МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
UNIVERSITY OF THE NATIONAL EDUCATION COMMISSION, POLAND
TECHNICAL UNIVERSITY IN PRAGUE, CZECH REPUBLIC
Наукова школа “Кібербезпека”
Навчально-науковий інститут Кібербезпеки та захисту інформації ДУІКТ
Кафедра кібербезпеки ЗУНУ
ГО «АСОЦІАЦІЯ СПЕЦІАЛІСТІВ КІБЕРБЕЗПЕКИ»
ГО «АВТОМАТИЗАЦІЯ І КІБЕРБЕЗПЕКА»

ITSec-2025

Безпека інформаційних технологій

МАТЕРІАЛИ

XIV Міжнародної науково-технічної конференції

22-24 травня 2025
м. Тернопіль (Україна)

УДК [003.26+004+519.816]:004.056:65(063)

ITSec: Безпека інформаційних технологій: матеріали XIV Міжнар. наук.-техн. конф., м. Тернопіль, 22-24 трав. 2025 р. Тернопіль-Київ: ЗУНУ-ДУІКТ, 2025. 243с.

Збірник містить тексти наукових матеріалів доповідей та тез учасників XIV міжнародної науково-технічної конференції «ITSec: Безпека інформаційних технологій». Основною метою конференції є ознайомлення з сучасними досягненнями та висвітлення результатів наукових досліджень з усіх аспектів кібербезпеки та захисту інформації.

Призначено вченим, інженерам, аспірантам наукових спеціальностей 05.13.21 – Системи захисту інформації, 21.05.01 – Інформаційна безпека держави, здобувачам вищої освіти спеціальності 125 – Кібербезпека та захист інформації, а також всім зацікавленим.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

- Міністерство освіти і науки україни
- Державний університет інформаційно-комунікаційних технологій
- Західноукраїнський національний університет
- University of the National Education Commission, Poland
- Technical University in Prague, Czech Republic
- Наукова школа “Кібербезпека”
- Навчально-науковий інститут Кібербезпеки та захисту інформації ДУІКТ
- Кафедра кібербезпеки ЗУНУ
- ГО «Асоціація спеціалістів кібербезпеки»
- ГО «Автоматизація і кібербезпека»

Почесні голови XIV Міжнародної науково-технічної конференції «Безпека інформаційних технологій: ITSEC-2025»

Оксана ДЕСЯТНЮК, доктор економічних наук, професор, ректор Західноукраїнського національного університету;

Володимир ШУЛЬГА, доктор історичних наук, професор, ректор Державного університету інформаційно-комунікаційних технологій.

Співголови XIV Міжнародної науково-технічної конференції «Безпека інформаційних технологій: ITSEC-2025»

Олександр КОРЧЕНКО, член-кореспондент НАН України, доктор технічних наук, професор, перший проректор Державного університету інформаційно-комунікаційних технологій, голова ГО «Асоціація спеціалістів кібербезпеки»;

Микола ДИВАК, доктор технічних наук, професор, проректор з наукової роботи Західноукраїнського національного університету.

Склад Програмного комітету XIV Міжнародної науково-технічної конференції «Безпека інформаційних технологій: ITSEC-2025»

Ірина УДОВИК, кандидат технічних наук, професор, декан факультету інформаційних технологій, Національного технічного університету «Дніпровська політехніка»;

Ігор ЯКИМЕНКО, кандидат технічних наук, доцент, декан факультету комп'ютерних інформаційних технологій Західноукраїнського національного університету;

Євгенія ІВАНЧЕНКО, доктор технічних наук, професор, директор навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій;

Libor DOSTALEK, Technical University in Prague, Czech Republic;

Mikolaj KARPINSKI, Professor, Doctor of Science, Head of Department of Software Engineering, University of the National Education Commission, Poland;

Oleksandr KUZNETSOV, eCampus University, Italy;

Bogdan ADAMYK, Aston Business School, Aston University, UK;

Wolfgang DORNER, Deggendorf Institute of Technology, Germany;

Olga TORSTENSSON, Halmstad University, Sweden;

Jan OWEDYK, Kujawy and Pomorze University in Bydgoszcz, Poland;

Юлія ХОХЛАЧОВА, кандидат технічних наук, професор, професор кафедри штучного інтелекту Державного університету інформаційно-комунікаційних технологій;

Василь ЯЦКІВ, доктор технічних наук, професор, завідувач кафедрою кібербезпеки Західноукраїнського національного університету;

Юлія ТКАЧ, кандидат технічних наук, доктор педагогічних наук, професор, завідувач кафедрою

кібербезпеки та математичного моделювання Національного університету «Чернігівська політехніка»;

Петро ВЕНГЕРСЬКИЙ, доктор фізико-математичних наук, професор, завідувач кафедрою кібербезпеки Львівського національного університету ім. Івана Франка;

Михайло КАСЯНЧУК, доктор технічних наук, професор, професор кафедри кібербезпеки Західноукраїнського національного університету.

Співголови Організаційного комітету XIV Міжнародної науково-технічної конференції «Безпека інформаційних технологій: ITSEC-2025»

Ігор ЯКИМЕНКО, кандидат технічних наук, доцент, декан факультету комп'ютерних інформаційних технологій Західноукраїнського національного університету;

Михайло КАСЯНЧУК, доктор технічних наук, професор, професор кафедри кібербезпеки Західноукраїнського національного університету.

Склад Організаційного комітету XIV Міжнародної науково-технічної конференції «Безпека інформаційних технологій: ITSEC-2025»

Сергій КУЛИНА, доктор філософії з кібербезпеки, доцент, заступник декана з наукової роботи факультету комп'ютерних інформаційних технологій Західноукраїнського національного університету;

Тарас ЦАВОЛИК, кандидат технічних наук, доцент, доцент кафедри кібербезпеки Західноукраїнського національного університету;

Михайло ПРИГАРА, кандидат технічних наук, доцент, доцент кафедри технології машинобудування Ужгородського національного університету;

Степан ІВАСЬЄВ, кандидат технічних наук, доцент, доцент кафедри кібербезпеки Західноукраїнського національного університету

Аліна ДАВЛЕТОВА, викладач кафедри кібербезпеки Західноукраїнського національного університету;

Людмила БАБАЛА, кандидат економічних наук, доцент, доцент кафедри кібербезпеки Західноукраїнського національного університету;

Ігор АВЕРІЧЕВ, кандидат економічних наук, доцент, доцент кафедри технічних систем кіберзахисту Державного університету інформаційно-комунікаційних технологій;

Марія ЛИСИК, інженер кафедри кібербезпеки Західноукраїнського національного університету;

Марта ШПАК, лаборант кафедри кібербезпеки Західноукраїнського національного університету;

Олена ВАСИЛЬКІВ, начальник відділу інформації та зв'язків з громадськістю Західноукраїнського національного університету.

ЗМІСТ

Побудова досконалої форми комплексної системи залишкових класів для асиметричних криптосистем

УДК 519.7 Андрій Алілуйко[1], Михайло Касянчук[2], Mikolaj Karpinski[3]
Західноукраїнський національний університет,
[1]aliluyko82@gmail.com, [2]kasyanchuk@ukr.net, [3]mpkarpinski@gmail.com

У сучасних обчислювальних системах система залишкових класів (СЗК) розглядається як перспективна альтернатива традиційній двійковій системі числення, відкриваючи нові можливості для організації виконання базових арифметичних операцій [1]. З огляду на широке застосування цілочисельної модулярної арифметики в криптографії особливий інтерес представляє використання комплексної модулярної арифметики. Очікується, що її впровадження сприятиме підвищенню швидкодії алгоритмів шифрування та покращенню стійкості комп'ютерних систем до різного виду атак. У зв'язку з цим метою даного дослідження є подальший теоретичний розвиток комплексної СЗК (КСЗК), зокрема її досконалої (ДФ) та модифікованої досконалої форм (МДФ).

Аналогічно до цілочисельної асиметричної криптографії, можна розглядати цілі комплексні числа (Гаусові числа). Будь-яке ціле комплексне число $\dot{A} = a + bi,\ a,b \in \mathrm{Z}$ можна подати в СЗК єдиним способом у вигляді набору своїх найменших або абсолютно найменших комплексних залишків $\dot{b}_j = \dot{A} \bmod \dot{m}_j,\ \ j = \overline{1,n}$ у системі $\dot{M}$ взаємно простих комплексних модулів $\dot{m}_1, \dot{m}_2, \ldots, \dot{m}_n$. Для представлення числа $\dot{A}$ в системі $\dot{M}$ найменших залишків, необхідно і достатньо, щоб виконувалися нерівності $0 \le ap_M + bq_M < N(\dot{M})$, $0 \le bp_M - aq_M < N(\dot{M})$, а в системі $\dot{M}$ абсолютно найменших залишків мають виконуватися нерівності $|ap_M + bq_M| \le \frac{1}{2}N(\dot{M}),\ |bp_M - aq_M| \le \frac{1}{2}N(\dot{M})$, де $N(\dot{M})$ – норма комплексного числа $\dot{M} = \prod_{j=1}^{n} \dot{m}_j = p_M + q_M i$.

Відновлення числа $\dot{A}$ з СЗК можна здійснити на основі китайської теореми про залишки в комплексній числовій області: $\dot{A} = \left(\sum_{j=1}^{n} \dot{b}_j \dot{M}_j \dot{f}_j \right) \bmod \dot{M}$, де $\dot{M}_j = \frac{\dot{M}}{\dot{m}_j}$, базисні числа $\dot{f}_j$ шукаються з виразу $\left(\dot{M}_j \dot{f}_j \right) \bmod \dot{m}_j = 1,\ j = \overline{1,n}$.

З метою зменшення обчислюваної складності пошуку обернених елементів $\dot{f}_j = \dot{M}_j^{-1} \bmod \dot{m}_j$ розглянемо побудову ДФ КСЗК, у якій для комплексних модулів мають місце вирази

$$\dot{M}_j \bmod \dot{m}_j = 1,\ j = \overline{1,n}, \tag{1}$$

тобто $\dot{f}_j = 1$.

Побудова ДФ КСЗК методом дробових перетворень. Розв'язування системи конгруенцій (1) приводять до умови:

$$\sum_{j=1}^{n}\frac{1}{m_j}=\gamma+\frac{1}{\prod_{j=1}^{n}m_j}. \tag{2}$$

де γ – ціле комплексне число.

Виконання дробових перетворень над рівнянням (2) приводить до закономірності побудови системи модулів ДФ КСЗК:

$$m_1, s_1=\gamma m_1-1,\quad m_2=\frac{m_1+s_2}{s_1},\quad m_k=\frac{\prod_{j=1}^{k-1}m_j+s_k}{s_{k-1}},\ 2<k<n,\quad m_n=\frac{\prod_{j=1}^{n-1}m_j-1}{s_{n-1}}. \tag{3}$$

Оскільки $m_1, m_2, \ldots, m_n$ цілі комплексні число, то мають виконуватися умови:

$$(m_1+s_2)\bmod s_1=0;\ \left(\prod_{j=1}^{k-1}m_j+s_k\right)\bmod s_{k-1}=0,\ 2<k<n;\left(\prod_{j=1}^{k-1}m_j-1\right)\bmod s_{n-1}=0. \tag{4}$$

Отже, вирази (3) та (4) визначають умови для знаходження довільної кількості модулів ДФ КСЗК.

Побудова ДФ КСЗК методом факторизації. Для двох останніх модулів в рівності (2), введемо заміну:

$$m_{n-1}, m_n=\frac{a, b-\prod_{j=1}^{n-2}m_j}{\prod_{j=1}^{n-2}m_j\left(\sum_{k=1}^{n-2}\frac{1}{m_k}-\gamma\right)}.$$

Математичні перетворення виразу (2) приводять до умови, що виконується для визначених наборів модулів ДФ КСЗК:

$$ab=\prod_{j=1}^{n-2}m_j\left(\sum_{k=1}^{n-2}\frac{1}{m_k}-\gamma+\prod_{j=1}^{n-2}m_j\right). \tag{5}$$

Параметри a і b шукаємо факторизувавши праву частину рівності (5). Оскільки модулі m_{n-1} та m_n цілі комплексні, то мають виконуватися умови:

$$\left(a, b-\prod_{j=1}^{n-2}m_j\right)\bmod\left(\prod_{j=1}^{n-2}m_j\left(\sum_{k=1}^{n-2}\frac{1}{m_k}-\gamma\right)\right)=0. \tag{6}$$

Відповідно, вирази (5) та (6) визначають спосіб знаходження будь-якої кількості модулів ДФ КСЗК, за умови наявності двох невідомих серед них.

1. Касянчук М., Карпінський М., Казмірчук С. Методологія опрацювання багаторозрядних чисел в асиметричних криптосистемах. *Захист інформації*. 2019. Т.21, №2. С. 65–73.

Вбудовування стеганографічного каналу в криптографічні протоколи на базі блокових симетричних криптосистем

УДК 004.056.55

Володимир Анікін[1], Ігор Муляр[2], Віктор Чешун[3]

Хмельницький національний університет,
[1]anikin_volodymyr@khmnu.edu.ua,
[2]muliariv@khmnu.edu.ua,[3]cheshunvn@khmnu.edu.ua

Поєднання криптографічних та стеганографічних методів захисту інформації є перспективною та широко досліджуваною темою в галузі сучасної кібербезпеки [1,2]. Криптографія та методи приховування інформації стали двома ключовими компонентами для захисту конфіденційних даних та каналів зв'язку, забезпечуючи ще один рівень безпеки [3].

У межах концепції нелінійних криптографічних примітивів, висвітленої у попередніх публікаціях авторів за даною тематикою [4,5], з’являється можливість органічного вбудовування стеганографічного каналу без потреби зміни базової структури шифрування. Це досягається шляхом використання модифікаторів шифрування як додаткового каналу для передачі прихованих повідомлень [4]. Концепція нелінійних криптографічних примітивів передбачає доповнення класичного симетричного алгоритму шифрування спеціальним модифікатором, який впливає на результат шифрування поряд із ключем та відкритими даними, що дозволяє зруйнувати лінійну залежність між вхідними та вихідними параметрами. Такий підхід забезпечує варіативність шифротексту навіть за однакових вхідних умов, ускладнює криптоаналіз і відкриває нові напрями застосування, зокрема у стеганографії, завдяки можливості контрольованого формування шифротексту [5].

Основною перевагою такого підходу є те, що зміни в шифротексті залишаються в межах допустимих варіацій криптографічного протоколу, що значно ускладнює виявлення самого факту наявності стеганографії. Наприклад, якщо система має кілька паралельних варіантів криптографічних перетворень із відповідними модифікаторами, кожен з них може бути інтерпретований як певна бітова послідовність. Таким чином, маніпулюючи вибором модифікаторів у рамках криптографічного алгоритму, можна приховано передавати дані, не змінюючи основну логіку шифрування.

Особливо ефективним є підхід, у якому стеганографічне повідомлення попередньо шифрується іншим, незалежним алгоритмом. Це підвищує ентропію модифікаторів і унеможливлює їх розпізнавання за статистичними ознаками. Самі модифікатори в такому випадку перетворюються на псевдовипадкову послідовність, з якої складно виділити сигнали, що несуть смислове навантаження.

Простий сценарій такого використання демонструє ситуація, в якій двоє абонентів, Аліса та Боб, здійснюють обмін зашифрованими повідомленнями. Вони погодилися заздалегідь, що час від часу змінюватимуть основний ключ шифрування, передаючи новий ключ через стеганографічний канал, реалізований у системі модифікаторів. У звичайному режимі модифікатори генеруються випадково, проте в певні моменти в них вбудовується спеціальне

повідомлення, що містить новий ключ та інструкції щодо моменту його активації. Потенційний зловмисник, який перехоплює канал, не лише не помітить момент передачі ключа, але й не зможе виявити різницю між модифікаторами зі стеганографічним навантаженням і звичайними.

Концепція стеганографічного використання модифікаторів у межах нелінійних криптографічних примітивів дозволяє організовувати приховані канали передачі інформації навіть у середині стандартних криптографічних протоколів. При цьому основний криптографічний алгоритм, наприклад DES чи його модифікації, залишається незмінним, що спрощує впровадження таких рішень у вже існуючі системи інформаційного захисту. У більш складних схемах можливо поєднувати кілька нелінійних криптографічних примітивів у рамках одного протоколу, формуючи приховані канали на основі співвідношень між їх модифікаторами.

