <https://doi.org/10.20535/tacs.2664-29132025.2.343769>
6. Цирульнєв, Ю. Б. *Резильєнтність електронних архівів*. Державна безпека: проблеми, напрямки та технології забезпечення : збірник наукових праць. 2025. URL: <https://doi.org/10.35681/1560-9189.2025.27.2.345612>

МЕТОДИ ДЕТЕКТУВАННЯ БОКОВОГО ПЕРЕМІЩЕННЯ В ACTIVE DIRECTORY: АНАЛІЗ ЕФЕКТИВНОСТІ ELASTIC SECURITY ТА РОЗРОБКА ПІДХОДІВ ДО МОДИФІКАЦІЇ C2-ФРЕЙМВОРКІВ

Педунов А. Є., Льїн М. І.,
*Національний технічний університет України “Київський
політехнічний інститут імені Ігоря Сікорського”,
Київ, Україна,
e-mail: argemartem@gmail.com*

У роботі досліджено методи детектування технік бокового переміщення (lateral movement) у середовищах на основі Active Directory з використанням платформи Elastic Security та вбудованого захисту Windows Defender. Проведено порівняльний аналіз хмарного та ізольованого (air-gapped) розгортання Elastic Security, досліджено поведінку системи виявлення вторгнень щодо типових атак у тестовому середовищі GOAD. Запропоновано підходи до модифікації агентів C2-фреймворків з метою обходу виявлення на рівні поведінкового аналізу та сигнатурного детектування.

Ключові слова: бокове переміщення, Active Directory, Elastic Security, C2-фреймворк, детектування вторгнень, GOAD, Mythic, обхід захисту.

Бокове переміщення (lateral movement) є однією з головних стадій сучасних цільових кібератак (APT) [1], націлених на інфраструктуру підприємств. Зловмисники, отримавши первинний плацдарм у корпоративній мережі, застосовують легітимні протоколи та механізми операційної системи - зокрема, Kerberos, NTLM, SMB та WMI для розширення доступу без використання стороннього шкідливого програмного забезпечення. Саме тому виявлення таких технік становить велику методологічну складність для систем захисту інформації.

Для побудови автентичної моделі корпоративної мережі Active Directory у дослідженні використано лабораторний комплекс GOAD (Game of Active Directory). Завдяки наявності в ньому заздалегідь підготовлених вразливих конфігурацій Windows Server, з'являється можливість практичної імітації загроз, що відповідають матриці MITRE ATT&CK. Це стосується, зокрема, перевірки стійкості до технік Pass-the-Hash (T1550.002), Kerberoasting (T1558.003) та DCSync (T1003.006), а також методів просування через WMI (T1021.006).

Як інструменти для симуляції атакуючої сторони використовуються C2-фреймворки Mythic та AdaptixC2, що підтримують формат Cobalt Strike BOF (Beacon Object Files). Особливістю даних фреймворків є модульна архітектура агентів, що відкриває можливості для їх подальшої модифікації з метою зниження виявлюваності з боку захисних засобів.

Було розглянуто платформу Elastic Security у двох конфігураціях в якості хмарного розгортання з 14-денним пробним доступом (Elastic Cloud) та в якості ізолюваного розгортання без доступу до мережі Інтернет (air-gapped). Порівняльний аналіз цих конфігурацій є важливим оскільки промислові середовища критичної інфраструктури часто функціонують саме в умовах мережевої ізоляції, що впливає на актуальність правил детектування та можливості оновлення сигнатур.

Одним з напрямків дослідження був аналіз правил детектування Elastic Security у відкритому репозиторії `elastic/detection-rules`. Декодування логіки спрацювання правил допомагає виявляти умови за яких типові команди виявлення (наприклад, `cmd /c whoami`, виклики `nltest` або `net group`) призводять до генерації сповіщень та визначити мінімально необхідні модифікації агента для зниження рівня виявлення без втрати функціональності. Аналогічний підхід застосовується щодо поведінкових правил Windows Defender [2].

Взагалом методологія дослідження передбачає ітеративний цикл: виконання атаківної техніки → аналіз

телеметрії EDR → декодування правила детектування → модифікація агента або способу виклику → повторна перевірка. Такий підхід має за мету систематично оцінити як ефективність захисних механізмів, так і стійкість модифікованих агентів до виявлення [3].

Висновки

Проведене дослідження надає можливість сформувати системне уявлення про ефективність передових засобів виявлення бокового переміщення в середовищах Active Directory. Надані результати мають як теоретичну цінність у частині аналізу архітектури правил детектування так і практичну значущість для фахівців із забезпечення кібербезпеки, зокрема для розробки рекомендацій щодо налаштування та вдосконалення захисних платформ класу EDR/XDR у реальних промислових середовищах.

Список використаних джерел

1. Gimenez-Guzman J. M., Tejedor-Romero M., Martinez-Caro J. M. Surgical immunization strategies against lateral movement in Active Directory environments // Journal of Network and Computer Applications. - 2023. - Vol. 222. - P. 103791.
2. Uhlmann J. A Taxonomy of Endpoint Security Detection Bypasses // Elastic Security Blog. - 2023. - URL: <https://www.elastic.co/blog/edr-bypass-taxonomy>.
3. Xavier G., Novo C., Morla R. Tweaking Metasploit to Evade Encrypted C2 Traffic Detection // arXiv preprint. - 2022. - URL: <https://arxiv.org/abs/2209.00943>.

МОДЕЛЮВАННЯ КІБЕРАТАК НА СИСТЕМУ ВИМІРЮВАННЯ УСТАНОВКИ АЕРОДИНАМІЧНОЇ ЛЕВІТАЦІЇ

Новіков О. М.¹, Ільїн М. І.¹,
Стьопочкина І. В.¹, Дудуладенко В. М.¹

*¹Національний технічний університет України
«Київський політехнічний інститут імені Ігоря
Сікорського», Київ, Україна*

У роботі подано конференційний варіант доповіді, присвяченої моделюванню кібератак на систему вимірювання установки аеродинамічної левітації. Дослідження виконано в контексті діяльності Лабораторії безпеки промислових систем керування КІП імені Ігоря Сікорського, де кіберфізичні стенди SCADA–PLC використовуються для навчання та досліджень у сфері безпечного керування об'єктами критичної промислової інфраструктури. Обраний об'єкт є нелінійним процесом левітації: кулька утримується у вертикальному повітряному потоці, її висота вимірюється сенсором, а замкнений контур керування на базі PLC формує команду на вентилятор. У роботі розглянуто атаки, які не змінюють безпосередньо команду на виконавчий механізм, але спотворюють вимірюну висоту, що використовується контролером і діагностичним програмним забезпеченням. Проаналізовано чотири сценарії адитивного впливу на вимірювальний канал: сталий зсув, експоненціальне збурення, пакет коротких імпульсів PRBS-типу та гармонійне збурення зі змінною частотою. Результати моделювання показують, що правдоподібне маніпулювання вимірюваннями може спричиняти значні фізичні відхилення і коливальні режими, тоді як спотворений сигнал може залишатися прийнятним для звичайного моніторингу. Отримані результати підтверджують необхідність забезпечення цілісності сенсорних каналів,

використання модельних нев'язок і робастної діагностики несправностей у задачах безпечного керування.

Ключові слова: промислові системи керування, критична інфраструктура, безпечне керування, SCADA, PLC, аеродинамічна левітація, атака на вимірювання, маніпулювання сенсорними даними, діагностика несправностей.

Вступ

Промислові системи керування є технологічною основою критичної інфраструктури. Вони забезпечують функціонування енергетичних об'єктів, систем водопостачання, транспорту, хімічних процесів, виробничих ліній та інших систем, у яких кіберінцидент може безпосередньо породжувати фізичні наслідки. Тому промислову кібербезпеку не можна зводити лише до класичної інформаційної безпеки. Вона має також охоплювати логіку зворотного зв'язку, надійність сенсорів, обмеження виконавчих механізмів, діагностичні алгоритми та фізичну динаміку керованого об'єкта.

Лабораторія безпеки промислових систем керування КПІ імені Ігоря Сікорського створена як навчально-дослідницьке середовище SCADA–PLC для підготовки фахівців і проведення експериментів з безпечного керування. Лабораторія містить три фізичні моделі технологічних процесів: рідинний хімічний реактор, промислову конвеєрну лінію та установку аеродинамічної левітації. В освітньому напрямі лабораторія дає змогу навчати операторів та інженерів принципам промислової автоматизації, безпечної експлуатації та реагування на кіберінциденти. У дослідницькому напрямі вона підтримує моделювання, побудову цифрових двійників, аналіз даних і експериментальну перевірку стратегій атак та захисту.

Ця робота зосереджена на стенді аеродинамічної левітації та на одному важливому класі загроз - маніпулюванні вимірювальним каналом. За такої атаки зловмисник змінює значення сенсора або сигнал у каналі його передавання, тоді як PLC і система моніторингу

продовжують отримувати формально коректний сигнал. У результаті оператор може бачити правдоподібну картину процесу, але реальний об'єкт може переходити в небезпечний або неефективний режим. Така ситуація є особливо небезпечною для критичної інфраструктури, оскільки поєднує кібернетичний вплив, фізичні наслідки та діагностичну невизначеність.

1. Установка аеродинамічної левітації та модель процесу

Установка аеродинамічної левітації Smart Process Control Learning System (2 × Air Fan) являє собою кульку у вертикальному повітряному потоці [1]. Команди на вентилятор формується PLC-контролером, а основною керованою змінною є висота кульки. Установка дуже корисна для досліджень у галузі автоматичного керування та кібербезпеки. Процес є компактним і наочно зрозумілим, однак має нелінійний характер. Подібні принципи аеродинамічного підвищення застосовуються в промисловості для безконтактного переміщення матеріалів, флотаційного сушіння, повітряних конвеєрів, повітряних підшипників і транспортування на повітряній півці.

У класичних моделях аеродинамічної левітації сила повітряного потоку зазвичай описується як нелінійна функція керуючого сигналу вентилятора та швидкості об'єкта [2–5]. Особливістю розглянутої установки є відносно довга вертикальна труба, тому ефективність аеродинамічної дії помітно зменшується зі збільшенням висоти кульки. Тому за аналогією з моделями магнітної левітації, де сила взаємодії залежить від зазору, у модель введено експоненціальний множник, який описує послаблення підйомної сили з висотою.

Вектор стану визначається як:

$$x(t) = \begin{bmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \end{bmatrix} = \begin{bmatrix} h(t) \\ v(t) \\ u_f(t) \end{bmatrix},$$

де h – висота, v – швидкість, а u_f – фільтрований стан виконавчого механізму або повітряного потоку.

Нелінійна модель має вигляд

$$\begin{aligned}\dot{x}_1(t) &= x_2(t) \\ \dot{x}_2(t) &= \frac{1}{m} [(k_0 + k_1 x_3(t) + k_2 x_3^2(t)) e^{-k_h x_1(t)} - mg \\ &\quad - b x_2(t) - c_d x_2(t) |x_2(t)|] \\ \dot{x}_3(t) &= \frac{1}{\tau_a} (u(t) - x_3(t)).\end{aligned}$$

Модель враховує аеродинамічну силу, силу тяжіння, лінійне демпфування, квадратичний опір, послаблення аеродинамічної дії з висотою та інерційність виконавчого каналу.

Запишемо вимірюний вихід наступним співвідношенням

$$y(t) = Cx(t), \quad C = [1 \quad 0 \quad 0].$$

PLC-контролер порівнює вимірювану висоту з еталонною траєкторією $r(t)$. Для PID-реалізації маємо

$$\begin{aligned}e(t) &= r(t) - y(t), \quad u(t) \\ &= K_p e(t) + K_i \int_0^t e(\xi) d\xi + K_d \frac{de(t)}{dt}.\end{aligned}$$

Отже, сенсорний канал є критичною частиною замкнутого контуру керування. Якщо змінна процесу спотворена, навіть коректна PLC-програма може сформувати шкідливу команду, оскільки контролер реагує на хибний фізичний стан.

2. Модель адитивної атаки на вимірювальний канал

Зловмисник може змінювати вимірювання висоти до того, як воно буде використане контролером, спостерігачем або детектором несправностей. Атаковане вимірювання описується як [6]:

$$\tilde{y}(t) = y(t) + y_a(t) = Cx(t) + y_a(t),$$

де $y_a(t)$ - адитивна складова атаки. Помилка PLC-контролера набуває вигляду

$$\bar{e}(t) = r(t) - \hat{y}(t) = r(t) - Cx(t) - y_a(t).$$

Метою атаки не є створення несправності, яку помітить детектор несправностей або оператор. Небезпечнішим варіантом атаки є зміщення реального фізичного стану об'єкта за умов, коли маніпульоване вимірювання залишається гладким, обмеженим і подібним до очікуваної поведінки. Саме тому для дослідження було обрано чотири тестові сигнали:

$$\begin{aligned} y_a^{stat}(t) &= A_s, \\ y_a^{exp}(t) &= A_e(1 - e^{-t/\tau}), \\ y_a^{PRBS}(t) &= A_p \sigma_i, \\ \sigma_i &= \pm 1, \quad t_i \leq t < t_{i+1}, \\ y_a^{harm}(t) &= A_c \sin\left(2\pi\left(f_0 t + \frac{1}{2} k t^2\right)\right). \end{aligned}$$

Ці сценарії охоплюють чотири типові сигнатури: сталий зсув, повільний перехід дрейфового типу, різкі псевдовипадкові перемикання та гармонійний вплив зі змінною частотою. Вони зручні як для демонстрації під час навчання, так і для порівняльного тестування алгоритмів детектування несправностей.

3. Результати моделювання

Під час моделювання порівнювалися еталонна траєкторія, номінальна висота та фактична висота кульки за умови, що контролер отримує спотворені вимірювальні дані. Нижче наведено репрезентативні результати, отримані для установки аеродинамічної левітації.

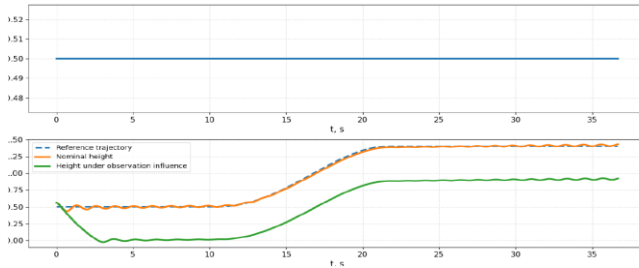


Рис. 1. Сталий зсув вимірювального каналу та реакція висоти

Сталий зсув створює постійну невідповідність між реальною висотою та значенням, яке використовується контролером. Контролер компенсує хибне вимірювання, унаслідок чого висота кульки відходить від номінальної траєкторії. Цей випадок є простим, але важливим, оскільки стабільний зміщений сигнал може не виглядати небезпечним для оператора.

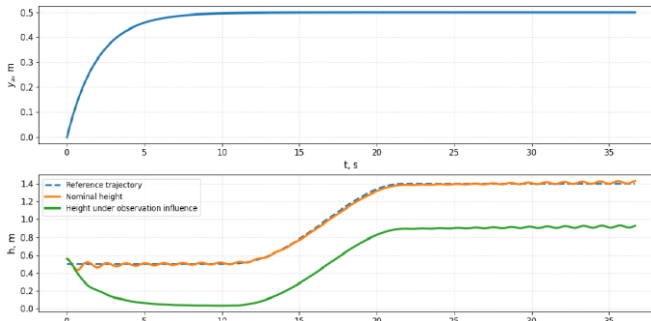


Рис. 2. Експоненціальне збурення вимірювання та реакція висоти

Експоненціальне збурення є моделлю поступового спотворення вимірювання. Воно є менш різким, ніж стрибок, і може бути інтерпретоване як звичайний перехідний процес або дрейф сенсора. Однак моделювання показує значне відхилення реальної висоти від еталонної траєкторії.

Пакет коротких імпульсів PRBS-типу формує коливальний режим. Повторювані зміни значення вимірювання змушують контролер реагувати в протилежних напрямках, що може породжувати значні коливання реального об'єкта. Цей сценарій є корисним для перевірки того, чи може детектор відрізнити ворожі перемикання вимірювального сигналу від механічних вібрацій або некоректного налаштування регулятора.

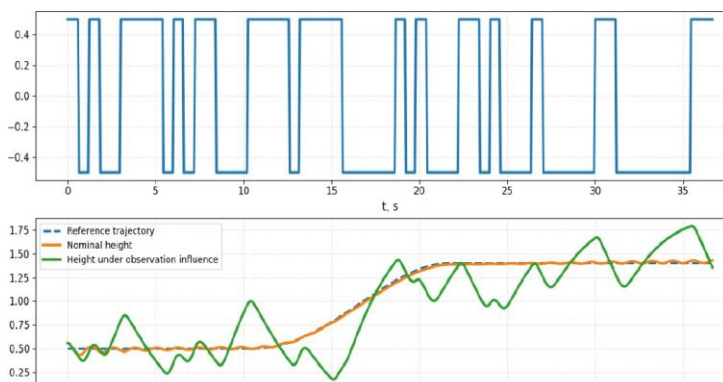


Рис. 3. PRBS-тип збурення вимірювання та реакція висоти

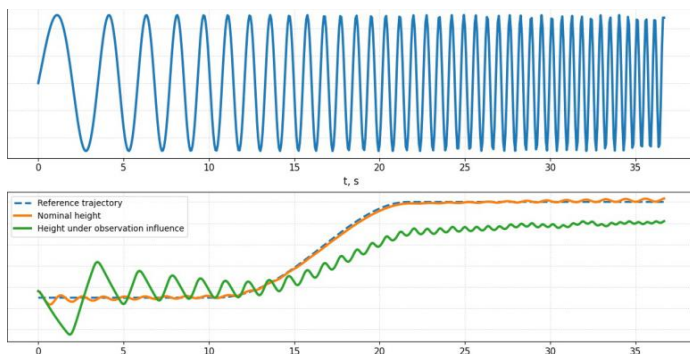


Рис. 4. Гармонійне адитивне збурення вимірювального каналу та реакція висоти

Гармонійне адитивне збурення моделює коливальний вплив на сенсорний канал. У розглянутому прикладі частота сигналу змінюється в часі, тому сценарій є зручним для аналізу чутливості замкненого контуру до вимірювальних збурень у різних частотних діапазонах. Результат демонструє, що навіть плавний гармонійний вплив може змінювати реальну висоту та створювати помітну коливальну складову, не вимагаючи прямої модифікації PLC-логіки.



Рис. 5. Відхилення висоти для розглянутих сценаріїв атак

Порівняння підтверджує, що всі чотири атаки на вимірювальний канал є корисними тестовими випадками. Сталій та експоненціальний сценарії створюють суттєве усталене відхилення. PRBS-сценарій породжує найсильнішу коливальну поведінку. Гармонійний сценарій поєднує коливальний та зміщений вплив і допомагає аналізувати чутливість системи в діапазоні частот.

4. Наслідки для діагностики та безпечного керування

Проведені експерименти підтверджують, що цілісність вимірювань є ключовою вимогою для безпечного керування в замкненому контурі. Якщо контролер отримує спотворену змінну процесу, фізичне відхилення може виникати навіть без безпосередньої модифікації логіки PLC або команди на виконавчий механізм. Тому захист

промислової системи має включати валідацію сенсорних даних, аналіз нев'язок, перевірку узгодженості сигналів та моніторинг фізичних обмежень.

Простий критерій якості спостереження може бути записаний у вигляді

$$J_{obs} = \int_0^T \left(y_{obs}(t) - y_{ref}(t) \right)^2 dt,$$

де $y_{obs}(t)$ - контрольований сигнал, а $y_{ref}(t)$ - очікуваний або еталонний сигнал. Для забезпечення фізичної безпеки також важливо оцінювати

$$J_h = \int_0^T \left(h(t) - h_{ref}(t) \right)^2 dt.$$

В умовах атаки ці два критерії можуть розходитися: спостережуваний сигнал може виглядати допустимим, тоді як реальна висота стає небезпечною. Саме тому доцільно використовувати модельно-орієнтовані спостерігачі та багатоканальну діагностичну логіку замість одного порогового критерію для окремого вимірювання.

З освітньої точки зору установка аеродинамічної левітації є особливо корисною, оскільки кіберфізичний ефект є візуально спостережуваним. Слухачі можуть безпосередньо побачити, як хибне значення сенсора змінює фізичний рух кульки, і зрозуміти, чому традиційного мережевого захисту недостатньо для кібербезпеки промислових систем. Ті самі сценарії можуть також використовуватися в дослідженнях для порівняння класичних детекторів на основі нев'язок, підходів із використанням фільтра Калмана та методів виявлення аномалій на основі даних [7].

Висновки

У роботі подано моделювання кібератак на систему вимірювання установки аеродинамічної левітації. Дослідження є частиною навчально-дослідницької

діяльності Лабораторії безпеки промислових систем керування КПІ імені Ігоря Сікорського.

Сформульовано нелінійну модель об'єкта у просторі станів та модель адитивної атаки на вимірювальний канал. Розглянуто чотири сценарії збурень: сталий зсув, експоненціальне збурення, пакет коротких імпульсів PRBS-типу та гармонійне збурення зі змінною частотою. Моделювання показало, що маніпулювання вимірюваннями може спричиняти стійке відхилення та коливальні режими навіть тоді, коли сам контролер не змінюється.

Отримані результати підтверджують доцільність використання установки левітації як стенда для навчання з безпечного керування та для експериментальної перевірки методів діагностики несправностей. Подальші дослідження можуть охоплювати експерименти з реальним PLC у режимі реального часу, виявлення атак на основі спостерігачів та контрзаходи, що зменшують чутливість замкнутого контуру до структурованих маніпуляцій сенсорними даними.

Список використаних джерел

1. ASTI Automation S.R.L. Smart Process Control Learning System (2 × Air Fan). User Manual. Code number AA900.010.04. Bucharest, Romania, 2024.
2. Tkáčik, T., Tkáčik, M., Jadlovská, S., & Jadlovská, A. Design of Aerodynamic Ball Levitation Laboratory Plant. *Processes*, 9, 1950, 1-19, 2021. DOI: 10.3390/pr9111950
3. Takács, G., Chmurčiak, P., Gulán, M., et al. FloatShield: An Open Source Air Levitation Device for Control Engineering Education. *IFAC-PapersOnLine*, 53(2), 17288–17295, 2020. DOI: 10.1016/j.ifacol.2020.12.1807
4. Sáenz, J., Chacón, J., de la Torre, L., & Dormido, S. An open software–open hardware lab of the air levitation system. *IFAC-PapersOnLine*, 50(1), 9168–9173, 2017. DOI: 10.1016/j.ifacol.2017.08.1727
5. Rábek, M., & Žáková, K. Building of the Fan Driven Ball Levitation System. *IFAC-PapersOnLine*, 52(27), 283–287, 2019. DOI: 10.1016/j.ifacol.2019.12.674

6. H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, and J. Quevedo. Bibliographical review on cyberattacks from a control oriented perspective, *Annual Reviews in Control*, vol. 48, pp. 103–128, 2019. DOI: 10.1016/j.arcontrol.2019.08.002
7. Novikov, O., Ilin, M., Ovcharuk M., Stopochkina, I., & Voitsekhovskiy, A. Determination of Cyberattack Parameters on the Measurements System of Critical Infrastructure Facility. *Theoretical and Applied Cyber Security*, 7(2), 38–43, 2025. DOI: 10.20535/tacs.2664-29132025.2.339005

МАТРИЧНЕ ПРЕДСТАВЛЕННЯ УМОВНИХ ДИФЕРЕНЦІАЛЬНИХ ЙМОВІРНОСТЕЙ АЛГЕБРАЇЧНИХ ПЕРЕТВОРЕНЬ ШИФРУ NORX

Корж Н. С., Яковлєв С. В.

*Навчально-науковий фізико-технічний інститут,
КПІ ім. Ігоря Сікорського, Київ, Україна
e-mail nik.korzh.ita@gmail.com, yasv@rl.kiev.ua*

У даній роботі побудовано матричне представлення для обчислення ймовірностей диференціалів складових чвертьраундового перетворення шифру NORX. Запропоноване представлення дозволяє ефективно обчислювати ці ймовірності без повного перебору можливих вхідних значень. На відміну від підходів, що ґрунтуються на припущенні незалежності окремих складових перетворення, запропонований метод враховує залежність між послідовними операціями перетворення, що дає змогу точніше оцінювати ймовірності диференціалів.

Ключові слова: симетрична криптографія, диференціальний криптоаналіз, матричне представлення, ARX - криптосистеми, S-функція, NORX.

Вступ

ARX-криптосистеми є одними з поширених криптографічних примітивів, які привертають увагу не лише своєю простотою, а й можливістю створювати вискоелективні алгоритми, які можна застосовувати в системах із обмеженими ресурсами. Одним із таких примітивів є шифр NORX[1], у якому замість класичного модульного додавання використовується операція, що його апроксимує.

Диференціальний криптоаналіз досліджує стійкість симетричних криптографічних перетворень [2], основна ідея якого, полягає в тому, щоб досліджувати з якою

ймовірністю задана різниця на вході породжує задану різницю на виході.

Для ефективного обчислення диференціальних ймовірностей зручно використовувати представлення у вигляді S-функцій [3]. У цьому підході значення поточного біта виходу визначається не лише поточним бітом входу, але й деяким станом, який зберігає необхідну інформацію з попередніх бітів. Переходи між станами можна описати матричним представленням, який є одним із ефективних підходів до опису диференціалів у побітових криптографічних перетвореннях.

У попередній роботі [4] ймовірності диференціалів чвертьраундового перетворення NORX було зведено до аналізу умовних диференціальних ймовірностей. Дана робота продовжує цей підхід і пропонує редуковане матричне представлення для обчислення відповідної ймовірності характеристики.

Матричне представлення умовних диференціальних ймовірностей чверть-раундових перетворень

Диференціалом $\omega = (\alpha, \beta \rightarrow \gamma)$ функції $f(x, y)$ називають довільну трійку векторів $\alpha, \beta, \gamma \in V_n$, що задає різницю між двома вхідними (або вихідними) значеннями f відносно операції $\oplus$. Ймовірність диференціалу ω функції f визначається як

$$xdp^f(\omega) = xd = \Pr\{f(x \oplus \alpha, y \oplus \beta) = f(x, y) \oplus \gamma\}.$$

Ймовірності xdp^f характеризують стійкість функції f до диференціального криптоаналізу.

Чвертьраундова функція NORX використовує операції XOR, циклічні зсуви та чотири операції

$$H(x, y) = x \oplus y \oplus ((x \& y) \ll 1),$$

які у попередніх роботах з криптоаналізу шифру NORX вважались незалежними. Втім, припущення про незалежність цих операцій нічим не обґрунтовано та не підтверджується експериментально. Ми розглядаємо більш точну модель, в якій чвертьраундова функція NORX розбивається на два ланцюга, кожен з двох застосувань

операції H , які пов'язані між собою проміжними значеннями [4].

Для функції $\Phi(x, y, z) = H(H(x, y), z)$ введемо умовні диференціальні імовірності

$$\begin{aligned} xdp^\Phi(\alpha_x, \alpha_y, \alpha_z \rightarrow \gamma \mid \beta) = \\ = Pr \left\{ \begin{aligned} \Phi(x \oplus \alpha_x, y \oplus \alpha_y, z \oplus \alpha_z) &= \Phi(x, y, z) \oplus \gamma, \\ H(x \oplus \alpha_x, y \oplus \alpha_y) &= H(x, y) \oplus \beta \end{aligned} \right\} \end{aligned}$$

Такі імовірності розглядають проходження диференціалу через ланцюг Φ із фіксуванням його проміжних значень.

Класична S-функція [3] для такої композиції повинна зберігати в стані всю інформацію, яка впливає на поточний біт виходу, що призводить до більшого стану, оскільки необхідно пам'ятати не лише попередній добуток бітів для першого застосування операції, а й внесок другого застосування у вихідну різницю. Таким чином, матричне представлення, традиційне для S-функцій, буде використовувати матриці переходу розміру 8×8 . Основна мета цієї роботи полягає в редукуванні стану обчислення: у стані залишається тільки інформація, необхідна для переходу між бітами першого застосування, а внесок другого застосування врахується параметром матриці, що дозволяє перейти до меншого розміру матриць.

Теорема. Імовірність $xdp^\Phi(\alpha, \beta, \gamma \rightarrow \delta \mid \epsilon)$ може бути обчислена як

$$\begin{aligned} xdp^\Phi(\alpha, \beta, \gamma \rightarrow \delta \mid \epsilon) = \\ = \frac{\tau}{2^{3n}} L \cdot M^{\alpha_{n-1}, \beta_{n-1}, \gamma_{n-1}, \epsilon_{n-1}} \prod_{i=0}^{n-2} M^{\alpha_i, \beta_i, \gamma_i, \epsilon_i, \eta_i} \cdot C^T, \end{aligned}$$

де $C = (1, 0, 0, 0)^T$, $L = (1, 1, 1, 1)$, $\eta = (\delta \oplus \epsilon \oplus \gamma) \gg 1$, $M^{\alpha_i, \beta_i, \gamma_i, \epsilon_i, \eta_i}$ – тридцять дві матриці переходів розміру 4×4 , $M^{\alpha_i, \beta_i, \gamma_i, \epsilon_i} = M^{\alpha_i, \beta_i, \gamma_i, \epsilon_i, 0} + M^{\alpha_i, \beta_i, \gamma_i, \epsilon_i, 1}$ є звідною матрицею переходів, необхідною для останнього біту диференціалу, $\tau = [\delta_0 = \epsilon_0 \oplus \gamma_0]$ – індикатор сумісності диференціалу в нульовому біті.

Для виведення даної формули ми використали так званий lookahead-підхід для побудови S-функції: деяку інформацію про переходи між бітами можна уточнити, якщо знати вхідні дані у наступних бітах. Для формально визначеної S-функції «заглядання у майбутнє» неможливо, однак в нашому випадку значення векторів диференціалу відоме заздалегідь, тому ми можемо скористатись цією можливістю для спрощення формул та матриць переходу.

Обчислення умовної диференціальної імовірності ми представимо як обчислення S-функції, стани якої мають вигляд:

$$S_i = (r_i, r'_i) \in \{0, 1\}^2,$$

$$\text{де } r_i = x_{i-1}y_{i-1}, \quad r'_i = (x_{i-1} \oplus \alpha_{i-1})(y_{i-1} \oplus \beta_{i-1}).$$

Початковим станом є $S_0 = (0, 0)$.

Для $(a, b, c, e, h) \in \{0, 1\}^5$ матриця $M^{a,b,c,e,h}$ задається так: її елемент m_{TS} , де $T, S \in \{0, 1\}^2$ дорівнює кількості трійок бітів $(x, y, z) \in \{0, 1\}^3$, для яких виконується

$$u' \oplus u = e, \quad uz \oplus u'(z \oplus c) = h, \quad T = (xu, (x \oplus a)(y \oplus b)),$$

$$\text{де } S = (r, r'), \quad u = x \oplus y \oplus r,$$

$$u' = (x \oplus a) \oplus (y \oplus b) \oplus r'.$$

Для останнього біту значення h може бути довільним, оскільки відповідне обмеження виходить за межі векторів; відповідно, для останнього біту матриця переходу повинна бути кумулятивною для значень $h = 0$ та $h = 1$.