Такий підхід відкриває нові можливості у сфері захисту інформації, зокрема для побудови розподілених криптографічно-стеганографічних протоколів, здатних забезпечити надійний захист навіть у умовах тривалого спостереження за каналом зв'язку. Завдяки вбудованій нелінійності, криптосистеми, побудовані на запропонованій моделі, демонструють високу стійкість до криптоаналізу, особливо до атак статистичного характеру, зберігаючи при цьому гнучкість та сумісність з існуючими стандартами.

Таким чином, вбудовування стеганографічного каналу у криптографічні протоколи на основі нелінійних примітивів дозволяє забезпечити додатковий рівень захисту без порушення базової логіки шифрування, створюючи приховані канали передачі, стійкі до виявлення та криптоаналізу, що робить такий підхід доцільним для практичного застосування в умовах підвищених вимог до конфіденційності.

1. Akash Badhan, Simarjit Singh Malhi. Enhancing Data Security and Efficiency: A Hybrid Cryptography Approach (AES + ECC) Integrated with Steganography and Compression Algortihm. 2025 3rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT). – 2025. – P.450-456.

2. Bodnia M., Yesina M., Ponomar V. Researching the possibilities of using steganographic and cryptographic algorithms for information hiding. *Computer Science and Cybersecurity*, – 2023. – № 2. – P. 43-57.

3. Halima Abbas Ahmed, Asmaa Mahfoud, Omar Ismael. Al-Sanjary Comprehensive Review of Cryptography and Steganography Algorithms. *Journal of Information Systems Engineering and Management*. – 2025. – Vol. 10, № 29s . – P. 211-228.

4. Muliar I., Anikin V., Yatskiv V., Kulyna S., Humennyy P., Kulyna H. Construction of Nonlinear Cryptographic Protocol based on Multiple Linear Cryptosystems. *In 2024 14th International Conference on Advanced Computer Information Technologies (ACIT). IEEE*. 2024. P. 500-504.

5. Анікін В.А., Джулій В.М., Муляр І.В., Орленко В.С., Тітова В.Ю. Симетрична криптосистема з нелінійним шифруванням та можливістю

контролю шифротексту з метою маскування. Вісник Хмельницького НУ. Технічні науки. – 2020. – № 6. – С. 12-19.

Огляд вразливостей пристроїв на ОС Android з підвищеними правами на основі clickjacking атак

УДК 004.056.55

Богдан Бараннік[1] Алессандро Царьков[2]
Західноукраїнський національний університет,
[1]bbo@wunu.edu.ua [2]burntheroot@gmail.com

З розвитком кастомних прошивок та поширенням root-доступу серед користувачів Android-пристроїв зростає ризик появи нових вразливостей, які не покриваються типовими механізмами захисту. Особливо небезпечними є загрози, пов'язані з фіксклік атаками — прихованим перенаправленням дій користувача на шкідливі елементи інтерфейсу. Такі атаки можуть бути реалізовані на рівнях системних сервісів, залишаючись непомітними для користувача.

Метою роботи є аналіз вразливостей у системах із підвищеними привілеями (root-доступом), що дозволяють реалізувати clickjacking атаки.

Одним із основних векторів атаки є модифікація файлу `/system/lib/libinput.so`, який обробляє вхідні події на низькому рівні [1]. Змінюючи цю бібліотеку, зловмисник може імплементувати механізм, який перехоплює координати дотику та перенаправляє їх на приховані елементи інтерфейсу. Важливо розуміти, що такий процес відбувається на рівні нижче, ніж можуть контролювати стандартні захисні механізми додатків, що робить атаку невидимою для користувача.

Інший небезпечний метод реалізується через втручання у роботу System Server, який координує всі взаємодії між додатками та системою. На рутованих пристроях можлива модифікація системних компонентів WindowManagerService та InputManagerService, що дозволяє здійснювати "прозоре" викрадення дотиків без стандартних індикаторів фішинг-атаки. Цей підхід особливо небезпечний, оскільки працює на рівні системних привілеїв. Окрему категорію вразливостей становлять пристрої з модифікованими прошивками на базі LineageOS та інших кастомних ROM. У таких системах часто порушується стандартна модель безпеки Android через перепідписані системні додатки. Механізм верифікації підписів у цих прошивках зазвичай змінений для забезпечення роботи модифікованих системних компонентів, що створює передумови для маскування шкідливих процесів під системні [2].

Технічно процес clickjacking атаки на пристрої з root-правами суттєво відрізняється від стандартних методів. Звичайна фіксклік атака базується на використанні прозорих накладок та механізмі TYPE_APPLICATION_OVERLAY. Натомість, на рутованих пристроях можливе використання системних типів вікон, таких як TYPE_SYSTEM_ALERT або навіть TYPE_SYSTEM, які мають вищий пріоритет і обходять багато обмежень.

Технічно механізм атаки полягає у зміні логіки методів WindowManagerService.addWindow() та InputDispatcher.dispatchTouchEvent(),

які відповідають за управління вікнами та розподіл подій дотику відповідно. Модифікація цих методів дозволяє обходити вбудовані механізми безпеки, такі як FLAG_SECURE, що використовуються банківськими та іншими чутливими додатками для запобігання знімкам екрану та накладкам, детально в таблиці 1.

Таблиця 1

Порівняння механізмів реалізації фіксклік атак

Аспект атаки	Стандартні пристрої	Пристрої з root-доступом
Рівень доступу	Обмежений правами додатку	Системний рівень
Візуальна детекція	Часто можлива	Складна або неможлива
Тип накладок	TYPE_APPLICATION_OVERLAY	TYPE_SYSTEM, TYPE_SYSTEM_ALERT
Можливість обходу FLAG_SECURE	Обмежена	Повна

Також проблемою безпеки є можливість модифікації файлової системи `/system`, яка на пристроях з root-доступом дозволяє впроваджувати шкідливі компоненти на рівень, що має підвищені привілеї.

Особливо небезпечним вектором атаки є використання технік hooking через інструменти на кшталт Xposed Framework, Magisk Module або Frida на рутованих пристроях. Ці інструменти дозволяють впроваджувати код на рівні віртуальної машини Dalvik/ART, перехоплюючи виклики методів Java та модифікуючи їх поведінку. Наприклад, метод перевірки доступності накладок через android.app.AppOpsManager може бути перехоплений та підроблений, щоб завжди повертати негативний результат, незважаючи на фактичну наявність шкідливої накладки.

Дослідження показало, що пристрої з root-доступом відкривають низку критичних вразливостей, які дозволяють реалізовувати складні clickjacking атаки на системному рівні. Такі атаки практично неможливо виявити звичайними засобами захисту, а модифікація системних бібліотек і використання фреймворків на кшталт Xposed чи Frida значно ускладнюють виявлення та нейтралізацію загроз. Це підтверджує необхідність посилення безпеки на рівні операційної системи, зокрема, для рутованих середовищ.

1. Zhihu. *How can Android apps detect system touch event interception (clickjacking)?* [Електронний ресурс]. – Режим доступу: https://www.zhihu.com/question/37378266 – Дата звернення: 29.04.2025.

2. Bai Qin. *Binder File Descriptor Usages*. Medium [Електронний ресурс]. – Режим доступу: https://baiqin-droid1001.medium.com/binder-file-descriptor-usages-b2b8a672873f – Дата звернення: 29.04.2025.

Огляд існуючих рішень в області управління доступом до хмарних середовищ

УДК 004.738.056

Володимир Бескровний[1], Олександр Сиропятов[2]

Національний університет «Одеська політехніка»,
[1]9560418@stud.op.edu.ua, [2]o.a.syropiatov@op.edu.ua

У сучасних умовах розвитку цифрових технологій та зростання обсягів обробки корпоративних даних у хмарних середовищах питання побудови безпечної та гнучкої системи управління доступом набуло особливої актуальності. Хмарна інфраструктура дозволяє підприємствам оптимізувати свої процеси, однак одночасно створює нові ризики, пов'язані з несанкціонованим доступом до ресурсів, витоком даних та інсайдерськими загрозами. Зокрема, важливо розглянути традиційні та сучасні підходи, що дозволяють гнучко адаптувати доступ відповідно до змін у бізнес-процесах, а також вивчити можливості реалізації цих моделей на найпопулярніших хмарних платформах.

Метою роботи є проведення аналізу моделі управління доступом у хмарних середовищах, а також провести порівняння можливостей найбільш поширених платформ IAM (AWS IAM, Azure AD, Google Cloud IAM) для побудови безпечної системи контролю доступу в умовах корпоративної хмарної інфраструктури.

Ефективне управління доступом у хмарних середовищах є ключовим аспектом безпеки корпоративних даних. Існує кілька базових моделей, які широко застосовуються у сучасних системах управління доступом.

Рольова модель доступу (RBAC) передбачає прив'язку прав доступу до певних ролей, які призначаються користувачам відповідно до їх посадових обов'язків [1]. Наприклад, розробник має доступ до репозиторіїв коду, а фінансовий аналітик — до фінансових звітів.

Атрибутна модель доступу (ABAC) дозволяє приймати рішення про надання доступу на основі атрибутів користувача (посада, місце роботи, час доступу, тип пристрою) та характеристик ресурсу [2].

Політично-орієнтована модель доступу (PBAC) формує доступ на основі динамічних політик та правил, що можуть змінюватися у реальному часі залежно від поведінки користувача або рівня ризику.

На практиці часто використовується комбінація моделей, де базова рольова модель доповнюється атрибутними правилами та політиками поведінки для підвищення гнучкості й безпеки.

У хмарному середовищі управління доступом реалізується за допомогою спеціалізованих платформ Identity and Access Management (IAM). Найпопулярнішими серед них є:

AWS IAM (Identity and Access Management) - сервіс в хмарі Amazon Web Services, який дозволяє організаціям безпечно керувати доступом до ресурсів AWS [3]. За допомогою IAM адміністратори можуть контролювати, хто має доступ до конкретних ресурсів у вашій інфраструктурі та що саме ці користувачі можуть робити з цими ресурсами.

Azure Active Directory (Azure AD) – рішення Microsoft для управління ідентифікацією в хмарних та гібридних середовищах. Він є базовим компонентом для багатьох корпоративних рішень Microsoft і часто використовується корпоративними системами, що робить його популярним серед великих компаній.

Google Cloud IAM – інструмент керування ідентичностями та доступом в хмарі Google, що дозволяє організаціям керувати тим, хто має доступ до ресурсів у Google Cloud Platform (GCP), і які саме права доступу ці користувачі мають.

Таблиця 1

Порівняння платформ

Платформа	**Підхід до управління доступом**	**Особливості**
AWS IAM	RBAC + умови доступу	Широкі можливості кастомізації через політики JSON
Azure AD	RBAC + умовні політики	Глибока інтеграція з Microsoft екосистемою
Google Cloud IAM	RBAC + ABAC	Деталізовані умови доступу на основі атрибутів

Всі розглянуті платформи підтримують гібридні підходи до управління доступом, поєднуючи RBAC з атрибутними та політико-орієнтованими механізмами.

Аналіз основних моделей управління доступом показав, що найкращі результати забезпечує комбіноване використання RBAC, ABAC та PBAC. Це дозволяє гнучко адаптувати політики під змінні бізнес-процеси та загрози. Розгляд платформ демонструє, що сучасні хмарні рішення підтримують складні механізми доступу, орієнтовані на мінімізацію ризиків. Таким чином, вибір платформи має базуватися на відповідності вимогам підприємства, інтеграційним можливостям і рівню захисту даних.

1. Sandhu R., Coyne E.J., Feinstein H.L., Youman C.E. Role-Based Access Control Models. IEEE Computer, 1996, Vol. 29(2), pp. 38-47

2. Hu V.C., Ferraiolo D.F., Kuhn D.R. Attribute-Based Access Control (ABAC) Definition and Considerations. National Institute of Standards and Technology, 2014. 78 p

3. Amazon Web Services. AWS Identity and Access Management (IAM) User Guide. Amazon, 2023.

Кібератаки як загроза критичній інфраструктурі

УДК 004.56.5(043.2)

Павло Билень

Західноукраїнський національний університет,
pavlobulen@gmail.com

За 2024–2025 роки енергетична інфраструктура виявилася у центрі уваги хакерських атак, що стали частиною ширшого спектра гібридних загроз. Зі зростанням залежності енергосистем від цифрових технологій, підвищується і рівень їхньої вразливості до кібервтручань. У цьому дослідженні представлено аналіз найрезонансніших інцидентів останніх двох років, виявлено типові сценарії атак, ймовірні джерела загроз, а також надано огляд заходів, що вживаються для підвищення стійкості енергетичної інфраструктури до подібних втручань.

Протягом 2024 року в Україні було зафіксовано понад 4300 кібератак на об'єкти критичної інфраструктури, що свідчить про 70-відсоткове зростання порівняно з попереднім роком [1]. Основною мішенню залишаються енергетичні компанії, державні інформаційні платформи, зокрема Міністерство енергетики, операційні центри енергосистем та системи обліку. У грудні 2024 року відбулася масштабна атака, яка вивела з ладу цифрові реєстри Міністерства юстиції, а також тимчасово зупинила роботу сервісу “Дія”. Характерною особливістю цих атак є використання складних багаторівневих методів, включно з соціальною інженерією, фішингом, шкідливим ПЗ типу wiper та атакою через ланцюг постачання [2].

На початку 2025 року увагу світової спільноти привернув масштабний збій в енергосистемах Іспанії та Португалії. 28 квітня близько 60% енергоспоживання цих країн було раптово втрачено через зупинку десятків електростанцій [3]. Попри те, що офіційні оператори електромереж REE (Іспанія) та REN (Португалія) не підтвердили факт кібератаки, експерти не виключають можливість цілеспрямованого зовнішнього втручання у частотну стабільність мереж. Ситуація ускладнювалася синхронністю збоїв, що є нетиповим для звичайних технічних аварій.

Паралельно з європейськими інцидентами, протягом 2024–2025 років фіксувалися атаки на енергетичні об'єкти в інших регіонах. Зокрема, у США відома атака на комунальне підприємство в Айові призвела до порушень в електропостачанні та витоку персональних даних. У Німеччині постачальник Tibber повідомив про злом систем збереження даних близько 50 тисяч споживачів. У Румунії та Камеруні кібератаки спричинили тимчасову втрату доступу до електронних сервісів та енергетичних даних споживачів.

Джерела атак залишаються різноманітними за походженням і мотивацією. Частина інцидентів ідентифікована як операції, проведені державними

акторами, зокрема хакерськими угрупованнями, афілійованими з РФ, Іраном, КНДР. Інші атаки здійснювалися хактивістами, які керуються політичними або ідеологічними мотивами. Значна кількість загроз надходить також від економічно зацікавлених кіберзлочинців, які використовують шантаж або вимагання після отримання доступу до критичних систем.

У відповідь на зростаючу кількість інцидентів, у червні 2024 року було проведено загальноєвропейське навчання "Cyber Europe 2024" за участі більш як тисячі фахівців з кібербезпеки з 30 країн. Метою навчання було моделювання сценаріїв масштабних кібератак на енергетичний сектор та перевірка національних і міждержавних протоколів реагування.

У таблиці 1 наведено приклади найбільш відомих атак на енергетичні системи у 2024–2025 роках.

Таблиця 1

Характеристика найбільш відомих кібератак на енергетичну

Країна	**Дата**	**Опис інциденту**	**Імовірне джерело**
Україна	Грудень 2024	Атака на реєстри Мін'юсту, збій у роботі сервісу "Дія"	Хак-група, афілійована з РФ
Іспанія/Португалія	Квітень 2025	Масове відключення електропостачання	Не встановлено
США (Айова)	Січень 2024	Порушення роботи комунального підприємства	Локальний хакер
Німеччина	2024	Злам бази даних постачальника Tibber	Злочинне ПЗ
Румунія	2024	Тимчасова зупинка цифрових сервісів енергокомпанії	Фішинг/вимагання

Аналіз кібератак на енергетичну інфраструктуру України у 2024–2025 роках свідчить про зростання їхньої складності та скоординованості, що становить серйозну загрозу для суспільної безпеки. Зокрема, у 2024 році кількість кібератак на критичну інфраструктуру України зросла на 70%, досягнувши 4315 інцидентів, порівняно з 2541 випадком у 2023 році. Основними цілями хакерів стали енергетичний сектор, урядові установи та телекомунікаційні системи .

1. Mukhina O. Russian cyberattacks on Ukraine surge 70% in 2024 with 4,315 assaults on critical infrastructure. Euromaidan Press. 2025. https://euromaidanpress.com/2025/01/12/russian-cyberattacks-on-ukraine-surge-70-in-2024-with-4315-assaults-on-critical-infrastructure/

2. Zoria Y. Massive cyber attack hits Ukrainian e-services. Euromaidan Press. 2024. https://euromaidanpress.com/2024/01/25/massive-cyber-attack-hits-ukrainian-e-services/

3. Reuters. Iberia mess places timely focus on grid resilience. 2025. https://www.reuters.com/breakingviews/iberia-mess-places-timely-focus-grid-resilience-2025-04-30/

Розробка системи для виявлення підозрілих текстових повідомлень

УДК 004.056.55:004.8:681.3

Іван Боцанюк[1], Олена Агаджанян[2]

Національний університет «Одеська політехніка»,
[1]9480582@stud.op.edu.ua, [2]o.v.ahadzhanian@op.edu.ua

Із зростанням кількості фішингових, шахрайських та шкідливих повідомлень, що надсилаються через електронну пошту, виникає потреба у створенні гнучких та ефективних засобів захисту користувачів[1], зокрема в межах особистих або корпоративних систем. Особливої актуальності набуває локальне фільтрування повідомлень без залучення хмарних сервісів, оскільки останні можуть порушувати вимоги до конфіденційності в процесі обробки чутливих персональних або службових даних. Електронна пошта, як один із найпоширеніших каналів цифрового спілкування, становить основну ціль зловмисників, оскільки дозволяє комбінувати соціальні та технічні вектори атаки[2]. Враховуючи це, тема роботи сфокусована саме на електронних листах як на найбільш уразливому, розповсюдженому та структурованому форматі цифрового повідомлення, де доцільно застосовувати багатоетапний аналіз.

Метою роботи стало створення програмного забезпечення для виявлення підозрілих електронних повідомлень, яке функціонує автономно на локальному комп'ютері користувача, використовує виключно бібліотеки з відкритим вихідним кодом і враховує обмеження ресурсів системи. Основною особливістю проєкту є розгортання повноцінної системи фільтрації, що поєднує різні підходи до аналізу: від евристичних методів до машинного навчання у єдиному середовищі, без потреби в зовнішніх обчислювальних або API-сервісах. Такий підхід може бути легко адаптований і до інших типів цифрових повідомлень (наприклад, повідомлень в соціальних мережах), за умови врахування специфіки структури повідомлення, протоколів або вмісту.

Розроблений застосунок включає модулі для аналізу ключових елементів електронного листа: вкладень, текстового вмісту, HTML-коду, заголовків та гіперпосилань. Додатково реалізовано оптичне розпізнавання тексту з зображень та автоматичний переклад тексту на англійську мову для уніфікації вхідних даних перед обробкою. Це дозволяє інтегрувати зображений контент у загальний аналіз тексту, що є важливою частиною сучасних фішингових кампаній. На основі сукупності показників кожного модуля реалізовано систему зваженої оцінки з відповідним нормуванням і логікою пріоритетів: найнебезпечніші ознаки автоматично переміщують повідомлення до категорії «Небезпечні», тоді як менш виразні ознаки оцінюються в сукупності. Глобальна

оцінка формується на основі порогових значень: нижче -50 - «Небезпечні/Спам», від -50 до 50 - «Підозрілі», вище 50 - «Прийнятні».

Текстова частина повідомлень аналізується з використанням донавченої трансформерної моделі DistilBERT, натренованої на корпусі з 18650 повідомлень (61 % безпечних, 39 % - фішинг або спам). Тестування на незалежному наборі з 3021 прикладу показало стабільну ефективність: precision 0.98 і recall 0.98 для безпечних листів, precision 0.96 і recall 0.97 для небажаних. Важливо, що класифікація може виконуватися навіть на бюджетному процесорі (Intel i3 11-го покоління) з використанням лише ~900 МБ оперативної пам'яті, що свідчить про придатність розробленої системи для широкого використання без потреби у високопродуктивному обладнанні.

Під час аналізу було виявлено як переваги, так і обмеження локального підходу. Система здатна ефективно виявляти шаблонні та повторювані атаки, включаючи окремі випадки цільового фішингу. Водночас, локальна природа рішення обмежує його здатність до глибокого аналізу вкладень (наприклад, емуляція виконання, sandboxing), що важливо при виявленні складних загроз, прихованих у, здавалося б, легітимному вмісті (наприклад, шкідливі скрипти у PDF-файлах). Окремо слід зазначити, що повністю автономне функціонування системи унеможливлює доступ до актуалізованих онлайн-баз загроз, без яких суттєво знижується ефективність захисту від нових або модифікованих типів атак.

З метою забезпечення балансу між захистом та конфіденційністю, доцільним є впровадження поміркованих компромісів: наприклад, здійснювати аналіз не повного посилання, а лише доменного імені; дозволяти обмежене використання зовнішніх сервісів виключно для тих повідомлень, які попередньо були класифіковані як підозрілі локально. Такий вибір зменшує ризик витоку приватних даних, зберігаючи при цьому можливість використання актуальних джерел у критичних випадках.

Також слід зважати на відставання деяких відкритих рішень (у сфері перекладу чи OCR) у порівнянні з комерційними аналогами. Утім, розвиток відкритих технологій, зокрема за рахунок залучення спільноти та поширення доступних моделей, дозволяє сподіватися на скорочення цього розриву в майбутньому. Противагою відсутності доступу до централізованих сервісів є зростання якості й оптимізації локальних інструментів, що з часом сприятиме підвищенню ефективності автономних систем без компромісу для конфіденційності користувача.

Загалом, створений застосунок демонструє, що використання комплексного аналізу електронної пошти в локальному середовищі є технічно можливим та ефективним навіть у рамках обмежених ресурсів. З огляду на тенденції розвитку відкритих бібліотек, моделей і технологій оптимізації, можна очікувати подальше зменшення розриву між локальними рішеннями та потужними хмарними платформами, що зробить приватні захищені системи дедалі доступнішими для широкого кола користувачів.

1. Anti-Phishing Working Group (APWG). Phishing Activity Trends Report: 4th Quarter 2024. 2024. URL: https://www.apwg.org/trendsreports/ (дата звернення: 25.04.2025)

Altulaihan E., Alismail A., Rahman M. M., Ibrahim A. Email security issues, tools, and techniques used in investigation. *Sustainability*. – 2023. – Vol. 15. – №10612.

Формалізація методики побудови безпечних інформаційних систем екологічного моніторингу

УДК 004.75

Кирило Вадурін[1], Андрій Перекрест[2]
Кременчуцький національний університет імені Михайла Остроградського, [1]kir3337@gmail.com, [2]pksg13@gmail.com

Наразі спостерігаються тенденції до розширення використання датчиків якості повітря в інфраструктурі Smart City для моніторингу екологічної ситуації. Існують платформи для збору та аналізу даних, проте питання безпеки інформаційних систем та формалізації відповідних методик залишаються поза увагою. Актуальність запланованої роботи пов'язана з необхідністю забезпечення безпеки та надійності інформаційних систем екологічного моніторингу в умовах розширення інфраструктури Smart City.

У ході аналізу подібних рішень виявлено, що питання безпеки інформаційних систем екологічного моніторингу, особливо в контексті Smart City, потребують додаткової уваги. Airly [1] пропонує комплексні рішення для моніторингу якості повітря, але питання безпеки даних не є пріоритетними. У той же час, існують дослідження, спрямовані на забезпечення безпеки та енергоефективності аутентифікації в розумних містах за допомогою біометрії та криптографічних методів [2], проте вони не враховують специфіку датчиків якості повітря. Платформи, такі як Kyiv Smart City [3], демонструють можливості моніторингу якості повітря, але потребують удосконалення в частині довгострокової підтримки та інтеграції з іншими міськими системами. Державна система моніторингу довкілля в Україні [4] потребує модернізації та впровадження сучасних технологій для забезпечення ефективного збору та аналізу даних. Таким чином, невирішеними залишаються питання формалізації безпеки, масштабування рішень та інтеграції даних моніторингу з іншими системами Smart City.

Метою роботи є формалізація методики побудови безпечних інформаційних систем екологічного моніторингу на основі розподіленої апаратної інфраструктури датчиків якості повітря та виконавчих пристроїв Smart City, що забезпечить захист даних та надійність функціонування системи.

Основними завданнями, що наразі не вирішені, є розробка конкретних методів формалізації безпеки інформаційних систем екологічного моніторингу, забезпечення захисту даних та надійності розподіленої апаратної інфраструктури датчиків якості повітря, а також вирішення питань масштабування, довгострокової підтримки та інтеграції даних моніторингу з іншими міськими системами.

Тому, ході роботи, передбачається розробка формалізованої методики побудови інформаційних систем, яка враховує специфіку розподіленої апаратної інфраструктури датчиків якості повітря та виконавчих пристроїв. Це дозволить підвищити захищеність даних, запобігти несанкціонованому доступу та забезпечити стабільне функціонування системи в цілому.

У рішенні заплановано використати такі методи: формалізація вимог до безпеки інформаційних систем, моделювання загроз та ризиків, криптографічні методи захисту даних, методи забезпечення відмовостійкості та відновлення даних, а також методи аналізу та візуалізації даних моніторингу. Планується застосування методів машинного навчання для виявлення аномалій та прогнозування змін якості повітря.

Рис.1. Графічне представлення сформованої концепції

Пропоноване рішення має функціонувати наступним чином: датчики якості повітря, розміщені в різних точках міста, безперервно збирають дані про концентрацію забруднюючих речовин. Ці дані передаються захищеними каналами зв’язку до центрального серверу, де вони обробляються та аналізуються на основі ретроспективних даних задля визначення загальних характеристик забруднення, а також ідентифікації цифрових патернів станцій, щоб запобігти ін’єкціям. У разі виявлення перевищень допустимих норм, втрати чи підміни даних, система автоматично формує оповіщення та надсилає їх відповідним службам, або населенню (у режимі оповіщення). Також, система забезпечує можливість автоматизованого керування виконавчими пристроями, такими, як системами вентиляції, очищення повітря у громадських будівлях.

1. The role of air quality sensors in smart city infrastructure. URL: https://airly.org/en/the-role-of-air-quality-sensors-in-smart-city-infrastructure/

2. Nyangaresi, V.O., Abduljabbar, Z.A., Mutlaq, K.AA. et al. Smart city energy efficient data privacy preservation protocol based on biometrics and fuzzy commitment scheme. Sci Rep 14, 16223 (2024). https://doi.org/10.1038/s41598-024-67064-z

3. Платформа, де можна перевірити якість повітря у Києві. URL: https://www.village.com.ua/village/city/city-news/285841-platforma-de-mozhna-pereviriti-yakist-povitrya-u-kieva

4. Екологічний моніторинг довкілля. URL: https://mepr.gov.ua/diyalnist/napryamky/ekologichnyj-monitoryng/ekologichnyj-monitoryng-dovkillya (дата звернення: 10.04.2025).

Сучасні виклики та використання командного підходу в управлінні інформаційними системами

УДК 342.95

Петро Венгерський[1], Михайло В`ячало[2]
Львівський національний університет ім.І.Франка,
[1]Petro.Venherskyy@lnu.edu.ua, [2]Mykhaylo.Vyachalo@lnu.edu.ua

Процес управління інформаційними системами (ІС) в умовах сучасної цифрової трансформації є надзвичайно складним та багаторівневим. Ефективність управління ІС впливає не лише на стабільність бізнес-процесів, але й безпосередньо на рівень кіберзахисту в організації. Зростання складності ІТ інфраструктури, поширення хмарних сервісів, розвиток кіберзагроз породжують нові виклики, які потребують системного та командного підходу.[1]

Нижче розглянемо ключові виклики сучасності в управлінні ІС та рішення які допоможуть організаціям впоратись з ними:

1. Гібридна інфрастуктура (on-premises + cloud). Дедалі більше організацій працюють в змішаних середовищах: локальні сервери, публічні/приватні хмари, SaaS – рішення. Це в свою чергу створює труднощі з контролем, моніторингом та забезпеченням безпеки.[3] Ефективними рішеннями, які можуть допомогти в покращенні управління ІС у даному випадку, можуть бути наступні:
   - впровадження ефективного контролю доступу (IAM, SSO)
   - використання хмарно-орієнтованих платформ управління безпекою (CSPM)
   - ефективна та тісна взаємодія адміністраторів хмарної та локальної інфрастурктури.
2. Зростання складності систем. API-інтеграції та автоматизація, мікросервіси, велике різноманіття ІТ-рішень створюють високий ризик конфігураційних помилок, несумісності та вразливостей.[1] Рішеннями можуть бути:
   - стандартизація розгортання (Infrastructure as Code)
   - автоматичні тести безпеки (DevSecOps)
   - регулярні код-рев`ю та конфігураційні аудити
3. Кадрові проблеми та перевантаження фахівців. Постійний розвиток технологій, збільшення навантаження на SOC-команди, брак кваліфікованих кадрів – все це безпосередньо впливає на якість управління ІС.[4] Рішеннями тут можуть бути:
   - побудова міжфункціональних команд підтримки (SRE, SecOps)

- автоматизація повторюваних задач
- впровадження системи менторства та обміну знаннями

4. Швідкість змін та потреба в гнучкості. Політики безпеки створюються набагато повільніше ніж поява та впровадження нових сервісів, що призводить до розриву між IT та безпекою.[2] Щоб бути більш гнучким та швидше реагувати на зміни необхідно:

- інтеграція безпеки в усі етапи життєвого циклу ІС (shift-left security)
- побудова культури «безпека відповідальність усіх»
- використання методик Agile/Scrum у керуванні змінами

5. Розпорошеність даних та віддалена робота. Багато організацій переходять на віддалений або гібридний формат роботи, що ускладнює контроль за доступом, шифруванням та резервним копіюванням.[3] Хорошими рішеннями тут будуть:

- впровадження Zero-Trust моделі доступу
- захист кінцевих точок (EDR/XDR)
- регулярні навчання з кібербезпеки

Слід також зазначити що перелічені вище виклики складно вирішити ізольовано. Успіх залежить від спільних зусиль різних команд які мали б включати наступні фактори:

- кроскоординації між різними відділами (IT, ІБ, розробка, керівництво)[2]
- крос-функціональні команди, які працюють над спільними задачами
- єдине бачення безпеки (усі учасники процесу повинні мати чітке розуміння загроз, цілей та засобів захисту)[1]
- роль лідерства (зокрема роль координатора/менеджера який відповідатиме за ефективну комунікацію та спільне ухвалення рішень)

Хорошим прикладом слугує DevSecOps підхід – коли розробники, інженери з безпеки та оператори інфраструктури працюють в одній команді над впровадженням рішень, де безпека закладається з першого рядка коду.

Підводячи підсумки, слід зазначити що сучасне управління ІС вимагає не лише технічної досконалості, а й організаційної зрілості. Виклики нової епохи вимагають командної стратегії, адаптивності та постійної взаємодії. Тільки синергія зусиль здатна забезпечити стійкість ІС та захист організації в умовах зростаючих кіберризиків.

1. NIST SP 800-160: Systems Security Engineering.
2. ISO/IEC 27001:2022 – Information Security Management
3. ENISA Threat Landscape Report 2023.
4. ISACA. 2024 State of Cybersecurity Report.

Підвищення рівня кіберстійкості в умовах глобальної цифровізації

УДК 621.395.7 (043.2)

Віталій Вербиненко[1], Сергій Зибін[2]
Державний університет інформаційно-комунікаційних технологій,
[1]*vv.q@ukr.net*, [2]*zysv@ukr.net*

Поширення дистанційної форми праці стало визначальним наслідком глобальних змін, спричинених пандемією COVID-19 та подальшими геополітичними трансформаціями. Підприємства у всьому світі були змушені адаптувати свої бізнес-процеси до нових умов, впроваджуючи цифрові рішення, які дозволяють співробітникам ефективно працювати поза межами офісу. Цей тренд набув особливої актуальності в Україні після 2022 року, коли мільйони громадян опинилися за кордоном, але продовжили професійну діяльність в українському економічному просторі. Як наслідок, підтримка цифрової взаємодії у віддаленому режимі стала не лише операційним, а й стратегічним завданням для організацій.

Зростання кількості дистанційних робочих місць, зумовлене глобальними викликами, трансформувало підхід до власних операційних процесів [1].

Організації, що діють у повністю віддаленому форматі, характеризуються відсутністю власної фізичної інфраструктури, зокрема офісних приміщень або локальних серверів. Із розвитком цифрових технологій, зокрема хмарних обчислень, комунікаційних платформ і сервісів дистанційного управління, подібна організаційна модель не лише стала технічно можливою, але й перетворилася на необхідну умову функціонування для багатьох підприємств, особливо зважаючи на збільшення вимог до гнучкості графіку зі сторони працівників та зменшенню кількості професій, які залежать від стабільного місця роботи [2].