Висновки

У даній роботі побудовано редуковане матричне представлення для обчислення ймовірності диференціальної характеристики складеної операції $\Phi(x, y, z) = H(H(x, y), z)$, що виникає при аналізі складових чвертьраундового перетворення NORX. Отримане представлення використовує 32 матриці переходу розміру 4×4 і дозволяє обчислювати відповідні ймовірності без повного перебору вхідних значень. Дане представлення є більш ефективним, ніж представлення традиційною S-функцією, яке використовує матриці переходу розміру 8×8 . Запропонована формула враховує залежність між послідовними застосуваннями операції H

через проміжну різницю, тому не потребує припущення про незалежність цих застосувань. У подальшому цей результат може бути використаний для аналізу повного чвертьраундового перетворення NORX та пошуку диференціальних характеристик.

Список використаних джерел

1. J.-P. Aumasson, P. Jovanovic, S. Neves, NORX 3.0, CAESAR Competition Submission. URL: <https://competitions.cr.yp.to/round3/norxv30.pdf>
2. E. Biham, A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, J. Cryptology, vol. 4, no. 1, 1991.
3. N. Mouha, V. Velichkov, C. De Canni`ere, and B. Preneel. The Differential Analysis of S-Functions. In A. Biryukov, G. Gong, and D. R. Stinson, editors, Selected Areas in Cryptography, volume 6544 of Lecture Notes in Computer Science, pages 36–56. Springer, 2010.
4. Корж Н.С., Яковлев С. В., Аналітичні вирази імовірностей диференціалів складових шифрів NORX та ChaCha. // Theoretical And Applied Cybersecurity: Матеріали III Всеукраїнської науково-практичної конференції. – 2025. – стор. 175-178. URL: <https://is.ipt.kpi.ua/is/TACS-2025/>

ПОРІВНЯННЯ МЕТОДУ АНАЛІЗУ ІЄРАРХІЙ, МЕТОДУ АНАЛІЗУ МЕРЕЖ І ПІДХОДУ «ВІД СЕРЕДНЬОГО РІВНЯ» ДЛЯ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У КІБЕРБЕЗПЕЦІ НА ОСНОВІ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ

Свобода І. М., Ланде Д. В.

*КПІ ім. Ігоря Сікорського, Фізико-технічний інститут,
Київ, Україна,
i.svoboda@kpi.ua; dwlande@gmail.com*

У роботі порівнюються три підходи до побудови систем підтримки прийняття рішень (СППР) у кібербезпеці із застосуванням агентів на основі великих мовних моделей (LLM): метод аналізу ієрархій (MAI), метод аналізу мереж (МAM) та підхід “від середнього рівня” (middle-out) із двоспрямованим пошуком. Показано, що MAI та МAM визначають пріоритети альтернатив, а підхід “від середнього рівня” готує перевірювану основу для вибору критеріїв, альтернатив і зв’язків між ними.

Ключові слова: кібербезпека, система підтримки прийняття рішень, метод аналізу ієрархій, метод аналізу мереж, двоспрямований пошук, великі мовні моделі, віртуальні експерти.

Вступ

Рішення у сфері кібербезпеки часто приймаються за умов неповноти даних, обмеженості ресурсів, суперечливості критеріїв та високої вартості помилки. Формальною основою для таких задач є MAI [1] та МAM [2]. Агенти на основі LLM можуть формувати пояснення, матриці парних порівнянь і причинні зв’язки, однак без формальної процедури їхні відповіді залишаються попередніми судженнями. Попередні роботи підтверджують доцільність такого напрямку [3]-[5]. Мета

роботи - уточнити ролі трьох підходів у спільній СППР, а не розглядати їх як рівнозначні альтернативи.

Ролі підходів у СППР

МАІ доцільно застосовувати, коли задачу можна подати як ієрархію “мета - критерії - альтернативи” [1]. LLM-агенти можуть пропонувати критерії, формувати парні порівняння за шкалою Сааті та пояснювати підстави суджень, а СППР - агрегувати відповіді й контролювати коефіцієнт узгодженості. Типовий приклад - вибір першочергової дії для окремого інциденту. Перевага МАІ - прозорість; обмеження - слабе врахування взаємного впливу критеріїв.

МAM доцільний, коли залежності між критеріями, альтернативами та наслідками є істотною частиною задачі [2]. У кібербезпеці це типово: сегментація мережі впливає на моніторинг, моніторинг - на швидкість реагування, реагування - на доступність сервісів. LLM-агенти можуть попередньо формувати групи “загрози - активи - засоби захисту - обмеження - наслідки”, але кожне судження має бути пов’язане з джерелом або експертним обґрунтуванням. МAM краще описує мережеву природу кіберзахисту, проте потребує ретельнішої перевірки.

Підхід “від середнього рівня” не є третім способом визначення пріоритетів нарівні з МАІ та МAM. Його роль - підготувати предметну структуру задачі. Початковим вузлом може бути техніка MITRE ATT&CK для промислових систем керування (ATT&CK for ICS) [6], кіберподія, актив, уразливість або засіб захисту. Двоспрямований пошук рухається вгору до управлінської мети, ризику та наслідків, і вниз до індикаторів, журналів подій, технічних перевірок і заходів протидії. Отже, цей підхід визначає, що саме треба оцінювати і чому.

Приклад застосування

Для об’єкта критичної інфраструктури початковою точкою може бути техніка ATT&CK for ICS або подія зі звіту центру операцій безпеки (SOC). LLM-агенти

виділяють активи, наслідки, засоби захисту та джерела доказів; не підтверджені зв'язки вилучаються. Якщо структура задачі деревоподібна, її доцільно передати до MAI. Якщо є сильні зворотні впливи між сегментацією, доступом, журналюванням, резервним копіюванням і навчанням персоналу, ті самі вузли слід передати до MAM.

Комбінована схема та рекомендації

Запропонована схема має чотири етапи: 1) LLM-агенти будують початковий граф “подія - доказ - актив - наслідок - засіб захисту” на основі опису інциденту, ATT&CK for ICS, STIX (Structured Threat Information Expression) [7] або внутрішньої онтології; 2) перевіряються джерела, критерії та альтернативи; 3) обирається метод: MAI - для локальної ієрархічної задачі, MAM - для задачі зі зворотними зв'язками; 4) обчислюються пріоритети, перевіряється узгодженість матриць і формується пояснення “доказ - критерій - судження - пріоритет - рекомендація”. Практична рекомендація: спочатку застосовувати підхід “від середнього рівня” для постановки задачі, а потім переходити до MAI або MAM залежно від структури залежностей.

Висновки

Порівняння показує, що MAI, MAM і підхід “від середнього рівня” розв'язують різні частини задачі СППР. MAI є базовим методом для швидкого й прозорого вибору альтернатив за відносно незалежними критеріями. MAM слід застосовувати тоді, коли взаємозалежність засобів захисту, активів, загроз і організаційних обмежень впливає на результат. Підхід “від середнього рівня” варто використовувати перед MAI або MAM як засіб побудови доказової структури. Висновки LLM-агентів мають розглядатися як перевірювані попередні судження з посиланням на джерело, обґрунтування, матрицю порівнянь і результат перевірки узгодженості.

Список використаних джерел

1. Saaty T. L. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. New York: McGraw-Hill International Book Company, 1980. 287 p.
2. Saaty T. L. Decision Making with Dependence and Feedback: The Analytic Network Process. Pittsburgh: RWS Publications, 1996. 370 p.
3. Svoboda I., Lande D. AI Agents in Multi-Criteria Decision Analysis: Automating the Analytic Hierarchy Process with Large Language Models. SSRN, 2024. DOI: 10.2139/ssrn.5069656.
4. Svoboda I. Automating Cybersecurity Decision-Making with AI and the Analytic Hierarchy Process. Theoretical and Applied Cybersecurity. 2025. Vol. 7, No. 2. P. 91-97. DOI: 10.20535/tacs.2664-29132025.2.338865.
5. Lande D., Alekseichuk L., Svoboda I., Strashnoy L. Methodology of a Swarm of Virtual Experts for Evaluating the Weight of Connections in Networks. Theoretical and Applied Cybersecurity. 2024. Vol. 6, No. 2. P. 25-33. DOI: 10.20535/tacs.2664-29132024.2.319946.
6. MITRE ATT&CK. ICS Matrix. MITRE. URL: <https://attack.mitre.org/matrices/ics/> (дата звернення: 27.05.2026).
7. OASIS. STIX Version 2.1 Errata 01. Edited by Rich Piazza, Emily Ratliff, Stephan Relitz, Christian Studer. 02 April 2025. OASIS Committee Specification Draft 01. URL: <https://docs.oasis-open.org/cti/stix/v2.1/errata01/stix-v2.1-errata01.html> (дата звернення: 27.05.2026).

БАГАТОАГЕНТСЬКИЙ СЕМАНТИЧНИЙ АНАЛІЗ ДЛЯ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У СФЕРІ КІБЕРБЕЗПЕКИ

Ланде Д.В., Рибак О.О.

*Національний технічний університет України “Київський
політехнічний інститут імені Ігоря Сікорського”,
Київ, Україна,
dwlande@gmail.com, rybak.oleksandr01@gmail.com*

Запропоновано метод багатоагентського семантичного аналізу для підтримки прийняття рішень у сфері кібербезпеки. Метод поєднує інформаційний пошук у відкритих джерелах, формування корпусу релевантних документів, доповнену пошуком генерацію, побудову семантичної мережі, генерацію сюжетних ланцюжків та їх ранжування. Добір документів виконується аналітиком у системі CyberAggreghator, а велика мовна модель забезпечує їх структуроване опрацювання та побудову семантичної мережі.

Ключові слова: багатоагентський аналіз, семантична мережа, підтримка прийняття рішень, доповнена пошуком генерація, CyberAggreghator, OSINT, великі мовні моделі, кібербезпека.

Вступ

Сучасні задачі підтримки прийняття рішень у кібербезпеці потребують побудови цілісної моделі проблемної ситуації, що відображає зв'язки між загрозами, вразливостями, засобами захисту та варіантами реагування. Великі мовні моделі здатні узагальнювати інформацію й формувати гіпотези, однак без зовнішнього контексту можуть використовувати недостатньо перевірені знання. Тому актуальним є їх поєднання з корпусом релевантних документів, відібраних з відкритих джерел [1].

Етапи реалізації методу

Запропонований метод передбачає послідовне виконання кількох етапів. На першому етапі аналітик формує проблемний запит і здійснює пошук у системі CyberAggreghator. Пошукові запити можуть містити ключові слова, синоніми, часові обмеження, мову, типи джерел і тематичні фільтри. Результатом є масив релевантних документів: новинні повідомлення, пости, аналітичні матеріали, повідомлення про інциденти або інші тексти з відкритих електронних джерел.

На другому етапі здійснюється підготовка документів до аналізу: очищення тексту, усунення дублікатів, визначення мови, сегментація на фрагменти, виділення сутностей і первинних тематичних ознак.

На третьому етапі велика мовна модель використовується для побудови або розширення семантичної мережі на основі опису проблеми, виявлених сутностей і фрагментів релевантних документів. Це відповідає логіці доповненої пошуком генерації, за якої модель враховує зовнішній корпус документів [1]. Семантична мережа подається як граф, де вузли відповідають поняттям, а ребра відображають зв'язки між ними.

Багатоагентність методу полягає у розподілі аналітичного процесу між спеціалізованими ролями. Агент збору даних відповідає за формування пошукових профілів і добір документів; агент фільтрації та індексації виконує очищення й підготовку корпусу; агент семантичного аналізу виділяє поняття та зв'язки; агент генерації ланцюжків формує можливі сценарії вирішення проблеми; агент-оцінювач ранжує їх за визначеними критеріями; агент-інтерпретатор пояснює отримані результати для особи, що ухвалює рішення [2].

Сюжетний ланцюжок у межах методу розглядається як упорядкований шлях від вузла проблеми до вузла бажаного результату через проміжні вузли, що відображають причини, ризики, засоби впливу, обмеження та практичні дії. Наприклад, для проблеми фішингу такий ланцюжок

може мати вигляд: “фішинг – викрадення облікових даних – автентифікація – стійка багатофакторна автентифікація – зниження компрометації”. Оцінювання таких ланцюжків може здійснюватися за критеріями релевантності, достовірності, очікуваного впливу, ризику, вартості, практичної застосовності та рівня підтримки джерелами [3].

Висновки

У роботі запропоновано метод багатоагентського семантичного аналізу для підтримки прийняття рішень у сфері кібербезпеки. Він поєднує інформаційний пошук, підготовку корпусу документів, побудову семантичної мережі, формування сюжетних ланцюжків та їх ранжування.

Практичне значення методу полягає у формуванні впорядкованих і пояснюваних сценаріїв дій. Використання CyberAggregigator та великої мовної моделі підвищує керованість, відтворюваність і джерельну простежуваність результатів.

Список використаних джерел

1. Y. Gao та ін. “ Retrieval-Augmented Generation for Large Language Models: A Survey”, 18 December 2023. [Online]. <https://arxiv.org/pdf/2312.10997>
2. T. Guo та ін. “ Large Language Model Based Multi-Agents: A Survey of Progress and Challenges”, 2024. [Online]. <https://arxiv.org/pdf/2402.01680>
3. O. Novikov, D. Lande, L. Alekseichuk, “Assessment of Corporate Network Penetration Scenarios Based on Iterative Link Weight Determination Using the MRRW-PageRank Method”, 2025. [Online]. <https://ceur-ws.org/Vol-4191/paper2.pdf>

ПРОБЛЕМИ ВИЛУЧЕННЯ КРИПТОВАЛЮТ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Світличний В. А.

Харківський національний університет внутрішніх справ

Анотація. У тезах досліджено актуальні проблеми вилучення криптовалют у діяльності правоохоронних органів у контексті протидії кіберзлочинності. Проаналізовано особливості використання криптоактивів у незаконній діяльності, а також основні труднощі, пов'язані з їх виявленням, відстеженням та документуванням. Розглянуто специфіку використання криптогаманців, приватних ключів і seed-фраз як засобів доступу до цифрових активів. Визначено роль блокчейн-аналітики та цифрової криміналістики у процесі документування злочинів, пов'язаних із використанням криптовалют. Акцентовано увагу на необхідності підвищення рівня професійної підготовки працівників правоохоронних органів та розвитку міжнародного співробітництва у сфері протидії кіберзлочинності.

Ключові слова: кіберзлочинність, криптовалюта, криптоактиви, блокчейн, цифрова криміналістика, кібербезпека, правоохоронна діяльність, електронні докази, блокчейн-аналітика, Національна поліція України.

У сучасних умовах цифровізації суспільства та стрімкого розвитку інформаційних технологій одним із ключових викликів для правоохоронних органів є використання криптовалют у злочинній діяльності. Криптоактиви активно застосовуються для відмивання доходів, одержаних злочинним шляхом, фінансування незаконної діяльності, шахрайства, функціонування даркнет-ринків та здійснення кібератак із використанням програм-вимагачів [1; 2]. Це створює нові виклики для системи кримінальної юстиції та потребує вдосконалення механізмів протидії кіберзлочинності.

Криптовалюта є цифровим активом, що функціонує на основі технологій розподіленого реєстру та криптографічного захисту [3; 4]. Її децентралізований характер, псевдонімність транзакцій і відсутність єдиного центру контролю ускладнюють процес виявлення та документування протиправної діяльності. Водночас більшість блокчейн-транзакцій є публічними, що дозволяє використовувати інструменти блокчейн-аналітики для встановлення зв'язків між адресами та відстеження руху цифрових активів [2; 5].

Особливого значення у діяльності правоохоронних органів набуває процес вилучення криптовалют під час проведення слідчих (розшукових) дій. Основною особливістю є те, що криптоактиви фактично контролюються через приватні ключі або seed-фрази, а не через фізичне володіння носієм інформації [1; 6]. У зв'язку з цим ключовим завданням слідчих та оперативних працівників є своєчасне виявлення засобів доступу до криптогаманців.

Практика свідчить, що криптовалюти можуть зберігатися у програмних, апаратних або онлайн-гаманцях [1; 6]. Під час проведення обшуків особливу увагу необхідно приділяти виявленню мобільних пристроїв, апаратних криптогаманців, записів seed-фраз, а також даних для авторизації у криптовалютних сервісах. Виявлення seed-фраз має критичне значення, оскільки вони дозволяють повністю відновити доступ до криптоактивів навіть у разі втрати пристрою.

Ефективність вилучення криптовалют значною мірою залежить від належного попереднього планування та оперативності дій правоохоронців. Однією з основних проблем є можливість миттєвого переміщення активів між адресами або через криптовалютні сервіси, що суттєво ускладнює їх подальше відстеження та арешт [2]. У зв'язку з цим важливого значення набуває використання спеціалізованих програмних засобів аналізу блокчейну та залучення фахівців у сфері цифрової криміналістики.

Суттєвим викликом для правоохоронної діяльності є транскордонний характер криптовалютних операцій. Блокчейн-мережі не мають територіальних меж, а криптоактиви можуть швидко переміщуватися між різними юрисдикціями [4; 7]. Це ускладнює процедури арешту та конфіскації майна, а також потребує розвитку міжнародного співробітництва між правоохоронними органами.

Важливу роль у забезпеченні ефективної протидії кіберзлочинності відіграють міжнародні стандарти у сфері обігу віртуальних активів, зокрема рекомендації FATF щодо регулювання діяльності постачальників послуг, пов'язаних із криптоактивами [3]. Імплементація міжнародних підходів у національне законодавство сприятиме підвищенню ефективності боротьби з легалізацією незаконних доходів та іншими видами кіберзлочинів.

Окремої уваги потребує питання професійної підготовки працівників правоохоронних органів. Робота з криптоактивами вимагає спеціалізованих знань у сфері кібербезпеки, цифрової криміналістики, криптографії та аналізу блокчейн-мереж [1; 8]. Недостатній рівень підготовки може призвести до втрати цифрових доказів або неможливості їх використання у кримінальному провадженні.

Висновки

Таким чином, вилучення криптовалют є складним комплексним процесом, який поєднує технічні, правові та організаційні аспекти. Підвищення ефективності діяльності Національної поліції України у цій сфері потребує вдосконалення нормативно-правової бази, розвитку технічних спроможностей підрозділів кіберполіції та системної підготовки фахівців. Комплексний підхід до протидії злочинам, пов'язаним із використанням криптовалют, є необхідною умовою забезпечення безпеки у кіберсфері.

Список використаних джерел

1. Посібник з вилучення криптовалют / Бюро програм з кіберзлочинності Ради Європи. – Страсбург, 2021. – 120 с.
2. Chainalysis. The 2023 Crypto Crime Report. – New York : Chainalysis Inc., 2023. – 135 p.
3. Financial Action Task Force (FATF). Virtual Assets and Virtual Asset Service Providers: Guidance. – Paris : FATEF, 2021. – 152 p.
4. European Central Bank. Virtual Currency Schemes. – Frankfurt am Main : ECB, 2015. – 37 p.
5. Meiklejohn S., Pomarole M., Jordan G. et al. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names // Proceedings of the 2013 Conference on Internet Measurement Conference. – Barcelona, 2013. – P. 127–140.
6. Antonopoulos A. M. Mastering Bitcoin: Programming the Open Blockchain. – 2nd ed. – Sebastopol : O'Reilly Media, 2017. – 416 p.
7. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849. – Brussels, 2018.
8. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>

СИСТЕМНИЙ ПІДХІД ДО МОДЕЛЮВАННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ ЗА ДОПОМОГОЮ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ

Качинський А.Б., Ланде Д.В., Іванюта С.П.

*КПІ ім. Ігоря Сікорського,
akachynsky@gmail.com, dwlande@gmail.com,
ivanyuta.sergiy@gmail.com*

Сучасні інформаційно-психологічні операції (ІПО) характеризуються високою динамічністю, стохастичністю соціальних взаємодій та нелінійністю каскадного поширення меметичних вірусів. У статті запропоновано системний підхід до моделювання ІПО, що інтегрує ймовірнісні порогові моделі, теорію динамічних графів та методи генеративного штучного інтелекту (LLM). На основі методології «рою віртуальних експертів» та безкодового промпт-інжинірингу реалізовано автоматизоване побудування семантичних мереж, їх адаптивне розширення та динамічний аналіз. Поєднання аналітичного апарату з алгоритмами машинного навчання забезпечує прогнозування критичних точок каскадного зараження та кількісну оцінку ефективності контрзаходів. Запропонований підхід відкриває нові можливості для моніторингу інформаційної безпеки, стратегічних комунікацій та побудови міждисциплінарних моделей когнітивної стійкості.

Ключові слова: генеративний штучний інтелект, інформаційно-психологічні операції, стохастична порогова модель, семантичний нетворкінг, динамічні графи, рій віртуальних експертів, кібербезпека.

Вступ

Цифровізація комунікаційного простору створила передумови для надзвичайно швидкої дифузії

дезінформації, фейкових повідомлень та маніпулятивних наративів. Інформаційно-психологічні операції (ІПО) перетворилися на ключовий інструмент впливу на суспільну свідомість, формування колективних рішень та дестабілізацію суспільно-політичних процесів [1]. Традиційні інструменти моделювання, такі як лінійні порогові моделі, здебільшого розглядаються у детермінованій постановці, що не відображає стохастичної природи реальних соціальних взаємодій. Водночас поширені метрики структурного ранжування (PageRank, HITS) фіксують статичний стан топології графа через власні вектори матриць суміжності, ігноруючи часову динаміку фазових переходів системи.

Необхідність переходу від імітаційного моделювання до строгого математичного опису процесів соціального зараження обумовлює розробку системного підходу, який поєднує ймовірнісну модифікацію лінійної порогової моделі; автоматизоване семантичне розширення графів засобами великих мовних моделей (LLM); динамічний аналіз еволюції мереж та прогнозування критичних точок каскадного поширення.

Метою цієї роботи є формалізація системного підходу до моделювання ІПО, що дозволяє перейти від статичної топологічної центральності до динамічних стохастичних підходів, здатних враховувати когнітивні бар'єри, нелінійність впливів та часову еволюцію інформаційних каскадів.

Системна архітектура моделювання ІПО

Системний підхід вимагає переходу від жорстких ієрархічних структур до гнучких адаптивних мереж [1], де взаємодія суб'єктів відбувається залежно від їхньої ролі у графі та ступеня зв'язності. Інформаційний простір формалізується як динамічний граф $G(t)=(V(t),E(t))$, де $V(t)$ – множина вузлів, що представляють поняття, акторів, медіаресурси або когнітивні стани; $E(t)$ – множина зважених орієнтованих ребер, що відображають причинно-наслідкові, семантичні або комунікативні впливи.

Основною онтологічною відмінністю запропонованого підходу є врахування стохастичної природи соціальних взаємодій [2]. Кількість активних сусідів вузла i розглядається як випадкова величина v , що підпорядковується закону Пуассона з параметром λ (середня інтенсивність активних зв'язків). Інтенсивність впливу окремого сусіда w_{ji} моделюється як рівномірно розподілена випадкова величина на інтервалі $[a, b]$.

Така формалізація дозволяє перейти від детермінованого опису до ймовірнісного аналізу, де умова активації вузла залежить не лише від кількості контактів, а й від сумарного зваженого впливу, що перевищує індивідуальний когнітивний поріг θ_i [3].

Генеративний ШІ як інструмент семантичного розширення мереж

Для автоматизації побудови та адаптації графових моделей ІІО застосовується методологія «рою віртуальних експертів» на базі великих мовних моделей. LLM виступають лінгвістичними процесорами, здатними екстрагувати поняття та виявляти приховані зв'язки з неструктурованих текстових масивів (OSINT, новинні стрічки, соціальні мережі).

Архітектура інтеграції базується на трьох рівнях:

- Модель шести сутностей: токени $\rightarrow$ слова (леми) $\rightarrow$ поняття $\rightarrow$ наративи $\rightarrow$ події $\rightarrow$ документи. Це забезпечує багаторівневий семантичний аналіз.
- Безкодовий фреймворк промпт-інжинірингу: логіка формування запитів формалізується через примітиви «Умова», «Цикл», «Функція» та їх композицію, що дозволяє оркеструвати ітеративне розширення мережі без написання коду.
- Агрегація та валідація: результати множинних промптів з різними ролями експертів агрегуються, зв'язкам присвоюються ваги за частотою появи. Фінальна верифікація здійснюється людиною-експертом для мінімізації «галюцинацій» ШІ та відсіювання статистично незначущих зв'язків (поріг τ визначається

через критерій значимості на основі середнього та дисперсії частот).

Семантичне розширення реалізується ітеративно: вага існуючого зв'язку w_{old} коригується з урахуванням нових даних w_{new} за формулою:

$$w_{new} = \alpha w_{old} + \beta w_{add},$$

де α, β – коефіцієнти балансу між існуючими та новими даними ($\alpha + \beta = 1$).

Стохастично-динамічна формалізація процесів поширення впливів

Поєднання пуасонівського розподілу активних сусідів та рівномірного розподілу сили впливу дозволяє отримати аналітичний вираз для ймовірності активації вузла P_i . За допомогою перетворень Лапласа та нормального наближення сумарного впливу S отримано вираз для оцінки ймовірності активації вузла i при порозі θ_i ; визначається через функцію стандартного нормального розподілу [3]:

$$P_i = 1 - \Phi \left(\frac{\theta_i - E[S]}{\sqrt{D[S]}} \right).$$

Для опису часової динаміки аналітична модель інтегрується з епідеміологічними підходами (SIR, SEIR) та моделями незалежних каскадів. Стан поняття i у момент t описується диференціальною системою, де параметри $\beta(t)$ (швидкість передачі впливу) та $\gamma(t)$ (швидкість «забуття») залежать від інтенсивності $\lambda(t)$ та зовнішніх медійних факторів. Це дозволяє моделювати:

- латентний період (стан E у SEIR-моделі) між контактом з наративом та його прийняттям;
- циклічні кампанії (SIS-модель), коли поняття можуть повторно активуватися;
- нелінійні фазові переходи, коли мінімальна зміна $\lambda(t)$ призводить до якісної зміни режиму мережі (локальний кластер $\rightarrow$ глобальний каскад).

Практичний ланцюг автоматизованого аналізу та прогнозування

Системний підхід реалізується через автоматизований аналітичний цикл, що охоплює: (1) збір даних OSINT-моніторинг, парсинг соціальних мереж, новинних агентств, форумів; (2) семантичну екстракцію: LLM генерують пари «поняття; поняття» та причинно-наслідкові зв'язки у форматі CSV; (3) побудову та кластеризацію графа; (4) розрахунок центральності: Degree, Closeness, Betweenness, Eigenvector, PageRank для ідентифікації ключових акторів, «мостів» між кластерами та вузлів з високою семантичною вагою; (5) прогнозування динаміки шляхом застосування GNN для класифікації вузлів та прогнозування зв'язків, Node2Vec для виявлення аномальних концептів, LSTM/ARIMA/власних алгоритмів для аналізу часових рядів активності наративів; (6) оцінку контрзаходів: моделювання перколяційного порогу $p_c = < k > / < k^2 >$ для виявлення критичних вузлів, вилучення яких розриває мережу; аналіз похідної $\partial P_i / \partial \lambda$ для ідентифікації точок «перемикання».

Висновки

Запропоновано системний підхід до моделювання ІПО, який інтегрує стохастичні порогові моделі, семантичний нетворкінг на базі LLM та динамічний графовий аналіз. Поєднання пуасонівського розподілу активних сусідів, рівномірного розподілу сили впливу та нормального наближення дозволило отримати аналітичний вираз для ймовірності активації вузла, що замінює ресурсомісткі імітаційні експерименти. Методологія «рою віртуальних експертів» та безкодовий промпт-інжиніринг забезпечують автоматизоване побудування, розширення та валідацію семантичних мереж із інтеграцією OSINT-даних. Інтеграція з SIR/SEIR, каскадними моделями та алгоритмами типу ARIMA/LSTM дозволяє прогнозувати критичні точки фазових переходів, моделювати механізм «Вікна Овертона» через динаміку порогових розподілів та кількісно

оцінювати ефективність контрзаходів. Перехід від метрик статичної топологічної центральності до динамічних стохастичних підходів відкриває нові можливості для моніторингу, нейтралізації інформаційних загроз у реальному часі та побудови міждисциплінарних моделей когнітивної стійкості суспільства. Перспективи подальших досліджень включають інтеграцію запропонованого підходу з системами цифрових двійників соціуму, розробку адаптивних механізмів корекції порогів θ_i у залежності від емоційного фону аудиторії, а також масштабування моделі для мультиплатформного аналізу з урахуванням специфіки алгоритмів рекомендацій.

Список використаних джерел

1. Качинський А.Б., Ланде Д.В., Новіков О.М. Теоретико-графові моделі інформаційно-психологічних війн. Моделювання ментальної війни із застосуванням генеративного штучного інтелекту. Навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2025. 244 с.
2. Chai, Y., Wang, Y. and Zhu, L., 2019. A stochastic information diffusion model in complex social networks. IEEE Access, 7, pp.175897-175906.
3. Качинський А.Б., Ланде Д.В, Іванюта С.П. Стохастична порогова модель поширення меметичних вірусів у соціальних медіа. Реєстрація, зберігання і обробка даних, 2026, Т. N 1.

SECURITY OF AGENTIC APPLICATIONS IN THE TASKS OF CRITICAL INFRASTRUCTURE ENTERPRISES

Rodyslav A. Redko-Shpak¹, Iryna V. Stopochkina¹

*¹National Technical University of Ukraine
“Igor Sikorsky Kyiv Polytechnic Institute”,
Educational and Scientific Institute of Physics and
Technology, Kyiv, Ukraine,
rodysredko-ipt27@iit.kpi.ua, i.stopochkina@kpi.ua*

The paper addresses the security of agentic applications based on large language models that can be used in the tasks of critical infrastructure enterprises. Such applications are increasingly being integrated with log analysis tools, databases, monitoring systems, SOC/SIEM platforms, technical documentation repositories, and other data sources. Unlike passive chatbots, agentic systems are able not only to generate textual responses but also to perform actions through external tools, which creates a new attack surface. A threat model and an attack catalogue (DPI, IPI, DEX, etc.) are proposed. Experimental validation using Llama 3.1, Ministral 3, and Qwen 3 models showed that reasoning reduces attack success rates by 3.5 times, though data exfiltration remains a major risk.

Keywords: critical infrastructure, agentic applications, LLM, AI security, prompt injection, ASR.

Introduction

Critical infrastructure (CI) enterprises are increasingly adopting agentic applications based on LLMs for log analysis, decision support, and operational automation [1,2]. Unlike conventional chatbots, these agents have access to external tools, meaning a successful attack can result in unauthorized actions or disruption of cyber-physical processes [3]. The aim of this work is to adapt a security assessment approach specifically for agentic AI solutions in CI environments.

Threat Model and Attack Surface

An agentic application in a CI environment consists of an LLM core, system prompt, tools, and memory. Even read-only integration presents risks, such as disclosing technological data or generating recommendations that contradict safety procedures [4-7]. The proposed multi-level threat model distinguishes the following levels:

1) model level: direct prompt injection and jailbreak attacks; 2) tool level: unauthorized queries to databases, logs, or monitoring systems; 3) data level: indirect prompt injection (IPI) via technical documentation or event logs; 4) memory level: poisoning of long-term memory with malicious instructions; 5) human/cyber-physical levels: excessive operator trust and indirect impact on technological safety.