Дослідження загроз моделі дистанційного управляння потребує комплексного аналізу підходів, інструментів та організаційно-правових засобів для забезпечення захищеної цифрової взаємодії. Для досягнення цієї мети необхідно дослідити наступні ключові аспекти: по-перше, сучасні програмні платформи та цифрові сервіси для комунікації, спільної роботи й захисту даних (хмарні середовища, системи автентифікації, VPN, концепції Zero Trust тощо) [3]; по-друге, управління користувацькими пристроями, включно з політикою BYOD (Bring Your Own Device), тобто використанням персональних пристроїв працівників, та засобами їх централізованого адміністрування (MDM (Mobile Device Management), Zero-Touch Deployment тощо) [4]; по-третє, правове регулювання сфери кібербезпеки й захисту інформації у різних юрисдикціях (дотримання стандартів GDPR, CCPA та відповідних національних законодавчих вимог). Застосування такого підходу дозволяє сформувати цілісне уявлення про наявні рішення та проблеми, а також визначити напрями для їх подальшого розвитку. Дотримання правових вимог є не менш важливим, ніж технічні рішення, оскільки порушення законодавства щодо обробки персональних даних може спричинити юридичні наслідки та втрату репутації [5].

Розподілені інфраструктури, що використовують інструменти від різних постачальників, потребують значно більшої складності в управлінні, а також створюють ризики несумісності політик шифрування, автентифікації та контролю доступу. Це може призвести до фрагментації безпекових механізмів і збільшення вразливостей у системі. Крім того, часто виникає явище створення тіньових даних, ситуацій, коли співробітники використовують сторонні сервіси без дозволу IT-відділу, що створює "сліпі зони" в інформаційній безпеці та підвищує ризик витоку даних.

У компаніях з віддаленим режимом роботи збільшилося навантаження на адміністрування пристроїв та послуг, значно розширивши цифрову інфраструктуру і, відповідно, – потенційний периметр атаки. Концепція BYOD дозволяє співробітникам працювати з власних ноутбуків або смартфонів. Це сприяє зручності, проте створює значні ризики.

Для забезпечення керованості та безпеки пристроїв джерела рекомендують впроваджувати стандартизовані засоби управління, які поєднують налаштування, політики й моніторинг.

Ключовими технічними загрозами, які пов’язані з пристроями для компаній із віддаленим режимом роботи являються: компрометація пристроїв, що використовуються поза корпоративним захистом.; незахищені домашні мережі Wi-Fi.; небезпечні дозволи мобільних застосунків; відсутність регулярних оновлень і патчів.

Фізична втрата пристрою, що не має шифрування або функцій віддаленого видалення даних, створює значний ризик несанкціонованого доступу до інформації.

Надійна система кібербезпеки для віддаленої роботи – це не лише питання технологій, а й відповідності юридичним стандартам. Щоб уникнути штрафів, санкцій або втрати довіри з боку клієнтів, компанії повинні постійно стежити за змінами у міжнародному та національному законодавстві і адаптувати свої внутрішні політики відповідно до нових вимог.

1. Radha P., Sayyed N., Fathima Y. The new normal: navigating cyber security challenges in remote work policies. NPRC journal of multidisciplinary research.2024. Vol. 1, no.8. P.106–118. https://doi.org/10.3126/nprcjmr.v1i8.73042.

2. Office I. L., Messenger J. C. Telework in the 21st century: an evolutionary perspective. International Labour Organisation (ILO), 2019.

3. Sabin J. The future of security in a remote-work environment. Network security. 2021. Vol. 2021, no.10. P.15–17. https://doi.org/10.1016/s1353-4858(21)00118-5.

4. Rhodes C., Bettany A. Automating windows deployment with zero touch. Windows installation and update troubleshooting. Berkeley, CA, 2016. P. 119–137. https://doi.org/10.1007/978-1-4842-1827-3_5.

5. AlShalaan M. R., Fati S. M. Enhancing organizational data security on employee-connected devices using BYOD policy. Information. 2023. Vol. 14, no. 5. P. 275. https://doi.org/10.3390/info14050275.

Кіберзахист критичних активів у хмарній екосистемі

УДК 004.056

Ірина Вінковська[1], Анастасія Орлова[2]
Іван Сигляник[3]
Національний університет «Одеська політехніка»,
[1]vinkovska.i.s@op.edu.ua, [2]9480755@stud.op.edu.ua, [3]9560429@stud.op.edu.ua

Віртуалізація виробничих та управлінських процесів істотно розширює цифрову поверхню атаки. Головним об'єктом захисту стають міжсервісні канали обміну та спільні сховища даних.

Мета роботи – визначити ключові компоненти моделі доступу для захищеного обміну даними в умовах цифрової трансформації.

Ключовими об'єктами захисту залишаються інженерні файли дронів, телеметрія польотів і клієнтські реєстри. Пріоритети інформаційної безпеки вибудовуються у порядку: «конфіденційність – доступність – цілісність».

Значну частку інцидентів у розподілених командах спричиняє компрометація ідентичності (фішинг, повторне використання поролів, зловживання інсайдерів), тому управління доступом є головним елементом захисту.

Комбінація моделей RBAC та ABAC поєднує структуроване розподілення ролей із динамічним урахуванням контексту (час, геолокація, стадія проекту), забезпечуючи керовану гнучкість прав.

Багатофакторна аутентифікація (MFA) встановлюється базовою вимогою для доступу до критичних ресурсів і практично усуває ризик brute-force атак. Контекстно-залежна авторизація додатково перевіряє параметри сесії; спробу входу поза робочим часом або з нетипової мережі, проходять розширений контроль і обов'язково фіксуються. Повне журналювання операцій аутентифікації, зміни ролей та запитів до конфіденційних об'єктів формує надійну доказову базу і підтримує відповідність стандартам GDPR та ISO 27001. Принцип Zero Trust реалізується через короткострокові токени JWT (не більше 15 хвилин), що мінімізує ризики без шкоди продуктивності. Для впровадження СКД доцільно обрати Keycloak (гнучкість) або Azure (SLA, вбудований SSO). Безперервна SIEM-кореляція та автоматизовані дії скорочують інтервал від виявлення аномалії до блокування облікового запису до десятків секунд. Щоквартальна перевірка прав доступу дозволяють виявити та усунути надлишкові або застарілі привілеї, знижуючи ризик інсайдерських загроз. Запропонована архітектура керування доступом масштабується разом із підприємством і полегшує інтеграцію нових сервісів без суттєвого перегляду базових політик безпеки.

1. Іванов, І.В. Віртуальні підприємства: особливості управління. Економічний вісник. - 2022. – № 3. – С. 45-52.

2. Сидоренко, Л.П. Загрози інформаційної безпеки віртуальних підприємств. Безпека інформації. – 2023. №2. – С. 89-97.

Приховування тексту на зображеннях

УДК 621.395.7 (043.2)

Валерія Власова[1], Олена Головачова[2]
Національний університет «Одеська Політехніка»,
[1]9480749@stud.op.edu.ua, [2]holovachova@op.edu.ua

У сучасних інформаційних системах актуальним є одночасне забезпечення конфіденційності даних і контроль за поширенням небажаного контенту. Ефективним рішенням виступає поєднання стеганографії з автоматизованою модерацією тексту. Метою дослідження є алгоритм приховування тексту на зображенні та здійснення змістовної перевірки тексту на основі попередньо визначених вагових коефіцієнтів слів.

Алгоритм LSB реалізує приховування тексту шляхом заміни найменш значущих бітів кольорових каналів (RGB) бітами повідомлення. Кожен символ конвертується у 8-бітовий код, що послідовно вбудовується у пікселі зображення. Етапи кодування включають: завантаження зображення й тексту, перетворення тексту у бітовий потік, вставку бітів у пікселі, збереження результату [1].

На рис. 1 показано вхідне зображення, на рис. 2 — зображення після приховування тексту.

Рис. 1 — Зображення до приховування тексту

Рис. 2 — Зображення після приховування тексту методом LSB

На рис. 3 подано блок-схему роботи алгоритму. Вона ілюструє послідовну обробку вхідних даних.

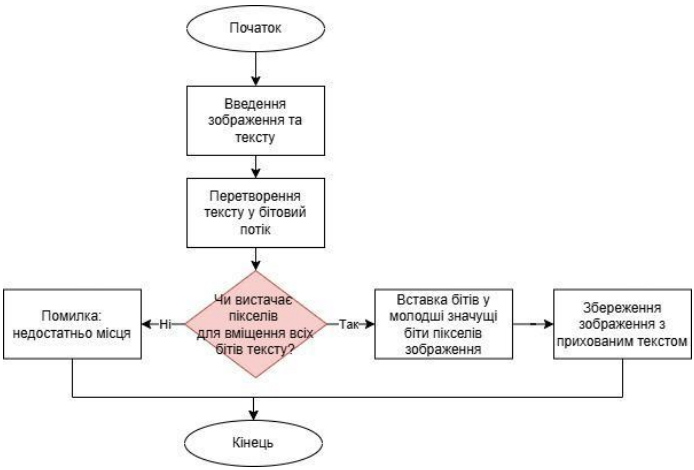


Рис. 3 — Блок-схема алгоритму LSB-стеганографії

Контент-фільтрація реалізована шляхом присвоєння кожному слову вагового коефіцієнта.

Сумарна оцінка повідомлення визначається як:

$$K = \sum_{i=1}^{n} k_i, \qquad (1)$$

де K— сума вагових коефіцієнтів, n — кількість проаналізованих слів,

k_i- вагові коефіцієнти

Якщо $K < 0$, система блокує повідомлення та фіксує користувача. Такий підхід дозволяє ефективно виявляти потенційно небезпечні повідомлення при мінімальних затратах обчислювальних ресурсів.

Метод LSB є ефективним для приховування текстової інформації в зображеннях без помітної втрати якості [2]. Його поєднання з системою фільтрації змісту дає змогу створювати прості, але надійні інструменти для безпечної передачі даних у цифрових каналах зв'язку.

1. Мішутін А.О. Стеганографія як метод забезпечення конфіденційності інформації. *Інформаційні технології та комп'ютерна інженерія*. – 2019. – №1(51). – С. 56–62.

2. Aldahdooh M., Jalab H.A. A Comprehensive Review on Medical Image Steganography Based on LSB Technique and Potential Challenges. Baghdad Science Journal. – 2021. – Vol. 18, No. 2(SI). – P. 74

Комерційні системи журналювання кіберінцидентів.

УДК 004.8:004.056

Ігор Власюк[1], Святослав Василишин[2]

Національний університет «Львівська політехніка»,
[1]Ihor.D.Vlasiuk@lpnu.ua, [2]sviatoslav.i.vasylyshyn@lpnu.ua

Процеси журналювання кіберінцидентів відіграють ключову роль у виявленні, аналізі, реагуванні та відновленні після інцидентів безпеки. Журналювання є не лише інструментом для виявлення, але й для розуміння повного обсягу інциденту, проведення післяінцидентного аналізу та виявлення слабких місць в організації системи комп'ютерної безпеки [1].

Особливістю сучасного етапу розвитку комерційних систем кібербезпеки є те, що абсолютна більшість компаній розвивають і включають в свої платформи інструменти штучного інтелекту. Для наукових і прикладних задач важливо мати узагальнену картину можливостей таких програмних продуктів щоб оцінювати існуючі тенденції та перспективи розвитку таких систем.

Мета роботи полягає в спробі оцінити їх можливості з точки зору розвитку можливостей штучного інтелекту (AI) в цілях журналювання кіберінцидентів

Серед систем журналювання кіберінцидентів прийнято розрізняти системи SIEM (Security Information and Event Management) [2] та системи XDR (Extended Detection and Response) [3]. Основні представлені на ринку системи мають в цілому подібний набір функціональних можливостей: централізований збір та агрегація журналів з різних джерел; механізми моніторингу та оповіщення в реальному часі; розширена кореляція подій та виявлення аномалій; інструменти розслідування інцидентів та криміналістичного аналізу; аналітика поведінки користувачів та об'єктів (UEBA); автоматизоване реагування на інциденти та оркестрація (SOAR); функції звітування, відповідності нормативним вимогам та візуалізації.

Останнім часом цей функціонал розширюється за рахунок інтеграції в системи журналювання AI систем сформованих на основі спеціалізованого машинного навчання (ML) та великих мовних моделей (LLM) універсального призначення. AI перетворює журналювання з пасивного процесу збору даних на активний інструмент для проактивного виявлення загроз, глибокого аналізу поведінки та прискорення реагування на кіберінциденти.

Таблиця 1

Особливості інтелектуальни функціональних можливостей комерційних систем журналювання кіберінцидентів

Постачальник	Назва продукту (+ система ШІ)	Інтелектуальні функції журналювання і аналізу кіберінцидентів
Splunk	Enterprise Security (+AI Assistant)	Генерація запитів: Використання LLM для створення SPL (Splunk Query Language) запитів з текстового опису. Автоматичний аналіз: Кластеризація логів, виявлення кореляцій між подіями.

		Підтримка рішень: Рекомендації щодо пріоритетності інцидентів
IBM	QRadar (+Watson AI)	Аналіз неструктурованих логів, автоматична класифікація інцидентів. Виявлення аномалій у шаблонах активності за допомогою машинного навчання (ML). Автоматичні пропозиції щодо реагування на основі історичних даних. Створення зрозумілих звітів за допомогою LLM .
Microsoft	Sentinel (+ OpenAI)	Сценарії реагування на інциденти на основі LLM. Перетворення сирих даних у структуровані інсайти за допомогою NLP. Виявлення трендів атак за допомогою ML-моделей. Copilot для кібербезпеки.
Google Cloud	(Google SecOps) (+ Vertex AI)	Попередження про загрози: Аналіз великих наборів даних для виявлення IoC (Indicators of Compromise). Пошук у логах за запитами природною мовою. ML-моделі для передбачення майбутніх векторів атак.
ManageEngine	Log360	UEBA: AI/ML використовується для виявлення аномальної активності. Моделі ML можуть виявляти відхилення від нормальних патернів у потоках логів. Обробка даних про загрози (Threat Intelligence): AI може допомагати в пріоритезації та кореляції індикаторів компрометації (IoC) з зовнішніх джерел з подіями в логах.
SolarWinds	Security Event Manager	Кореляція подій: ML для виявлення більш складних або неочевидних зв'язків між подіями з різних логів. AI/ML сприяє автоматичній класифікації та нормалізації логів з інших джерел
CrowdStrike	Falcon (+ Charlotte AI)	Виявлення загроз, аналіз інцидентів, автоматизація, звітування природною мовою Чат-інтерфейс для отримання інформації про загрози. Переклад технічних логів у зрозумілі інсайти. Генерація рекомендацій для нейтралізації інцидентів.

Palo Alto Networks	Cortex XDR	Автоматизація від виявлення до усунення загрози. LLM для інтерпретації логів у контексті бізнес-процесів. Динамічні шаблони - групування подій на основі поведінкових моделей UEBA.
ServiceNow	Security Operations - SecOps	Аналіз інцидентів (пріоритезація і виявлення аналогів), автоматизація, резюмування, запити і звітування природною мовою, рекомендації дій.

1. George, D. A. S., George, A. H., Baskar, T., Pandey, D. XDR: the evolution of endpoint security solutions-superior extensibility and analytics to satisfy the organizational needs of the future. *International Journal of Advanced Research in Science, Communication and Technology* . 2021. Vol. 8. No. 1. P. 493–501.
2. Kern, M., Landauer, M., Skopik, F., Weippl, E. A logging maturity and decision model for the selection of intrusion detection cyber security solutions. *Computers & Security*. 2024. Vol. 141. (10384).
3. Vielberth, M. Security information and event management (SIEM). In: *Encyclopedia of Cryptography, Security and Privacy*. Cham: Springer Nature Switzerland, 2025. P. 2304–2306.

Оптимізація адитивних генераторів Фібоначчі на основі примітивних поліномів для усунення слабких ключів

УДК 004.056

Олег Гарасимчук[1], Іван Опірський[2]
Національний університет "Львівська політехніка",
[1]oleh.i.harasymchuk@lpnu.ua, [2]ivan.r.opirskyi@lpnu.ua

Адитивні генератори Фібоначчі є різновидом генераторів псевдовипадкових чисел, що базуються на послідовності Фібоначчі та операції додавання. Завдяки своїй простоті та ефективності, вони знаходять широке застосування, зокрема в галузі кібербезпеки [1–2]. З огляду на зростаючий інтерес до таких генераторів, актуальним залишається завдання вдосконалення методів генерації псевдовипадкових послідовностей.