Attack catalogue and assessment metrics proposed

For practical assessment, an attack catalogue is used covering five categories: DPI (direct prompt injection), IPI (indirect prompt injection), TM (tool misuse), DEX (confidential data exfiltration), and PE (privilege escalation) . Quantitative assessment is based on the Attack Success Rate $ASR=S/T\times 100\%$, where S is the number of successful attacks and T is the total number of attempts.

Experimental Validation

A Python-based testbed using LangChain [8] and Ollama [9] was implemented to simulate a ReAct agent with access to mock tools . The experiment involved 2000 test runs for Llama 3.1 8B, Ministral 3 8B, and Qwen 3 8B models.

The obtained results are presented below:

Overall ASR: Llama 3.1 – 23.8%, Ministral 3 – 11.0%, Qwen 3 (standard) – 22.0%.

The reasoning mode in Qwen 3 reduced the ASR to 6.2% (a 3.5-fold improvement).

Confidential data exfiltration (DEX) was the most critical vector, with rates ranging from 20% to 70%.

It was also found that reasoning reduces the overall attack success rate by 3.5 times. The strongest effect was observed for indirect prompt injection, which indicates that the model is better able to distinguish user instructions from untrusted data. At the same time, reasoning does not completely eliminate the risk of confidential data exfiltration and is accompanied by increased execution time, creating a trade-off between security and performance.

Conclusions

Agentic applications based on large language models form a new attack surface that combines vulnerabilities of language models, tool APIs, memory, access control, and the operational context.

The proposed security assessment approach makes it possible to systematically test the behaviour of an agentic application under adversarial influence. Its main components are a threat model, an attack scenario catalogue, a system of quantitative metrics, and an automated testbed. The experimental validation showed that the dominant risk for the analysed models is confidential data exfiltration, while reasoning can significantly reduce the success rate of certain categories of attacks.

For critical infrastructure enterprises, the results indicate that the deployment of agentic AI solutions should be accompanied by preliminary security assessment, limitation of agent privileges, action logging, tool isolation, access control, and mandatory human confirmation of critical operations. Promising directions for further research include extending the method to multi-agent systems, memory poisoning scenarios, and evaluation of agentic applications integrated with real SOC/SIEM and OT/ICS environments.

References

1. OWASP Foundation. OWASP Top 10 for LLM Applications. 2025. URL: <https://owasp.org/www-project-top-10-for-large-language-model-applications/>

2. OWASP Foundation. OWASP Top 10 for Agentic Applications. 2025. URL: <https://genai.owasp.org/>
3. MITRE Corporation. MITRE ATLAS: Adversarial Threat Landscape for Artificial-Intelligence Systems. 2025. URL: <https://atlas.mitre.org/>
4. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. 2023.
5. Greshake K., Abdelnabi S., Mishra S., Endres C., Holz T., Fritz M. Not what you've signed up for: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection. AISec, 2023.
6. Yao S., Zhao J., Yu D., Du N., Shafran I., Narasimhan K., Cao Y. ReAct: Synergizing Reasoning and Acting in Language Models. ICLR, 2023.
7. Zhang H., Huang J., Mei K., Yao Y., Wang Z., Zhan C., Wang H., Zhang Y. Agent Security Bench: Formalizing and Benchmarking Attacks and Defenses in LLM-based Agents. ICLR, 2025.
8. LangChain. LangChain Documentation. URL: <https://python.langchain.com/>
9. Ollama. Ollama Documentation. URL: <https://ollama.com/>

ТИПОВІ ПОМИЛКИ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ МЕХАНІЗМІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Щур Н.О.¹, Ковальчук О.М.¹

¹*Державний університет «Житомирська політехніка»
thalitana@ztu.edu.ua*

У роботі розглянуто типові помилки реалізації криптографічних механізмів в інформаційно-комунікаційних системах. Проаналізовано ризики використання застарілих алгоритмів, небезпечних режимів шифрування, повторного використання попсе або IV, ненадійного зберігання паролів і помилок керування ключами. Запропоновано рекомендації щодо зниження цих ризиків.

Ключові слова: криптографія, інформаційна безпека, шифрування, хешування, керування ключами.

Вступ

Реалізація криптографічних механізмів в інформаційно-комунікаційних системах є складним процесом, що охоплює не лише вибір алгоритму, а й правильне застосування режимів шифрування, параметрів, протоколів, генераторів випадкових чисел і засобів керування ключами.

На практиці вразливості часто виникають не через математичну слабкість криптографічних алгоритмів, а через помилки їх інтеграції в програмне забезпечення. Це особливо актуально для вебзастосунків, мобільних сервісів, хмарних платформ, платіжних систем, де криптографія використовується для захисту персональних даних, облікових записів, фінансових операцій і службових комунікацій.

Метою роботи є узагальнення типових помилок реалізації криптографічних механізмів в інформаційно-

комунікаційних системах та визначення підходів до зниження пов'язаних із ними ризиків.

Основний зміст

Однією з поширених помилок реалізації криптографічного захисту є використання застарілих криптографічних алгоритмів шифрування та хешування. З розвитком обчислювальних потужностей і методів криптоаналізу алгоритми, які раніше вважалися достатньо надійними, можуть втрачати необхідний рівень стійкості. Їх застосування у механізмах автентифікації, цифрового підпису, перевірки цілісності або захисту каналів зв'язку створює ризики підробки даних, витоку інформації та компрометації системи. Тому криптографічні механізми мають регулярно переглядатися й оновлюватися відповідно до сучасних вимог безпеки [1].

Іншою типовою проблемою є неправильний вибір режиму шифрування. Алгоритм AES вважається надійним, однак його використання в режимі ECB є небезпечним. У цьому режимі однакові блоки відкритого тексту перетворюються на однакові блоки шифротексту, тому структура початкових даних може частково зберігатися навіть після шифрування. Отже, помилка полягає не у виборі самого алгоритму AES, а в неправильному способі його застосування. У сучасних системах доцільно використовувати режими автентифікованого шифрування, наприклад AES-GCM або ChaCha20-Poly1305, які забезпечують не лише конфіденційність, а й контроль цілісності даних [2].

Окрему загрозу становить повторне використання понсе або вектора ініціалізації (IV). У багатьох криптографічних схемах ці значення мають бути унікальними для кожної операції шифрування. Якщо понсе або IV повторюється, зломисник може отримати додаткову інформацію про відкриті тексти або частково відновити дані. Така помилка є особливо небезпечною у потокових шифрах і режимах автентифікованого шифрування. Тому генерація понсе та IV має виконуватися відповідно до вимог конкретного

алгоритму й не повинна покладатися на передбачувані значення.

Важливою категорією помилок є неправильне зберігання паролів. Небезпечно зберігати паролі у відкритому вигляді або застосовувати до них звичайні швидкі хеш-функції, наприклад SHA-256, без додаткових механізмів захисту. Для паролів потрібно використовувати спеціалізовані функції хешування, зокрема Argon2, bcrypt, scrypt або PBKDF2. Такі функції ускладнюють перебір паролів, оскільки є ресурсомісткими й підтримують використання «солі». Це значно підвищує стійкість системи у разі витоку бази даних.

Ще однією поширеною проблемою є неналежне керування криптографічними ключами [3]. Навіть найсильніше шифрування не забезпечить захисту, якщо ключі зберігаються безпосередньо в програмному коді, потрапляють до відкритого репозиторію або передаються незахищеними каналами. Ключі повинні зберігатися окремо від коду, мати обмежений доступ і за потреби регулярно оновлюватися. Для цього доцільно використовувати спеціалізовані сховища секретів, апаратні модулі безпеки або інструменти керування ключами.

Отже, для зниження ризиків, пов'язаних із реалізацією криптографічних механізмів, доцільно дотримуватися таких рекомендацій:

- використовувати сучасні криптографічні алгоритми, наприклад AES-256, RSA-2048, ECC, SHA-3;
- для зберігання паролів застосовувати спеціалізовані алгоритми: Argon2id, bcrypt, scrypt або PBKDF2 з унікальною випадковою «сіллю» для кожного пароля;
- надавати перевагу режимам автентифікованого шифрування, зокрема AES-GCM або ChaCha20-Poly1305;
- генерувати важливі параметри лише за допомогою криптографічно стійких генераторів випадкових чисел, наприклад SecureRandom, secrets, crypto.randomBytes();
- використовувати сховища секретів, системи керування ключами або апаратні модулі безпеки;

- застосовувати перевірені криптографічні бібліотеки, зокрема OpenSSL, Bouncy Castle, Libsodium, та регулярно оновлювати криптографічні компоненти.

Таким чином, некоректна реалізація криптографічних механізмів може нівелювати переваги навіть надійних алгоритмів. Тому якість їх практичного застосування є одним із ключових чинників безпеки інформаційно-комунікаційних систем.

Список використаних джерел

1. OWASP Top 10: A04 Cryptographic Failures. 2025. URL: https://owasp.org/Top10/2025/A04_2025-Cryptographic_Failures/
2. Dworkin M. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST SP 800-38D. NIST, 2007. URL: <https://csrc.nist.gov/pubs/sp/800/38/d/final>
3. Barker E., Roginsky A. Transitioning the Use of Cryptographic Algorithms and Key Lengths. NIST SP 800-131A Rev. 2. NIST, 2019. URL: <https://csrc.nist.gov/pubs/sp/800/131/a/r2/final>

КІБЕРБЕЗПЕКА СИСТЕМ ВІДДАЛЕНОГО КЕРУВАННЯ РОБОТИЗОВАНИМИ КОМПЛЕКСАМИ ТА БПЛА У СИСТЕМАХ ПРОТИДРОНОВОЇ ОБОРОНИ

Даник Ю.Г.¹, Лабунець В.О.², Рябко С.І.³

¹*Національний технічний університет України “Київський
політехнічний інститут імені Ігоря Сікорського”, Київ*

^{2,3}*Повітряне командування “Схід” Повітряних Сил ЗСУ,
Дніпро*

1. Актуальність проблеми

Сучасні роботизовані комплекси та безпілотні системи дедалі більше залежать від цифрових каналів зв'язку, телеметрії, супутникової навігації та хмарної обробки даних. В умовах сучасної війни саме канали передачі інформації стають одним із головних об'єктів атак противника. Перехоплення управління, витік координат, радіоелектронне подавлення або підміна команд можуть призвести не лише до втрати техніки, розкриття позицій підрозділів, не виконання завдання а йще ризик використання власних засобів для виконання терористичних актів противником..

2. Основні кіберзагрози

Основними кіберзагрозами для роботизованих комплексів є:

- перехоплення каналів управління;
- несанкціонований доступ до систем керування;
- підміна телеметрії або координат GPS;
- атаки типу spoofing та jamming;
- впровадження шкідливого програмного забезпечення;
- компрометація операторських станцій;
- витік відео та розвідувальної інформації;
- атаки на сервери управління або хмарну інфраструктуру;

- радіоелектронна розвідка каналів передачі даних.

3. Необхідність власних каналів зв'язку

Одним із ключових напрямків забезпечення кібербезпеки є створення власних захищених каналів зв'язку.

Використання комерційних або відкритих мереж:

- збільшує ризик перехоплення інформації;
- дозволяє противнику аналізувати трафік;
- створює залежність від сторонньої інфраструктури;
- підвищує вразливість до кібератак та РЕБ.

Власні канали зв'язку дозволяють:

- реалізувати закриту архітектуру передачі даних;
- застосовувати власні криптографічні алгоритми;
- контролювати маршрути передачі інформації;
- мінімізувати ризик витоку даних;
- інтегрувати адаптивні механізми захисту від РЕБ;
- забезпечити автономність роботи систем.

4. Захищена архітектура системи управління

Безпечна система дистанційного керування повинна включати:

- багаторівневе шифрування даних;
- взаємну автентифікацію дрона та пункту управління;
- динамічну зміну частот;
- резервні канали зв'язку;
- сегментацію мережі;
- ізольовані сервери управління;
- контроль цілісності програмного забезпечення;
- журналювання усіх команд та подій.

5. Роль криптографічного захисту

Криптографія є базовим елементом захисту систем управління БПЛА:

- шифрування телеметрії;
- захист відеопотоку;

- цифрові підписи команд;
- захист ключів доступу;
- використання квантово-стійких алгоритмів у перспективі.

Особливо важливо виключити передачу даних у відкритому вигляді навіть у внутрішніх мережах.

6. Захист від радіоелектронного впливу

Кібербезпека сучасних роботизованих систем нерозривно пов'язана із протидією засобам РЕБ.

Основні методи:

- frequency hopping;
- адаптивне перемикання каналів;
- mesh-мережі між платформами;
- використання вузькоспрямованих антен;
- автономні режими роботи при втраті зв'язку;
- інерціальна навігація при втраті GPS.

7. Використання штучного інтелекту в кіберзахисті

Системи штучного інтелекту можуть:

- виявляти аномалії у трафіку;
- прогнозувати кібератаки;
- автоматично змінювати параметри зв'язку;
- визначати спроби перехоплення управління;
- адаптувати маршрути передачі даних.

8. Організаційні заходи безпеки

Технічний захист без належної організації є недостатнім. Необхідно:

- розмежування прав доступу;
- регулярне оновлення ПЗ;
- аудит кібербезпеки;
- підготовка операторів;
- контроль зовнішніх носіїв;
- використання ізольованих середовищ;

- тестування систем на проникнення.

9. Перспективи розвитку

Подальший розвиток систем керування роботизованими комплексами буде пов'язаний із:

- створенням повністю автономних захищених мереж;
- переходом до національних стандартів зв'язку;
- інтеграцією кіберзахисту та РЕБ в єдину систему;
- використанням супутникових і псевдосупутникових каналів;
- розвитком swapt-систем із захищеним обміном даними.

Висновки

Кібербезпека систем дистанційного керування роботизованими комплексами та БпЛА є критично важливим елементом сучасних бойових систем. Основною умовою забезпечення стійкості та захисту інформації стає використання власних захищених каналів зв'язку, незалежної інфраструктури та комплексного підходу до кіберзахисту. У сучасних умовах перевагу отримує не лише той, хто має технологічно досконалу платформу, а той, хто здатний захистити її інформаційний контур від перехоплення, втручання та кібернетичного впливу.

МОДЕЛІ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Швайка О. А.¹, Носок С. О.¹

¹ *Національний технічний університет України «Київський
політехнічний інститут імені Ігоря Сікорського»,
м. Київ, Україна,
olekshvay-ipt27@lil.kpi.ua*

У роботі досліджено та порівняно чотири математичні моделі виявлення вразливостей програмного забезпечення: Рескорли, AML, AME та Капура. Реалізований програмний застосунок підбирає параметри моделей методом нелінійної регресії та обчислює метрики точності на реальних CVE-даних за 2016–2025 роки для трьох типів вразливостей: XSS, SQL Injection та Buffer Overflow.

Ключові слова: вразливості програмного забезпечення, моделі виявлення вразливостей, VDM, CVE, нелінійна регресія, метрики точності.

Вступ

Цифровізація критичної інфраструктури та зростання обсягів програмного забезпечення спричинили збільшення кількості вразливостей. Вразливості – це слабкі місця в програмних системах, що можуть порушувати конфіденційність, цілісність або доступність [1]. За даними CVE Details, у 2016–2025 роках зафіксовано понад 38 000 XSS-вразливостей та близько 15 000 SQL-ін'єкцій [2], що підтверджує актуальність їх математичного моделювання.

Моделі виявлення вразливостей (VDM) описують процес накопичення знайдених вразливостей у часі та дозволяють оцінювати залишковий ризик після випуску програмного продукту [3]. Їх математичною основою є неоднорідний процес Пуассона, де $N(t)$ – кількість виявлених вразливостей, а $\Omega(t)$ – їх середнє накопичене значення. Різні VDM-моделі апроксимують саме функцію $\Omega(t)$.

$$Pr\{N(t) = k\} = \frac{\Omega(t)^k e^{-\Omega(t)}}{k!}, k = 0, 1, 2, \dots \quad (1)$$

Метою роботи є порівняльний аналіз чотирьох VDM-моделей – Рескорли, AML, AME та Капура – за точністю на реальних CVE-даних.

Моделі виявлення вразливостей

Усі розглянуті моделі описують функцію $\Omega(t)$ – накопичену кількість виявлених вразливостей на момент часу t [3]. Спільна нотація: N – гранична кількість вразливостей; $r > 0$ – швидкість виявлення.

Модель Рескорли – увігнута експоненціальна крива. Припущення: швидкість виявлення пропорційна кількості ще не знайдених вразливостей [3]:

$$\Omega(t) = N(1 - e^{-rt}) \quad (2)$$

Логістична модель Алхазмі–Малії (AML) — S-подібна крива, що моделює три фази: навчання дослідників, активний пошук та насичення. Швидкість виявлення пропорційна водночас накопиченій кількості знайдених та кількості ще не знайдених вразливостей [3]:

$$\Omega(t) = \frac{N}{1 + N C e^{-r N t}} \quad (3)$$

де $C > 0$ – константа інтегрування, що визначає зміщення кривої відносно початку координат.

Модель зусиль Алхазмі–Малії (AME) – структурно аналогічна моделі Рескорли, але аргументом є накопичені зусилля E — зважена сума аудиторії продукту [3]:

$$\Omega(E) = N(1 - e^{-rE}), \quad E = \sum_{i=0}^n U_i \cdot P_i, \quad (4)$$

де U_i – кількість користувачів у момент i ; P_i – частка ринку продукту в цей момент.

Логістична модель Капура – S-подібна крива з явним параметром навчання $\beta \geq 0$ [3]:

$$\Omega(t) = N \frac{1 - e^{-rt}}{1 + \beta e^{-rt}} \quad (5)$$

При $\beta = 0$ модель Капура вироджується в модель Рескорли, тобто остання є окремим випадком першої. Чим більше β , тим виразнішою є початкова фаза навчання.

Порівняльний аналіз моделей

Моделі Рескорли та АМЕ простіші й стійкіші до перенавчання, але не відтворюють початкову фазу повільного виявлення, характерну для більшості реальних даних [3]. S-подібні моделі (AML, Капур) гнучкіші, але потребують більшого обсягу спостережень для надійної оцінки параметрів. Ключова відмінність AML і Капура – механізм формування S-подібної кривої: в AML прискорення зумовлене зростаючим ринковим прийняттям продукту (член $r\Omega(t)$ у диференціальному рівнянні), тоді як у Капура – явним накопиченням знань детекторами (логістичний множник $r/(1 + \beta e^{-rt})$). Завдяки цьому параметр β безпосередньо інтерпретується: більше значення відповідає тривалішій фазі навчання.

Метрики оцінювання точності

Для кількісного порівняння моделей використано такі метрики, де $\hat{\Omega}(t_i)$ – значення, передбачене моделлю; $\Omega(t_i)$ – фактичне спостережуване значення; k – кількість часових точок; p – кількість параметрів моделі; $\underline{\Omega}$ – середнє фактичних значень;

Усі метрики наведено за [3].

MSE — середньоквадратична похибка:

$$MSE = \sum_{i=1}^k \frac{(\hat{\Omega}(t_i) - \Omega(t_i))^2}{k-p} \quad (6)$$

R^2 – частка поясненої дисперсії:

$$R^2 = 1 - \frac{\sum_{i=1}^k (\Omega(t_i) - \hat{\Omega}(t_i))^2}{\sum_{i=1}^k (\Omega(t_i) - \underline{\Omega})^2} \quad (7)$$

PRR – нормована похибка прогнозу (виявляє систематичне зміщення):

$$PRR = \sum_{i=1}^k \frac{(\hat{\Omega}(t_i) - \Omega(t_i))}{\hat{\Omega}(t_i)} \quad (8) .$$

Результати та висновки

Для порівняння моделей реалізовано програмний застосунок, який будує накопичені криві виявлення за річними даними CVE Details і апроксимує їх кожною з чотирьох моделей методом нелінійної регресії (NLLS). Результати показали, що моделі Рескорли та АМЕ схильні до недооцінювання на пізніх етапах через вихід на фіксоване плато. АМЛ краще описує процеси з вираженою S-подібною динамікою, тоді як модель Капура є найбільш гнучкою та забезпечує кращу апроксимацію для випадків незавершеного насичення завдяки параметру β .

Список використаних джерел

1. GeeksforGeeks. Vulnerabilities in Information Security. — 2025. — URL: <https://www.geeksforgeeks.org/ethical-hacking/vulnerabilities-in-information-security/>
2. CVE Details. Vulnerabilities By Type. — 2025. — URL: <https://www.cvedetails.com/vulnerabilities-by-types.php>
3. Anand A., Bhatt N., Alhazmi O. H. Software Vulnerability Discovery Process: Concepts and Applications. — 1-е вид. — Gistrup : River Publishers, 02.2025. — (River Publishers Series in Mathematical and Engineering Sciences).

АДАПТИВНА ЕВОЛЮЦІЯ ДОВІРИ У ФЕДЕРАТИВНИХ СИСТЕМАХ ЗАХИСТУ МІКРОМЕРЕЖ

Шибасєв Г. Д.¹, Гальчинський Л. Ю.¹, Носок С. О.¹

¹*Національний технічний університет України «Київський
політехнічний інститут імені Ігоря Сікорського»,
K233@ukr.net, hleonid@gmail.com, nossvol@gmail.com*

У роботі розглянуто підхід до підвищення кіберстійкості розподілених мікромереж на основі федеративного навчання з адаптивною еволюцією довіри. Актуальність дослідження зумовлена тим, що сучасні мікромережі містять велику кількість гетерогенних розподілених енергетичних ресурсів, зокрема фотоелектричні установки, вітрові турбіни, системи накопичення енергії, інтелектуальні лічильники та локальні контролери. Такі компоненти генерують значні обсяги операційних даних, які є чутливими, розподіленими та часто не можуть бути централізовано зібрані через обмеження конфіденційності, пропускну здатності й безпеки.

Запропоновано концепцію адаптивної моделі довіри, у якій довіра до вузлів мікромережі розглядається не як статична характеристика, а як динамічна змінна, що еволюціонує в часі під впливом історичної поведінки, якості локальних оновлень, аномальних відхилень, дрейфу даних та результатів навчання з підкріпленням. На відміну від класичних підходів федеративного навчання, де всі учасники неявно вважаються добросовісними, запропонована система враховує можливість отруєння моделі, прихованої компрометації вузлів, змови, нестабільності датчиків та природного дрейфу локальних розподілів даних. Довіра використовується як керуючий сигнал для визначення ваги вузла під час агрегації, обмеження його участі в навчанні та активації захисних контрзаходів.

Ключові слова: федеративне навчання, мікромережі, кібербезпека, адаптивна довіра, навчання з підкріпленням, отруєння моделі, дрейф даних, LSTM, trust-weighted aggregation.

Вступ

Мікромережі є важливою складовою сучасної енергетичної інфраструктури, оскільки забезпечують локальну генерацію, накопичення, балансування та споживання електроенергії. До їх складу можуть входити фотоелектричні панелі, вітрові турбіни, системи накопичення енергії, інтелектуальні лічильники, локальні контролери та інші розподілені енергетичні ресурси. Особливістю таких систем є висока гетерогенність, нестационарність режимів роботи та залежність від зовнішніх фізичних чинників, таких як погодні умови, сезонні зміни, коливання навантаження, деградація обладнання та якість зв'язку.

Водночас цифровізація мікромереж підвищує їх вразливість до кіберфізичних атак. Компрометація окремого вузла, підміна показань сенсорів, маніпуляція локальними моделями або навмисне спотворення навчальних оновлень можуть негативно вплинути на загальну якість керування, прогнозування та виявлення аномалій. Особливо небезпечними є атаки отруєння у федеративному навчанні, коли зловмисний вузол надсилає шкідливі оновлення моделі з метою зміщення глобальної моделі у хибному напрямку. Не менш важливою проблемою є дрейф даних, який може виникати не через зловмисні дії, а внаслідок природних змін у фізичному середовищі мікромережі. Це створює складну ситуацію: система має відрізнити шкідливу поведінку від доброякісних, але статистично нетипових змін.

Федеративне навчання є перспективним підходом для побудови систем виявлення аномалій у таких умовах, оскільки дозволяє навчати спільну модель без централізованої передачі сирих операційних даних. Кожен вузол або локальний контролер виконує навчання на

власному наборі даних, після чого передає агрегатору лише параметри моделі або градієнти. Це зменшує ризики розкриття конфіденційної інформації та знижує навантаження на комунікаційну інфраструктуру. Однак класичне федеративне навчання, зокрема алгоритм FedAvg, не враховує різну надійність учасників і може бути вразливим до отруєних або нестабільних локальних оновлень.

Постановка проблеми

У класичній схемі федеративного навчання центральний сервер ініціалізує глобальну модель, надсилає її обраним клієнтам, після чого кожен клієнт навчає модель локально на власних даних і повертає оновлення. Узагальнено локальна цільова функція клієнта може бути подана як:

$$F_i(w) = \frac{1}{n_i} \sum_{j=1}^{n_i} l(w, x_{ij}, y_{ij}),$$

де $F_i(w)$ - локальна функція втрат клієнта i , n_i - кількість локальних зразків, x_{ij} - вхідні дані, y_{ij} - відповідна мітка або цільове значення, а $l(w, x_{ij}, y_{ij})$ -- функція втрат моделі.

Після локального навчання сервер агрегує оновлення, наприклад за допомогою FedAvg:

$$w^{(t+1)} = \sum_{i \in S^{(t)}} \frac{n_i}{\sum_{j \in S^{(t)}} n_j} w_i^{(t+1)}.$$

Такий підхід є ефективним за умови, що всі клієнти поведуться добросовісно, а їхні дані хоча й можуть бути неоднорідними, але не є навмисно спотвореними. У реальних мікромережах це припущення не виконується. Частина вузлів може бути скомпрометована, частина може працювати в умовах деградації сенсорів, а частина - генерувати оновлення, що відхиляються через природний дрейф розподілу даних.

Атака отруєння може бути подана як навмисне додавання шкідливого збурення до локального градієнта:

$$g_i^{adv} = g_i + \delta_i,$$

де g_i - коректний локальний градієнт, а δ_i - зловмисне збурення. У свою чергу дрейф даних також може спричиняти відхилення локального оновлення, але без зловмисного наміру:

$$g_i^{received} = g_i + \epsilon_i.$$

Проблема полягає в тому, що на рівні агрегатора обидва випадки можуть виглядати подібно: система отримує оновлення, яке відхиляється від очікуваного напрямку навчання. Тому просте відкидання всіх нестандартних оновлень може бути надто грубим рішенням, оскільки воно може покарати вузли, що працюють у складних, але фізично нормальних умовах. Саме тому необхідна адаптивна модель довіри, здатна враховувати історію поведінки вузла, його фізичний контекст, якість внеску в глобальне навчання та довгострокову стабільність.

Запропонована модель адаптивної еволюції довіри

У запропонованому підході довіра до вузла розглядається як динамічна змінна:

$$T_i(t) \in [0,1],$$

де значення, близьке до нуля, означає низьку довіру або потенційно шкідливу поведінку, а значення, близьке до одиниці, означає стабільну, корисну та надійну участь вузла у федеративному навчанні.

На відміну від статичних методів, у яких довіра визначається лише за поточним оновленням,

запропонована модель враховує попередній стан довіри та нові поведінкові докази:

$$T_i(t+1) = \alpha T_i(t) + (1 - \alpha) S_i(t),$$

де $\alpha \in [0,1]$ – коефіцієнт пам'яті, що визначає **вплив** історичної поведінки, а $S_i(t)$ – поточна оцінка надійності вузла. Така форма дозволяє уникнути різких і необґрунтованих змін довіри. Якщо вузол короткочасно демонструє нетипову поведінку через фізичний дрейф або шум, його довіра не повинна миттєво падати до нуля. Водночас вузол із тривалою історією підозрілої поведінки не повинен швидко відновлювати повну довіру після одного коректного оновлення.

Поточна оцінка $S_i(t)$ може формуватися на основі кількох груп ознак: помилки локального детектора аномалій, подібності градієнта до глобального напрямку, стабільності зв'язку, якості локального навчання та контекстуальної очікуваної мінливості. Наприклад, якщо локальний LSTM-детектор фіксує значну помилку реконструкції, це може бути ознакою аномального стану вузла:

$$e_i(t) = \|x_i(t) - \hat{x}_i(t)\|,$$

де $x_i(t)$ – спостережуване вікно часової послідовності, а $\hat{x}_i(t)$ – реконструйоване або передбачене значення. На основі цієї помилки можна побудувати штрафний компонент довіри:

$$S_i(t) = \exp(-\beta e_i(t)) Q_i(t),$$

де β визначає чутливість довіри до аномальної поведінки, а $Q_i(t)$ відображає якість внеску вузла у федеративне навчання.

Важливим компонентом є також оцінка геометричної узгодженості локального оновлення з глобальним

напрямком навчання. Для цього може використовуватися косинусна подібність:

$$sim_i(t) = \frac{\Delta w_i(t) \cdot \Delta w_{global}(t)}{\|\Delta w_i(t)\| \|\Delta w_{global}(t)\|}.$$

Якщо оновлення вузла систематично рухає модель у напрямку, протилежному глобальній оптимізації, це є підставою для зниження довіри. Однак така оцінка не повинна використовуватися ізольовано, оскільки гетерогенні вузли мікромережі можуть мати різні локальні розподіли даних, і певне відхилення може бути фізично обґрунтованим.

Інтеграція навчання з підкріпленням

Для підвищення адаптивності запропонованої системи довіра коригується не лише за фіксованими правилами, а й за допомогою навчання з підкріпленням. У цьому випадку агрегатор або спеціальний контролер довіри розглядає стан системи як сукупність значень довіри, а дії - як можливі стратегії коригування довіри, наприклад підвищення, зниження, обмеження участі вузла або його тимчасову ізоляцію.

Процес може бути поданий як марковський процес прийняття рішень:

$$P(T(t+1) | T(t), a(t)),$$

де $T(t)$ - поточний стан довіри, а $a(t)$ - дія контролера довіри. Метою є максимізація кумулятивної дисконтованої винагороди:

$$\max E \left[\sum_{t=0}^{\infty} \gamma^t a(t) R(T(t), a(t)) \right],$$

де $R(T(t), a(t))$ - функція винагороди, а γ - коефіцієнт дисконтування.

Функція винагороди може враховувати кілька цілей: зменшення впливу шкідливих вузлів, збереження участі добросовісних вузлів, підвищення точності виявлення аномалій, зниження хибнопозитивних спрацювань і стабільність глобальної моделі. Таким чином, довіра стає не лише пасивним показником, а активним механізмом керування захистом.

Для реалізації такої адаптації може застосовуватися Q-learning. Значення функції якості дії оновлюється після кожного раунду федеративного навчання:

$$Q_{t+1}(T(t), a(t)) = Q_t(T(t), a(t)) + \eta R(t) + \gamma \max_{a'} |Q_{t+1}(T(t+1), a') - Q_t(T(t), a(t))|,$$

де η – швидкість навчання, $R(t)$ – отримана винагорода, а a' – можлива наступна дія. Такий підхід дозволяє системі поступово навчатися оптимальній політиці довіри, не покладаючись повністю на заздалегідь задані пороги.

Довіро-зважена агрегація як механізм захисту

Після обчислення значень довіри вони використовуються під час агрегації локальних оновлень. Замість того щоб усереднювати внески клієнтів лише пропорційно до кількості даних, агрегатор враховує рівень довіри кожного вузла. Узагальнено це можна подати як:

$$w(t+1) = w(t) - \eta \sum_{i=1}^N \tilde{T}_i(t) \Delta w_i(t),$$

де $\tilde{T}_i(t)$ – нормалізована довіра до вузла, $\Delta w_i(t)$ – локальне оновлення моделі, а η – швидкість навчання. Нормалізована довіра визначає, наскільки сильно конкретний вузол впливає на глобальну модель.

Такий механізм забезпечує поступову маргіналізацію скомпрометованих або нестабільних вузлів. Якщо вузол генерує оновлення, що систематично погіршують якість

глобальної моделі, його довіра зменшується, а отже зменшується і його вплив на наступні раунди навчання. Якщо ж вузол демонструє стабільну поведінку та корисні оновлення, його внесок зберігається або посилюється. Це особливо важливо для мікромереж, де повне виключення вузла не завжди є бажаним: окремі вузли можуть бути критично важливими для відображення локального фізичного контексту.

Очікувані та експериментальні результати

Експериментальна логіка дослідження передбачає порівняння стандартного FedAvg із довіро-зважена агрегація в умовах кількох типів загроз: цілеспрямованого отруєння, постійного дрейфу, прихованої компрометації та змішаної поведінки вузлів. У таких сценаріях оцінюються не лише загальні втрати моделі, а й функціональна якість виявлення аномалій, зокрема MSE, recall, FPR та F1-score.

За результатами моделювання, адаптивне підкріплення довіри дозволяє зменшити пошкодження глобальної FL-моделі, стабілізувати розподіл довіри та підвищити якість виявлення аномалій. У статті зазначено, що запропонований підхід зменшує пошкодження моделі на 35–82%, відновлює нормальний розподіл довіри протягом 20–40 раундів комунікації та збільшує загальний F1-score виявлення аномалій до 16%.

Важливо, що поведінка довіри відрізняється для різних типів вузлів. Добросовісні вузли зберігають високий рівень довіри навіть за наявності незначних локальних коливань. Вузли з поступовим дрейфом демонструють повільніше зниження довіри, що дозволяє системі не карати їх надто агресивно. Натомість вузли, які генерують постійно шкідливі оновлення, швидко втрачають довіру й практично ізолюються від впливу на глобальну модель. Така поведінка є бажаною для кіберфізичної системи, оскільки вона поєднує стійкість до атак із здатністю адаптуватися до природної зміни фізичного середовища.

Наукова новизна та практичне значення

Наукова новизна запропонованого підходу полягає у представленні довіри як адаптивної динамічної змінної, що формується не лише на основі поточного відхилення оновлення, а й з урахуванням історичної поведінки, контексту мікромережі та результатів підкріплювального навчання. На відміну від класичних методів робастної агрегації, які часто працюють як одноразові статистичні фільтри, запропонована модель підтримує довготривалу пам'ять про поведінку вузлів і дозволяє формувати індивідуальні траєкторії довіри.

Практичне значення роботи полягає в можливості застосування такого підходу для побудови самовідновлюваних систем кіберзахисту мікромереж. У реальних умовах система не може спиратися лише на фіксовані правила або статичні пороги, оскільки поведінка енергетичних ресурсів змінюється залежно від фізичних, технічних та мережевих умов. Адаптивна довіра дозволяє зменшити вплив скомпрометованих вузлів, зберегти участь корисних вузлів із локальною специфікою та підвищити загальну стійкість федеративного навчання.

Висновки

У роботі запропоновано підхід до побудови адаптивної системи довіри для федеративного захисту мікромереж. Показано, що класичне федеративне навчання є перспективним для мікромереж завдяки збереженню конфіденційності локальних даних, але воно залишається вразливим до отруєння, дрейфу даних і компрометації окремих вузлів. Для подолання цих обмежень запропоновано модель еволюції довіри, яка враховує історичну поведінку вузла, локальні аномалії, геометричну узгодженість оновлень, критичність вузлів і сигнали навчання з підкріпленням.

Застосування довіро-зваженої агрегації дозволяє зменшити вплив шкідливих або нестабільних оновлень на глобальну модель, а використання навчання з підкріпленням забезпечує адаптивне налаштування

політики довіри відповідно до довгострокових результатів системи. Запропонований підхід формує основу для самовідновлюваного механізму кіберзахисту, здатного не лише виявляти шкідливу поведінку, а й поступово змінювати рівень участі вузлів у процесі навчання.

Подальші дослідження доцільно спрямувати на розширення експериментальної бази, перевірку моделі на реальних або напівреальних даних мікромереж, порівняння різних RL-стратегій корекції довіри та дослідження стійкості системи до більш складних сценаріїв атак, зокрема змови кількох вузлів, прихованого отруєння та комбінованого впливу отруєння й довготривалого дрейфу.

Список використаних джерел

1. McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Agüera y Arcas, B. Communication-Efficient Learning of Deep Networks from Decentralized Data. *Proceedings of AISTATS*, 2017.
Це базова робота з федеративного навчання та FedAvg, на яку варто посилатися при поясненні загальної FL-архітектури.
2. Blanchard, P., El Mhamdi, E. M., Guerraoui, R., & Stainer, J. Machine Learning with Adversaries: Byzantine Tolerant Gradient Descent. *NeurIPS*, 2017.
Джерело для пояснення Byzantine-загроз і методу Krum як робастної агрегації.
3. Yin, D., Chen, Y., Ramchandran, K., & Bartlett, P. Byzantine-Robust Distributed Learning: Towards Optimal Statistical Rates. *ICML*, 2018.
Підходить для обґрунтування coordinate-wise median і trimmed mean як захисту від шкідливих оновлень.
4. Tian, Z., Cui, L., Liang, J., & Yu, S. A Comprehensive Survey on Poisoning Attacks and Countermeasures in Machine Learning. *ACM Computing Surveys*, 2022.
Корисне оглядове джерело для опису poisoning attacks і захисних стратегій у ML/FL.
5. Zhang, Z., Rath, S., Xu, J., & Xiao, T. Federated Learning for Smart Grid: A Survey on Applications and Potential

Vulnerabilities. *ACM Transactions on Cyber-Physical Systems*, 2025.

Дуже релевантне джерело саме для FL у smart grid: генерація, передача, розподіл, споживання, а також потенційні вразливості.

6. Abdel-Basset, M., Moustafa, N., & Hawash, H. Privacy-Preserved Generative Network for Trustworthy Anomaly Detection in Smart Grids: A Federated Semi-Supervised Approach. *IEEE Transactions on Industrial Informatics*, 2022. DOI: 10.1109/TII.2022.3165869.

РОЗПОДІЛ РЕСУРСІВ КІБЕРЗАХИСТУ НА ОСНОВІ МОДЕЛІ ГРИ ПОЛКОВНИКА БЛОТТО ТА ВИРОБНИЧОЇ ФУНКЦІЇ КОББА–ДУГЛАСА

Смирнов С. А., Полуциганова В. І.

*Національний технічний університет «Київський
політехнічний інститут імені Ігоря Сікорського»,
м. Київ, Україна,
e-mail: sergsmr@gmail.com, medvika@ukr.net*

У роботі запропоновано інтегровану методику розподілу наявних обчислювальних ресурсів та залучених людських зусиль для задач кіберзахисту, що поєднує ймовірнісну модель гри полковника Блотто для конфліктної взаємодії сторін з функцією Кобба-Дугласа для оцінки ефективності сумісного впливу вкладених ресурсів. Методика дозволяє формалізувати процес прийняття оптимальних рішень щодо розподілу обмежених ресурсів захисту між критичними активами з урахуванням їхньої цінності, технологічної готовності та уточнених параметрів еластичності впливу людських зусиль та ресурсних факторів.

Ключові слова: гра полковника Блотто, функція Кобба-Дугласа, кібербезпека, розподіл ресурсів, ймовірнісна модель, оптимізація.

Вступ

Гра полковника Блотто як модель конкурентної боротьби двох сторін на декількох майданчиках є класичною задачею теорії ігор [1]. У кібербезпеці ця модель може інтерпретуватися як опис протистояння захисника та атакуючого у боротьбі за критичні інформаційні активи [2]. Довгий час результати обмежувалися симетричними або однорідними випадками [3–5], що знижує практичну придатність моделей для

реальних сценаріїв, де ресурси сторін нерівні, а цінність активів різна. Нещодавно обмеження вдалося зняти [6]. Зі свого боку виробнича функція Кобба–Дугласа використовується в економіці для моделювання залежності продуктивності від комбінації факторів виробництва [7]. Властива їй фіксована еластичність впливів дозволяє враховувати локальну взаємозамінність ресурсів та ефект спадаючої віддачі. Мета роботи – розробити метод розподілу ресурсів у сфері кібербезпеки, що спирається на ймовірнісну модель гри полковника Блотто, функцію Кобба-Дугласа та експертні оцінки для коректного врахування сумісного впливу людських та технічних факторів на ефективність захисту.

1. Концептуальна основа інтегрованої моделі

Класична модель гри Блотто не враховує різноманітність наявних ресурсів, сумісний вплив людського фактору та технічних засобів на ефективність кіберзахисту. Для усунення цього обмеження у роботі використовується виробнича функція Кобба-Дугласа, яка дозволяє моделювати синергетичну взаємодію між автоматизованими засобами захисту та людськими зусиллями.

У ймовірнісній моделі гри полковника Блотто ймовірність перемоги першого гравця на майданчику i визначається як

$$p_i = \frac{x_i}{x_i + y_i},$$

де x_i , y_i – ресурси, виділені гравцями 1 та 2 відповідно на майданчик i [1]. Інтерпретація у контексті кібербезпеки:

- майданчики – критичні активи (сервери, мережеві сегменти, бази даних);
- ресурси – впливи людських зусиль та комп'ютерних засобів підтримки (обробка інцидентів, детектори атак, інтелект та інтенсивність кібератак);
- ймовірність перемоги – ймовірність успішного відбиття атаки на актив.

Виробнича функція Кобба–Дугласа для такої ситуації має вигляд:

$$V_i = A_i \cdot H_i^\alpha \cdot I_i^\beta,$$

де V_i – ефективність захисту активу i ; H_i – людські ресурси (нормо-години); I_i – інформаційне забезпечення (одиниці інтелекту загрози); A_i – технологічний коефіцієнт; α, β – коефіцієнти еластичності ($\alpha + \beta \leq 1$ – умова, що вказує, що при збільшенні ресурсів для одного майданчика – обов’язково зменшується ресурс для іншого) [7].

2. Математичне формулювання гібридної моделі

Цільова функція захисника (гравця 1) формулюється як максимізація очікуваної захищеної цінності:

$$\max_{\{H_i, I_i\}} \sum_{i=1}^n v_i \cdot \frac{A_i H_i^\alpha I_i^\beta}{A_i H_i^\alpha I_i^\beta + B_i X_i^\gamma Y_i^\delta},$$

за обмежень:

$$\sum_{i=1}^n H_i \leq H_{\text{total}}, \sum_{i=1}^n I_i \leq I_{\text{total}}, H_i, I_i \geq 0,$$

де v_i – цінність активу i ; $B_i, X_i, Y_i, \gamma, \delta$ – відповідні параметри для оцінки впливу атакуючого, що вважається відомим (моделюється або оцінюється експертно).

Використовуючи метод множників Лагранжа та підхід зі зниження розмірності [6], систему рівнянь зводимо до однопараметричного рівняння:

$$\Phi(\lambda) = \sum_{i=1}^n \left[\frac{\alpha v_i A_i^{1/\alpha} I_i^{\beta/\alpha}}{\lambda^{1/\alpha}} \right] - H_{\text{total}} = 0.$$

Оптимальні стратегії обчислюються як:

$$H_i^* = \left(\frac{\alpha v_i A_i I_i^\beta}{\lambda} \right)^{\frac{1}{1-\alpha}}, I_i^* = \left(\frac{\beta v_i A_i H_i^\alpha}{\mu} \right)^{\frac{1}{1-\beta}}.$$

Наведені формули є точним розв'язком для оптимізації дій захисника, де вплив атакуючого враховується через калібрування параметрів v_i та A_i , або на першому кроці ітераційного пошуку рівноваги. Для практичного застосування в кібербезпеці це стандартний і обґрунтований підхід, оскільки точні параметри супротивника рідко відомі, а модель має залишатися обчислювально стійкою.

Формули описують стратегії саме в такому вигляді, тому що вони є аналітичним розв'язком умови «Гранична ефективність ресурсу» дорівнює «Тіньова ціна ресурсу» для функції Кобба-Дугласа. Цей вигляд забезпечує:

- Врахування неможливості збільшувати ресурси для певного майданчика без обмежень для іншого ($\alpha + \beta \leq 1$);
- Баланс між людськими та інформаційними факторами;
- Можливість зниження розмірності задачі до 1–2 параметрів (λ, μ);
- Пряму інтерпретованість для управлінських рішень SOC.

3. Алгоритм практичної реалізації

Крок 1. Підготовка даних: ідентифікація активів, оцінка їх цінності v_i , технологічних коефіцієнтів A_i , початкових оцінок параметрів атакуючого.

Крок 2. Знаходження параметрів еластичності: використовується аналітичний метод на основі локального коефіцієнта заміщення для виробничої функції Кобба-Дугласа як функції корисності.

1. Визначається локальний коефіцієнт заміщення ресурсів (ЛКЗ): $\lambda(x, y) = -\frac{dy}{dx} = \frac{\alpha y}{\beta x}$ – показник компенсуючого заміщення для значень x і y .

2. Експерти надають набір локальних оцінок балансуючого заміщення для різних значень ресурсних параметрів $\langle \lambda_i, x_i, y_i \rangle$.

3. Для оцінювання значень параметрів α і β застосовується метод найменших квадратів (МНК), він дає:

$$\frac{\alpha}{\beta} = \sum_{x_i} \frac{y_i}{x_i} \lambda_i / \sum_{x_i} \left(\frac{y_i}{x_i} \right)^2.$$

4. Для уточнення конкретних значень α та β використовується опорна початкова точка з відомою ефективністю $\Phi(x_0, y_0) = C_0$. За відсутності експертних даних можуть бути використані стартові значення $\alpha=0.6$, $\beta=0.4$ для SOC через пріоритетність людського впливу, тобто значення $\alpha=0.6$ закріплено за людськими ресурсами (аналітиками та інженерами), а $\beta=0.4$ – за інформаційним забезпеченням (даними про загрози).

Крок 3. Чисельне розв'язання: використання методу Лагранжа для знаходження λ та обчислення H_i^*, I_i^* .

Крок 4. Ітераційна корекція: щоквартальне оновлення параметрів на основі метрик SOC (MTTD, MTTR, % відбитих атак) та сценарний аналіз для обліку невизначеності.

4. Результати чисельного експерименту

Для ілюстрації розглянуто сценарій з 5 критичними активами. При $H_{\text{total}}=190$ люд-год/тиждень, $I_{\text{total}}=280$ одиниць інтелекту загроз, отримано розподіл, наведений у табл. 1.

Таблиця 1 – Оптимальний розподіл ресурсів та ймовірності захисту

Актив	v_i	H_i^*	I_i^*	p_i
Критична БД	0.40	85	120	0.78
Веб-шлюз	0.25	45	80	0.65
Кінцеві пристрої	0.15	30	40	0.52
Резервні системи	0.12	20	25	0.48
Тестове середовище	0.08	10	15	0.35

Результати підтверджують, що ресурси розподіляються відповідно цінності активів та еластичності факторів, з урахуванням спадаючої віддачі.

Висновки

Запропоновано інтегровану методику розподілу ресурсів кіберзахисту, що поєднує ймовірнісну модель Блотто для конфліктної взаємодії сторін з функцією Кобба-Дугласа для оцінки впливу вкладених ресурсів на ісход конфлікту. Методика дозволяє формалізувати оцінювання впливу людських та інформаційних факторів на ефективність захисту через уточнені параметри еластичності α , β їх дії на основі експертних оцінок. Перспективи дослідження включають розширення моделі на випадок більшої кількості параметрів впливу та інтеграцію з методами машинного навчання для динамічного калібрування.

Список використаних джерел

1. Borel E. La théorie du jeu les équations intégrales à noyau symétrique // Comptes Rendus de l'Académie. 1921. Vol. 173. P. 1304–1308.
2. Boix-Adserà E., Edelman B.L., Jayanti S. The Multiplayer Colonel Blotto Game. URL: <https://arxiv.org/abs/2002.05240v3>
3. Friedman L. Game-theory Models in the Allocation of Advertising Expenditure // Operations Research. 1958. Vol. 6. P. 699–709.
5. Robson R.W. Multi-Item Contest. Australian National University. Working Paper № 446, 2005. 27 p.
6. Roberson B. The Colonel Blotto Game // Economic Theory. 2006. Vol. 29. P. 1–24.
7. Smirnov S.A., Tereschenko I.M. A probabilistic model of the Colonel Blotto game without symmetry and homogeneity constraints // System research and information technologies. 2026. No 1. P. 92-102.
8. Cobb C.W., Douglas P.H. A Theory of Production // The American Economic Review. 1928. Vol. 18(1). P. 139–165.

КОМПЛЕКСНИЙ АНАЛІЗ ЦИФРОВИХ АРТЕФАКТІВ ДЛЯ РЕКОНСТРУКЦІЇ WINDOWS-ІНЦИДЕНТУ

Худоба А. Г., Коломицев М. В.

*КПІ ім. Ігоря Сікорського, Навчально-науковий фізико-
технічний інститут,
м. Київ, Україна,
e-mail: arsenhudob-ipt27@lil.kpi.ua*

Розглянуто підхід до реконструкції кіберінциденту у Windows-середовищі засобами цифрової криміналістики та реагування на інциденти. Запропоновано DFIR-методику, що поєднує аналіз мережевого трафіку, журналів Windows і Sysmon, дискового образу, оперативної пам'яті та реєстрових артефактів. Для перевірки змодельовано лабораторний інцидент із завантаженням підозрілого виконуваного файлу та подальшим мережевим підключенням. Результати показали, що кореляція різних груп доказів дає змогу відновити послідовність подій і оцінити придатність доказового набору.

Ключові слова: цифрова криміналістика, DFIR, Windows, цифрові докази, цифрові артефакти.

Вступ

Сучасні кіберінциденти у Windows-середовищах залишають цифрові сліди у файловій системі, журналах подій, оперативній пам'яті, мережевому трафіку та реєстрі. Окремий артефакт рідко дає повну картину: запис мережевого трафіку фіксує факт з'єднання, але не пояснює, який процес його створив; журнали подій підтверджують активність системи, однак потребують зіставлення з файловими та пам'яттєвими даними [1]. Тому для реконструкції інциденту важливо не лише зібрати різні джерела доказів, а й перевірити їхню узгодженість та доказову цінність. Метою роботи є перевірка комплексної DFIR-методики для реконструкції Windows-інциденту та

оцінювання доказового набору на основі кореляції зібраних цифрових артефактів.

1. Методика дослідження

Для перевірки підходу сформовано ізольоване середовище з двох віртуальних машин: Windows 11 як досліджуваної системи та Kali Linux як вузла атакуючої сторони. Сценарій передбачав завантаження файла Invoice_04_2026.pdf.exe з HTTP-ресурсу, його запуск у Windows і встановлення зворотного мережевого підключення. Одна дія мала залишати сліди у кількох незалежних джерелах: мережевому трафіку, журналах Windows і Sysmon, дисковому образі, реєстрі та дампі оперативної пам'яті.

Збір доказів виконувався з урахуванням пріоритету легких даних: спочатку фіксувалися оперативна пам'ять, активні процеси й мережеві з'єднання, після цього – журнали подій, дисковий образ, файли та реєстрові дані [2, 3]. Для аналізу використовувалися Magnet RAM Capture, FTK Imager, Autopsy, Volatility 3, Wireshark, Windows Event Viewer і Sysmon. Перед аналізом було обчислено контрольні суми SHA-256 для основних файлів доказового набору [4].

Окремо фіксувався зв'язок кожного джерела з конкретною подією сценарію, що дало змогу коректно розподілити ваги груп доказів.

Для кількісного узагальнення використано два індикатори. Індекс якості доказового набору EQI визначався як середнє арифметичне оцінок груп доказів:

$$EQI = \frac{\sum Q_j}{n}, \quad (1)$$

де Q_j – якість окремої групи цифрових доказів, n – кількість груп. Індекс внеску доказового набору DEI враховував вагу кожної групи у реконструкції інциденту:

$$D = \sum (Q_j \times W_j), \quad (2)$$

де W_j – вага групи доказів, $\sum W_j = 1$. Ваги задано відповідно до ролі джерела: мережеві артефакти – 0,20; журнали – 0,25; дискові артефакти – 0,225; оперативна пам'ять – 0,25;

реєстрові артефакти – 0,075. Такий підхід прозоро показує значущість кожного джерела.

2. Результати дослідження

У PCAPNG-файлі зафіксовано HTTP GET-запит до ресурсу, з якого завантажувався файл Invoice_04_2026.pdf.exe, відповідь сервера 200 OK і подальшу TCP-взаємодію між Windows 11 та Kali Linux. Журнали Windows і Sysmon відобразили запуск файла, створення cmd.exe та виконання команд PowerShell. Дисковий аналіз підтвердив наявність файла у каталозі завантажень, Prefetch-запис і файлові сліди після виконання. Результати оцінювання наведено на рис. 1.

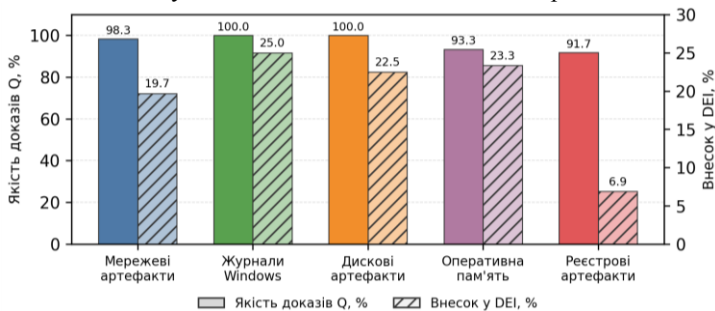


Рис. 1. Якість і внесок груп цифрових доказів

Аналіз оперативної пам'яті у Volatility 3 виявив процесні об'єкти, фрагменти командних рядків, файлові об'єкти та RAM-рядки, пов'язані з URL завантаження. Реєстр використано як допоміжне джерело для перевірки змін у системі.

EQI становить 96,7 %, а DEI – 97,4 %. Найбільший внесок дали журнальні, дискові та пам'яттєві артефакти, бо вони підтверджують запуск файла, процесну активність і локальні зміни; реєстр виконував допоміжну роль.

Зіставлення виконувалося через три питання: звідки файл потрапив у систему, чи був виконаний і які сліди залишив. Тому висновки спиралися на кореляцію

мережевих, журнальних, дискових, пам'яттєвих і реєстрових даних, а не на окремий артефакт.

Висновки

У роботі запропоновано й перевірено комплексний DFIR-підхід до дослідження Windows-інциденту: збір легких і сталих даних, перевірку цілісності, аналіз артефактів і оцінювання доказового набору.

Практичний сценарій показав, що поєднання Wireshark, Autopsy, Volatility 3, FTK Imager, Magnet RAM Capture, Windows Event Logs і Sysmon дає змогу відновити послідовність подій: завантаження файла, його запуск, створення дочірніх процесів, виконання команд і зміни у системі. Значення DEI = 97,4 % та EQI = 96,7 % підтверджують придатність доказів для реконструкції інциденту.

Практичне значення роботи полягає у використанні підходу в навчальних DFIR-лабораторіях, підготовці фахівців із кібербезпеки та розробці процедур розслідування Windows-інцидентів. У реальних умовах індикатори доцільно поєднувати з експертною перевіркою часової лінії та цілісності носіїв.

Список використаних джерел

1. Kävrestad J., Birath M., Clarke N. Fundamentals of Digital Forensics. 3rd ed. Cham: Springer, 2024.
2. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response. NIST SP 800-86. Gaithersburg: NIST, 2006.
3. ISO/IEC 27037:2012. Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO, 2012.
4. Tykushin A., Ostrovskaya S. Incident Response for Windows. Birmingham: Packt Publishing, 2024.

ОРТОГОНАЛЬНИЙ MERKLE-ЛІС ДЛЯ ЗМЕНШЕННЯ КОМПОЗИЦІЙНОСТІ ЛОКАЛЬНИХ КОЛІЗІЙ У ДЕРЕВОПОДІБНИХ ГЕШ-ФУНКЦІЯХ

Казміревський В. В.¹

¹*Вінницький національний технічний університет,
м. Вінниця, Україна,
ORCID ID: 0009-0005-4056-5385,
e-mail: kazmirevskiy1999@gmail.com*

У роботі пропонується підхід до зменшення композиційності локальних колізій у деревоподібних геш-функціях на основі дерева Merkle. У класичному дереві Merkle локальна колізія внутрішнього вузла робить відповідні піддерева взаємозамінними для всіх вищих рівнів. Така властивість може бути використана для побудови мультиколізій шляхом незалежного комбінування локальних колізій у різних частинах дерева.

Запропоновано структуру, яку можна розглядати як ортогональний ліс дерев Merkle. Її основна ідея полягає у побудові кількох дерев Merkle над одним і тим самим набором блоків, але з різними детермінованими перестановками їхніх індексів. Унаслідок цього блоки, які є сусідніми в одному дереві, потрапляють в інші локальні контексти в інших деревах. Тому локальна колізія, знайдена для однієї геометрії спарювання, не повинна автоматично переноситися на інші геометрії. На відміну від підходів, що збільшують розмір внутрішнього геш-значення або вводять повну залежність від глобального стану повідомлення, запропонована структура спрямована на зміну самої геометрії локальності. Це дає змогу зберегти можливість часткового оновлення даних із складністю порядку $O(k \log N)$, де k – кількість дерев, а N – кількість блоків.

У роботі сформульовано концепцію підходу, наведено його обґрунтування та окреслено напрями подальшої перевірки.

Ключові слова: Merkle-дерево; ортогональний Merkle-ліс; геш-функція; локальна колізія; мультиколізія; рекомбінація колізій; деревоподібне гешування; криптографічна стійкість; атака Joux.

Вступ

Дерева Merkle є однією з базових структур у сучасних системах криптографічного захисту інформації [1]. Вони використовуються для перевірки цілісності даних, побудови автентифікованих структур, організації розподілених реєстрів, зберігання стану в блокчейні та ефективного доведення належності окремого елемента до великого набору даних. Їхня популярність пояснюється поєднанням трьох властивостей: компактного кореневого геш-значення, можливості перевіряти окремі елементи без повного перегляду всього набору та логарифмічної складності оновлення.

У класичному дереві Merkle кожен внутрішній вузол обчислюється на основі двох дочірніх геш-значень:

$$h_v = H(h_L \parallel h_R), \quad (1)$$

де h_L та h_R – геш-значення лівого і правого дочірніх вузлів, а H – криптографічна геш-функція.

Така побудова є простою та ефективною, однак вона має важливу особливість. Якщо для певного вузла знайдено локальну колізію:

$$H(h_L \parallel h_R) = H(h'_L \parallel h'_R), \quad (2)$$

то відповідні піддерева стають невідрізнюваними для всіх вищих рівнів дерева. Інакше кажучи, локальна колізія перетворюється на локальну взаємозамінність. Якщо таких локальних колізій знайдено кілька, їх можна комбінувати між собою, отримуючи множину різних повідомлень з однаковим кореневим геш-значенням [2].

Саме ця властивість становить інтерес у контексті мультиколізій. Проблема полягає не лише в існуванні

окремої колізії, а в тому, що локальні колізії в класичному дереві Merkle можуть поводитися як незалежні складові, придатні для рекомбінації. Тому захист від такого механізму має бути спрямований не тільки на ускладнення пошуку колізій як таких, а й на зменшення їхньої переносимості між різними контекстами дерева.

Відомі підходи до посилення деревоподібного гешування мають різну природу. Додавання службових міток рівня, позиції або типу вузла допомагає уникати неоднозначності між листами та внутрішніми вузлами, але не усуває взаємозамінність колізії, знайденої для конкретного вузла [3]. Збільшення розміру внутрішнього геш-значення підвищує вартість пошуку локальної колізії, однак не змінює саму властивість підстановки після її знаходження [4]. Підходи з глобальним зворотним зв'язком можуть суттєво зменшувати переносимість локальних колізій, але при цьому часто погіршують можливість ефективного часткового оновлення. Підходи з використанням додаткових параметрів у процесі гешування також розглядаються як спосіб посилення класичних ітеративних схем [5]. Однак схеми з повною залежністю від глобального стану можуть погіршувати можливість ефективного часткового оновлення.

У цій роботі пропонується інший напрям – змінити не лише локальну формулу обчислення вузла, а геометрію локальності в цілому. Ідея полягає у побудові кількох дерев Merkle над тим самим набором блоків, але з різними детермінованими перестановками індексів. Наприклад, у першому дереві блоки можуть спарюватися у природному порядку, а в інших – за перестановками, які розносять сусідні блоки в інші локальні контексти.

У такій структурі локальна колізія, коректна для одного дерева, не обов'язково залишатиметься коректною для інших дерев. Блоки, які утворюють пару в одному дереві, в іншому дереві можуть бути спарені з іншими блоками. Отже, для успішної глобальної підміни атакуючий має забезпечити узгодженість не в одному локальному вузлі, а одночасно в кількох різних геометріях спарювання.

Запропонований підхід не скасовує загальних обмежень для геш-функцій із фіксованою довжиною виходу. Зокрема, він не усуває загальну межу складності пошуку колізій для фінального n -бітного геш-значення. Його мета зменшити ефективність структурного механізму побудови мультиколізій через незалежне комбінування локальних колізій.

Таким чином, метою роботи є підвищення криптографічної стійкості деревоподібних геш-функцій шляхом формулювання та обґрунтування підходу до зменшення переносимості локальних колізій при збереженні можливості часткового оновлення даних.

Подальше дослідження передбачає формалізацію метрик оцінювання такої переносимості, побудову експериментальної моделі та порівняння запропонованої структури з класичним деревом Merkle й іншими відомими підходами.

Основна частина

Запропонований підхід полягає у побудові кількох дерев Merkle над одним і тим самим набором блоків, але з різним порядком їх розміщення у листках. Таку структуру доцільно розглядати як ортогональний ліс дерев Merkle.

Нехай повідомлення подано у вигляді послідовності блоків:

$$M = (m_0, m_1, \dots, m_{N-1}). \quad (3)$$

Для побудови структури задається набір перестановок індексів:

$$\pi_0, \pi_1, \dots, \pi_{k-1}, \quad (4)$$

де k – кількість дерев. Перше дерево може будуватися у звичайному порядку:

$$\pi_0(i) = i. \quad (5)$$

Інші дерева будуються над тим самим набором блоків, але в іншому порядку:

$$m_{\pi_j(0)}, m_{\pi_j(1)}, \dots, m_{\pi_j(N-1)}. \quad (6)$$

Для кожного дерева обчислюється окремий корінь:

$$R_j = H(m_{\pi_j(0)}, m_{\pi_j(1)}, \dots, m_{\pi_j(N-1)}). \quad (7)$$

Фінальне геш-значення визначається як геш від коренів усіх дерев:

$$R = H(R_0 \parallel R_1 \parallel \dots \parallel R_{k-1}). \quad (8)$$

Основна ідея полягає в тому, що різні перестановки змінюють локальне сусідство блоків. У класичному дереві Merkle локальна колізія в одному вузлі автоматично зберігається на всіх вищих рівнях. Тому така колізія може бути використана як локальна підстановка.