Встановлено, що адитивні генератори Фібоначчі (АГФ), реалізовані на основі примітивних поліномів у полі GF(p), формують псевдовипадкову послідовність з періодом повторення $p^k–1$, де k — ступінь полінома, для довільного початкового стану генератора (seed) [3]. Проте при непарних значеннях p вихідна бітова послідовність не відповідає статистичним вимогам, що зумовлено асиметрією у формуванні розрядів, внаслідок чого середнє співвідношення між 0 та 1 є нерівномірним.

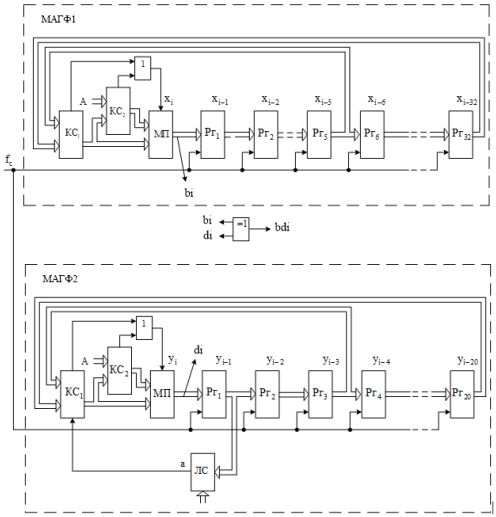
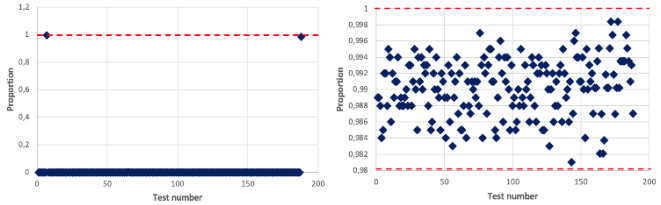


Рис. 1. Апаратна схема комбінованого генератора

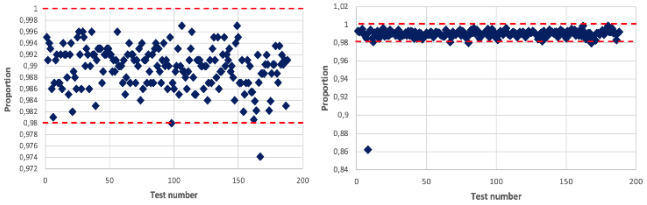
На рис. 1 наведена схема комбінованого генератора реалізованого на двох МАГФ: МАГФ1 – на основі примітивного поліному x32+x5+2 в полі GF(3) і МАГФ2 – на основі поліному y20+y3+1 з додатковою ЛС. Вихідна бітова послідовність формується на виході логічного елемента XOR.

Оцінювання проводилось за методикою NIST. Результати тестування комбінованого генератора наведено на рис. 2–3.



а б

Рис. 2. Статистичні портрети комбіновано генератора при z = 4:
а – без використання ЛС (hhh = 0), б – з ЛС (hhh = h0 xor h1)



а б

Рис. 3. Статистичні портрети комбіновано генератора при z = 10:
а – без використання ЛС (hhh = 0), б – з ЛС (hhh = h0 xor h3)

Результати дослідження показали, що додавання логічної схеми до комбінованого генератора суттєво покращує статистичні характеристики послідовності та забезпечує усунення слабких ключів завдяки збереженню максимального періоду повторення для всього діапазону початкових значень у MAFG на основі примітивних поліномів у полі GF(p).

1. Agarwal P., Agarwal N., Saxena R. Data encryption through fibonacci sequence and unicode characters, MIT International Journal of Computer Science and Information Technology, Vol. 5, No. 2, (August 2015), pp. 79-82 79 ISSN 2230-7621©MIT Publications.
2. Maksymovych, V.; Shabatura, M.; Harasymchuk, O.; Karpinski, M.; Jancarczyk, D.; Sawicki, P. Development of Additive Fibonacci Generators with Improved Characteristics for Cybersecurity Needs. Appl. Sci. (2022), 12(3), 1519.
3. Schneier, B. Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C; John Wiley & Sons, Inc.: Indianapolis, Indiana, 2015; ISBN 9781119183471.

Дослідження методів аналізу для вивчення різних аспектів ринку криптовалют

УДК 004 (519.8) Олександр Корченко[1], Антон Герасименко[2]
ДУІКТ, [1]o.korchenko@duikt.edu.ua, [2]a.herasymenko@stud.duikt.edu.ua

Розвиток методів аналізу для вивчення різних аспектів ринку криптовалют спрямовано на допомогу трейдерам та інвесторам приймати обґрунтовані рішення. До основних видів аналітики можна віднести [1]:

Технічний аналіз: вивчення історичних графіків цін та обсягів торгів для виявлення тенденцій та закономірностей, які можуть передбачити майбутні рухи цін. Використання різних індикаторів, таких як ковзні середні, RSI (індекс відносної сили), MACD (сходження/розбіжність ковзних середніх), смуги Боллінджера та рівні Фібоначчі. Використання графічних патернів для інтерпретації ринкової ситуації.

Фундаментальний аналіз: Оцінка внутрішньої вартості криптовалюти на основі різних факторів, таких як технологія, команда розробників, рівень

прийняття, партнерства, токеноміка та активність у ланцюжку (аналіз у мережі). Аналіз новин, подій та настроїв на ринку, які можуть вплинути на ціну криптовалют.

Ончейн-аналіз: Вивчення даних блокчейну, таких як кількість активних гаманців, обсяги транзакцій, комісії, розподіл монет, активність майнерів та смарт-контракти. Він допомагає виявити тенденції та настрої учасників ринку, а також оцінити стан та активність мережі.

Для забезпечення збору даних для аналізу криптовалют існує безліч платформ та інструментів [2]: Воні надають дані та функціонал для проведення аналізу: **Аналітичні платформи**: Santiment, Glassnode, Messari, CryptoQuant, Nansen (надають ончейн-дані, соціальні метрики та інші передові аналітичні інструменти). **Платформи технічного аналізу**: TradingView, Coinigy (пропонують широкий вибір графіків, індикаторів та інструментів для малювання). **Агрегатори даних**: CoinMarketCap, CoinGecko (надають інформацію про ціни, ринкову капіталізацію, обсяги торгів та іншу базову інформацію про різноманітні криптовалюти). **Crypto trackers**: програми та веб-сайти для відстеження цін на криптовалюти та портфелів. **Індикатори та боти**: Різні торгові індикатори та автоматизовані торгові системи (боти) для допомоги в аналізі та торгівлі. **Новинні та інформаційні ресурси**: сайти новин про криптовалюти, соціальні мережі та блоги для відстеження останніх подій та настроїв на ринку.

С точки зору авторів найбільш цікавим є ончейн-аналіз – це метод вивчення активності та даних, записаних безпосередньо в блокчейні. На відміну від технічного та фундаментального аналізу, який зосереджений на ринкових цінах та зовнішніх факторах, аналіз у ланцюжку вивчає самі транзакції, гаманці та смарт-контракти, щоб отримати уявлення про поведінку учасників мережі та загальний стан криптовалюти.

Ось деякі ключові аспекти ончейн-аналізу: **Основні принципи**: Прозорість: Більшість блокчейнів є загальнодоступними, що означає, що будь хто може переглядати історію всіх транзакцій і баланси гаманців. Незмінність:

дані, записані в блокчейні, не можуть бути підроблені або видалені, що забезпечує високий ступінь надійності. Відстеження: Хоча власники гаманців часто анонімні, рух коштів між гаманцями повністю відстежується. **Ключові метрики та індикатори**: Аналіз у ланцюжку використовує різноманітні показники для оцінки стану мережі та поведінки користувачів. Ось деякі з найважливіших з них: Кількість активних адрес; Обсяг транзакції; Середній розмір транзакції; Кількість нових адрес; Кількість нульових адресних

балансів; Розподіл монет (власність) ; Coin Age (HODL Waves; Обмінні потоки; Плата за газ; Активність розробника; Активність смарт-контрактів (для мереж з такими функціями, як Ethereum); Загальна заблокована вартість (TVL) у DeFi.

Існує ряд платформ та інструментів, які надають дані та візуалізації для аналізу в мережі: • Glassnode: одна з провідних платформ, яка пропонує широкий спектр ончейн-метрик та інструментів аналітики. • Santiment: надає не тільки дані в мережі, але й соціальні метрики та дані про настрої ринку. •

Nansen: спеціалізується на аналізі активності розумних грошей та відстеженні потоків капіталу. • Messari: пропонує як фундаментальні дані, так і деякі ончейн-метрики з акцентом на якість даних. • CryptoQuant: надає дані про обмінні потоки, активність майнерів та інші корисні показники. • Dune

Analytics: дозволяє користувачам створювати власні інформаційні панелі та аналізувати дані смарт-контрактів. • Etherscan, BscScan, Arbiскан та інші блокчейн-експловери: надають основну інформацію про транзакції, гаманці та смарт-контракти конкретних мереж.

Цей огляд демонструє зростаючий інтерес наукової спільноти до використання аналізу в ланцюжку для вивчення різних аспектів ринку крипто валют. Дані дослідження охоплюють широкий спектр тем, від прогнозування цін і виявлення ринкових аномалій до аналізу безпеки і фундаментальних характеристик блокчейн-мереж. Подальші дослідження в цій галузі сприятимуть більш глибокому розумінню динаміки та потенціалу крипто валютних активів.

1. Jin, M., Liu, R., & Monperrus, M. (2025). *On-Chain Analysis of Smart Contract Dependency Risks on Ethereum*. arXiv. https://arxiv.org/abs/2503.19548

2. Dalia Elbanna, Ema Izati Zull Kepili1 , Nik Hadiyan Nik Azman. *Beyond Conventional Methods: Advancing Ethereum Price Prediction through Integrated Technical, On-Chain, and Machine Learning Approaches*. INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ACCOUNTING, FINANCE & MANAGEMENT SCIENCES Vol. 1 5 , No. 2, 2025, E-ISSN: 2225-8329 © 2025. https://hrmars.com/papers_submitted/24968/beyond-conventional-methods-advancing_ethereum-price-prediction-through-integrated-technical-on-chain-and_machine-learning-approaches.pdf

Розробка алгоритму перевірки інформаційної складової сайтів на фейкшопінг та фішинг

УДК 004.056.53

Софія Гіленко
Національний університет «Одеська політехніка»,
9480588@stud.op.edu.ua

Фейкові інтернет-магазини та фішингові вебсайти є одними з найпоширеніших форм онлайн-шахрайства[1], які завдають щорічно мільярдних збитків споживачам і бізнесу. Візуальна подібність таких ресурсів до легітимних магазинів, їх активна реклама в соцмережах, високоякісний дизайн і фейкові відгуки суттєво ускладнюють відрізнення шахрайських сторінок від справжніх. З іншого боку, фішинг як окремий напрям використовує соціальну інженерію, URL-омографи, маніпуляції з доменами та глибокі підробки для виманювання конфіденційних даних. У сучасних умовах, коли багато таких ресурсів працюють лише кілька днів, традиційні методи, що спираються на чорні списки чи ручну перевірку, стають неефективними[2].

Метою цієї роботи є розробка ефективного, автоматизованого алгоритму для виявлення фейкових онлайн-магазинів та фішингових ресурсів на основі комплексного аналізу вебконтенту, метаінформації та структури URL. Для цього використано мову програмування Python та набір бібліотек, зокрема: requests для отримання HTML, BeautifulSoup для парсингу структури сторінки, Scikit-learn для машинного навчання, tldextract для аналізу доменів та інші засоби роботи з вебданими.

Сформовано набір ознак, які відображають найбільш характерні властивості шахрайських сайтів. Сюди входять: відсутність HTTPS-захисту, довжина та структура доменного імені, присутність підозрілих слів у URL ("sale", "discount", "secure"), використання IP-адреси замість домену, відсутність контактної інформації на сторінці, кількість форм для введення особистих даних, повторювані шаблони HTML-структури тощо. Також враховувались часові характеристики, такі як вік домену та термін реєстрації.

Для навчання моделі використано збалансовану вибірку реальних вебсайтів, що включала як фейкові магазини й фішингові сторінки, так і легітимні ресурси популярних брендів. Було протестовано декілька моделей класифікації: Decision Tree, Random Forest, Logistic Regression, із подальшим вибором Random Forest через його стабільність, високу точність та збалансовані значення метрик, зокрема точності, повноти та F-міри[3]. Векторизацію виконано через словникове кодування категоріальних ознак та нормалізацію числових.

Результати експериментів показали точність класифікації понад 80 % при збереженні високих значень Precision і Recall. Також було проведено аналіз важливості ознак, який дозволив встановити, що найбільший внесок у детекцію дають показники URL, наявність форм авторизації, вік домену та ознаки копіпейст-дизайну. Це підтверджує практичну значущість використаних фіч.

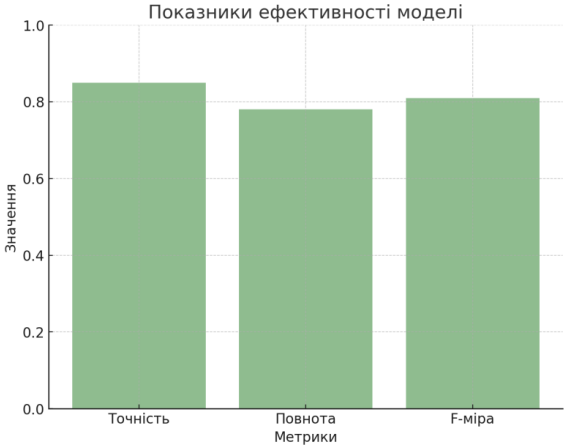


Рис. 1 – Показники ефективності моделі.

Розроблений алгоритм легко масштабовується та може бути використаний як окремий компонент у браузерному розширенні, у системі внутрішнього моніторингу трафіку компаній або як частина інтерактивного навчального інструменту з кібергігієни. Крім цього, він має потенціал до розвитку — у подальших роботах планується інтеграція моделей глибокого навчання для контентного аналізу, включення аналізу зображень та впровадження динамічного аналізу поведінки сторінки при взаємодії з користувачем.

Таким чином, створений інструмент є гнучким, адаптивним рішенням для реального виявлення шахрайських сайтів і дозволяє значно підвищити інформаційну безпеку користувачів у сфері електронної комерції.

1. Sabillon R., Cano M. J., Serra-Ruiz J., Cavaller V. Cybercrime and Cybercriminals: A Comprehensive Study. International Journal of Computer Networks and Communications Security. 2016. Vol. 4. P. 165–176.
2. Zhang Y., Hong J. I., Cranor L. F. CANTINA: A Content-Based Approach to Detecting Phishing Web Sites. Proceedings of the 16th International Conference on World Wide Web (WWW'07). 2007. P. 639–648.
3. Marchal S., Saari K., Singh N., Asokan N. Know Your Phish: Novel Techniques for Detecting Phishing Sites and Their Targets. IEEE Transactions on Dependable and Secure Computing. 2017. Vol. 15(4). P. 594–607.

Модифікація квантового протоколу BB84 за допомогою системи залишкових класів

УДК 004.056.55

Анастасія Гнатюк[1], Михайло Касянчук[2], Павло Басістий[3]

[1,2]Західноукраїнський національний університет, [3]Тернопільський національний педагогічний університет імені Володимира Гнатюка,
[1]anastasia.hn88@gmail.com, [2]kasyanchuk@ukr.net, [3]basi@ukr.net

Квантова криптографія використовує принципи квантової механіки для встановлення каналів зв'язку між двома об'єктами і визначає методи безпечного спілкування через введення принципів квантової механіки для генерації ключів шифрування [1]. На відміну від класичної, квантова криптографія забезпечує свою безпеку через незмінні закони фізики, що призводить до її виняткової захищеності навіть відносно найскладніших обчислювальних систем [2].

Квантовий протокол розподілу ключів BB84 покладається на такі принципи квантової фізики:

1) принцип невизначеності Гейзенберга, який стверджує, що в квантовій системі можна точно визначити лише одну з пари спряжених величин, наприклад, координата та імпульс (вимірювання положення частинки призведе до порушення її швидкості). Квантова криптографія використовує це, застосовуючи поляризацію фотонів;

2) теорема про заборону клонування як наслідок попереднього принципу стверджує, що неможливо створити ідентичні копії невідомого квантового

стану. Завдяки цьому можна виявити, чи хтось перехопив квантовий канал під час критичної передачі інформації;

3) квантова заплутаність: незалежно від відстані дві квантові частинки можуть бути заплутані. Коли певна властивість вимірюється в одній частинці, то корельований стан цієї властивості з'явиться в іншій частинці.

Протокол BB84 використовує квантові стани для обміну секретним ключем між двома сторонами — Алісою (відправником) та Бобом (отримувачем). Він складається з двох фаз: квантової (передача фотонів) і класичної (узгодження ключа та виправлення помилок).