В ортогональному лісі ситуація інша. Пара блоків, яка є сусідньою в одному дереві, в іншому дереві, як правило, вже не є локальною парою. Наприклад, для восьми блоків перше дерево може мати пари (0, 1), (2, 3), (4, 5), (6, 7), а друге – (0, 4), (2, 6), (1, 5), (3, 7). У цьому випадку локальна колізія для пари (0,1), знайдена в першому дереві, не гарантує збереження кореня другого дерева, оскільки блоки 0 і 1 у другому дереві мають інших сусідів. Отже, локальна колізія в одному дереві не є достатньою умовою для глобальної підстановки в усій структурі.

Це дозволяє розділити два поняття: існування локальної колізії та придатність локальної колізії для побудови мультиколізії. У класичному дереві Merkle ці поняття фактично збігаються: якщо локальна колізія знайдена, вона одразу може бути використана для рекомбінації з іншими локальними колізіями. В ортогональному лісі локальна колізія має бути узгоджена з кількома різними геометриями спарювання, що суттєво ускладнює її використання.

Якщо розмір внутрішнього геш-значення дорівнює n , то складність знаходження локальної колізії в одному окремому дереві залишається порядку $2^{n/2}$. Проте в класичному дереві Merkle така локальна колізія автоматично є корисною для глобальної підстановки. Тому побудова 2^m -мультиколізії через m незалежних локальних колізій має орієнтовну складність $m \cdot 2^{n/2}$ [2].

В ортогональному лісі дерев Merkle локальна колізія має зберегтися не в одному, а в кількох деревах з різними

перестановками. За евристичної оцінки, якщо ці дерева поводяться як незалежні представлення одного набору даних, складність пошуку локальної колізії, придатної для всієї структури, може наближатися до $2^{kn/2}$. Тоді орієнтовна складність структурної побудови 2^m -мультиколізії може бути оцінена як:

$$m \cdot 2^{kn/2}. \quad (9)$$

Слід підкреслити, що запропонований підхід не усуває загальну межу пошуку колізій для фінального п-бітного геш-значення. Його призначення полягає не в подоланні загальної межі $2^{n/2}$, а в руйнуванні дешевого структурного способу побудови мультиколізій через незалежне комбінування локальних колізій.

Перевагою запропонованої структури є збереження можливості часткового оновлення. Якщо змінюється один блок, у кожному з k дерев потрібно перерахувати лише один шлях від листа до кореня. Тому складність оновлення становить:

$$O(k \cdot \log N). \quad (10)$$

Для малого фіксованого k , наприклад $k = 2$ або $k = 3$, це залишається близьким до класичного дерева Merkle, але дає додатковий захист від рекомбінації локальних колізій.

Наукова новизна полягає у цільовому застосуванні кількох різних геометрій спарювання блоків для зменшення переносимості локальних колізій, а не лише для організації або перевірки структури даних.

Запропонована структура може розглядатися як компроміс між класичним деревом Merkle та схемами з повною глобальною залежністю. Вона не вимагає перебудови всієї структури після зміни одного блока, але водночас зменшує незалежність локальних колізій, яка є характерною для класичного дерева Merkle.

Висновки

Запропоновано підхід до зменшення композиційності локальних колізій у деревоподібних геш-структурах шляхом побудови кількох дерев Merkle над одним набором

блоків із різними перестановками індексів. Така зміна геометрії локальності робить локальну колізію, знайдену в одному дереві, недостатньою для глобальної підстановки в усій структурі.

На відміну від класичного дерева Merkle, де локальні колізії можуть незалежно рекомбінуватися у мультиколізії, ортогональний ліс дерев Merkle спрямований на розрив зв'язку між локальною колізією та її придатністю для глобальної рекомбінації. При цьому зберігається можливість часткового оновлення з орієнтовною складністю $O(k \cdot \log N)$.

Подальші дослідження доцільно спрямувати на формалізацію вимог до перестановок, експериментальну перевірку переносимості локальних колізій, а також поєднання запропонованої схеми з підходом розширеного внутрішнього стану, тобто wide-pipe, для одночасного підвищення вартості локальних колізій і зменшення їхньої рекомбінаційної придатності [6].

Список використаних джерел

1. Merkle R. C. A Digital Signature Based on a Conventional Encryption Function. *Advances in Cryptology – CRYPTO '87*. Lecture Notes in Computer Science. 1988. Vol. 293. P. 369-378.
2. Joux A. Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions. *Advances in Cryptology – CRYPTO 2004*. Lecture Notes in Computer Science. 2004. Vol. 3152. P. 306-316.
3. Bertoni G., Daemen J., Peeters M., Van Assche G. Sakura: A Flexible Coding for Tree Hashing. 2014. URL: <https://eprint.iacr.org/2013/231.pdf> (дата звернення: 20.05.2026).
4. Lucks S. Design Principles for Iterated Hash Functions. Cryptology ePrint Archive. Report 2004/253. 2004. URL: <https://eprint.iacr.org/2004/253.pdf> (дата звернення: 20.05.2026).
5. Biham E., Dunkelman O. *A Framework for Iterative Hash Functions – HAIFA*. Second NIST Cryptographic Hash

- Workshop. 2006. URL: <https://scispace.com/pdf/a-framework-for-iterative-hash-functions-haifa-210jx34dff.pdf> (дата звернення: 20.05.2026).
6. Al-Bassam M., Sonnino A., Buterin V. *Fraud and Data Availability Proofs: Maximising Light Client Security and Scaling Blockchains with Dishonest Majorities*. arXiv preprint. 2018. URL: <https://arxiv.org/pdf/1809.09044> (дата звернення: 20.05.2026).

ВІЯВЛЕННЯ АНОМАЛІЙ АКУСТИЧНОЇ ІМПУЛЬСНОЇ ВІДПОВІДІ ДЛЯ МОНІТОРИНГУ ВТОРГНЕНЬ У ПРИМІЩЕННЯ

Терлецький О. І.¹, Трушевський В. М.¹

¹Львівський національний університет імені Івана Франка,
вул. Університетська, 1, Львів, 79000, Україна,
oleksandr.terletskyi@lnu.edu.ua,
valeriy.trushevsky@lnu.edu.ua

Запропоновано систему виявлення вторгнень у масштабах кімнати на основі безперервного моніторингу акустичної імпульсної відповіді (АІВ) у частотному діапазоні 20–48 кГц. Захищена кімната моделюється як лінійний стаціонарний акустичний канал, АІВ якого є геометричним відбитком простору. Аномалії — зловмисники, відчинені двері, переміщені предмети — змінюють відбивну геометрію і породжують вимірюване відхилення, яке виявляється класифікатором на основі відстані Махаланобіса та однокласового SVM. Пілотні експерименти в офісному приміщенні 5,0×4,0×2,7 м показали 100 % виявлення відчинення дверей і 99,8 % виявлення людини на відстані 4 м при затримці 250 мс на апаратурі класу мікроконтролера.

Ключові слова: акустична імпульсна відповідь, виявлення вторгнень, виявлення аномалій, відстань Махаланобіса, однокласовий SVM, ультразвукове зондування

Вступ

Традиційні системи виявлення вторгнень усередині приміщень спираються на пасивні інфрачервоні датчики (PIR), магнітні контактні вимикачі та відеоспостереження. Кожна технологія має притаманні обмеження: PIR потребує прямої видимості й легко блокується меблями; контактні

датчики перекривають лише окремі точки входу; камери залежать від освітлення та створюють проблеми конфіденційності. Ці недоліки спонукають до пошуку додаткових сенсорних модальностей, непомітних для зломисника та здатних контролювати весь об'єм приміщення.

Акустичне зондування в ультразвуковому діапазоні пропонує низку привабливих властивостей: звук огинає перешкоди, залишається непомітним для людини і взаємодіє з усіма поверхнями кімнати. Акустична імпульсна відповідь (AIB) кодує повну геометрію акустичного середовища: прямі шляхи поширення, ранні відбиття та пізні реверберантне поле. Будь-яка фізична зміна в кімнаті — людина, що увійшла, відчинені двері, переміщений предмет — збурює відбивну геометрію і залишає вимірюваний слід в AIB [1].

Модель акустичного каналу

Кімната моделюється як лінійний стаціонарний (ЛС) акустичний канал. Фіксований ультразвуковий випромінювач надсилає зондувальний сигнал $s(t)$ у діапазоні 20–48 кГц. Мікрофон фіксує

$$y(t) = s(t) * h(t) + n(t) \quad (1),$$

де $*$ — операція згортки, $h(t)$ — AIB кімнати, $n(t)$ — адитивний шум. Деконволюція $y(t)$ за відомим $s(t)$ дає оцінку $h(t)$, що описує прямий шлях поширення, ранні відбиття та реверберантне поле. Поки кімната незмінна, $h(t)$ є наближено стаціонарною і слугує базовою лінією $h_0(t)$. Вторгнення, відчинені двері або переміщений предмет змінюють відбивну геометрію та спричиняють вимірюване відхилення $\Delta h(t) = h(t) - h_0(t)$ [2].

Зондувальний сигнал і видобування ознак

Серед кандидатів — послідовності максимальної довжини (MLS), комплементарні пари Голея та експоненційно розгортна синусоїда (ESS) — перевагу надано ESS, оскільки вона дозволяє відокремити лінійну

відповідь кімнати від гармонійних спотворень випромінювача: усі нелінійні продукти потрапляють у від'ємний часовий діапазон і видаляються часовим вікнуванням [2].

Обраний зонд – ESS тривалістю 100 мс у діапазоні 22–44 кГц, що повторюється з частотою 4 Гц і дискретизується з частотою 96 кГц. Когерентне усереднення $K = 4$ сусідніх вимірювань підвищує відношення сигнал/шум (ВСП) на 6 дБ ціною мінімальної затримки виявлення 250 мс. Із кожної оціненої АІВ обчислюється вектор ознак $\varphi(h)$ розмірності $D = 38$: крива затухання енергії та час реверберації T_{60} , спектральні енергії по третинно-октавних смугах, часи приходу та амплітуди перших 5–10 дискретних відбиттів, а також короткочасна перехресна кореляція між послідовними АІВ — чутливий до руху людини оцінювач ефекту Доплера [3].

Адаптивна базова лінія та виявлення аномалій

Протягом фази реєстрації 100–500 послідовних АІВ використовуються для оцінювання вектора середнього μ та матриці коваріації Σ розподілу ознак. Повільний дрейф через температуру та вологість компенсується оновленням середнього за допомогою експоненційного ковзного середнього:

$$\bar{h}_n = (1 - \alpha)\bar{h}_{n-1} + \alpha h_n, \quad \alpha \approx 10^{-3} \quad (2)$$

Стала часу $1/\alpha \approx 1000$ кадрів (≈ 250 с при 4 Гц) достатньо велика, щоб придушити транзйентні події вторгнення, але достатньо мала, щоб відстежувати поступові сезонні зміни.

Два детектори працюють паралельно. Первинний статистичний детектор обчислює квадрат відстані Махаланобіса:

$$d^2 h_n = (\varphi(h_n) - \mu)^T \Sigma^{-1} (\varphi(h_n) - \mu). \quad (3)$$

За нульовою гіпотезою $d^2(h_n)$ підпорядковується розподілу χ^2 з $D = 38$ ступенями свободи. Поріг τ

встановлюється з розподілу реєстрації для досягнення цільового рівня хибної тривоги 10^{-3} за кадр. Вторинний детектор – однокласовий SVM (метод опорних векторів), навчений на ознаках реєстраційної фази, – забезпечує нелінійну межу рішення та зменшує хибні тривоги при корельованому дрейфі кількох ознак. Виходи обох детекторів об'єднуються логічною операцією АБО.

Експериментальні результати

Експерименти проводилися в офісному приміщенні $5,0 \times 4,0 \times 2,7$ м при температурі 23 ± 1 °С. Для кожного з трьох сценаріїв вторгнення виконано 50 незалежних спроб. Базова відстань Махаланобіса незбуреної кімнати: $d^2 = 28 \pm 7$; поріг виявлення: $\tau = 60$.

Таблиця 1 – Ефективність виявлення для характерних сценаріїв

Сценарій	Сер. d^2	P_d при $\tau=60$	Затримка, мс	Спроби
Відчинення дверей, 3 м	850	1,00	250	50
Людина стоїть, 4 м	220	0,998	250	50
Стілець зміщений на 30 см	75	0,74	500	50

Відчинення дверей на відстані 3 м дає значну зміну відбиттів (сер. $d^2 = 850$) — ідеальне виявлення в усіх 50 спробах. Людина, що стоїть на відстані 4 м, дає сер. $d^2 = 220$ і ймовірність виявлення $P_d = 0,998$. Найскладніший сценарій — зміщення стільця на 30 см — дає сер. $d^2 = 75$ і ймовірність виявлення 0,74. Адаптивна базова лінія успішно усунула вплив дрейфу сигналу, спричинені вмиканням і вимиканням системи вентиляції (перепад температури ± 2 °С), не генеруючи хибних тривог. Однокласовий SVM знизив частоту хибних тривог з

$1,2 \times 10^{-3}$ до 3×10^{-4} за кадр порівняно з детектором Махаланобіса.

Висновки

Запропоновано систему виявлення вторгнень у масштабах кімнати на основі моніторингу ультразвукової акустичної імпульсної відповіді. Розглядаючи кімнату як ЛС-акустичний канал і безперервно оцінюючи її AIB за допомогою зонда ESS, система забезпечує об'ємне перекриття без обмежень прямої видимості, залежності від освітлення та розкриття відеозображень. Детектор на основі відстані Махаланобіса, доповнений однокласовим SVM, забезпечує високу ймовірність виявлення ($P_d \geq 0,998$) для вторгнень масштабу людини при частоті хибних тривог $\approx 3 \times 10^{-4}$ за кадр на недорогому п'єзoeлектричному обладнанні.

Подальші дослідження будуть спрямовані на формування пучків мікрофонної решітки для локалізації подій, ідентифікацію мовця за звуками дихання чи кроків та інтеграцію з PIR- і контактними датчиками у мультимодальній системі злиття даних.

Список використаних джерел

1. Schroeder M. R. Integrated-impulse method for measuring sound decay without using impulses. Journal of the Acoustical Society of America. 1979. Vol. 66, No. 2. P. 497–500.
2. Farina A. Simultaneous measurement of impulse response and distortion with a swept-sine technique. Preprint 5093, 108th AES Convention. 2000. 24 p.
3. Stowell D. et al. Detection and classification of acoustic scenes and events. IEEE Transactions on Multimedia. 2015. Vol. 17, No. 10. P. 1733–1746.

ОПТИМІЗАЦІЯ МЕТОДУ ЗГЛАДЖЕНИХ ЧАСТИНОК У ЗАСТОСУВАННІ ДО ЗАДАЧ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Грицишин О.О.¹, Трушевський В.М.¹

¹Львівський національний університет імені Івана Франка,
ostap.hrytsyshyn@lnu.edu.ua, valeriy.trushevsky@lnu.edu.ua

Розглянуто проблему ефективного пошуку сусідніх частинок у методі SPH. Запропоновано адаптацію компактного просторового хешування з паралельним Bitonic Sort для GPU з попередньо виділеною хеш-таблицею та хеш-функцією для тривимірного простору. Експерименти на 75 000 частинок показали прискорення одного кроку моделювання з 690 мс (однопотоковий CPU) і 250 мс (багатопотоковий CPU) до 10 мс на GPU, що забезпечує моделювання динаміки рідин у реальному часі.

Ключові слова: метод згладжених частинок, SPH, пошук сусідів, компактне хешування, Bitonic Sort, GPU, обчислювальні шейдери, моделювання у реальному часі

Вступ

Метод згладжених частинок (SPH) — безсітковий лагранжевий підхід до розв'язування рівнянь Нав'є-Стокса, поширений у комп'ютерній графіці, інженерії та обчислювальній гідродинаміці [1]. Рідина дискретизується множиною частинок, кожна з яких взаємодіє лише із сусідами в межах радіуса згладжування h , що надає методу природну адаптивність до складних геометрій і вільних поверхонь. Це робить SPH придатним для моделювання аварійних подій на об'єктах критичної інфраструктури: руйнування дамб, прориви водогонів, затоплення урбанізованих територій [2].

Однак на кожному кроці для кожної частинки необхідно визначити множину сусідів. Пряма перевірка всіх пар має складність $O(n^2)$, що непрактично при сотнях тисяч частинок. Класичні підходи (рівномірна сітка, просторове

хешування) знижують складність до $O(n)$, проте адаптація до GPU потребує узгодженого доступу до пам'яті та ефективного паралельного сортування. У цій роботі розглядається адаптація компактного хешування з алгоритмом Bitonic Sort для GPU [3, 4].

Постановка задачі

Нехай у момент часу t задано набір із n частинок з координатами $\{x_i\}$, $i = 1, \dots, n$. Для кожної частинки i необхідно сформувати множину сусідів

$$N(i) = \{j : \|x_i - x_j\| < h, j \neq i\}, \quad (1),$$

де h – радіус згладжування ядра. Множина $N(i)$ використовується на наступних етапах розв'язувача SPH для обчислення густини, сил тиску та в'язкості. Мета — побудувати алгоритм, який забезпечує лінійну за n складність формування цих множин, добре паралелізується на GPU та зберігає передбачуваний час виконання при великих n .

Метод компактного хешування

Над областю моделювання будується рівномірна сітка з розміром комірки d , що дорівнює радіусу згладжування h . Кожна частинка приписується до однієї комірки сітки на основі її просторових координат. Згідно з підходом, запропонованим у [3], для відображення тривимірних координат у одновимірний індекс хеш-таблиці використовується функція:

$$c = (\lfloor x/d \rfloor p_1 \oplus \lfloor y/d \rfloor p_2 \oplus \lfloor z/d \rfloor p_3) \bmod m, \quad (2),$$

де p_1, p_2, p_3 – великі прості числа, $\oplus$ – побітова операція виключного «або», m – розмір хеш-таблиці. Така функція мінімізує колізії за рахунок рівномірного розподілу значень. Для двовимірного простору z -координата опускається.

Для забезпечення передбачуваного доступу до пам'яті хеш-таблиця попередньо виділяється з розміром, рівним кількості частинок. Хоч такий підхід не усуває колізій повністю, він мінімізує витрати на динамічне виділення пам'яті та дозволяє ефективно паралельне опрацювання.

Запит сусідів для частинки і зводиться до перевірки 27 (у тривимірному випадку) або 9 (у двовимірному) комірок у безпосередньому околі її комірки, що забезпечує лінійну за n складність.

Паралельне сортування Bitonic Sort

Для сортування набору за хеш-індексами обрано алгоритм Bitonic Sort [4], який природно паралелізується на GPU. Послідовність є бітонічною, якщо вона спочатку зростає, а потім спадає. Алгоритм рекурсивно будує такі підпослідовності та об'єднує їх операціями порівняння й обміну, що виконуються паралельно окремими потоками. Складність — $O(n \log^2 n)$, але кожен рівень виконується повністю паралельно, що забезпечує перевагу за фактичним часом. Після сортування частинки сусідніх комірок зберігаються послідовно, суттєво покращуючи використання кешу.

Експериментальні дослідження

Схему реалізовано засобами обчислювальних шейдерів і протестовано на 75 000 частинок. GPU-реалізація виконує один крок моделювання за ~ 10 мс, тоді як багатопотоковий CPU потребує ~ 250 мс, а однопотоковий — ~ 690 мс, що відповідає прискоренню $25\times$ та $65\times$ відповідно. Основна частка приросту досягається за рахунок паралельного пошуку сусідів. Попереднє виділення хеш-таблиці стабілізує час кроку, що особливо важливо для IISPH, де на кожному кроці виконується кілька ітерацій методу Якобі [5].

Застосування до моделювання аварійних подій

Досягнута продуктивність відкриває можливості для застосування методу до задач безпеки об'єктів критичної інфраструктури: моделювання прориву дамби з оцінкою фронту хвилі та зон затоплення, аналізу поширення води при аваріях на магістральних водогонах у міському середовищі, оцінки впливу повеней на транспортну інфраструктуру. У всіх таких задачах принципово є

здатність розв'язувача природно опрацьовувати вільні поверхні та складну геометрію перешкод, що є сильною стороною методу SPH порівняно зі сітковими підходами. Можливість виконувати моделювання в режимі, близькому до реального часу, є особливо цінною для систем підтримки прийняття рішень у надзвичайних ситуаціях.

Висновки

Запропоновано адаптацію компактного просторового хешування з паралельним Bitonic Sort до архітектури GPU для пошуку сусідів у методі SPH. Підхід забезпечує лінійне масштабування та продуктивність реального часу: прискорення $25\times$ порівняно з багатопотоковим CPU і $65\times$ порівняно з однопотоковим, що робить його придатним для комп'ютерної графіки, інженерної візуалізації та систем оцінки наслідків аварій. Подальші дослідження охоплюватимуть адаптивне змінювання розміру хеш-таблиці та підтримку конфігурацій з кількома GPU.

Список використаних джерел

1. Monaghan J. J. Smoothed particle hydrodynamics. Reports on Progress in Physics. 2005. Vol. 68. P. 1703–1759.
2. Liu M. B., Liu G. R. Smoothed particle hydrodynamics (SPH): an overview and recent developments. Archives of Computational Methods in Engineering. 2010. Vol. 17, No. 1. P. 25–76.
3. Ihmsen M., Akinci N., Becker M., Teschner M. A parallel SPH implementation on multi-core CPUs. Computer Graphics Forum. 2011. Vol. 30, No. 1. P. 99–112.
4. Batchner K. E. Sorting networks and their applications. Proceedings of the AFIPS Spring Joint Computer Conference. 1968. Vol. 32. P. 307–314.
5. Грицишин О., Трушевський В. Реалізація методу SPH за допомогою обчислювальних шейдерів. Вісник Львівського ун-ту. Сер. прикл. матем. та інформ. 2024. Вип. 33. С. 55–68.

КІЛЬКІСНА ОЦІНКА ПОГЛИНАЛЬНОЇ ЗДАТНОСТІ КІБЕРСТІЙКОСТІ ІТ-МЕРЕЖІ ЕНЕРГЕТИЧНОГО ОБ'ЄКТА

Личик В.В.¹, Гальчинський Л.Ю.¹

¹*НН ФТІ НТУУ «Київський політехнічний інститут імені
Горя Сікорського», м. Київ, Україна
lychyk.vlad@gmail.com, hleonid@gmail.com*

В умовах гібридних війн та незворотної конвергенції інформаційних (ІТ) і операційних (ОТ) технологій об'єкти критичної інфраструктури перетворились на пріоритетні мішені для складних багатовекторних кібератак (зокрема класу АРТ). Оскільки енергетичний сектор є фундаментальною основою для безперебійної роботи всіх інших життєво важливих галузей держави, експоненційне зростання загроз для його технологічних мереж створює безпрецедентні ризики дестабілізації. З огляду на неможливість уникнення цілеспрямованих деструктивних впливів у сучасному цифровому середовищі, на даному етапі особливо актуальним завданням стає саме оцінка абсорбуючої (поглинальної) здатності кіберстійкості складних систем, що дозволяє ефективно витримувати удари та зберігати базові процеси життєзабезпечення.

Ключові слова: кіберстійкість, POMDP, BAG, ІТ-мережа енергооб'єкта, критична інфраструктура.

Вступ

Для вирішення означеної проблематики, зокрема для кількісного оцінювання та практичного забезпечення абсорбуючої здатності кіберстійкості [1] енергетичних об'єктів було розроблено метод активної протидії кібератакам у реальному часі. В його основі лежить інтеграція баєсових графів атак (BAG) у математичний апарат частково спостережуваних марковських процесів прийняття рішень (POMDP) [2]. На відміну від класичних евристичних підходів, такий гібридний метод уникає

невиправданих витрат на перманентне блокування критичних сегментів, натомість фокусуючись на оптимальному розподілі ресурсів відповідно до найбільш ймовірних векторів атаки.

Основна частина

У ході експериментальних досліджень було виявлено, що ручне відтворення високодеталізованих сценаріїв кібератак є неефективним через закриту архітектуру SCADA-систем, вимоги конфіденційності та надмірну ресурсоемність. Тому для формування об'ємної вибірки даних здійснено перехід до автоматизованого симуляційного моделювання з використанням фреймворку MITRE Caldera, в рамках якого реалізовано понад 800 модулів деструктивних впливів.

Щоб забезпечити обчислювальну досяжність алгоритмів POMDP та уникнути експоненційного зростання простору станів, складну топологію досліджуваної ІТ-мережі було зведено до 6 макро-станів на базі концепції Cyber Kill Chain. На основі масштабного моделювання розроблено матрицю впливу контрзаходів («Дія vs Стан»), яка формалізує ресурсні витрати та визначає рівень залишкової працездатності (поглинальної здатності) системи, а також порівняльні таблиці розроблених політик протидії із підсумковим розрахунком інтегрального показника кіберстійкості.

Програмна реалізація у середовищі pomdp-solve дозволила провести порівняльний аналіз різних стратегій кіберзахисту із застосуванням наборів контрзаходів та синтезувати оптимальну політику протидії. Отримані результати довели, що впровадження низьковартісних інформаційних операцій розвідки, таких як аудит, опитування контролерів та верифікація цілісності, радикально змінює поведінку системи захисту, забезпечуючи перехід від реактивного стримування до проактивної точкової ліквідації загроз [3].

Водночас удосконалення функції винагороди шляхом її жорсткої прив'язки до реальних фізичних коефіцієнтів

деградації цільової функції (наприклад, контрольованого скидання навантаження) переводить завдання забезпечення кіберстійкості у площину безпосередньої мінімізації економічних збитків підприємства, тим самим максимізуючи здатність інфраструктури абсорбувати деструктивні впливи [4].

Таблиця 1 – Порівняльна таблиця стратегій протидії

Тактика MITRE	Стратегія 1: Пасивна (2 дії)	Стратегія 2: Міопічна (4 дії)	Стратегія 3: Стимування (4 дії+)	Стратегія 4: Оптиміальна (8 дії)
Defense Evasion	46.5%	22,20%	15,50%	6,10%
Discovery	46.5%	23,30%	16,40%	5,20%
Credential Access	46.5%	26,70%	18,80%	7,90%

Висновок

Ключовим здобутком дослідження стало створення та реалізація методу структурної агрегації топології технологічних мереж (SCADA-систем) на базі концепції Cyber Kill Chain. Це дозволило застосувати точний математичний апарат POMDP, повністю зберігши при цьому логіку поширення атаки. Практично доведено, що інтеграція функції вартості в простір дій та запровадження низьковартісних операцій розвідки докорінно трансформують поведінку автономного агента. Таким чином, відбувається еволюція захисної стратегії від звичного «реактивного стримування» до «превентивної ліквідації», що гарантує ранню локалізацію загроз і дозволяє уникнути невиправдано дорогих операцій з повної ізоляції інфраструктурних вузлів.

Список використаних джерел

1. Гальчинський, Л., & Личик, В. (2023). Метрики оцінки кібервідмовостійкості (аналітичне оглядове дослідження). Інформаційні технології та суспільство, (2 (8), С. 27-33. DOI: 10.32689/maup.it.2023.2.3

2. Личик В.В., Гальчинський Л.Ю. (2025). Використання моделі мереж Баєса для раннього оцінювання загроз кібератак об'єкта електроенергетики. Інститут проблем реєстрації інформації НАН України. Реєстрація, зберігання і оброб. даних. 2025, Т. 27, № 2. С. 70-85. DOI: 10.35681/1560-9189.2025.27.2.345591
3. Vugrin, E. D., Castillo, A., & Silva-Monroy, C. A. (2017). Resilience metrics for the electric power system: A performance-based approach (No. SAND2017-1493). Sandia National Laboratories.
4. Sharifi, A., & Yamagata, Y. (2016). Principles and criteria for assessing urban energy resilience: A self-assessment strategy. *Applied Energy*, 173, 36-54. DOI: 10.1016/j.apenergy.2016.04.013.

АДАПТИВНА МОДЕЛЬ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ З ВИКОРИСТАННЯМ ПЛАТФОРМ WAZUH, ELK STACK, THEHIVE

Мельник М. М.¹, Чешун В. М.¹, Чешун Д. В.², Олексюк Д.А.²

¹*Хмельницький національний університет,*

²*Хмельницький фаховий економіко-технологічний коледж
Університету економіки і підприємництва,
melnyk.masia@gmail.com, cheshunvn@khmnu.edu.ua,
dmytro.cheshun@gmail.com, oleksuk.dima@gmail.com*

Стан нормативно-правового регулювання у сфері розслідування кіберінцидентів в Україні перебуває на етапі глобальної модернізації та гармонізації із європейськими стандартами, що обумовлено необхідністю протидії масштабній та системній кіберагресії. Базове законодавство зазнало оновлень у 2025-2026 роках, трансформувавши фрагментарні процедури реагування в єдину державну екосистему. Закон України № 4336-IX [1] впровадив ризикоорієнтований підхід, розділивши профілі безпеки на базовий, цільовий та галузевий, та законодавчо закріпив запуск оновленої Національної системи реагування на кіберінциденти. Закон України «Про основні засади забезпечення кібербезпеки України» [2] залишається рамковим документом, що визначає понятійний апарат (індикатори загрози, кіберінцидент) та зобов'язання суб'єктів. Постановою КМУ № 1533 [3] затверджено новий Національний план реагування на кіберінциденти, кібератаки та кіберзагрози. Постанова КМУ № 1471 [4] затвердила чіткий Порядок взаємодії суб'єктів кібербезпеки.

Результати аналізу сучасної архітектури кіберзахисту [5-7] свідчать про наявність деструктивних чинників в існуючих парадигмах реагування. Найбільш критичними є низький рівень автоматизації процесів оркестрації та моніторингу подій інформаційної безпеки (SIEM/SOAR), а

також відсутність уніфікованої системи акумуляції та верифікації цифрових доказів.

Метою дослідження є розробка системно-інтегрованого підходу до розслідування кіберінцидентів, орієнтованого на формалізацію криміналістичного процесу Digital Forensics від етапу первинної детекції аномальної активності і до генерації фінального структурованого аналітичного звіту.

Авторським колективом пропонується адаптивна архітектурна модель, яка поєднує інструменти автоматизованого аналізу системної телеметрії з нормативно-регламентованими інтерфейсами та міжвідомчою взаємодією суб'єктів забезпечення кібербезпеки. Фундаментальним аспектом дослідження є архітектурно-методологічна конвергенція вимог міжнародних стандартів серії ISO/IEC 27035 [8] та фреймворків NIST SP 800-61 / SP 800-86 [9, 10] із урахуванням специфіки функціонування та правового режиму державних інформаційних ресурсів України.

Рішення базується на об'єднанні кількох технологічних платформ у єдину логічну систему реагування та аналізу. Основними етапами реалізації методу є реагування на інциденти, робота з доказами і взаємодія учасників. На етапі реагування впроваджено ієрархічний підхід, де кожен інцидент проходить фази ідентифікації, локалізації, аналізу та «навчання». Акцент зроблено на безперервності – результати розслідування обов'язково мають оновлювати бази індикаторів компрометації (IoC). Для роботи з доказами регламентовано порядок збору волатильних даних (RAM) та створення посекторних копій дисків; використання хеш-функцій (SHA-256) гарантує недоторканність доказів для подальшого судового розгляду. Взаємодія передбачає 4-рівневу систему обміну інформацією (локальний–галузевий–національний–міжнародний), що дозволяє оперативно попереджати інших суб'єктів про нові загрози через платформу MISP.

Практична реалізація методу була успішно здійснена з використанням стеку технологій та відповідних їм інструментів: Wazuh – моніторинг кінцевих точок та

виявлення аномалій у реальному часі; ELK Stack (Elasticsearch, Logstash, Kibana) – централізований збір та візуалізації терабайтів логів; TheHive для управління процесами розслідування інцидентів; MISP для автоматизований оперативний обмін індикаторами загроз серед спільноти фахівців; криміналістичний софт включно з Autopsy (аналіз файлових систем), Volatility (аналіз оперативної пам'яті), Wireshark (мережева форензика).

Пропонований підхід може стати корисним для створення внутрішніх регламентів CSIRT-підрозділів, забезпечуючи швидке відновлення систем та недопущення повторних атак. Автоматизація через Wazuh дозволила скоротити час реакції на типові вектори атак (фішинг, несанкціонований доступ) на 30-40%. Алгоритм фіксації артефактів забезпечує повну реконструкцію дій атакуючого. Використання інструментів із відкритим кодом робить метод економічним і доступним для державних установ з обмеженим фінансуванням.

Список використаних джерел

1. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27 березня 2025 року № 4336-IX. URL: <https://urli.info/1vm9F> (дата звернення: 8.05.2026).
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : редакція від 19.10.2025. URL: <https://urli.info/1pZSi> (дата звернення: 8.05.2026).
3. Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози : Постанова Кабінету Міністрів України від 26 листопада 2025 р. № 1533. URL: <https://urli.info/1pZS8> (дата звернення: 8.05.2026).
4. Про затвердження Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними,

розвідувальними органами та суб'єктами оперативно-розшукової діяльності : Постанова Кабінету Міністрів України від 13 листопада 2025 р. № 1471. URL: <https://url.info/1pZS0> (дата звернення: 8.05.2026).

5. ENISA Threat Landscape 2025. European Union Agency for Cybersecurity (ENISA). 2025. URL: <https://url.info/1uHEw> (date of access: 8.05.2026).
6. Річний звіт 2025: системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. URL: <https://url.info/1uHEt> (дата звернення: 8.05.2026).
7. Огляд кіберзагроз та стратегій захисту в 2025 році: досвід CERT-UA. URL: <https://url.info/1pmEF> (дата звернення: 8.05.2026).
8. ISO/IEC 27035-1:2023 Information technology – Information security incident management – Part 1: Principles and process. International Organization for Standardization. 2023. URL: <https://url.info/1uHEW> (date of access: 12.12.2025).
9. NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide. URL: <https://url.info/1uHEA> (date of access: 8.05.2026).
10. NIST SP 800-61r3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management – A CSF 2.0 Community Profile. <https://url.info/1pmEm> (date of access: 8.05.2026).

ПРАВОВІ АСПЕКТИ ІМПЛЕМЕНТАЦІЇ ДРУГОГО ДОДАТКОВОГО ПРОТОКОЛУ ДО КОНВЕНЦІЇ ПРО КІБЕРЗЛОЧИННІСТЬ

Гуцалюк М.В.

*Міжвідомчий науково-дослідний центр з проблем боротьби
з організованою злочинністю при РНБО України,
ORCID: 0000-0003-4496-5173*

Імплементація Другого додаткового протоколу до Конвенції про кіберзлочинність [1] є стратегічним завданням для України в умовах гібридної агресії РФ та транснаціоналізації кіберзлочинності. За даними CERT-UA, лише у 2025 році було опрацьовано близько 6000 кіберінцидентів, а динаміка ворожих кібератак зросла на 37% [2]. Використання зловмисниками іноземних хмарних сервісів, VPN-інфраструктур та анонімайзерів критично ускладнює збирання цифрових доказів у межах класичних процедур міжнародної правової допомоги, що зумовлює ризик втрати волатильних даних. Окрім прикладного значення, ратифікація Протоколу є обов'язковим кроком на шляху європейської інтеграції України та гармонізації кримінального процесуального законодавства зі стандартами Ради Європи та ЄС.

Сучасні транскордонні кібератаки характеризуються високою швидкістю та анонімністю правопорушників, через що цифрові сліди є надзвичайно волатильними. Традиційний механізм взаємодії правоохоронних органів (Mutual Legal Assistance, MLA) демонструє інституційну кризу: проходження запитів через дипломатичні канали триває від 6 до 18 місяців. Оскільки життєвий цикл електронних доказів (динамічних IP-адрес, логів серверів, метаданих) часто вимірюється годинами, такий часовий розрив унеможливорює притягнення винних до відповідальності.

Другий додатковий протокол (CETS № 224) змінює архітектуру міжнародної співпраці, здійснюючи перехід від

моделі «держава–держава» до парадигми «держава–приватний сектор». Статті 6 та 7 Протоколу легалізують прямий правовий канал зв'язку між правоохоронними органами та іноземними постачальниками електронних комунікаційних послуг (Microsoft, Google, AWS тощо) або реєстраторами доменних імен. Цей механізм дозволяє отримувати реєстраційні дані та інформацію про абонентів за кілька годин замість місяців [3].

Системне порівняння нормативно-правової бази України із стандартами CETS № 224 дозволяє виділити два ключові блоки правових розривів.

Першим та найбільш фундаментальним розривом є відсутність у Кримінальному процесуальному кодексі України терміна «електронні докази» та чітко визначених криміналістичних вимог до їх збирання. Чинна ст. 99 КПК розглядає «електронні носії інформації» лише як різновид документів. Такий підхід ігнорує специфічну правову та фізичну природу цифрових даних [4].

У КПК України відсутній термін «електронні докази» та криміналістичні вимоги до їх фіксації. Чинна ст. 99 КПК визначає «електронні носії інформації» лише як різновид документів, ігноруючи специфіку цифрових даних: віртуальність, здатність до миттєвого копіювання без втрати властивостей та вразливість до змін.

Іншим процесуальним бар'єром є імперативне положення статті 545 КПК України, яке закріплює право Офісу Генерального прокурора та Міністерства юстиції як єдиних центральних органів, уповноважених направляти та приймати запити про міжнародну правову допомогу. Ця норма суперечить філософії статей 6 та 7 Другого додаткового протоколу. Без внесення спеціальних змін (зокрема, доповнення КПК окремою статтею щодо порядку прямого транскордонного співробітництва) вітчизняні слідчі та прокурори позбавлені легального права самостійно адресувати запити безпосередньо іноземним провайдерам, а отримані у такий спосіб дані апріорі перебуватимуть поза межами правового поля України.

Разом з тим впровадження Протоколу покладає нові зобов'язання на вітчизняних постачальників електронних комунікаційних послуг, які повинні надавати інформацію на легітимні запити іноземних правоохоронних органів.

Також у Законі України «Про електронні комунікації» не врегульовано механізм реалізації ст. 9 Протоколу щодо термінового збереження даних (data preservation) [5] в екстрених ситуаціях, відсутні відповідні технічні регламенти та захищені державні шлюзи.

Для ліквідації виявлених правових розривів та практичної реалізації положень CETS № 224 пропонується доповнити Розділ IX КПК України спеціальною Статтею 562-1 «Особливості прямого співробітництва з постачальниками електронних комунікаційних послуг». У даній нормі необхідно чітко регламентувати процесуальний алгоритм, який дозволить вітчизняним слідчим та прокурорам за погодженням із процесуальним керівником напрямку надсилати запити іноземним сервіс-провайдерам для отримання інформації про абонентів та реєстраційних даних. Водночас на засадах взаємності слід нормативно закріпити обов'язок українських постачальників послуг опрацьовувати аналогічні прямі запити від компетентних органів іноземних держав-учасниць Конвенції, забезпечивши їх законодавчим імунітетом від цивільної та адміністративної відповідальності за добросовісне розкриття відомостей, якщо це не суперечить базовим інтересам національної безпеки.

Також необхідно модернізувати інститут невідкладних слідчих дій на виконання ст. 9 Протоколу шляхом внесення змін до ч. 1 ст. 163 КПК України слід надати правоохоронцям право у випадках безпосередньої загрози життю або критичній інфраструктурі вимагати від провайдерів негайного екстреного розкриття чи збереження комп'ютерних даних без ухвали слідчого судді. Для дотримання засад верховенства права та ст. 14 Протоколу, таке невідкладне збирання даних має підлягати судовій легалізації протягом 24 годин.

Висновки

Імплементація Другого додаткового протоколу до Конвенції про кіберзлочинність є необхідною умовою підвищення ефективності розслідування транскордонних кіберзлочинів та адаптації українського законодавства до сучасних європейських стандартів електронних доказів. У перспективі це сприятиме формуванню в Україні сучасної системи міжнародного співробітництва у сфері електронних доказів, сумісної з архітектурою та стандартами Ради Європи.

Водночас імплементація Другого додаткового протоколу повинна здійснюватися з урахуванням сучасних підходів ЄС у сфері транскордонного доступу до електронних доказів, насамперед положень EU e-Evidence Package [6]. Для України як держави-кандидата на вступ до ЄС це має не лише прикладне значення, але й виступає важливим елементом гармонізації кримінального процесуального законодавства із *acquis* ЄС та формування сумісної системи цифрового правосуддя й міжнародного співробітництва у сфері електронних доказів.

Список використаних джерел

1. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) URL: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=224>
2. CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів: кількість ворожих атак зросла на 37% URL: <https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracuyovala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37>
3. Н. Ахпирська, М. Гуцалюк Правові засоби боротьби з кіберзагрозами під час воєнного стану в світлі використання механізмів Другого додаткового протоколу до Конвенції про кіберзлочинність // Актуальні питання розвитку юридичної науки та практики: матеріали Міжнар.

- наук.-практ. конф (12 травня 2022 року) / За заг. ред. д.ю.н., акад. НАПрН України О.П. Орлюк, К., 2022. – С. 283-286
4. Гуцалюк М.В. Імплементація європейських стандартів у боротьбі з кіберзлочинністю: проблеми правового регулювання електронних доказів в Україні // Слово Національної школи суддів України. - № 2 (51) 2025. – С. 167-176. DOI: 10.37566/2707-6849-2025-2(51)-16
 5. М. Гуцалюк Процесуальний механізм термінового збереження електронних доказів у світлі Будапештської конвенції та Другого додаткового протоколу: потреба імплементації в КПК України : Матеріали круглого столу «Євроінтеграційні процеси та їх вплив на правову політику України: теоретичні та практичні аспекти» від 13 березня 2026 р., м. Київ, 2026.
 6. The EU Electronic Evidence Legislative Package URL: <https://www.eurojust.europa.eu/publication/eu-electronic-evidence-legislative-package>

ПРОТОТИП СИСТЕМИ ВИЯВЛЕННЯ ЗАКЛАДНИХ ПРИСТРОЇВ ЗА ДОПОМОГОЮ SDR-ПРИЙМАЧА

Уманський Є. А., Щербина М. Ю.

*Львівський національний університет імені І. Франка,
м. Львів, Україна,
yevhenii.umanskyi@lnu.edu.ua,
mykola.shcherbina@lnu.edu.ua*

Розроблено та протестовано прототип системи моніторингу радіочастотного спектра та виявлення ознак функціонування закладних пристроїв із використанням SDR-приймача RTL-SDR Blog V4 та алгоритмів цифрової обробки сигналів на базі Python.

Ключові слова: Python, SDR, software defined radio, T3I, алгоритм адаптивного порогу, закладні пристрої, медіана абсолютних відхилень, метод Велча, метод частотних стрибків, технічна розвідка, технічний захист інформації, технічні канали витоку інформації

Вступ

Забезпечення технічного захисту інформації (ТЗІ) набуває особливої значущості в умовах російсько-української війни, коли противник інтенсифікує технічну розвідку для отримання даних із обмеженим доступом. Виявлення та нейтралізація закладних пристроїв є важливою складовою безпеки [1].

Традиційні засоби радіомоніторингу часто є високовартісними та закритими системами. Натомість технологія Software Defined Radio (SDR) відкриває можливості для створення гнучких, доступних та ефективних комплексів пошуку загроз, що здійснюють аналіз сигналів у реальному часі [2].

Нами розроблено прототип системи моніторингу радіочастотного спектра та виявлення ознак

функціонування закладних пристроїв із використанням алгоритмів цифрової обробки сигналів на базі Python.

Для реалізації апаратної частини прототипу обрано SDR-приймач RTL-SDR Blog V4 на базі мікросхеми RTL2832U та тюнера Rafael Micro R828D. Ця конфігурація забезпечує перекриття радіочастотного спектра в діапазоні від 500 кГц до 1,766 ГГц.

Метод частотних стрибків

Центральною інженерною задачею є забезпечення неперервного покриття широкого частотного діапазону засобами приймача з обмеженою миттєвою смугою пропускання у 2,4 МГц. Для перекриття цільового діапазону застосовано метод послідовних частотних стрибків. Крок між сусідніми центральними частотами встановлено рівним 80% від частоти дискретизації:

$$f_{step} = f_s \cdot 0,8 = 2,4 \cdot 106 \cdot 0,8 = 1,92 \cdot 106 \text{Гц}, \quad (1)$$

де f_s — частота дискретизації у герцах. Перекриття у 20% між сусідніми кроками гарантує, що будь-яка частота цільового діапазону потрапляє у зону впевненого приймання принаймні одного кроку сканування. Загальна кількість кроків N :

$$N = \text{ceil}((f_{stop} - f_{start})/f_{step}) = 844. \quad (2)$$

Розрахований загальний час сканування становить близько двох хвилин.

Оцінка спектральної щільності потужності

Для отримання надійної оцінки спектральної щільності потужності з одиночної вибірки IQ -відліків у прототипі застосовано метод Велча.

Вибірка довжиною N розбивається на K сегментів довжиною L кожен з перекриттям у 50%. До кожного сегменту застосовується вагова функція Ганна:

$$w[n] = 0,5 \cdot (1 - \cos(2\pi n/(L - 1))), 0 \leq n \leq L - 1 \quad (3)$$

Оцінка спектральної щільності потужності методом Велча:

$$P_{Welch}[m] = \frac{1}{K \cdot U} \sum_{k=0}^{K-1} |X_k[m]|^2, \quad (4)$$

де U – нормуючий коефіцієнт для компенсації енергетичних втрат від вікна. Переводимо у дБм:

$$P_{dBm}[m] = 10 \cdot \log_{10}(|P_{Welch}[m]| + \varepsilon), \quad (5)$$

де $\varepsilon = 10^{-12}$ запобігає обчисленню логарифму нуля.

Алгоритм адаптивного порогу

У розробленому прототипі реалізовано триступеневий адаптивний поріг. Перший ступінь — абсолютний мінімальний поріг $THRESHOLD_dB = 95$ дБм – відсікає зони спектра нижче чутливості приймача. Другий ступінь базується на медіані спектра:

$$T_2 = median(P_{dBm}) + DETECTION_MARGIN_dB \quad (6)$$

Третій ступінь використовує медіанне абсолютне відхилення MAD :

$$MAD = median(|P_{dBm}[m] - median(P_{dBm})|), \quad (7)$$

$$\sigma_{noise} = MAD \cdot 1,4826, \quad (8)$$

$$T_3 = median(P_{dBm}) + 5,0 \cdot \sigma_{noise}. \quad (9)$$

де коефіцієнт 1,4826 перетворює MAD у незміщену оцінку стандартного відхилення. Фінальний адаптивний поріг:

$$T_{adapt} = \max(THRESHOLD_DB, T_2, T_3). \quad (10)$$

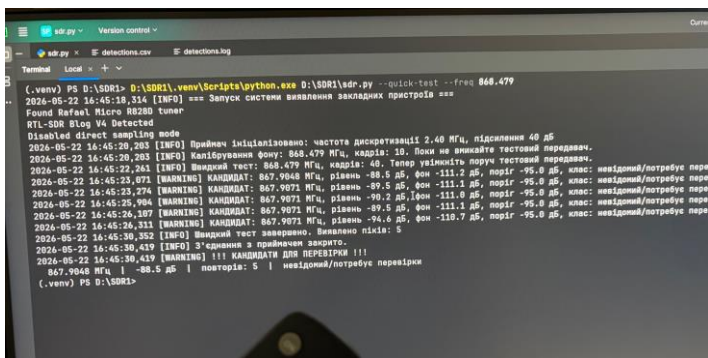
Такий підхід забезпечує стійкість до флуктуацій рівня шуму в різних частинах спектра та унеможливорює масові хибні спрацювання через FM-радіостанції або Wi-Fi.

Тестування прототипу та висновки

На синтетичних IQ -вибірках підтверджено коректність роботи функцій обчислення спектра та детектування піків.

Під час широкосмугового сканування система успішно зафіксувала легальні FM-радіостанції в діапазоні 87,5–108,0 МГц. Після інтеграції фільтра відомих сервісних діапазонів ці сигнали автоматично виключалися з переліку потенційних загроз.

Тестування з реальним радіопередавачем на частоті 868 МГц показало стабільне виявлення цільового сигналу (Рис. 1). Відсутність хибних спрацювань підтвердила ефективність адаптивного порогу з MAD.



```
(.venv) PS D:\SDR1> D:\SDR1\.venv\Scripts\python.exe D:\SDR1\sdra.py --quick-test --freq 868.479
2026-05-22 16:45:18,316 [INFO] == Запуск системи виявлення закладних пристроїв ==
Found Rafael Micro R820D tuner
RTL-SDR Blog V4 Detected
Disabled direct sampling mode
2026-05-22 16:45:20,203 [INFO] Прийомач ініціалізовано: частота дещопонижувача 2.40 МГц, підсилення 40 дБ
2026-05-22 16:45:20,203 [INFO] Налаштування фону: 868.479 МГц, кадрів: 10. Поки не вникайте поруч тестовий передавач.
2026-05-22 16:45:22,943 [INFO] Вихідний тест: 868.479 МГц, рівень: -88.5 дБ, фон: -111.2 дБ, noise: -95.0 дБ, клас: невідомий/потребує пере
2026-05-22 16:45:23,073 [WARNING] КАНДИДАТ: 867.9048 МГц, рівень: -88.5 дБ, фон: -111.2 дБ, noise: -95.0 дБ, клас: невідомий/потребує пере
2026-05-22 16:45:23,274 [WARNING] КАНДИДАТ: 867.9071 МГц, рівень: -89.5 дБ, фон: -111.1 дБ, noise: -95.0 дБ, клас: невідомий/потребує пере
2026-05-22 16:45:25,994 [WARNING] КАНДИДАТ: 867.9071 МГц, рівень: -90.2 дБ, фон: -111.0 дБ, noise: -95.0 дБ, клас: невідомий/потребує пере
2026-05-22 16:45:26,107 [WARNING] КАНДИДАТ: 867.9071 МГц, рівень: -89.5 дБ, фон: -111.1 дБ, noise: -95.0 дБ, клас: невідомий/потребує пере
2026-05-22 16:45:26,313 [WARNING] КАНДИДАТ: 867.9071 МГц, рівень: -94.5 дБ, фон: -113.7 дБ, noise: -95.0 дБ, клас: невідомий/потребує пере
2026-05-22 16:45:30,352 [INFO] Вихідний тест завершено. Виведено сигналів: 5
2026-05-22 16:45:30,419 [INFO] З'єднання з приймачем закрито.
2026-05-22 16:45:30,419 [WARNING] !!! КАНДИДАТИ ДЛЯ ПЕРЕВІРКИ !!!
867.9048 МГц | -88.5 дБ | повторів: 5 | невідомий/потребує перевірку
(.venv) PS D:\SDR1>
```

Рис. 1. Тестування з реальним радіопередавачем

Список використаних джерел

1. Wireless spy devices: A review of technologies and detection methods [Електронний ресурс]. URL: https://www.researchgate.net/publication/267751871_Wireless_spy_devices_A_review_of_technologies_and_detection_methods.
2. Щербина М. Ю. Використання SDR-приймачів у навчальному процесі за спеціальністю «Кибербезпека» / Щербина М. Ю. // ITSec: Безпека інформаційних технологій: матер. міжнар. наук.-техн. конф., Львів, Україна, 9-11 трав. 2024 р. – Львів : ЛНУ ім. І. Франка, 2024. – С. 245-246.

АНАЛІЗ СТАНУ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ЯК ІНДИКАТОР ЕФЕКТИВНОСТІ КІБЕРБЕЗПЕКИ

Гавловський В. Д.

*Міжвідомчий науково-дослідний центр з проблем боротьби
з організованою злочинністю при РНБО України?*
ORCID: <https://orcid.org/0000-0001-7496-9904>

Стрімка цифровізація суспільства викликала масштабну трансформацію злочинності, перемістивши її значну частину у віртуальну площину. Зростання кількості кіберзлочинів актуалізує необхідність глибокого аналізу стану протидії кіберзлочинності, складовою якого є кримінологічний аналіз, для оцінки реального масштабу загрози.

У цих умовах проведення комплексного кримінологічного аналізу структури, динаміки та детермінант кіберзлочинності є фундаментальною основою для розробки проактивних стратегій кібербезпеки та адаптації правоохоронних механізмів до сучасних загроз.

Кримінологічний аналіз протидії кіберзлочинності є науково-методологічним фундаментом для побудови ефективної кібербезпеки.

Без постійного аналізу стану протидії кіберзлочинності, система кібербезпеки втрачає здатність виявляти загрози, стає статичною. Вона захищає від загроз минулого, залишаючись безпорадною перед новими викликами.

Кримінальна статистика є фундаментальною складовою кримінологічного аналізу. Вона забезпечує емпіричну базу, необхідну для визначення кількісних і якісних показників, що характеризують стан, структуру, динаміку та географію злочинності.

Отже, статистичні дані про кіберзлочинність є абсолютно необхідними для забезпечення ефективності

кібербезпеки, оскільки без них неможливо побудувати точну модель загроз діяти на випередження.

Проте, на сьогодні в Україні не вистачає державної офіційної статистичної звітності про кіберзлочини для проведення цих досліджень. Нова звітність щодо правопорушень, які вчинено у сфері кібербезпеки (кіберзлочини) не відповідає поставленим вимогам.

Аналізу стану протидії кіберзлочинності впродовж останніх років приділяється значна увага як науковцями різних галузей знань так і практиками. Разом з тим, слід відмітити, що їхні дослідження, у переважній більшості, ґрунтувалися на окремих повідомленнях правоохоронних органів, їхніх відомчих звітностях, дослідженнях щодо вчинення окремих кримінальних правопорушень, аналізі офіційних державних звітностей про кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Так, до 2025 року в офіційних статистичних звітностях (Звіти Генеральної прокуратури України та Державної судової адміністрації України) відображалися лише кримінальні правопорушення, передбачені статтями Розділу XVI КК України. Протягом останніх років кількість таких облікованих кримінальних правопорушень зростала хвилеподібно від 595 облікованих у 2013 році до 2987 у 2025 році.

І на цих показниках, в основному, проводився аналіз стану протидії кіберзлочинності. Але ці кримінальні правопорушення, передбачені статтями Розділу XVI КК України, складають лише незначну частину від усіх кіберзлочинів, зокрема, у 2025 році вони склали 7,7 % (5 896 із 76 555) від усіх розслідуваних кримінальних правопорушень, які вчинено у сфері кібербезпеки (кіберзлочини) та 14,5 % (2505 із 17267), що обліковані у 2025 році.

Лише у 2025 році затверджено нову звітність «ФОРМА № 1-КІБ (місячна) «Звіт про результати діяльності органів правопорядку щодо стану запобігання та протидії

правопорушенням, які вчинено у сфері кібербезпеки (кіберзлочини)».

Але у Звіті подано значно скорочений перелік кримінальних правопорушень, які вчинено у сфері кібербезпеки (кіберзлочини). Окрім кримінальних правопорушень, передбачених статтями Розділу XVI КК України додано лише 5 статей КК України: Крадіжка (ст. 185 КК України); Шахрайство (частини четверта, п'ята ст. 190 КК України); Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження (ст. 301-1 КК України); Зловживання повноваженнями особами, які надають публічні послуги (ст. 365-2 КК України); Несанкціоноване втручання в роботу автоматизованих систем в органах та установах системи правосуддя (ст. 376-1 КК України).

Не висвітлені у Звіті кіберзлочини віднесено до – «Всі інші».

Разом з тим, протягом 2025 року із 76555 розслідуваних кримінальних правопорушень, які вчинено у сфері кібербезпеки (кіберзлочини), 24762 кримінальних правопорушень відносяться до «Інших», не вказаних кримінальних правопорушень, що складає 32,3%. Тобто третя частина кримінальних правопорушень, які вчинено у сфері кібербезпеки (кіберзлочини), невідомо за якими статтями КК України вони вчинені, що в свою чергу не дає змогу проведення повного аналізу структури кримінальних правопорушень у зазначеній сфері.

Слід відміти, що у новому Звіті вкрай обмежені статистичні дані про осіб, які вчинили кіберзлочини, що унеможливує проведення аналізу соціально-демографічної структури цих осіб.

До того, цей Звіт вперше сформовано і викладено на сайті, що на сьогодні унеможливує проведення аналізу динаміки кримінальних правопорушень, які вчинено у сфері кібербезпеки (кіберзлочини).

Отже, слід констатувати, в Україні до цього часу бракує державної офіційної статистичної звітності про

кіберзлочини. А відсутність необхідної кримінологічно значимої інформації про їхні масштаби та поширення, яку отримують у результаті проведення цілеспрямованих і поглиблених досліджень, передусім впливає на ефективність протидії кіберзлочинності і забезпечення кібербезпеки.

Слід також відмітити, що на сьогодні відсутні рекомендації, інструкції щодо віднесення кримінальних правопорушень до кіберзлочинів.

Крім того, серед науковців та практиків немає єдиної думки з цього приводу, а тому й єдиного підходу до окреслення підстав віднесення протиправних діянь до таких кримінальних правопорушень.

Висновки

Донині не вистачає державної офіційної статистичної звітності про кіберзлочини для проведення цілеспрямованих і поглиблених досліджень, що передусім впливає на ефективність протидії кіберзлочинності та забезпечення кібербезпеки.

ОЦІНЮВАННЯ НАДІЙНОСТІ ЕНЕРГЕТИЧНОГО ОБ'ЄКТА ПРИ ПРОВЕДЕННІ КІБЕРАТАК НА ОСНОВІ МОДЕЛІ НАПІВМАРКОВСЬКИХ ПРОЦЕСІВ

Снігур А.Ю., Гальчинський Л.Ю.

*НН ФТІ НТУУ «Київський політехнічний інститут імені
Горя Сікорського», м. Київ, Україна
tohasnigur139@gmail.com, hleonid@gmail.com*

Як для усіх складних систем, однією з головних проблем для SCADA-системи є їх надійність, бо вони є базовою інфраструктурою, яка забезпечує моніторинг і керування технологічними процесами в енергетиці[2]. Новим питанням в контексті надійності є поява феномену кіберзагроз, які спричиняють порушення системи управління і, як наслідок, збої системи енергетики в цілому. Класична теорія надійності не надає релевантних підходів для оцінки нового різновиду загроз надійності і ставить питання про поняття кібернадійності. Кібернадійність (cyber reliability) – це здатність системи зберігати коректне надання послуг з прийнятною частотою та тривалістю відмов попри наявність кіберризиків. Поняття кібернадійності корелюється з поняттям кіберстійкості (cyber resilience) як компонент абсорбційної здатності системи поглинати кіберзагрозу на певному етапі кібератаки [2]. Пошук таких нових підходів для оцінки кіберстійкості SCADA систем вказує на використання моделі напівмарківських процесів (SMP). Зокрема для оцінки часу перебування на кожному кроці багатетапної атаки та можливості оцінити рівень кібернадійності SCADA в залежності від кваліфікації зловмисника.

Основна частина

Об'єктом дослідження в даному дослідженні кібернадійності є локальна мережа (LAN) центру

управління, через яку зловмисники намагаються проникнути в глибші шари системи SCADA для подальшої компрометації та завдання шкоди. На Рисунку 1 показана спрощена діаграма схеми кібератак на LAN-мережу центра управління.

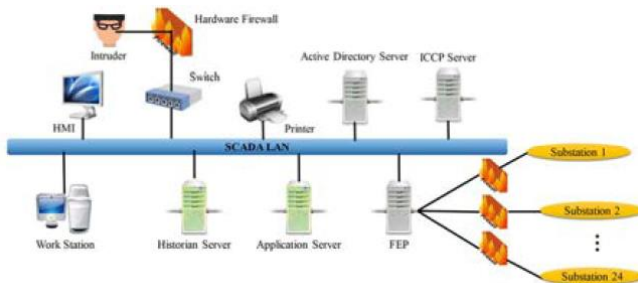


Рис. 1. Схема кібератаки на LAN управління

Для локальної мережі центру керування у випадку зовнішніх атак, після обходу брандмауера зловмисник може отримати доступ до комутатора шляхом сканування портів. Далі, після сканування хостів та серверів мережі, він може скопрометувати сервер історичних даних та проникнути на сервер застосунків, що може бути однією з цілей вторгнення. В Таблиці 1 показана матриця ймовірностей переходів від одного вузла до іншого [3].

Таблиця 1 – Ймовірність переходів між вузлами

0	0,434286	0,565714	0
0,168067227	0	0,831933	0
0,168067227	0	0	0,831933
1	0	0	0

Оцінки значень ймовірностей переходів від одного вузла до іншого отримані на основі показників бази даних CVSS. У моделюванні кібератак на SCADA-системи важливо враховувати не тільки ймовірності переходів між етапами атаки, а й тривалість перебування зловмисника в

кожному зі станів. Саме часовий компонент визначає реалістичність моделі та є ключовим для оцінки кібернадійності, зокрема під час обчислення середнього часу до компрометації (МТТС).

Характерною особливістю процесу атаки на мережу є та обставина, що час переходу між кожними з двох хостів є не константою, а випадковою величиною. Відзначимо також, що припущення про те, що ця випадкова величина розподілена за однаковим законом є занадто спрощеною гіпотезою як, наприклад, для марківського процесу. Тому модель напівмарківських процесів більш релевантна для обчислення такого показника кібернадійності як середній час до компрометації. Оцінювання цього показника здійснено методом Монте-Карло на основі марковських ланцюгів, відомого як метод МСМС[4]. Для розрахунку підбиралися апріорні функції розподілу. Найкраще сходження процесу МСМС до квазістаціонарного розподілу МТТС за процедурою Метрополіса-Гастінгса показали функції розподілу Вейбулла.

Висновки

Проведене дослідження показало перспективність застосування SMP-підходу для оцінки кібернадійності SCADA-систем, який поєднує топологію кроків атаки з часовою динамікою їх проходження.

Емпірично підтверджено правосторонню асиметрію розподілу МТТС. При цьому встановлено, що стаціонарний розподіл ймовірностей компрометацій при кібератаках на IT SCADA заданої архітектури може належати до сімейства розподілів типу гамма-функцій.

Список використаних джерел

1. Theodore J. Williams (1992) The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation. Research Triangle Park, NC: Instrument Society of America.