Передбачається два способи використання СЗК в протоколі BB84: для кодування квантових станів та постобробки ключа. Розглянемо кожен спосіб окремо.

Для використання СЗК в кодуванні станів, Аліса та Боб перед початком формування секретного ключа повинні обрати певний модуль та довільні залишки при діленні на нього, а також присвоїти деякий залишок кожному фільтру поляризації. Після цього відбувається процес формування ключа згідно протоколу BB84. Далі отриманий секретний ключ перевіряється на підслуховування та обчислюється за заздалегідь обраним модулем. Таким чином отримується фінальний ключ.

Даному методу інтеграції протоколу BB84 та СЗК властиві такі переваги:

1) збільшення пропускної здатності ключа, оскільки у класичному виконанні протоколу BB84 одним фотоном кодується один біт. При використанні СЗК із модулем m кожен фотон передаватиме $\log_2 m$ бітів. Наприклад, для модуля 4 із залишками (0, 1, 2, 3) буде передаватися 8 бітів замість чотирьох, як в класичному протоколі;

2) гнучкість кодування досягається за допомогою можливості адаптації протоколу BB84 до різних модулів, що дає змогу масштабувати обсяг інформації залежно від потреб системи без зміни апаратної основи;

3) сумісність із криптосистемами, які працюють із багатозначними станами, що може бути корисним для майбутніх квантових алгоритмів;

4) збереження квантової безпеки завдяки основному принципу протоколу BB84 – виявлення підслуховування через квантові помилки.

Для використання СЗК в постобробці ключа Аліса та Боб спершу повинні виконати ті ж кроки, що і в класичному протоколі BB84. Після цього по класичному каналу вони обговорюють кількість модулів та їх значення і отриманий секретний ключ переводять в десяткову систему числення. Фінальний ключ отримується після обчислення залишків секретного ключа за обраними модулями.

Перевагами даного методу інтеграції є:

1) стиснення ключа внаслідок перетворення двійкового числа в десяткове і пошук його залишку за модулем;

2) простота інтеграції з модульними криптосистемами досягається через використання ключа у форматі залишку, який може бути застосованим в системах на основі модульної арифметики без додаткових перетворень;

3) оптимізація корекції помилок через використання залишків в якості контрольних сум для блоків ключа, що полегшить виявлення помилок при передачі каналами зв'язку;

4) гнучкість масштабування через можливість зміни модуля, що дозволить адаптувати розмір ключа до потреб системи без змін у квантовій частині протоколу;

5) збереження безпеки в зв'язку з незмінністю квантової частини протоколу BB84.

Отже, введення СЗК у кодування квантових станів більше підходить для систем, де пріоритетом є максимізація пропускної здатності квантового каналу, а введення СЗК у постобробку ключа є простішим у реалізації та ідеальним для систем із обмеженими ресурсами чи потребою в інтеграції з модульними алгоритмами. Крім того, перший метод передбачає кодування квантових станів в СЗК за допомогою обраних залишків певного модуля та обрахунок отриманого секретного ключа за модулем. Другий метод дозволяє стиснути отриманий з протоколу BB84 двійковий секретний ключ у більш компактний вигляд через переведення його в десяткову систему числення та обчислення за обраним модулем.

1. S.Pirandola at al. "Advances in quantum cryptography." *Advances in Optics and Photonics*. Vol.12, no.4, pp.1012-1236, 2020.

2. M.Swan, R. dos Santos, F.Witte. "Quantum Information Science." *IEEE Internet Comput.* Vol.26, pp.7–14, 2021.

Метод шифрування на основі афінних перетворень в системі залишкових класів

УДК 004.056.55

Михайло Голембйовський[1], Михайло Касянчук[2], Олег Момотюк[3]

Західноукраїнський національний університет,
[1]mykhailo.2097@gmail.com, [2]kasyanchuk@ukr.net , [3]momotjuk98@gmail.com

Забезпечення захисту інформаційних потоків є одним із ключових викликів сучасного цифрового середовища. Для вирішення цього завдання важлива роль відводиться криптографічним методам [1]. Афінні шифри завдяки своїй простоті та швидкодії часто застосовуються у пристроях з обмеженими обчислювальними ресурсами, таких як мобільні телефони, вбудовані системи та Інтернет речей. Крім того, важливим є врахування того, що з кожним роком зростає кількість пристроїв, які потребують захищеного обміну даними. Саме тому необхідність у легких і стійких до атак шифрах постійно зростає, що підкреслює актуальність удосконалення афінного шифру, який має відому вразливість до частотного аналізу, що обмежує сферу його застосування.

У класичному афінному шифрі кожному символу повідомлення x відповідає числовий код, над яким виконується лінійне перетворення за модулем розміру алфавіту: $X=(ax+s) \bmod n$. При цьому параметри a та s виступають ключами шифрування. Недоліком такого методу є те, що знання кількох відкритих пар «символ-шифр» дозволяє легко відновити ключі. Для подолання цієї проблеми

використовується система залишкових класів (СЗК), де повідомлення представляється через набір залишків b_i по відношенню до кількох взаємно простих модулів p_i. Такий підхід значно ускладнює процес криптоаналізу для сторонніх осіб, оскільки зловмиснику необхідно враховувати кілька модулів одночасно, що потребує набагато більше ресурсів для злому [2].

В запропонованому методі блок відкритого повідомлення N подається у вигляді залишків $b_i=N \bmod p_i$. Далі над кожним залишком незалежно виконується афінне перетворення: $B_i=(a_ib_i+s_i) \bmod p_i$. Отримані змінені залишки або об'єднуються в єдине число за допомогою китайської теореми про залишки (КТЗ), або конкатенуються для формування шифртексту. Такий підхід забезпечує не тільки розподіл обчислень між незалежними модулями, але й значно збільшує кількість можливих комбінацій ключів, що підвищує стійкість системи до атак перебором. Таким чином, кожна операція над окремим залишком є самостійною та незалежною, що підвищує гнучкість системи та полегшує її масштабування під різні вимоги.

Процес розшифрування передбачає обчислення початкових залишків шляхом застосування зворотних афінних перетворень та використання КТЗ для відновлення оригінального повідомлення. Наведено приклади практичного використання методу для різних конфігурацій модулів і ключів, у тому числі для часткових випадків афінного шифру: шифру зсуву та лінійного шифру без зсуву. Варто відзначити, що коректний вибір модулів суттєво впливає на якість розшифрування, адже вибір взаємно простих чисел забезпечує однозначність відновлення вихідного повідомлення.

Важливим аспектом розгляду є оцінка криптографічної стійкості системи. Проаналізовано вплив кількості модулів та їх розрядності на загальну стійкість алгоритму до криптоаналізу. Показано, що із збільшенням кількості модулів та їх розрядності стійкість системи значно підвищується. Проведено оцінку параметрів, при яких криптостійкість запропонованої системи відповідає рівню безпеки симетричного алгоритму AES-256, що є сучасним еталоном захищеного шифрування. Зростання розрядності модулів також збільшує складність підбору правильного ключа методом перебору, що суттєво покращує загальну безпеку системи.

Дослідження підтвердило, що використання афінного шифру в СЗК дозволяє поєднати високу швидкодію шифрування та дешифрування з підвищеним рівнем безпеки. Такий підхід є перспективним для впровадження у системах з високими вимогами до швидкодії та обмеженими ресурсами. Окремо відзначено можливість масштабування методу шляхом вибору відповідної кількості модулів та їх розрядності. Це дозволяє пристосовувати систему до різних сценаріїв використання — від захисту коротких повідомлень до забезпечення безпеки великих обсягів даних у хмарних обчисленнях.

Перспективними напрямами подальших досліджень є розробка матричних афінних шифрів у СЗК, а також програмно-апаратна реалізація запропонованого алгоритму для оцінки його практичної ефективності в реальних умовах. Застосування досконалої та модифікованої досконалої форм СЗК відкриває нові можливості для оптимізації швидкодії та стійкості розробленої криптосистеми. Подальший розвиток цього напряму може

забезпечити створення нових типів симетричних шифрів, що будуть відзначатися особливою ефективністю і високим рівнем захисту інформації.

Крім того, важливим є питання оптимізації процесів генерації та управління ключами у запропонованій криптографічній системі. Завдяки використанню СЗК можливо здійснювати ефективну генерацію ключів з високим ступенем випадковості, що додатково підвищує загальний рівень захисту шифрування. Такий підхід дозволяє враховувати вимоги до безпеки в умовах різного рівня загроз та адаптувати параметри системи під конкретні застосування.

Особливу увагу приділено аналізу потенційних напрямів атак на розроблений алгоритм, серед яких виділено атаки перебору, частотний аналіз змінених залишків та спроби відновлення структури модулів. Запропоновано базові методи протидії цим загрозам шляхом збільшення кількості модулів, вибору великих простих чисел як модулів та варіювання способу представлення шифртексту. Це забезпечує високий рівень надійності навіть за умови застосування розширених криптоаналітичних технік зі сторони потенційного зловмисника.

1. Kasianchuk M.M., Yakymenko I.Z., Nykolaychuk Y.M. Symmetric Cryptoalgorithms in the Residue Number System. *Cybernetics and Systems Analysis*. 2021. Vol. 57(2). P. 329–336.

2. Kasianchuk M, Shevchuk R, Adamyk B, Benson V, Shylinska I, Holembiovskyi M. Affine Cipher Encryption Technique Using Residue Number System. *Cryptography*. 2025. Vol. 9(2): 26.

Розробка програмного застосунку для захисту акустичного каналу витоку інформації

УДК 004.056.5:004.4

Богдан Горбатій

Національний університет «Одеська політехніка»

Кожного дня зв’являються нові різноманітні види кіберзагроз, які становлять пряму проблему для захисту конфіденційної інформації. На сьогодні, існує досить велика кількість каналів витоку інформації, які можуть бути скомпрометовані за допомогою різних пристроїв, які надають можливість перехоплювати важливі дані, які доступні невеликій кількості людей [1].

Одним із найпоширеніших каналів витоку інформації є акустичний. Акустичний канал витоку інформації – це спосіб передачі конфіденційної інформації через звукові сигнали, які можуть бути перехоплені або прослухані. Це явище стає все більш актуальним у сучасному світі, де захист інформації є критично важливим. Основним середовищем для акустичних сигналів є повітря. Звукові хвилі можуть поширюватися на значні відстані, що робить їх вразливими для прослуховування. Джерелами акустичної інформації можуть бути голосові зв'язки, динаміки та інші вібруючі тіла [1].

Класифікація акустичних каналів має наступну конфігурацію (рис. 1):

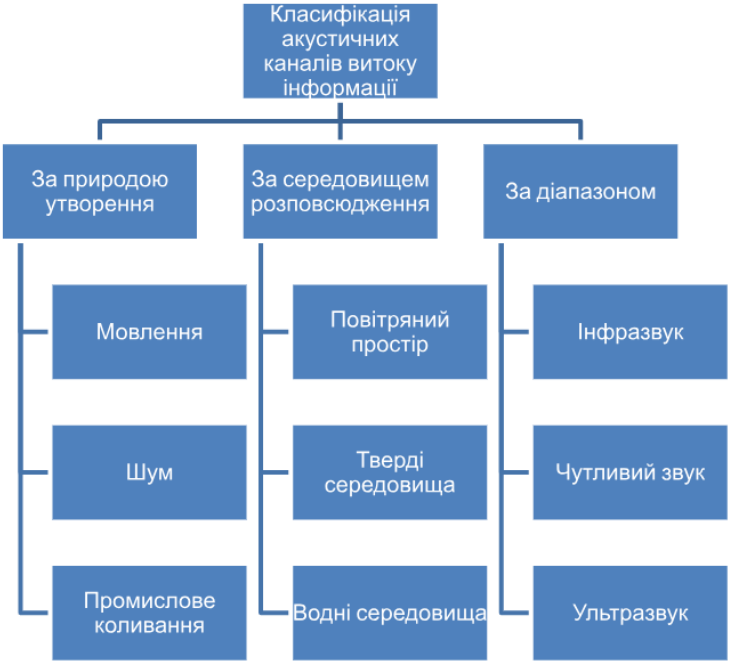


Рис. 1 Класифікація акустичних каналів витоку інформації

Існуючі алгоритми захисту акустичного каналу витоку інформації генеруючи маскуючі сигнали не проводять оцінку акустичної ситуації, яка існує в контрольованому приміщені. Це в свою чергу створює передумови для витоку конфіденційної інформації.

Для попередження витоку інформації було розроблено програмне забезпечення на мові програмування Python, яке дозволяє створювати шумові перешкоди в залежності від акустичної ситуації, яка існує в підконтрольному приміщенні. Програмний застосунок дозволяє регулювати рівень амплітуди шуму, показник SNR (відношення сигналу до шуму) та налаштовувати діапазони нижніх та верхніх частот, щоб підвищити рівень перешкоджання витоку інформації по акустичному каналу.

Приклад графічного інтерфейсу застосунку представлений на рис. 2:

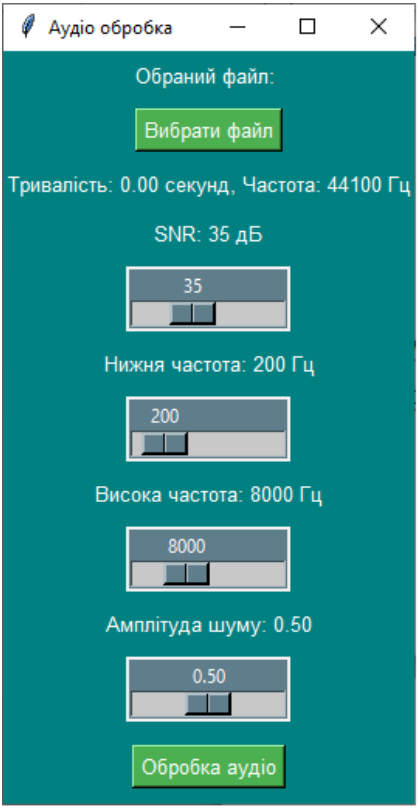


Рис. 2 Графічний інтерфейс програмного застосунку для захисту акустичного каналу витоку інформації

Таким чином, даний застосунок, в залежності від акустичного фону в приміщенні дозволяє створювати достатньо сильні шумові перешкоди, які не дозволяють перехопити конфіденційну інформацію.

1. Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник. Київ: ІСЗЗІ НТУУ «КПІ», 2016. 104 с.

2. Глоба О. В., Білецький С. В., Чубар А. А. Захист інформації: підручник. Київ, 2018. 430 с.

3. Златопольський Д.М. Основи програмування мовою Python. Київ, 2017. 284 с.

Забезпечення безпеки зберігання паролів у застосунках за допомогою бібліотеки Bcrypt

УДК 621.395.7 (043.2)

Дмитро Гріднєв[1], Юлія Козіна[2]

Національний університет "Одеська політехніка",
[1]9560448@stud.op.edu.ua , [2]yuliya.kozina@keenethics.com

Паролі є ключовим засобом аутентифікації, але їхнє зберігання без захисту або із застосуванням слабких алгоритмів хешування (наприклад, MD5, SHA-1) робить системи вразливими до атак rainbow table та brute force. Так, у 2012 році через погане хешування зламали 6,5 млн акаунтів LinkedIn, а у 2022 році було скомпрометовано понад 24 млрд паролів. Сучасні обчислювальні можливості, зокрема паралельні обчислення на GPU та FPGA, ще більше підкреслюють необхідність вибору надійних методів, таких як Bcrypt, для захисту конфіденційної інформації[1].

У даній роботі досліджується використання бібліотеки Bcrypt як оптимального рішення для безпечного зберігання паролів. Bcrypt поєднує в собі адаптивну складність, використання солі та простоту інтеграції, що робить його стійким до сучасних атак і придатним для широкого спектру застосунків.

Bcrypt це бібліотека для хешування паролів, заснована на алгоритмі шифрування Blowfish, розробленому Брюсом Шнаєром. На відміну від традиційних хеш-функцій (наприклад, MD5 чи SHA), які були створені для швидкого обчислення, Bcrypt розроблений спеціально для зберігання паролів і має вбудовані механізми захисту від атак[2].

Основними компонентами Bcrypt є сам пароль(P) це текст, введений користувачем, який потрібно захешувати. Bcrypt підтримує паролі довжиною до 72 байтів, що є важливим обмеженням для врахування. Другим компонентом

є "сіль(S)" це випадково згенерована послідовність бітів (128 біт або 16 байтів), яка додається до пароля для унікальності кожного хешу. Останній компонент це робочий фактор(cost) це ціле число (зазвичай від 4 до 31), яке визначає логарифмічну кількість ітерацій у процесі хешування. Чим вище cost, тим більше часу потрібно для обчислення хешу.

Процес хешування в Bcrypt складається з кількох етапів.В першому етапі використовуючи криптографічно стійкий генератор випадкових чисел, створюється унікальна сіль для кожного пароля. Наступним етапом пароль і сіль передаються до функції EksBlowfish (Expensive Key Schedule Blowfish), яка виконує серію обчислень, залежних від параметра cost. Кількість ітерацій визначається як 2^{cost}. Наприклад, при cost = 12 виконується $2^{12} = 4096$ ітерацій.

$$Key = EksBlowFish(P,\ S,\ cost) \quad (1)$$

де P – пароль, S = сіль, cost = робочий фактор.

В другому етапі фіксований текст шифрується, отриманий ключ використовується для шифрування константи "OrpheanBeholderScryDoubt" (24 байти) за допомогою алгоритму Blowfish у режимі ECB.

$$H = Encrypt(Key, "OrpheanBeholderScryDoubt") \quad (2)$$

де Key – створений ключ, OrpheanBeholderScryDoubt – константа для шифрування.

Bcrypt розроблений для захисту від двох основних типів атак на паролі.

Атаки типу Rainbow Table це заздалегідь обчислені таблиці хешів для популярних паролів. Завдяки унікальній солі для кожного пароля, Bcrypt робить ці таблиці марними, адже довелося б генерувати нову таблицю для кожної солі, що є обчислювально невигідним. Ще одною атакою є Brute Force передбачає перебір усіх можливих комбінацій пароля. Параметр cost значно уповільнює цей процес. Наприклад для пароля з 8 символів, кількість можливих комбінацій $62 = 2.18 \times 10^{14}$, при cost = 12, час на один хеш = 0.3 секунди. Загальний час атаки буде становити $= 0.3 \times 2.18 \times 10^{14} \approx 2.07$ мільйони років. Навіть для коротких паролів Bcrypt забезпечує високу стійкість, а для довших комбінацій час атаки стає астрономічним.

У розробленому тестовому середовищі було проведено випробування методом brute force для розшифровування пароля "toras3$" (довжина 7 символів, cost = 10), що у зашифрованому вигляді представлений як $2a$10$e9QzH0VTWujn.38u9Zm0hOv8/IjSnLOquij1d8iQqVLzBFJPWUkj2.

Протягом п'яти днів систематичного перебору комбінацій за допомогою високопродуктивних обчислювальних ресурсів, пароль так і не був підібраний, що додатково підтверджує стійкість алгоритму Bcrypt до атак типу brute force.

Для оцінки переваг Bcrypt розглянемо його порівняння з іншими методами:

1) MD5 і SHA-1 їх основною перевагою є швидкість обчислень, але головним недоліком є висока вразливість до rainbow table і brute force атак.. 2)Argon2 перевагою є Використання пам’яті для ускладнення атак на GPU/FPGA, та недоліками є складність в реалізації та використання великої кількості ресурсів[3].

Отже з виділених методів можна виділити такі переваги Bcrypt це простота інтеграції (доступні бібліотеки для Python, Node.js, C# тощо). Адаптивність (cost) можна збільшувати зі зростанням обчислювальних потужностей. Але головним недоліком методу є менша стійкість до атак на спеціалізованому обладнанні порівняно з Argon2. Тому в результаті дослідження можна сказати що Bcrypt є ефективним інструментом для захисту паролів в більшості застосунках завдяки своїй адаптивності та стійкості до атак.

1. Hope A. Over 24 Billion Compromised User Credentials Circulating on the Dark Web Market. *CPO Magazine*. 2022. URL: http://cpomagazine.com/cyber-security/over-24-billion-compromised-user-credentials-circulating-on-the-dark-web-market/.

2. Batubara T. P., Efendi S., Nababan E. B. Analysis Performance BCRYPT Algorithm to Improve Password Security from Brute Force. *Journal of Physics:*. 2021. URL: https://doi.org/10.1088/1742-6596/1811/1/012129

3. Password Hashing Competition - Survey and Benchmark. George Hatzivasilis, Ioannis Papaefstathiou , Charalampos Manifavas, 2020, 2- 8 p.

Розробка захищеного веб-застосунку для бронювання місць у ресторанах

УДК 004.738.5 (043.2)

Владислава Громова[1], Олена Агаджанян[2]

Національний університет «Одеська Політехніка»,
[1]9480585@stud.op.edu.ua, [2]o.v.ahadzhanian@op.edu.ua

Стрімкий розвиток веб-технологій та активне впровадження онлайн-сервісів у сфері обслуговування зумовлюють підвищені вимоги до забезпечення інформаційної безпеки [1]. Однією з актуальних задач є захист даних у веб-застосунках для бронювання місць у ресторанах, де обробляються персональні дані користувачів і платіжна інформація.

Метою дослідження є розробка захищеного веб-застосунку, що дозволяє користувачам здійснювати реєстрацію, авторизацію, бронювання місць та оформлення замовлень із гарантованим захистом даних від поширених загроз, таких як несанкціонований доступ, SQL-ін'єкції, атаки типу XSS та Brute Force [1].

Архітектура системи реалізована відповідно до принципів клієнт-серверної моделі. У веб-застосунку передбачено окремі модулі для аутентифікації, управління сесіями, обмеження частоти запитів, обробки даних про замовлення та резервування [2].

На рис. 1 представлено класову діаграму, яка ілюструє основні компоненти системи, їхні атрибути та методи, а також зв'язки між об'єктами. Особливу увагу приділено класам User, Token, Limiter, що реалізують механізми безпеки.

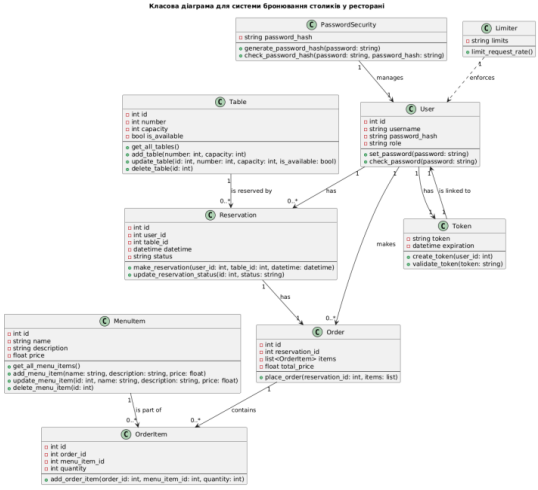


Рис. 1 — Діаграма класів системи

У реалізації захисту авторизації було використано хешування паролів із застосуванням алгоритму bcrypt, що забезпечує надійний захист паролів навіть у випадку компрометації бази даних. Для контролю доступу застосовуються JWT-токени, які дозволяють уникати зберігання сесій на сервері.

На рис. 2 показано загальну діяльність системи в процесах реєстрації, входу, обробки замовлень та адміністрування. Видно, як у процесі реєстрації створюється користувач, виконується перевірка даних і формується токен.

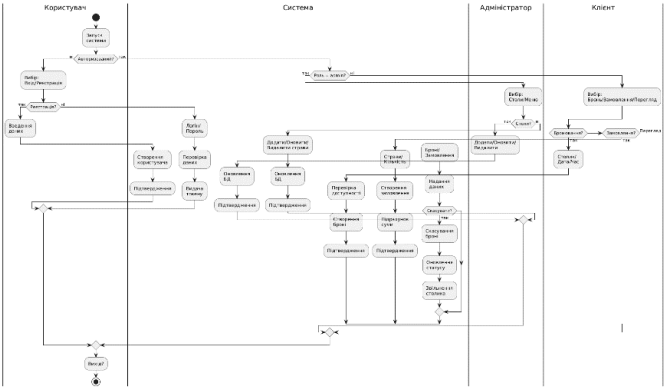


Рис. 2 — Діаграма діяльності процесу автентифікації та обробки замовлень

Серверна частина системи реалізована на Flask із підключенням SQLite як легковагого рішення для зберігання інформації. Реалізовано такі компоненти безпеки: 1. Шифрування трафіку з використанням HTTPS; 2. Захист від SQL-ін'єкцій шляхом використання параметризованих запитів; 3. Захист від CSRF-атак через впровадження унікальних токенів; 4. Обмеження кількості запитів з однієї IP-адреси для запобігання брутфорс-атакам [3].

Результати тестування засвідчили ефективність впроваджених механізмів. Система коректно реагує на спроби повторного входу з неправильними обліковими даними, блокує підозрілу активність та забезпечує цілісність транзакцій під час взаємодії з базою даних.

Запропонований веб-застосунок є універсальним прикладом для створення безпечних систем у сфері ресторанного сервісу, а запропоновані підходи можуть бути масштабовані на інші галузі електронного обслуговування.

1. Goodrich, M.T. та Tamassia, R. Introduction to Computer Security. Boston: Addison-Wesley, 2011. 478 с.

2. Гонтар, О. Аналіз впливу іноземного IT-бізнесу на ландшафт загроз кібербезпеці держави [Електронний ресурс] / О. Гонтар // ResearchGate. 2023. – Режим доступу: https://www.researchgate.net/publication/375035877

3. Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: філософія, філософія права, політологія, соціологія. – Харків: Право, 2022. – № 3(54). – 240 с.

Дослідження методів розпізнавання обличчя

УДК 621.395.7(043.2)

Анатолій Давиденко[1], Олена Висоцька[2], Михайло Пригара[3], Володимир Щербина[4]

[1]Інститут проблем моделювання ім.Г.Є. Пухова НАНУ davidenkoan@gmail.com, [2] Державний університет «Київський авіаційний інститут», Lek_Vys@ukr.net, [3] Ужгородський національний університет, misha_prigara@ukr.net, [4] Державний університет «Київський авіаційний інститут», shcherbyna.v.p@gmai.com

Розпізнавання обличчя – це технологія, яка використовує алгоритми штучного інтелекту для ідентифікації або верифікації особи з цифрового зображення або відеокадру. Існує кілька методів розпізнавання обличчя[1]:

1. Геометричні методи (на основі рис обличчя):

Аналіз рис обличчя: Вимірює відстані та співвідношення між певними точками на обличчі, такими як очі, ніс, рот і підборіддя.

Метод власних облич (Eigenfaces): Перетворює зображення обличчя в набір "власних облич", які є основними компонентами обличчя. Потім обличчя порівнюється з базою даних власних облич.

2. Фотометричні методи (на основі текстури обличчя):

Локальні бінарні шаблони (LBP): Аналізує текстуру обличчя, порівнюючи кожен піксель з його сусідніми пікселями.

Глибинне навчання: Використовує нейронні мережі для вивчення складних шаблонів і характеристик обличчя. Цей метод є найбільш точним і широко використовуваним на сьогоднішній день.

3. 3D-розпізнавання обличчя:

Використовує 3D-датчики для збору інформації про форму обличчя, що робить його менш чутливим до змін освітлення та виразу обличчя.

4. Аналіз текстури шкіри:

Використовує візуальні деталі шкіри, зафіксовані на сканованих зображеннях видимого світла.

Застосування розпізнавання обличчя:

Безпека: контроль доступу, спостереження, ідентифікація злочинців.

Маркетинг: персоналізована реклама, аналіз поведінки клієнтів.

Соціальні мережі: тегування фотографій, фільтри.

Медицина: діагностика генетичних захворювань.

Мобільні пристрої: розблокування телефону, оплата.

Переваги розпізнавання обличчя:

Висока точність (особливо з використанням глибокого навчання).

Не потребує фізичного контакту.

Може використовуватися в режимі реального часу.

Недоліки розпізнавання обличчя:

Може бути неефективним у поганому освітленні або зміні виразу обличчя.

Викликає занепокоєння щодо конфіденційності та етичних питань.

Можливість помилок, особливо при розпізнаванні облич людей з іншим кольором шкіри.

Важливо зазначити, що технологія розпізнавання обличчя постійно розвивається, і нові методи та алгоритми з'являються регулярно.

Основні напрями розвитку технології розпізнавання облич зосереджені на покращенні точності, надійності та етичності систем. Ось деякі ключові напрями:

Покращення точності та надійності:

Розвиток алгоритмів глибокого навчання: Дослідження спрямовані на створення більш ефективних нейронних мереж, здатних розпізнавати обличчя в складних умовах, таких як погане освітлення, зміна ракурсів та виразів обличчя.

3D-розпізнавання обличь: Впровадження 3D-датчиків для отримання більш точної інформації про форму обличчя, що підвищує стійкість до змін освітлення та ракурсів.

Розпізнавання обличчя у відео: Розробка методів для ефективного розпізнавання обличчя у відеопотоках, що є важливим для систем спостереження та безпеки.

Розв'язання етичних та соціальних питань:

Захист конфіденційності: Розробка методів, які мінімізують збір та зберігання персональних даних, а також забезпечують прозорість використання технології.

Боротьба з упередженістю: Усунення упередженості алгоритмів, що може призвести до дискримінації певних груп людей.

Регулювання та стандартизація: Розробка міжнародних стандартів та законодавчих норм для регулювання використання технології розпізнавання обличчя.

Розширення застосувань:

Медицина: Розробка систем для діагностики генетичних захворювань, аналізу емоційного стану пацієнтів та персоналізації медичного обслуговування.

Роздрібна торгівля: Використання для персоналізації обслуговування клієнтів, аналізу їх поведінки та запобігання крадіжкам.

Автомобільна промисловість: Інтеграція систем розпізнавання обличчя у автомобілі для підвищення безпеки водіння та персоналізації налаштувань.

Криміналістика: ідентифікація злочинців, пошук зниклих людей.

Розвиток технології розпізнавання обличчя іде в напрямку створення більш ефективних, надійних і етичних систем, які можуть бути використані в різних сферах життя.

1. Florian Schroff, Dmitry Kalenichenko, James Philbin FaceNet: A Unified Embedding for Face Recognition and Clustering]," 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). [Online]. Доступно: https://ieeexplore.ieee.org/document/7298682 DOI: 10.1109/CVPR.2015.7298682.

Дослідження складності атак на криптосистеми на основі кодів

УДК 004

Аліна Давлетова

Західноукраїнський національний університет,
a7davletova@gmail.com

Система McEliece є перспективним алгоритмом постквантової криптографії, що підтверджує її входження до фіналу в 4-му раунді NIST зі стандартизації постквантових криптографічних алгоритмів [1]. В основі класичної McEliece лежать коди Гоппа [2], проте для її реалізації також успішно застосовуються коди Хеммінга побудовані в скінченних полях Галуа GF(p) [3]. Криптосистема характеризується високою швидкістю шифрування та розшифрування, що сприяє її практичному використанню. Її стійкість ґрунтується на складності декодування випадкових лінійних кодів, що є NP-складною задачею навіть для квантових комп'ютерів. Проте існують специфічні методи криптоаналізу, спрямовані на зменшення складності цієї задачі.

Метою роботи є дослідження обчислювальної складності атак на криптосистеми, що базуються на кодах, зокрема криптосистему McEliece, з урахуванням сучасних криптоаналітичних підходів та постквантових загроз.

Ключовими компонентами криптоаналізу є:

- розв'язання задачі декодування - знаходження найближчого кодового слова до отриманого повідомлення;
- аналіз структури публічного ключа - намагання відновити приватний ключ із матриці публічного ключа;
- зменшення задачі до відомих математичних проблем, наприклад, задача найкоротшого вектора (SVP) у решітках.

Відомі атаки на криптосистему McEliece, зокрема атака інформаційного набору (Information-Set Decoding, ISD), спрямована на безпосереднє знаходження розв'язку задачі декодування. Складність алгоритмів ISD зростає експоненційно з довжиною коду, але вона все ще залишається значною загрозою для параметрів із недостатньо великими кодами. Проте такі атаки не отримують суттєвого прискорення за допомогою квантових алгоритмів [4].

Метою атак на основі структурного аналізу є знаходження структури, схожої на породжуючий код, у генераторній матриці [5]. Ефективність таких атак значно зменшується зі збільшенням параметрів системи, наприклад, розміру коду, його ступеня, або розміру поля GF(p).

Атаки на основі решіток (Lattice-based attacks) передбачають інтерпретацію публічної генераторної матриці як решітки. Вони базуються на пошуку найкоротшого вектора, що відповідає приватному ключу. Як правило, атаки даного типу, не є ефективними за великих параметрів на McEliece, що суттєво підвищує складність задачі [6].

Алгоритм Гровера, що забезпечує квадратичне прискорення перебору, теоретично може зменшити ефективний рівень стійкості McEliece шляхом зниження безпеки симетричних компонентів криптосистеми [7]. Однак це не є основною загрозою, оскільки основна складність для McEliece полягає в задачі декодування та ISD.