2. S. Tang, Z. Liu and L. Wang, "Power System Reliability Analysis Considering External and Insider Attacks on the SCADA System," *2020 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, Chicago, IL, USA, 2020, pp. 1-5, DOI: 10.1109/TD39804.2020.9299922.
3. Личик, В. В., Гальчинський Л.Ю. (2025). Використання моделі мереж Баєса для раннього оцінювання загроз кібератак об'єкта електроенергетики. Інститут проблем реєстрації інформації НАН України. Реєстрація, зберігання і оброб. даних. 2025, Т. 27, № 2. С. 70-85. URL: DOI: 10.35681/1560-9189.2025.27.2.345591
4. Matthew D. Hoffman & Andrew Gelman, 2011, "*The No-U-Turn Sampler: Adaptively Setting Path Lengths in Hamiltonian Monte Carlo*"

ОЦІНКА РИЗИКУ ПОРУШЕННЯ СТАНУ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО- КОМУНІКАЦІЙНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Кудінов В.А.

*Національна академія внутрішніх справ, м. Київ, Україна,
e-mail: kudinov_va@ukr.net*

У роботі наведено науково-методичний підхід до оцінки ризику порушення стану захищеності інформаційно-комунікаційних систем спеціального призначення Національної поліції України. Цей підхід дозволяє отримати прогностичні значення критичного часу аналізу ситуації та прийняття рішень залежно від інтенсивності подій, пов'язаних із загрозами безпеці ресурсів, інтенсивності включення механізмів запобігання вторгненням, а також від рівня ефективності засобів кіберзахисту та ступеня небезпеки загроз безпеці.

Ключові слова: інформаційно-комунікаційні системи, системи спеціального призначення, ризик, кіберзахист, Національна поліція України.

Вступ

Протягом останнього десятиріччя в Міністерстві внутрішніх справ (далі – МВС) України вживаються заходи щодо створення єдиної інформаційної системи (далі – ЄІС). У пункті 12 Положення про ЄІС МВС наведено перелік функціональних підсистем, які входять до її структури [1].

Серед зазначених функціональних підсистем найбільш потужнішою є інформаційно-комунікаційна система «Інформаційний портал Національної поліції України» (далі – «ПНП») [2]. До складу ПНП входить низка інформаційно-комунікаційних систем спеціального призначення (далі – ІКСП). Пункт 46 Плану реалізації

Стратегії кібербезпеки України серед заходів для досягнення Цілі К.1 (Національна кіберготовність та надійний кіберзахист) передбачає проведення такого заходу, як «запровадження на постійній основі оцінки стану захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на вразливість» [3]. Отже, проведення оцінки ризику порушення стану захищеності ІКССП є актуальною проблемою.

Для зазначених систем нами вже розглянуто проблеми оптимізації розкладу їх роботи [4], мінімізації помилок при функціонуванні у системах управління кібербезпекою [5], алгоритму вибору засобів кіберзахисту та аналізу ефективності їх реалізації [6], оцінки ефективності комплексної системи кіберзахисту інформації за показниками проектної надійності та живучості [7].

Результати та їх обговорення

Одним з найважливіших компонентів ІКССП є модуль управління завданнями (далі – МУЗ), який виконує функції розподілу завдань, що виконуються, між ресурсами, у тому числі завдань, що пов'язані з управлінням безпекою ІССП. Порушення функціонування МУЗ, зокрема, тимчасові затримки під час аналізу критичних ситуацій та прийняття рішень щодо реакції на них, потенційно призводить до порушення або навіть до повного припинення функціонування ІКССП. Тобто важливим аспектом є аналіз параметрів та зниження ризику порушення стану захищеності МУЗ.

Фактично завдання захищеності пов'язане з оцінкою ризику перевищення заданого максимально допустимого часу аналізу ситуації та прийняття рішень у МУЗ ІКССП. Це завдання залежить від двох факторів: ймовірності та наслідків здійснення події перевищення часу аналізу ситуацій та прийняття рішень. Ймовірність перевищення заданого часу функціонально пов'язана зі значеннями верхньої та нижньої меж допустимого інтервалу часу аналізу ситуації та прийняття рішень.

Введемо параметри α_i і β_j – інтенсивності, відповідно, реалізації i -ої загрози безпеці та включення j -ого каналу засобів захисту. Природно, що на захищеність впливає інтенсивність використання засобів захисту, тобто швидкість реакції на ті чи інші небезпечні події. У разі, якщо кількість загроз перевищила потенціал засобів захисту, реалізується атака на ресурси. Далі вводимо нормувальні коефіцієнти K_3 , K_a і параметр R_0 – початковий ризик захищеності, при цьому K_3 – нормувальний коефіцієнт, що визначає ступінь ефективності заходів (подій) захисту інформації; K_a – нормувальний коефіцієнт, що визначає ступінь небезпеки загроз (подій) реалізації несанкціонованого доступу до інформації.

Для оцінки безпеки ІКССП введемо експоненційну функцію ризику:

$$R_{ij}(t) = R_0 e^{-(K_3 \beta_j - K_a \alpha_i)t} \quad (1)$$

Функція $R_{ij}(t)$ є ризиком реалізації i -ої загрози для j -ого каналу захисту цінного ресурсу залежно від часу t . Тоді надійність (локальна захищеність) S_{ij} засобів захисту інформації з погляду запобігання i -ій загрозі за j -им каналом захисту визначається як:

$$S_{ij} = 1 - R_{ij}. \quad (2)$$

Інтегральний рівень надійності засобів захисту ІКССП за j -им каналом захисту S_j оцінюється як:

$$S_j = \prod_{i=1}^n (1 - R_{ij}), \quad (3)$$

де n – кількість загроз безпеці.

Тоді, у свою чергу, інтегральний ризик ІКССП R_j від усіх загроз безпеці для j -ого каналу захисту дорівнює:

$$R_j = 1 - S_j = 1 - \prod_{i=1}^n (1 - R_{ij}). \quad (4)$$

В результаті, загальний інтегральний ризик ІКССП R за всіма загрозами безпеці та всіма каналами захисту може розраховуватися як:

$$R = 1 - \prod_{j=1}^m S_j = 1 - \prod_{j=1}^m \left[\prod_{i=1}^n (1 - R_{ij}) \right], \quad (5)$$

де m – кількість каналів захисту ІКССП.

У загальному вигляді функцію інтегрального ризику системи від часу t можна записати як:

$$R(t) = 1 - \prod_{j=1}^m \left[\prod_{i=1}^n (1 - R_{ij} e^{-(K_3 \beta_j - K_a \alpha_i)t}) \right]. \quad (6)$$

Можливі різні варіанти розвитку ситуацій з погляду безпеки ІКССП, які залежать від співвідношення між параметрами $K_a \alpha_i$ та $K_3 \beta_j$. Якщо $K_a \alpha_i > K_3 \beta_j$, виникає ситуація, коли загальний ризик $R(t)$ стрімко зростає (захищеність падає), і загрози можуть перетворитися на реальну атаку. Навпаки, якщо $K_a \alpha_i < K_3 \beta_j$, то має місце зниження ризику безпеки та зменшується можливість реалізації атак.

Висновки

Таким чином, у роботі сформовано науково-методичний підхід до оцінки загального інтегрального ризику ІКССП Національної поліції України. Цей підхід дозволяє отримати прогнози значення критичного часу аналізу ситуації та прийняття рішень залежно від інтенсивності подій, пов'язаних із загрозами безпеці ресурсів, інтенсивності включення механізмів запобігання вторгненням, а також від рівня ефективності засобів кіберзахисту та ступеня небезпеки загроз безпеці. Це уможливує комплексний аналіз динаміки розвитку вторгнень, процесів відновлення системи та відповідної

зміни рівня кіберзахищеності інформаційно-комунікаційних систем спеціального призначення.

Список використаних джерел

1. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку пріоритетних електронних інформаційних ресурсів її суб'єктів : Постанова Кабінету Міністрів України від 14 листоп. 2018 р. № 1024. URL: <https://zakon.rada.gov.ua/laws/show/en/1024-2018-%D0%BF#Text> (дата звернення: 20.05.2026).
2. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» : Наказ МВС України від 03 серп. 2017 р. № 676. URL: <https://zakon.rada.gov.ua/laws/show/z1059-17#Text> (дата звернення: 20.05.2026).
3. Про рішення РНБО України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України» : Указ Президента України від 01 лют. 2022 р. № 37/2022. <https://zakon.rada.gov.ua/laws/show/37/2022#Text> (дата звернення: 20.05.2026).
4. Хорошко В. О., Кудінов В. А. Оптимізація розкладу роботи інформаційних систем спеціального призначення МВС України. Сучасна спеціальна техніка. 2022. № 1(68). С. 66–83. [https://doi.org/10.36486/mst2411-3816.2022.1\(68\)](https://doi.org/10.36486/mst2411-3816.2022.1(68))
5. Капустян М. В., Кудінов В. А., Хорошко В. О. Мінімізація помилок при функціонуванні у системах управління кібербезпекою. Інформатика та математичні методи в моделюванні. 2022. Том 12, № 1-2. С. 65–72. <https://doi.org/10.15276/imms.v12.no1-2.65>
6. Кудінов В. А. Алгоритм вибору засобів кіберзахисту систем спеціального призначення МВС України та аналіз ефективності їх реалізації. *Шкідливі програми як загрози об'єктам критичної інфраструктури в умовах війни*: матеріали міжвідомч. круглого столу (Київ, 21

- лют. 2023 р.). Київ: Укр. НДІ спец. техн. та судов. експертиз СБУ, 2023. С. 71–74.
7. Кудінов В. А. Оцінка ефективності комплексної системи кіберзахисту інформації інформаційно-комунікаційних систем спеціального призначення за показниками проєктної надійності та живучості. *Протидія кіберзлочинності та торгівлі людьми*: матеріали міжнар. наук.-практ. конф. (Кам'янець-Подільський, 23 трав. 2024 р.). Кам'янець-Подільський: Харківський нац. ун-т внутр. справ, 2024. С. 187–189.

ПОТОКОВИЙ ШИФР НА ОСНОВІ ЛАТИНСЬКИХ КВАДРАТІВ

В.А. Лужецький¹, Т. Г. Кирилашук²

Вінницький національний технічний університет,

Вінниця, Україна,

¹lva.kzi2002@gmail.com, ²kgt0998@gmail.com

У роботі запропоновано поточковий шифр на основі латинських квадратів, особливiсть якого полягає в тому що на кожному кроці шифрування елементи гами та елементи зашифрованого повідомлення формуються як результат керованого вибору застосованого латинського квадрату. Засіб, що реалізує метод шифрування має апаратні витрати, які задовольняють вимоги малоресурсної криптографії.

Ключові слова: шифрування, поточковий шифр, гама, латинські квадрати, апаратний засіб, малоресурсна криптографія, IoT-пристрої.

Поточкові шифри широко застосовуються для захисту інформації в системах реального часу, мережєвих протоколах та IoT-пристроєх. Відомі поточкові шифри базуються на принципі гамування і використовують для створення гами реєстри зсуву з лінійним зворотнім зв'язком. Оскільки, відомі методи зламу гами, що генеруються одним реєстром, то практично використовують кілька реєстрів зсуву, що призводить до певного ускладнення апаратних засобів. Крім того, накладання гами виконується з використанням операції додавання за модулем 2. Для того щоб спростити апаратуру формування гами та ускладнити для зловмисників аналіз процесу накладання гами в доповіді пропонується використовувати набір латинських квадратів [1].

Метод поточкового шифрування

Вхідне повідомлення M подається у вигляді послідовності двобітових елементів:

$$M = m_0, m_1, \dots, m_n.$$

Секретний ключ довжини 64 біти також подається як сукупність двобітових елементів:

$$K = k_1, k_2, \dots, k_{32}.$$

Результатом шифрування є послідовність:

$$C = c_1, c_2, \dots, c_n$$

де c_i – зашифрований двобітовий елемент.

Формування гами здійснюється на основі секретного ключа з наступною заміною обчисленими елементами. Частина гами використовується як певний стан, що забезпечує керування обчисленнями.

Початковий стан $S^{(0)}$ з елементів секретного ключа:

$$S^{(0)} = S_1^{(0)}, S_2^{(0)}, \dots, S_{32}^{(0)} = k_1, k_2, \dots, k_{32}.$$

На кожному кроці шифрування формується новий стан:

$$S^{(i)} = S_1^{(i)}, S_2^{(i)}, \dots, S_{32}^{(i)}.$$

Оновлення стану відбувається шляхом обчислень, що реалізується з використанням чотирьох латинських квадратів згідно з формулою:

$$s_1^{(i+1)} = \begin{cases} L_0(s_1^{(i)}, m_i), & \text{якщо } s_2^{(i)} = 00; \\ L_1(s_1^{(i)}, m_i), & \text{якщо } s_2^{(i)} = 01; \\ L_2(s_1^{(i)}, m_i), & \text{якщо } s_2^{(i)} = 10; \\ L_3(s_1^{(i)}, m_i), & \text{якщо } s_2^{(i)} = 11. \end{cases} \quad (1)$$

Оскільки далі використовується лише один результат обчислень, то для вибору використовуються біти $s_2^{(i)}$.

Таким чином забезпечується динамічна зміна нелінійних перетворень.

Оновлення інших елементів стану відбувається шляхом зсуву попередніх елементів:

$$s_2^{(i+1)} = s_1^{(i)}, s_3^{(i+1)} = s_2^{(i)}, \dots, s_{32}^{(i+1)} = s_{31}^{(i)}.$$

Шифротекст формується шляхом накладання гами на повідомлення:

$$c_i = \begin{cases} L_4(m_i, s_3^{(i)}), & \text{якщо } s_4^{(i)} = 00; \\ L_5(m_i, s_3^{(i)}), & \text{якщо } s_4^{(i)} = 01; \\ L_6(m_i, s_3^{(i)}), & \text{якщо } s_4^{(i)} = 10; \\ L_7(m_i, s_3^{(i)}), & \text{якщо } s_4^{(i)} = 11. \end{cases} \quad (2)$$

Використання набору латинських квадратів забезпечує підвищення стійкості до статистичного аналізу та ускладнює прогнозування елементів послідовності гами. Зміна латинських квадратів у процесі шифрування забезпечує додаткову варіативність перетворень, що також ускладнює злам шифру.

Структура апаратного засобу для потокового шифрування

Структурна схема апаратного засобу, що реалізує запропонований метод потокового шифрування наведений на рис. 1.

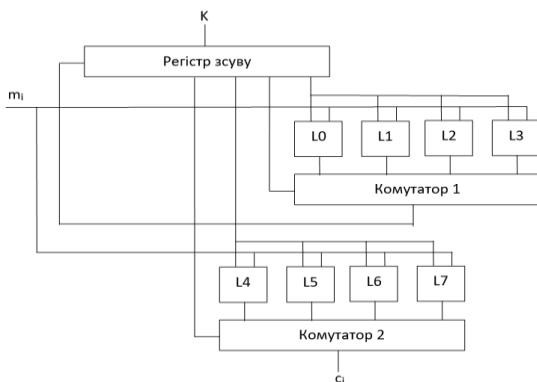


Рис. 1. Структурна схема апаратного засобу

Формування станів $S^{(i)}$ забезпечують регістр зсуву, логічні схеми, що реалізують функції латинських квадратів L0–L3 та Комутатор 1. При цьому виконуються дії, що

описуються формулою (1). Накладання гами здійснюється за допомогою латинських квадратів L4-L7 та Комутатора 2, які реалізують дії згідно з формулою (2).

Таким чином, під час шифрування динамічно змінюються операції формування гами та операції накладання гами на повідомлення.

Оцінювання апаратної складності засобу для потокового шифрування проводилося в умовних одиницях GE для технології 0.18 мкм із використанням бібліотеки стандартних комірок UMCL18G212T3 [2]. Апаратна складність дорівнює 593 GE, яка є меншою за апаратну складність реалізації відомих шифрів Trivium (≈ 2000 GE) [3], Grain (≈ 1300 GE) [3].

Список використаних джерел

1. A. Donald Keedwell and József Dénes *Latin Squares and their Applications*. Elsevier, 2015. 439 с. URL: <https://doi.org/10.1016/c2014-0-03412-0>.
2. Virtual Silicon Inc. 0.18 μm VIP standard cell library tape out ready (part number: UMCL18G212T3). Process: UMC logic 0.18 μm generic II technology. – 2004. – Технічна документація.
3. Martin Feldhofer. Comparison of Low-Power Implementations of Trivium and Grain. eSTREAM, ECRYPT Stream Cipher Project, Report 2007/027, 2007. <http://www.ecrypt.eu.org/stream/papersdir/2007/027.pdf>.

ПОБУДОВА МОДИФІКАЦІЇ ПОСТКВАНТОВОГО МЕХАНІЗМУ ІНКАПСУЛЯЦІЇ КЛЮЧА AJPS-KEM₂

А. В. Ковальчук¹ Д. В. Ядужа²

НН ФТІ, КПІ ім. Ігоря Сікорського, м. Київ, Україна

У роботі виконано модифікацію механізму інкапсуляції ключа AJPS-KEM₂ шляхом зміни класу чисел, що використовується як модуль. Побудовано модифікацію функції Solve, яка застосовується у процедурі декапсуляції AJPS-KEM₂, для класу узагальнених чисел Мерсенна. Отримані результати підтверджують можливість збільшення варіативності параметрів криптопримітиву завдяки використанню арифметики за модулем узагальненого числа Мерсенна.

Ключові слова: механізм інкапсуляції ключа AJPS-KEM₂, числа Мерсенна, узагальнені числа Мерсенна

Вступ

Стійкість найбільш поширених на сьогодні асиметричних криптопримітивів ґрунтується на складності розв'язання таких задач, як факторизація та дискретне логарифмування. Однак П. Шор ще в 1997 році представив алгоритм, з застосуванням якого ці задачі можуть бути ефективно розв'язані в квантовій моделі обчислень. Як наслідок, використання криптопримітивів, стійкість яких ґрунтується на основі задач факторизації та дискретного логарифмування, залишається захищеним тільки через те, що науковцям досі не вдалося побудувати масштабований квантовий комп'ютер. У зв'язку з цим, NIST в 2017 році оголосив конкурс на створення постквантових криптопримітивів, які залишатимуться стійкими до атак з використанням як класичних, так і квантових комп'ютерів.

¹ anastkova-ipt27@lil.kpi.ua

² yadukhadv-ipt@lil.kpi.ua

Одним із учасників конкурсу є механізм інкапсуляції ключа Mersenne-756839, побудований на основі схеми шифрування AJPS-2, особливістю якої є використання арифметики за модулем числа Мерсенна $M_n = 2^n - 1$, $n \in N$ [1]. В роботі [2] побудовано модифікацію схеми AJPS-2, а саме механізм інкапсуляції ключа AJPS-KEM₂, в якій підвищено пропускну здатність схеми шляхом застосування функції Solve у процедурі декапсуляції. Також для збільшення варіативності параметрів криптопримітиву було запропоновано модифікацію схеми AJPS-2, в якій замінено клас чисел Мерсенна на клас узагальнених чисел Мерсенна $GM_{n,m} = 2^n - 2^m - 1$, де $n, m \in N$, $n > m$ [3]. Ця робота спрямована на побудову модифікації механізму інкапсуляції ключа AJPS-KEM₂ для класу узагальнених чисел Мерсенна $GM_{n,m}$.

Побудова модифікації механізму інкапсуляції ключа AJPS-KEM₂ для класу чисел $GM_{n,m}$

Нехай AJPSGM-KEM₂ – модифікація механізму інкапсуляції ключа AJPS-KEM₂ для класу узагальнених чисел Мерсенна, що визначається трьома процедурами: генерація ключів (KeyGen), інкапсуляція ключа (Encap) та декапсуляція ключа (Decap).

Процедура KeyGen. Враховуючи параметр захищеності λ обираються узагальнене число Мерсенна $GM_{n,m}$ та ціле додатне число h , що задовольняють умовам $10h^2 < n \leq 16h^2$ та $h = \lambda$. Рівноймовірно та незалежно із множини лишків за модулем $GM_{n,m}$ обираються два числа F та G , що мають вагу Геммінга h , тобто $Ham(F) = Ham(G) = h$, та число R , для якого виконується $0 < Ham(R) \leq h$. Обчислюється значення $T = F \cdot R - G \pmod{GM_{n,m}}$, та відкритий ключ визначається як $pk := (R, T)$, особистий ключа – $sk := F$, а число G є секретним.

Процедура Encap. Шифротекст $C = (C_1, C_2)$ обчислюється за таким співвідношенням:

$C_1 = A \cdot R + B_1 \pmod{GM_{n,m}}$, $C_2 = A \cdot T - B_2 \pmod{GM_{n,m}}$, де числа A , B_1 та B_2 , обрані із множини лишків за модулем $GM_{n,m}$ з вагою Геммінга h , є інкапсульованим ключем.

Процедура Decap. Отримувач розв'язує рівняння $F \cdot C_1 - C_2 \pmod{GM_{n,m}} = Fx + Gy + z \pmod{GM_{n,m}}$ за допомогою функції Solve. Якщо розв'язок знайдено, то повертається інкапсульований ключ (A, B_1, B_2) , де $A = x$, $B_1 = y$, $B_2 = z$.

Особливості реалізації функції Solve

Реалізація функції Solve, яка використовується при декапсуляції ключа в оригінальному AJPS-KEM₂, ґрунтується на тому, що добуток числа та степеня двійки за модулем M_n є циклічним зсувом цього числа, і, як наслідок, таке множення не змінює вагу Геммінга. На основі цього функція Solve ітеративно обчислює для i -тих, j -тих та k -тих бітів невідомих чисел A , B_1 та B_2 значення

$$\begin{aligned}\Delta_i &= \text{Ham}(W) - \text{Ham}(W - 2^i \cdot F \pmod{M_n}), \\ \Delta_j &= \text{Ham}(W) - \text{Ham}(W - 2^j \cdot G \pmod{M_n}), \\ \Delta_k &= \text{Ham}(W) - \text{Ham}(W - 2^k \pmod{M_n}),\end{aligned}$$

де $W = F \cdot C_1 - C_2 = A \cdot F + B_1 \cdot G + B_2 \pmod{M_n}$, після чого відновлює відповідні біти невідомих чисел таким чином:

$$\begin{cases} 1, \text{ якщо } \Delta_i = h, \text{ або } \Delta_j = h, \text{ або } \Delta_k = 1, \\ 0, \text{ якщо } \Delta_r \approx 0 \ (\Delta_r \neq h), \text{ де } r \in \{i, j, k\}. \end{cases}$$

Функція Solve для узагальнених чисел Мерсенна

Однак в ході дослідження можливості реалізації функції Solve для класу узагальнених чисел Мерсенна було встановлено, що множення числа на степінь двійки за модулем $GM_{n,m}$ не є циклічним зсувом, через що побудова функції Solve потребує модифікації. Далі наведено метод задання функції Solve для нового класу чисел, який використовує жадібну стратегію та ґрунтується на тому, що невідомі числа x , y та z мають вагу Геммінга h , та їх двійкові представлення у співвідношенні для W мають такий вигляд:

$$W = \sum_{i=0}^{n-1} x_i (2^i F) + \sum_{j=0}^{n-1} y_j (2^j G) + \sum_{k=0}^{n-1} z_k 2^k \pmod{GM_{n,m}}.$$

В функції визначається початкова змінна $del := W$, а далі на кожній ітерації для всіх i та j обчислюються значення Δ_i та Δ_j як:

$$\Delta_i = Ham(W) - Ham(W - 2^i \cdot F \pmod{GM_{n,m}}),$$

$$\text{та } \Delta_j = Ham(W) - Ham(W - 2^j \cdot G \pmod{GM_{n,m}}),$$

обирається максимальне значення з усіх Δ_i та Δ_j , виокремлюється відповідний обраному максимуму доданок $2^i \cdot F \pmod{GM_{n,m}}$ або $2^j \cdot G \pmod{GM_{n,m}}$, припускається, що відповідний біт x_i або y_j дорівнює одиниці, та оновлюється значення змінної del як:

$$del := (del - \text{обраний доданок}).$$

Причому на кожній новій ітерації циклу обчислюються Δ для всіх i та j , які ще не були використані в del і цикл повторюється доти, доки не знайдеться потрібна кількість одиниць для чисел x та y . Після чого число z визначається як $z := del$.

Висновки

У роботі досліджено механізм інкапсуляції ключа AJPS-KEM2, що базується на використанні арифметики за модулем числа Мерсенна та функції Solve при декапсуляції ключа. Запропоновано модифікацію AJPSGM-KEM2, побудовану шляхом заміни класу чисел Мерсенна на клас узагальнених чисел Мерсенна, а також побудовано функцію Solve, адаптовану до нового класу чисел. Отримані результати підтверджують можливість коректного перенесення схеми AJPS-KEM2 на клас узагальнених чисел Мерсенна, що забезпечує розширення варіативності параметрів криптопримітиву.

Список використаних джерел

1. A New Public-Key Cryptosystem via Mersenne Numbers / D. Aggarwal, A. Joux, A. Prakash, M. Santha. *Cryptology ePrint Archive*. 2017. URL: <https://eprint.iacr.org/2017/481>.

2. Ferradi H., Naccache D. Integer Reconstruction Public-Key Encryption. *Cryptology ePrint Archive*. 2017. URL: <https://eprint.iacr.org/2017/1231>.
3. Yadukha D. The Forgery Attack on the Post-Quantum AJPS-2 Cryptosystem and Modification of the AJPS-2 Cryptosystem by Changing the Class of Numbers Used as a Module. *Theoretical and Applied Cybersecurity*. 2023. URL: <https://tacs.ipt.kpi.ua/article/view/286166>.

ACTIVE MASKING OF ACOUSTIC DATA LEAKAGE CHANNELS USING MARKOV PROCESSES

V.Palahin, O.Palahina, O.Ivchenko, O.Protsenko,
Y.Heorhii

*Department of Robotic and Telecommunication Systems and
Cybersecurity,
Cherkasy State Technological University, Cherkasy, Ukraine,
v.palahin@chdtu.edu.ua*

Traditional active methods of speech information protection based on white noise or static Babble Noise create excessive psychoacoustic load and are ineffective against modern digital filters and advanced deep learning-based techniques. To overcome these limitations, this paper proposes a method for the dynamic synthesis of speech-like noise using the apparatus of Markov chains. This allows for the real-time generation of a non-stationary jamming signal, significantly increasing the simulation resistance of active speech masking systems

Keywords: technical data protection, acoustic data leakage, babble noise, Markov chains, speech masking, "Plug-and-Protect" concept

Introduction

Ensuring the confidentiality of speech information is a critical aspect of cybersecurity amid the rapid development of technical intelligence equipment. Acoustic and vibroacoustic information leakage channels remain the most vulnerable due to the adversaries' use of laser microphones, stethoscopes, and other devices, which creates an urgent need for active protection methods. Traditional approaches to neutralizing these threats are based on the application of vibroacoustic systems and white or pink noise generators, which create a uniform noise barrier across the frequency spectrum and significantly

reduce the SNR at the input of intercepting receiver devices, thereby complicating the recovery of the useful signal.

Despite its widespread use, traditional energetic masking causes significant acoustic discomfort for those present and can be partially neutralized by modern neural network-based filtering algorithms. This drives the transition to more complex speech-like noise, particularly Babble Noise technology (simulating the chatter of a large crowd) [1, 2]. However, standard recordings of "chatter" are cyclic in nature, which allows intelligent deep learning filters to identify and subtract the noise profile. Furthermore, it fails to ensure adaptability to dynamic changes in the acoustic environment in real time, while still imposing a high psychoacoustic load on the occupants.

The aim of the work is to investigate and develop a speech information protection system through the generation of speech-like jamming, which ensures energetic and linguistic masking of acoustic leakage channels with statistical characteristics closest to real human speech.

Methodology

The problem statement consists in developing algorithmic, software, and hardware support for speech information protection against leakage through acoustic and vibroacoustic channels by designing a method for the synthesis of a dynamic masking jamming signal that minimizes the probability of useful signal recognition against the background of their mixture. The primary task is addressed by forming a speech-like signal through the synthesis of acoustic fragments, the sequence of which is determined by a Markov chain based on the real-time statistical characteristics of the interlocutors' speech. This approach allows for the simulation of natural linguistic transitions and spectral properties of the voice, making the extraction of the useful signal impossible by means of digital processing and AI methods. The solution to this problem involves the following stages:

- synthesis of the jamming signal as a discrete Markov process with a set of states $S = \{s_1, s_2, \dots, s_k\}$, where

each state corresponds to a specific spectral-energy pattern of a speech segment;

- forming the transition probability matrix $P = [p_{ij}]$, where $p_{ij} = P(S_{t+1} = s_j | S_t = s_i)$, to ensure the statistical similarity of the jamming signal to real speech and its resistance to adaptive filtering;
- minimizing the SNR subject to constraints on the integrated radiation power to maintain acoustic comfort within the room;
- software implementation of the state selection procedure S_t for real-time generation of the non-stationary jamming signal.

Comparative analysis demonstrates that within the critical range for maintaining acoustic comfort ($\text{RMS} = 0.1 \dots 0.2$) (Root Mean Square), the proposed Markovian method provides a security gain ranging from +6.3 dB to +7.8 dB compared to white noise. At the minimum jamming level ($\text{RMS} = 0.1$), the stationary profile of white noise is easily neutralized by attack algorithms (Adaptive Spectral Subtraction), leading to an increase in speech recovery quality up to $\text{SNR} = +7$ dB, whereas the Markovian jamming steadily maintains the resulting post-attack SNR in the negative zone (-0.8 dB). As the intensity increases to $\text{RMS} = 0.8$, the efficiency curves converge at the point of -2.8 dB; however, the dynamic alteration of the spectral-energy patterns of the Markov process guarantees higher simulation resistance of the system to spectral subtraction across the entire investigated range.

Analysis of the simulation results confirmed the high simulation resistance of the developed method: unlike white noise, which demonstrates a linear increase in speech recovery quality as its power decreases, the Markovian speech-like jamming effectively protects the original signal due to the high correlation of the statistical structures of the jamming and speech. The practical implementation of the method is based on the autonomous 'Plug-and-Protect' concept, enabling the creation of mobile security devices that do not require complex engineering preparation of the premises. The system software

automatically initializes the model and synthesizes the jamming via acoustic or vibroacoustic transducers immediately after booting, ensuring reliable real-time masking.

Conclusions

The developed Markovian method for speech-like jamming generation provides higher simulation resistance compared to traditional noise, significantly complicating digital speech filtering. The implementation of the algorithms on microprocessor platforms enables the creation of an energy-efficient, mobile device based on the "Plug-and-Protect" concept for reliable active masking of acoustic information. Future research will focus on optimizing the transition probability matrix to adapt to the individual acoustic and linguistic characteristics of the interlocutors' voices in real time.

References

1. N. Mohammadiha and A. Leijon, "Nonnegative HMM for Babble Noise Derived From Speech HMM: Application to Speech Enhancement," in *IEEE Transactions on Audio, Speech, and Language Processing*, vol. 21, no. 5, pp. 998-1011, May 2013, DOI: 10.1109/TASL.2013.2243435
2. InfoMasker: Preventing Eavesdropping Using Phoneme-Based Noise [Electronic resource] / Peng Huang [et al.] // *Proceedings 2023 Network and Distributed System Security Symposium*. –2023. – Mode of access: DOI: 10.14722/ndss.2023.24457

АНАЛІЗ СИСТЕМИ ЗАХИЩЕНОГО ОБМІНУ ПОВІДОМЛЕННЯМИ XCHAT

Навроцька І.

*Національний технічний університет України “Київський
політехнічний інститут імені Ігоря Сікорського”*

У роботі розглянуто новий месенджер XChat, який використовує протокол Juicebox для розподіленого зберігання і відновлення секретних даних з використанням простих PIN-кодів.

Вступ

Однією з проблем сучасних месенджерів є необхідність складних і довгих паролів, які стійкі до сучасних атак. Оскільки довгі паролі з багатьма різними символами незручні для користувачів, виникає потреба в пошуку компромісу між безпекою і зручністю. Juicebox у 2023 р. створили протокол [1], який полягає у використанні складних функцій для перетворення простих PIN-кодів і розділенні й збереженні секретного значення в декількох місцях. У 2026 р. компанія Ілона Маска X Corp. створила новий месенджер на основі протоколу Juicebox.

XChat

Головна ідея протоколу Juicebox полягає в розділенні секрету й збереженні різних частин на різних серверах, які є двох типів: програмні й апаратні, та збираються в конфігурацію. Умовою стійкості є незалежність серверів, тобто коли вони контролюються різними операторами.

Після того як Juicebox припинили розробку свого протоколу й зробили його відкритим у 2025 р., його використали X Corp. У квітні цього року вони зробили реліз свого нового додатку для спілкування XChat [3].

Особливостями цього месенджера є:

- Забезпечення повної конфіденційності й наскрізного шифрування.
- Використання PIN-коду, який ніколи не залишає пристрій і дозволяє безпечно відновити доступ.
- Особистий ключ користувача розділений на частини, які зберігаються на трьох серверах, що обслуговуються компанією X. Два з них апаратні, захищені з допомогою модулів HSM. Для відновлення потрібно 2 з 3, причому хоча б один має бути апаратним.
- Для захисту від онлайн атак, встановлено ліміт у 20 спроб введення PIN-коду. Після перевищення якого доступ до ключових даних стає неможливим.
- Інтеграція Grok, штучного помічника X, безпосередньо в інтерфейс обміну повідомленнями.

Проте XChat має суттєві проблеми. Ключі статичні, немає механізму їхнього оновлення, тому не забезпечується ні пряма, ні зворотня секретність. Також зазначено, що метадані не шифруються. Все, що надсилається Grok, обробляється поза межами зашифрованого каналу, і хоча сам чат залишається зашифрованим, все, що бачить ШІ, більше не захищене наскрізним шифруванням. Цікавим є і те, що, можливо, використання зашифрованого чату залежить від взаємодії між користувачами і статусу їхнього облікового запису в X. Це включає взаємну підписку, історію попередніх приватних повідомлень, прийняття запитів на зашифровані приватні повідомлення або спільне членство в Premium Business/Organization. Важливим є і те, що зараз не забезпечується постквантова стійкість. Немає властивості заперечуваності, оскільки кожне повідомлення підписується, щоб підтвердити від кого воно.

Ще одним недоліком є те, що PIN-код складається лише з 4 цифр, що дає 10^4 різних значень і є 20 спроб, щоб ввести правильне значення. В таких умовах успіх онлайн

атаки складатиме 0.2 відсотка. Якщо зловмисник матиме доступ до інформації, коли користувач знову авторизується (введе правильний PIN і скине лічильник спроб), він міг би перевірити певну кількість, яка не перевищує ліміт і зачекати авторизації та спробувати знову вгадати PIN, але це збільшує успіх залежно від частоти й кількості входів користувача. Проте якщо зловмисник володіє деякою додатковою інформацією про користувача, він може перевірити більш особисті або тривіальні варіанти PIN-коду. І хоча 20 спроб не покривають усі варіанти, але дозволяють перебрати ті, які здаються найбільш імовірними. Тому такий ліміт дає зловмиснику більші шанси на успіх.

Суттєва проблема XChat полягає в тому, що всі три сервери контролюються X і фактично безпека еквівалентна одному серверу. Під час офлайн атаки зловмиснику не треба отримувати доступ до кожного з них, достатньо контролювати оператора. Отримавши доступ він може перейти до перебору PIN-коду, і головним захистом тут має стати складна функція виведення ключів (KDF). За рекомендаціями Juicebox, швидше за все, використовується Argon2id [2], складність якої залежить від обсягу пам'яті, кількості ітерацій і ступеня паралелізму, що робить атаки методом грубої сили ресурсомісткими. Оскільки XChat гарантує, що PIN не покидає пристрій користувача, то обчислення там і відбуваються, тому параметри Argon2id мають бути збалансованими, щоб не сповільнювати роботу додатка на звичайному смартфоні, але й не дозволити зловмиснику провести ефективну атаку.

Зараз X Chat підтримується лише на iOS, яка має більш оптимізовану архітектуру порівняно з Android, особливо з бюджетними пристроями. Можна припустити, що з огляду на більші можливості пристроїв Apple були обрані вищі параметри, однак це невідомо, а PIN лише з 4 цифр все одно залишається слабким.

У майбутньому розробники планують зробити XChat доступним і на Android, що створить додаткову проблему, бо на бюджетних пристроях параметри доведеться знизити, але тоді безпека користувача залежатиме від можливостей

його смартфона. Також можливе і рекомендоване збільшення довжини PIN-коду.

Висновки

Аналіз XChat показує, що він є незахищеним. Компрометація статичних ключів дає зловмиснику доступ і до минулих, і до майбутніх сесій. Відсутність наскрізного шифрування під час запитів до Grok може порушувати приватність користувачів. Централізація X всіх серверів, між якими розподілено секрет, суперечить ідеям протоколу Juicebox і спрощує атаки для зловмисників. PIN-код лише з 4 цифр і 20 спроб введення також сприяють можливим атакам.

Список використаних джерел

1. Trapp, N., Ongaro, D., Juicebox Protocol: Distributed Storage and Recovery of Secrets Using Simple PIN Authentication, 2023. URL: <https://eprint.iacr.org/2023/1597>
2. Biryukov, A., Dinu, D., Khovratovich, D., Josefsson, S., Argon2 memory-hard function for password hashing and proof-of-work applications, RFC Editor, 2021. URL: <https://www.rfc-editor.org/info/rfc9106>
3. XChat: Private Messaging, 2026. URL: <https://xchats.chat>

ВИБІР АЛГОРИТМІВ І СТРУКТУР ДАНИХ ДЛЯ БЕЗПЕЧНОГО ЗБЕРІГАННЯ ТА ОБРОБКИ МЕТАДАНИХ В ІОТ-СИСТЕМАХ НА ОСНОВІ БЛОКЧЕЙНУ ETHEREUM

Зарудний І. С., Любчак В. О.

*Сумський державний університет, м. Суми, Україна,
i.zarudnyi@elit.sumdu.edu.ua
v.liubchak@dcs.sumdu.edu.ua*

Розглянуто підхід до вибору алгоритмів і структур даних для безпечного зберігання та обробки метаданих в ІоТ-системах із використанням Ethereum. Увагу зосереджено на Merkle-Patricia Trie, Multi-State MPT, батчуванні транзакцій та гібридному ончейн/офчейн зберіганні. Запропоновано модель взаємодії ІоТ-пристроїв, edge-вузлів і смарт-контрактів для забезпечення цілісності та верифікованості метаданих.

Ключові слова: Інтернет речей; Ethereum; блокчейн; метадані; Merkle-Patricia Trie; смарт-контракти; кібербезпека.

Вступ

Розвиток Інтернету речей супроводжується зростанням кількості службових даних, що описують стан сенсорів, часові мітки, ідентифікатори пристроїв, журнали доступу та параметри взаємодії між вузлами. Ці метадані необхідні для підтвердження походження інформації, контролю цілісності та підтримання узгодженого стану в розподіленому середовищі.

Централізовані моделі зберігання залишаються вразливими до компрометації серверів, підробки записів і несанкціонованої зміни журналів. Ethereum дає змогу застосувати децентралізовану модель довіри, однак пряме розміщення всіх ІоТ-даних у блокчейні є неефективним

через вартість gas, обмежену пропускну здатність і затримки транзакцій.

Метою роботи є узагальнення принципів вибору алгоритмів і структур даних для безпечної та ресурсно ефективної обробки IoT-метаданих у системах, що використовують Ethereum як рівень верифікації.

Основна частина

Базовою структурою зберігання стану в Ethereum є Merkle-Patricia Trie (MPT), яка поєднує префіксне дерево та мерклеву хеш-структуру. Її перевагою є можливість формувати компактні докази включення: вузол перевірки може підтвердити наявність або коректність запису без отримання всієї бази стану. Для IoT-середовищ це важливо, оскільки кінцеві пристрої мають обмежену пам'ять, енергоспоживання й обчислювальні ресурси.

Рациональний підхід полягає у тому, що IoT-пристрій формує канонічний запис метаданих і підписує його, edge-шлюз виконує агрегацію та батчування, а в Ethereum фіксується не повний запис, а хеш або корінь верифікаційної структури. Повні метадані можуть зберігатися поза ланцюгом, але їхня достовірність перевіряється через кореневий хеш, опублікований у блокчейні.

Ефективність MPT значною мірою залежить від схеми формування ключів. Використання стабільного префікса пристрою та часової сегментації зменшує фрагментацію дерева, кількість змінених вузлів і число операцій читання/запису стану. Це безпосередньо впливає на gas-вартість транзакцій і швидкість обробки подій.

Для сценаріїв із багатьма запитами доцільним є використання Multi-State Merkle Patricia Trie, що дає змогу спільно використовувати проміжні вузли між різними знімками стану. Для інфраструктурних компонентів, таких як індексатори та аналітичні вузли, перспективним є GPU-прискорення побудови й перевірки гілок MPT. Такі оптимізації не змінюють ончейн-модель довіри, але зменшують затримки позаланцюгової обробки.

Запропонована архітектура передбачає розподіл функцій між трьома рівнями: IoT-пристрій виконує мінімальні криптографічні операції; edge-вузол агрегує записи, формує докази та готує транзакції; смарт-контракт фіксує кореневі хеші й забезпечує перевірку політик доступу. Такий поділ знижує навантаження на периферійні пристрої та зменшує обсяг даних, що передаються у блокчейн.

Висновки

Вибір структур даних є визначальним чинником ефективної інтеграції Ethereum з IoT-системами. Merkle-Patricia Trie забезпечує криптографічну верифікацію та інкрементальне оновлення стану, однак потребує оптимізації схеми ключів, батчування та перенесення частини обробки на edge-рівень.

Найбільш доцільною для ресурсно обмежених IoT-сценаріїв є гібридна модель, у якій повні метадані зберігаються поза блокчейном, а в Ethereum публікуються лише хеші або корені верифікаційних структур. Застосування MSMPT і апаратного прискорення на інфраструктурних вузлах може додатково підвищити продуктивність багато-запитних сценаріїв.

Подальші дослідження доцільно спрямувати на формальну оцінку gas-витрат для різних схем ключів, моделювання навантаження у гетерогенних IoT-мережах і перевірку стійкості оптимізованих структур до атак на рівні стану та доказів включення.

Список використаних джерел

1. Zarudnyi I., Liubchak V. Methods and information technologies for secure integration of Ethereum blockchain with Internet of Things (IoT). *Cybersecurity: Education, Science, Technique*. 2025. Vol. 4(28). P. 104–114. DOI: 10.28925/2663-4023.2025.28.758.
2. Mardiansyah V., Muis A., Sari R. F. Multi-State Merkle Patricia Trie (MSMPT): High-performance data structures for multi-query processing based on lightweight blockchain.

- IEEE Access. 2023. Vol. 11. DOI: 10.1109/ACCESS.2023.3325748.
3. Deng Y., Yan M., Tang B. Accelerating Merkle Patricia Trie with GPU. Proceedings of the VLDB Endowment. 2024. Vol. 17(8). P. 1856–1869. DOI: 10.14778/3659437.3659443.
 5. Zhang L., Zhao Q., Liu M. Towards efficient integration of blockchain for IoT security. Future Generation Computer Systems. 2021. Vol. 116. P. 215–228. DOI: 10.1016/j.future.2020.10.024.
 6. Ethereum Foundation. Merkle-Patricia Trie data structure overview. URL: <https://ethereum.org/en/developers/docs/data-structures-and-encoding/patricia-merkle-trie/>.

КАРТУВАННЯ ПОЛІГОНІВ ТПВ ЗА СПЕКТРАЛЬНИМИ ІНДЕКСАМИ ДЗЗ

С. Ю. Даншина

*Національний аерокосмічний університет
«Харківський авіаційний інститут»,
Харків, Україна, s.danshyna@khai.edu*

Систематизовано інформацію про спектральні індекси для дослідження полігонів ТПВ за знімками Sentinel-2. На прикладі полігону «Правобережний» проведено порівняльний аналіз різних способів візуалізації території для вирішення завдань визначення меж звалища та оцінки стану прилеглих земель.

Ключові слова: відкрити джерела інформації, моніторинг, Sentinel-2 L2A, спектральні індекси.

У контексті реалізації Цілей сталого розвитку питання екологічної безпеки та раціонального поводження з відходами набувають особливої актуальності. Однією з найгостріших проблем залишається стан полігонів ТПВ, які значно впливають на довкілля та якість життя населення. Тому ефективне управління інфраструктурою поводження з ТПВ потребує застосування геоінформаційних технологій, здатних забезпечити об'єктивну оцінку подібних об'єктів, ґрунтуючись на актуальних просторово-розподілених даних.

Об'єктом дослідження обрано полігон ТПВ «Правобережний» (м. Дніпро). Виявлення та окреслення меж цього об'єкта методом прямого візуального дешифрування є ускладненим. Його розташування в степовій зоні, нерівномірна морфологія, неоднорідний склад відходів і високе техногенне навантаження призводять до того, що ключові дешифрувальні ознаки полігону мають переважно непрямий характер. За таких умов виникає потреба переходу від візуального аналізу до автоматизованих методів, зокрема розрахунку спектральних індексів.

Найпоширенішими індексами, які використовують для ідентифікації та моніторингу сміттєзвалищ, є NDVI (нормалізований диференційний вегетаційний індекс) і NDWI (нормалізований диференційний водний індекс). Також для ідентифікації звалищ використовують індекс DDI (індекс ідентифікації звалищ). Він поєднує спектральну інформацію про стан рослинного покриття через SAVI – індекс рослинності, скоригований на вплив ґрунту, що є модифікацією NDVI, і розраховується:

$$DDI = SAVI \cdot Entropy = \frac{(NIR - RED)(1 + L)}{(NIR + RED + L)} Entropy, \quad (1)$$

де **NIR** – діапазон інфрачервоного спектра або спектральний канал B08; **RED** – діапазон червоного спектра або спектральний канал B04; **L** – коефіцієнт корекції фону рослинності (дорівнює 0,5); **Entropy** – статистична міра випадковості (ентропія).

Ентропія як характеристика текстури вхідного зображення визначається на основі матриці спільного розташування рівнів сірого (GLCM), яка фіксує кількість співвідношень спільної появи між пікселем та його сусідніми пікселями для заданого напрямку та відстані.

Забруднені території зазвичай характеризуються нижчими значеннями SAVI та вищими значення ентропійної текстури. Відповідно, індекс DDI побудовано так, щоб набувати високих значень у межах полігонів, що зазнають техногенного впливу.

Для розрахунку індексу DDI вихідні канали Sentinel-2 (B04 і B08) було імпортовано в QGIS, де за допомогою калькулятора растру спершу обчислено SAVI відповідно до формули (1).

Значення індексу SAVI варіюють від –0,147 до 1,239, що вказує на високу гетерогенність поверхневого покриття. Найнижчі значення (–0,147...0,075) спостерігаються у північно-західній частині знімка, де розташоване діюче «тіло» полігону та відсутня рослинність. Проміжні значення (0,076–0,287) характерні для схилів і частково

стабілізованих ділянок по периферії, де відбувається фрагментарне поновлення трав'янистої рослинності.

Наступним етапом було обчислення ентропії за допомогою модуля GRASS r.texture, доступного через Processing Toolbox. Параметри обчислення: **Input raster** – SAVI-растр; **Statistics to calculate** – entropy; **GLCM matrix size** – вікно 3×3; **Distance** – 1; **Maximum Number of Categories** – 64. У полі *Entropy* зазначено шлях для збереження вихідного шару. Інші статистики вимкнено.

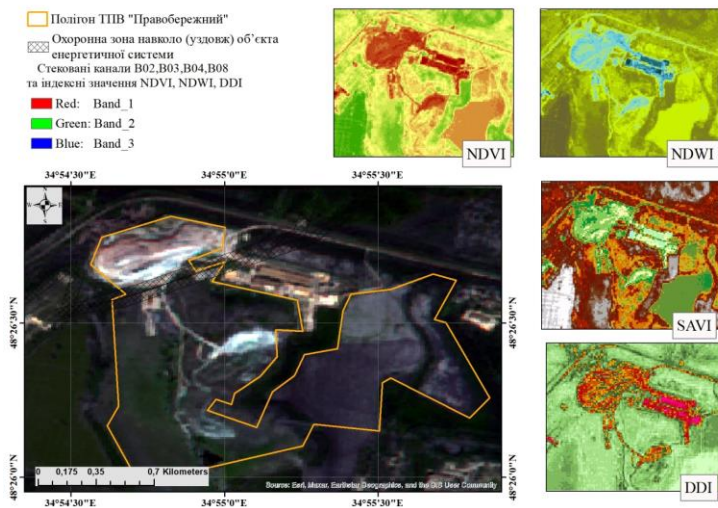


Рис. 1. Картування полігону ТПБ «Правобережний» за даними ДЗЗ: True Color, NDVI, NDWI, SAVI, DDI

Поеднавши створений шар ентропії та SAVI у Raster Calculator, побудовано зображення з використанням індексу DDI. Діапазон значень DDI від $-0,342$ до $-0,147$ відповідає зоні активного складування відходів у північно-західній частині знімка. Такі значення характерні для територій з інтенсивним складуванням ТПБ, де спостерігається слабка або фрагментарна вегетація у поєднанні з високою неоднорідністю покриття, спричиненою перемішуванням сміття, ґрунту, промислових

відходів і технічного засипання. До цієї категорії також належать асфальтовані покриття, частина ґрунтових доріг і ділянки будівництва, які мають подібні спектрально-текстурні характеристики.

Показники нижче $-0,341$ охоплюють території з рослинністю різного рівня фотосинтезуючої активності. Значення в межах $-0,341 \dots -0,430$ можна трактувати як ознаку деградованої, пригніченої рослинності.

Отже, дані ДЗЗ є ефективним джерелом інформації для прийняття управлінських рішень при забезпеченні сталого розвитку. Використання спектральних індексів при аналізі полігонів ТПВ забезпечує: простоту та швидкість отримання результатів; високу точність визначення техногенний об'єктів; стабільність результатів незалежно від атмосферних умов; розширення спектру завдань моніторингу.

ЗАСТОСУВАННЯ ЗК-ПРОТОКОЛІВ ДЛЯ ДОКАЗУ БЕЗПЕЧНОСТІ ТА КОРЕКТНОСТІ НАВЧАЛЬНИХ ДАНИХ

Іван Кудін

*Національний технічний університет України «КПІ імені
Ігоря Сікорського»*

Ключові слова: ЗК-протоколи, машинне навчання, dataset, гомоморфне шифрування, прозорість даних, спам-фільтр.

Актуальність

Якість навчальних даних безпосередньо визначає ефективність, коректність і безпеку систем штучного інтелекту. Водночас реальні dataset часто є комерційною таємницею або містять чутливу інформацію, тому їх повне розкриття є небажаним. Це знижує довіру користувачів до моделей, особливо у сферах кібербезпеки, медицини та фільтрації небажаного контенту.

Для задач виявлення аномалій у мережевому трафіку та фільтрації спаму відкриті набори даних мають істотні обмеження: застарілість, дублікати, неповну відповідність сучасним атакам і невідповідність конкретній інфраструктурі. В ідеалі навчальні дані мають збиратися саме в середовищі, де модель буде застосована, але тоді виникає потреба доводити їхню якість без розкриття змісту.

Мета і постановка задачі

Метою роботи є побудова схеми, яка дає змогу довести наявність у закритому dataset заданих статистичних властивостей, важливих для безпечного й коректного навчання моделі, без передавання самого dataset верифікатору.

Задача формулюється як ЗК-доведення твердження про дані: власник dataset (prover) повинен переконати verifier,

що набір даних D задовольняє предикат безпеки $P(D)=1$, не розкриваючи D та не надаючи доступу до окремих записів. Новизна запропонованого підходу полягає у формулюванні задачі перевірки dataset як задачі ZK-доведення статистичних властивостей навчальних даних. Такий підхід переносить акцент із розкриття набору даних на доказ його релевантних властивостей.

Практичне значення полягає у можливості застосування протоколу в середовищах, де відкриття dataset є небажаним: корпоративні системи кібербезпеки, антиспам-рішення, медичні або фінансові системи, а також аудит моделей машинного навчання.

Ідея та формальний опис запропонованого протоколу

Нехай D - приватний набір даних, φ - статистична функція або набір функцій, що характеризують якість даних, τ - порогові значення, а $P(D)$ - предикат прийнятності dataset. У загальному вигляді:

$$P(D)=1 \Leftrightarrow \varphi(D) \in \Omega(\tau),$$

де $\Omega(\tau)$ - допустима область значень статистик. Наприклад, для задачі спам-фільтрації $\varphi(D)$ може включати частку спам/не-спам повідомлень, частоти ознак, ентропію словника, межі дисбалансу класів та інші агреговані характеристики.

Нехай S_g – повністю гомоморфний шифр [14], тобто для довільних $Y_1 = S_g(X_1, K), Y_2 = S_g(X_1, K)$ виконується рівняння $Y_1 \circ Y_2 = S_g(X_1 \circ X_2, K)$, де $\circ$ - будь-який оператор (сума, множення, і т.п.).

Це дозволяє виконувати довільні обчислення над зашифрованими даними (шифротекстом) без необхідності їх попереднього розшифрування. В принципі, гомоморфні шифри четвертого покоління можуть обчислювати будь-яку функцію f над зашифрованими даними, в тому числі як f можна розглядати будь-яку статистику. Тоді із застосуванням такого гомоморфного шифру ідея побудови ZK протоколу для доведення статистичних властивостей датасету без його розкриття стає практично тривіальною:

ми, як верифікатор обираємо потрібну статистику над датасетом та випадковий ключ. Prover виконує цю операцію над зашифрованим на нашому ключі датасеті та надає нам результат. Ми розшифровуємо дані та порівнюємо з еталонними.

Наведемо простий приклад. Нехай ми хочемо переконатись, що наш датасет є числом D , більшим ніж деяке A : $D > A$. Verifier генерує випадковий запит A . Prover обирає випадковий ключ K_1 для S_g обчислює та надсилає $S_g(K_1, A)$ та $S_g(K_1, D)$ (на цей момент він не знає **що саме буде перевіряти** Verifier відносно A та фіксує свій вибір). Verifier повідомляє, яку саме операцію (параметр функції) йому потрібно обчислити від D та A (в нашому випадку – різницю $D - A$. Prover обчислює $S_g(K_1, D - A)$ та надсилає його Verifier. Verifier обчислює $S_g(K_1, A) - S_g(K_1, D)$ та перевіряє рівність $S_g(K_1, D - A) = S_g(K_1, D) - S_g(K_1, A)$.

У доповіді розглянуто базові алгоритми класифікації: наївний Байєс, нейронні мережі, дерева рішень, k -найближчих сусідів, випадковий ліс, метод опорних векторів, логістичну регресію та підходи на основі скінченних автоматів. Для задач кібербезпеки особливо важливо, що точність цих методів залежить не лише від алгоритму, а й від релевантності та репрезентативності навчальних даних.

Для попереднього аналізу трафіку та побудови спам-фільтра практично зручним є наївний Байєс: він простий, швидкий і може працювати як базовий метод для proof-of-concept. Водночас навіть простий класифікатор потребує якісного dataset, тому перевірка статистичних властивостей даних є окремою задачею довіри.

Запропоновану схему апробовано на тестовому наборі електронних листів для навчання спам-фільтру. У proof-of-concept поєднано байєсівський класифікатор та ZK-підхід на основі гомоморфного шифрування. Перевіряються не самі листи, а агреговані статистики, які характеризують придатність dataset для навчання. Практична цінність підходу полягає в тому, що власник моделі може підтвердити якість і безпечність даних, не розкриваючи

комерційно або безпеково чутливу інформацію. Користувач або аудитор, своєю чергою, отримує перевірювані підстави довіряти dataset.

Висновки

Якісні навчальні дані є основою надійної роботи алгоритмів машинного навчання, але саме вони часто залишаються конфіденційними. Запропонована схема застосування ZK-протоколів і гомоморфного шифрування дає змогу доводити безпечність та коректність dataset через перевірку статистичних властивостей без розкриття самих даних.

Подальший розвиток підходу доцільно пов'язати з оптимізацією обчислень над гомоморфно зашифрованими даними, вибором статистик для різних типів ML-задач та експериментальною оцінкою швидкодії протоколу на реальних наборах даних.

ЗМІСТ

<i>Програмний комітет конференції TACS-2026.</i>	
Передмова	3
<i>Щербина М. Ю., Венгерський П. С.</i>	
Модель загроз MITRE EMB3D і матриця загроз MITRE ESTM	4
<i>Vasyl Ustymenko, Oleksandr Pustovit and Tymofii Svyrydenko</i>	
On new Postquantum stream ciphers defined in terms of temporal algebraic graphs	8
<i>Ланде Д.В., Даник Ю.Г.</i>	
Конфліктологія автономного ШІ в державних цифрових екосистемах: ризики домінування та умови структурної стійкості	12
<i>Oleg Gutik, Yurii Kuzbyt</i>	
On the modified multi-diagonal cipher	19
<i>Pronin Y.V., Zubok V.Y.</i>	
Search and Seizure as a Cyber-Physical Operation: A Conceptual Model for Ensuring the CIA Triad of Digital Evidence	23
<i>Цирульнев Ю.Б.</i>	
Кіберрезильєнтність улектронних архівів з LL/CL-архітектурою	28
<i>Педунов А.Є., Ільїн М.І.</i>	
Методи детектування бокового переміщення в active directory: аналіз ефективності Elastic Security та розробка підходів до модифікації C2-фреймворків	32
<i>Новіков О.М., Ільїн М.І., Степочкіна І.В., Дудуладенко В.М.</i>	
Моделювання кібератак на систему вимірювання установки аеродинамічної левітації	35
<i>Корж Н.С., Яковлев С.В.</i>	
Матричне представлення умовних диференціальних ймовірностей алгебраїчних перетворень шифру NORX	46
<i>Свобода І.М., Ланде Д.В.</i>	
Порівняння MAI, MAM і підходу «Від середнього рівня» для систем підтримки прийняття рішень у кібербезпеці на основі великих мовних моделей	51

Рибак О.О., Ланде Д.В.

Багатоагентський семантичний аналіз для підтримки прийняття рішень у сфері кібербезпеки 55
Світличний В.А.

Проблеми вилучення криптовалют у протидії кіберзлочинності 58

Качинський А.Б., Ланде Д.В., Іванюта С.П.

Системний підхід до моделювання інформаційно-психологічних операцій за допомогою генеративного штучного інтелекту 62

Redko-Shpak R.A., Stopochkina I.V.

Security of agentic applications in the tasks of critical infrastructure enterprises 68

Щур Н.О., Ковальчук О.М.

Типові помилки реалізації криптографічних механізмів в інформаційно-комунікаційних системах 72

Даник Ю.Г., Лабунець В.О., Рябко С.І.

Кібербезпека систем віддаленого керування роботизованими комплексами та БПЛА у системах протидірової оборони 76

Швайка О.А., Носок С.О.

Моделі виявлення вразливостей програмного забезпечення 80

Шибачев Г.Д., Гальчинський Л.Ю., Носок С.О.

Адаптивна еволюція довіри у федеративних системах захисту мікромереж 84

Смирнов С.А., Полуциганова В.І.

Розподіл ресурсів кіберзахисту на основі моделі гри полковника Блотто та виробничої функції Кобба–Дугласа 95

Худоба А.Г., Коломицев М.В.

Комплексний аналіз цифрових артефактів для реконструкції WINDOWS-інциденту 101

Казміревський В.В.

Ортогональний Merkle-ліс для зменшення композиційності локальних колізій у деревоподібних геш-функціях 105

<i>Терлецький О.І., Трушевський В.М.</i> Виявлення аномалій акустичної імпульсної відповіді для моніторингу вторгнень у приміщення	113
<i>Грицишин О.О., Трушевський В.М.</i> Оптимізація методу згладжених частинок у застосуванні до задач критичної інфраструктури	118
<i>Личик В.В., Гальчинський Л.Ю.</i> Кількісна оцінка поглинальної здатності кіберстійкості IT-мережі енергетичного об'єкта	122
<i>Мельник М.М., Чешун В.М., Чешун Д.В., Олексюк Д.А.</i> Адаптивна модель реагування на кіберінциденти з використанням платформ WAZUH, ELK STACK, THEHIVE	126
<i>Гуцалюк М.В.</i> Правові аспекти імплементації другого додаткового протоколу до конвенції про кіберзлочинність	130
<i>Уманський Є.А., Щербина М.Ю.</i> Прототип системи виявлення закладних пристроїв за допомогою SDR-приймача	136
<i>Гавловський В.Д.</i> Аналіз стану протидії кіберзлочинності як індикатор ефективності кібербезпеки	140
<i>Снігур А.Ю., Гальчинський Л.Ю.</i> Оцінювання надійності енергетичного об'єкта при проведенні кібератак на основі моделі напівмарковських процесів	144
<i>Кудінов В.А.</i> Оцінка ризику порушення стану захищеності інформаційно-комунікаційних систем спеціального призначення національної поліції України	147
<i>Лужецький В.А., Кирилащук Т.Г.</i> Потоковий шифр на основі латинських квадратів	153
<i>Ковальчук А. В. Ядуха Д. В.</i> Побудова модифікації постквантового механізму інкапсуляції ключа AJPS-KEM2	157
<i>Palahin V., Palahina O., Ivchenko O., Protsenko O., Heorhii Y.</i> Active masking of acoustic data leakage channels using markov processes	162

Навроцька І.

Аналіз системи захищеного обміну повідомленнями XChat 166

Зарудний І.С., Любчак В.О.

Вибір алгоритмів і структур даних для безпечного зберігання та обробки метаданих в IoT-системах на основі блокчейну Ethereum 170

Данишина С.Ю.

Картування полігонів ТПВ за спектральними індексами ДЗЗ 174

Кудін І.

Застосування ZK-протоколів для доказу безпечності та коректності навчальних даних 178

Міністерство освіти і науки України
Національний технічний університет України "Київський
політехнічний інститут імені Ігоря Сікорського"
Навчально-науковий фізико-технічний інститут

THEORETICAL AND APPLIED CYBERSECURITY

Матеріали IV Всеукраїнської
науково-практичної конференції

Випуск 4

Всі матеріали надані в авторській редакції

Підп. до друку 30.09.2026. Формат 60x84^{1/16}. Папір офс. Гарнітура Times.
Спосіб друку – ризографія. Ум. друк. арк. 8,1. Обл.-вид. арк. 24,36. Наклад
100 пр. Зам. № 15-200.

ТОВ "Інжиніринг" ISBN 978-617-8180-08-9