Таблиця 1

Порівняння складності атак на криптосистему McEliece

Метод атаки	**Алгоритм**	**Складність**	**Обмеження параметрів**	**Вразливість для квантових атак**
Декодування	ISD (Becker et al.)	260-80	Невелика довжина коду	Часткова
Структурний аналіз	Overbeck, Wieschebrink	250-70	Залежить від структури коду	Ні
Решіткові атаки	BKZ (Block Korkin-Zolotarev)	280+	Висока розмірність решітки	Так
Квантові атаки	Grover	2n	Всі параметри	Так

Наведені в таблиці 1 значення можуть варіюватися в залежності від конкретної реалізації або параметрів криптосистеми, проте вони ілюструють, як складність атак змінюється залежно від параметрів McEliece.

Проведені дослідження показали, що незважаючи на існування ряду атак, система McEliece залишається стійкою, зберігаючи високий рівень безпеки за умови правильно обраних параметрів.

1. Alagic G., Bros M., Ciadoux P., Cooper D., Dang Q., Dang T., Kelsey J., Lichtinger J., Miller C., Moody D., Peralta R., Perlner R., Robinson, A., Silberg H., Smith-Tone D., Waller N. *NIST Internal Report NIST IR 8545: Status report on the fourth round of the NIST post-quantum cryptography standardization process*. 2025. https://doi.org/10.6028/NIST.IR.8545

2. McEliece R..J. A Public-Key Cryptosystem Based on Algebraic Coding Theory. *DSN Progress Report*. 1978. Vol. 42(44). P. 114-116.

3. Davletova A., Yatskiv V., Ivasiev S., Karpinskyi M. Encryption Method Based on Codes. *Advances in Cyber-Physical Systems.*2024. Vol.9, N.1-. pp. 24 – 31. https://doi.org/10.23939/acps2024.01.024

4. Biswas S., Gupta I., Bera D. On the Comparative Study of Recent Information Set Decoding (ISD) Attacks for QC-LDPC Code-Based McEliece Cryptosystem. *2024 IEEE International Conference on Public Key Infrastructure and its Applications*, 2024, pp. 1-8, doi: 10.1109/PKIA62599.2024.10727868.

5. Couvreur A., Mora R., Tillich J.-P. A new approach based on quadratic forms to attack the McEliece cryptosystem. 48550/arXiv.2306.10294.

6. Horlemann A.-L., Khathuria K., Newman M., Sakzad A., Cabello C. Lattice-Based Vulnerabilities in Lee Metric Post-Quantum Cryptosystems. 2024. 10.48550/arXiv.2409.16018.

7. Opiłka F., Niemiec M., Gagliardi M., Kourtis M. A., 2024. Performance Analysis of Post-Quantum Cryptography Algorithms for Digital Signature. *Applied Sciences*. 2024. Vol. 14, no. 12: 4994. doi: 10.3390/app14124994.

Машинне навчання та текстовий майнінг у моделюванні кібервразливостей

УДК 004.056.5

Владислав Денисюк
Національний технічний університет "Харківський політехнічний інститут",
Vladyslav.Denysiuk@cs.khpi.edu.ua

Зі зростанням кількості кібератак на критичні інформаційні ресурси актуалізується завдання своєчасного виявлення вразливостей. Існуючі підходи здебільшого орієнтовані на вже відомі загрози, тоді як вразливості нульового дня (zero-day vulnerabilities) залишаються невиявленими до моменту атаки. Це потребує постійного вдосконалення моделей валідації та впровадження інтелектуальних методів аналізу.

Метою роботи є аналіз та дослідження моделей валідації вразливостей, які поєднують машинне навчання, Big Data та гібридні методи аналізу. Особлива увага приділяється теоретичному обґрунтуванню підходів, що дозволяють підвищити ефективність виявлення як відомих, так і нових типів загроз, з урахуванням складності сучасних інформаційних систем. Робота охоплює огляд поточних тенденцій у сфері автоматизованого аналізу коду, обробки телеметричних даних, а також можливостей інтеграції з системами моніторингу безпеки в режимі реального часу.

Новітні тенденції у валідації вразливостей зосереджені на інтеграції з AI-технологіями, зокрема машинним навчанням і Big Data. Це дає змогу автоматизувати перевірки та виявляти приховані закономірності. Зокрема, текстовий майнінг змін у коді дозволяє прогнозувати потенційно вразливі компоненти. Наприклад, аналіз історії комітів у репозиторіях за допомогою NLP-алгоритмів дає можливість ідентифікувати шаблони коду, які часто супроводжуються виправленням вразливостей. Такі підходи дозволяють формувати базу знань з поведінки розробників та типових помилок. Крім того, обробка великих обсягів телеметричних даних з серверів і мережевих журналів у реальному часі дає змогу виявляти аномальні дії, що можуть свідчити про експлуатацію Zero-Day вразливостей. Поєднання цих методів у рамках гібридних систем дозволяє не лише знаходити відомі загрози, а й ефективно прогнозувати нові [1].

З метою підвищення ефективності валідації вразливостей перспективним напрямом є інтеграція розроблених моделей у сучасні SIEM-системи (Security Information and Event Management). Це дозволяє не лише автоматизувати процес виявлення аномалій на основі історичних і потокових даних, а й забезпечити адаптивну реакцію на нові загрози в режимі реального часу. Зокрема, поєднання модулів машинного навчання з механізмами кореляції подій у SIEM сприяє формуванню динамічного профілю безпеки, який може оновлюватися в залежності від змін у поведінці користувачів, конфігурації систем або зовнішніх кіберзагроз. Такий підхід значно підвищує рівень ситуаційної обізнаності та зменшує час реагування на інциденти.

Суттєвим викликом залишається проблема масштабованості та адаптації таких моделей до нових типів систем — від хмарних платформ до вбудованих

IoT-рішень. У цьому контексті особливе місце займають гібридні моделі, які поєднують статичний і динамічний аналіз з інтелектуальним моделюванням поведінки систем. Такі моделі довели свою ефективність у виявленні SQL-ін'єкцій навіть у випадках, коли вони були приховані за багаторівневими обробниками введення. Крім того, їх гнучкість дозволяє враховувати контекст виконання, часові залежності та взаємодію компонентів, що критично важливо для складних розподілених систем. Подальший розвиток гібридних моделей передбачає інтеграцію з системами машинного навчання для автоматичного оновлення сигнатур загроз і підвищення точності прогнозування потенційних вразливостей [2].

Попри значні переваги, використання інтелектуальних та гібридних моделей валідації вразливостей супроводжується низкою викликів. По-перше, ефективність моделей значною мірою залежить від якості вхідних даних та їх метаданих — наявність зашумлених, неповних або некоректно маркованих даних може суттєво знизити точність виявлення. По-друге, складність налаштування та інтеграції таких систем у вже існуючу інфраструктуру безпеки потребує додаткових ресурсів та експертизи. Крім того, варто враховувати ризики хибно позитивних та хибно негативних результатів, які можуть або перевантажити аналітиків, або залишити реальні загрози поза увагою [3].

Виходячи із вищесказаного важливим напрямом подальших досліджень є підвищення інтерпретованості моделей, удосконалення процедур валідації результатів та розвиток засобів автоматичного коригування помилок на основі зворотного зв'язку.

У доповіді розглянуто концептуальні засади побудови моделей валідації вразливостей з акцентом на гібридні та AI-орієнтовані підходи. Проаналізовано сучасні методи, зокрема текстовий майнінг змін у коді, аналіз шаблонів комітів, обробку телеметричних даних та можливості інтеграції з SIEM-системами. Зроблено висновок, що поєднання цих технологій дозволяє сформувати більш адаптивні та ефективні механізми виявлення вразливостей, здатні реагувати на нові типи загроз у динамічному середовищі. Такі підходи є перспективними для впровадження в сучасні системи кіберзахисту як у державному, так і в корпоративному секторі.

1. Scandariato, R., Walden, J., Hovsepyan, A., & Joosen, W. (2014). Predicting Vulnerable Software Components via Text Mining. *IEEE Transactions on Software Engineering*, 40(10):993-1006, 2–7 с.

2. Shahriar, H., North S., Wei-Chuen Chen (2013). Hybrid Static and Dynamic Analysis for Detecting SQL Injection Vulnerabilities. *Proceedings of the 25th IEEE International Conference on Advanced Information Networking and Applications (AINA)*, 56–57 с.

3. Risse N., Böhme M. Uncovering the Limits of Machine Learning for Automatic Vulnerability Detection. Proceedings of the 33rd USENIX Security Symposium (USENIX Security 2024). 1–2.

Кіберризики цифрових інвестиційних платформ: виклики для економічного відновлення України

УДК 336.1 : 336.5 : 338.2
Наталія Дзюбановська[1], Іван Цегельний[2]
Західноукраїнський національний університет,
[1] n.dziubanovska@wunu.edu.ua, [2] i.tsehelnyi@st.wunu.edu.ua

Україна стрімко впроваджує цифрові фінансові технології, особливо на тлі війни та необхідності відбудови економіки. Цифрові інвестиційні платформи – від криптовалютних бірж до краудфандингових сервісів і державних онлайн-платформ для інвестування – стали важливими каналами залучення капіталу. Це допомагає країні вистояти та готує підґрунтя для післявоєнної відбудови. Водночас зростає і залежність економіки від цифрових фінансових інструментів, що робить питання їхньої кібербезпеки надзвичайно актуальним.

Цифрові платформи стикаються з численними кіберзагрозами. Зокрема, хакери та шахраї націлюються на криптовалютні біржі, щоб привласнити активи користувачів. Зловмисники створюють фейкові сайти та кампанії для крадіжки коштів довірливих інвесторів. Ворожі спецслужби здійснюють атаки на українські фінансові системи – від DDoS-атак на банки до впровадження шкідливого ПЗ, – прагнучи посіяти хаос і підірвати довіру до цифрової інфраструктури [1], [2]. Усі ці ризики становлять серйозний виклик для економічного відновлення України: вони можуть знизити інвестиційну довіру, призвести до прямих фінансових втрат і загальмувати відбудову.

Кіберризики – це не вузькотехнічне питання ІТ-відділу, а фактор, що впливає на самі основи відновлення економіки: довіру, гроші, темпи розвитку. У сучасному світі економічна безпека тісно пов'язана з кібербезпекою. Тому держава повинна враховувати ці виклики при плануванні політики відбудови.

Наведемо основні ризики, їх вплив та напрями реагування у таблиці 1.

Таблиця 1

Ключові кіберризики цифрових інвестиційних платформ, їх наслідки та можливі заходи реагування

Кіберзагроза	Приклади інцидентів (Україна)	Наслідки для економічного відновлення	Можливі заходи реагування
Злам і крадіжка коштів (хакерські атаки)	• (хакерські атаки) – 2017: вірус NotPetya паралізував банки, збитки $10 млрд [3]. • 2023: рос. група UAC-0006 намагалася	• Прямі фінансові втрати (викрадені кошти не підуть на відбудову). • Підрив довіри інвесторів до безпеки фінсистеми.	• Посилення ІТ-захисту платформ (2FA, шифрування, cold-wallet для крипто). • Регулярні аудити безпеки, пентести. • Створення фондів відшкодування

	вкрасти десятки млн грн з банків [2].		збитків для постраждалих.
Шахрайство та соціальна інженерія	• 2022: тисячі зламаних акаунтів збирали фейкові «донати» [4]. • Масові фішингові розсилки від імені держорганів («отримайте виплату»).	• Втрата коштів і благодійних внесків громадян. • Зниження добровільної підтримки (донорської активності) через страх шахрайства. • Репутаційні втрати для платформ та держави.	• Освітні кампанії з кібергігієни для населення. • Верифікація офіційних зборів (реєстри перевірених волонтерських фондів). • Фішинг-фільтри в електронних поштах, блокування фейкових сайтів (через співпрацю з хостингами).
DDoS-атаки (відмова в обслуговуванні)	• 2022: DDoS на ПриватБанк і Ощадбанк перед вторгненням [1]. • 2025: атака 56 млн запитів на держпортал, відбита Головним управлінням розвідки Міністерства оборони України [5].	• Непрацездатність платформ у критичний момент (зрив інвестиційних угод, зупинка онлайн-банкінгу). • Паніка користувачів, відтік клієнтів до більш «стабільних» каналів.	• Інвестиції в інфраструктуру захисту (мережеві екрани, анти-DDoS сервіси). • Резервні канали доступу для критичних систем. • Міжбанківська координація: швидке інформування про атаки, переключення на офлайн-режими, якщо потрібно.
Втручання державних спецслужб (кібердиверс	• 2017: атака NotPetya від Головного розвідувального управління	• Системні ризики: маніпуляція даними реєстрів, зрив роботи фінансових установ.	• Розвиток кіберрозвідки: виявлення та нейтралізація APT (Advanced

її, шпигунство)	Генерального штабу Збройних сил РФ, уражено держсектор і бізнес. • 2024: злам держреєстрів та «Дії», підозра на РФ [6]. • Спроби російських APT-груп (Advanced Persistent Threat group) проникнути в системи держфінансів для шпигунства (постійно).	• Витік конфіденційної інформації (використання проти України на переговорах). • Стримування міжнародної допомоги (донори можуть боятися, що кошти нецільово використаються через втручання).	Persistent Threat) на ранніх стадіях. • Інтеграція з НАТО/ЄС для спільної протидії державним кіберзагрозам [7]. • Строгий контроль доступу до критичних держсистем, моніторинг аномалій (SOC (Security Operations Center) – центри оперативного реагування).

Наведені заходи реагування вимагають координації між урядом, регуляторами та приватним сектором. Жоден з цих кроків окремо не гарантує повної безпеки, але їх поєднання підвищує кіберстійкість фінансової екосистеми.

Для успіху економічного відновлення необхідно реалізувати комплексну стратегію кіберстійкості: від технічних заходів (захист платформ) до організаційних (навчання персоналу, кіберстрахування) та міжнародних (координація з партнерами).

Тільки захистивши свої цифрові платформи, Україна зможе повною мірою скористатися їх можливостями для відбудови – залучити мільярди доларів інвестицій, побудувати прозору та ефективну економіку, інтегровану у світовий фінансовий простір. Кібербезпека більше не є другорядним питанням, вона стала необхідною умовою економічного зростання і національного процвітання у XXI столітті.

1. Ukraine conflict: Digital and cyber aspects | Digital Watch Observatory. (n.d.). Digital Watch Observatory. https://dig.watch/trends/ukraine-conflict-digital-and-cyber-aspects#:~:text=The%20war%20in%20Ukraine%20started,making%20the%20whole%20system%20inoperable.

2. Antoniuk, D. (2024, May 3). Ukraine records increase in financially motivated attacks by Russian hackers. The Record. https://therecord.media/ukraine-russia-increase-financially-motivated-cyberattacks#:~:text=During%20the%20period%20that%20CERT,were%20related%20to%20financial%20theft.

3. Greenberg, A., & Excerpt. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. WIRED. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/#:~:text=To%20get%20a%20sense%20of,%E2%80%9D.

4. Knowles, J., & Pistone, A. (2022, March 18). How to spot scams pretending to raise money for Ukraine during war with Russia. ABC7 Chicago. https://abc7chicago.com/russia-ukraine-donations-donate-to/11658942/#:~:text=Thousands%20of%20hacked%20social%20media,identified%20by%20cybersecurity%20group%20Bitdefender.

5. Brizard, L. (2025, April 8). Ukrainian forces successfully thwart Russian DDOS attack on War&Sanctions Portal. UNITED24 Media. https://united24media.com/latest-news/ukrainian-forces-successfully-thwart-russian-ddos-attack-on-warsanctions-portal-7437#:~:text=The%20attack%20involved%20a%C2%A0large,or%C2%A0roughly%2040%2C000%20requests%20per%20second.

6. Kramarenko, D., & Dmytriieva, D. (2024, December 20). Ukraine suffers largest cyberattack since 2022: Russian hackers disrupt key services. RBC-Ukraine. https://newsukraine.rbc.ua/news/ukraine-suffers-largest-cyberattack-since-1734704699.html#:~:text=Ukraine%20was%20hit%20by%20one,app%2C%20with%20suspected%20data%20breaches.

Prots, Y. (2025, March 14). Ukraine, EU move to deepen cybersecurity cooperation as Russian threat rises. The Kyiv Independent. https://kyivindependent.com/ukraine-eu-look-to-deepen-cybersecurity-cooperation-as-russian-threat-rises/#:~:text=Appathurai%20told%20EBU.

Розробка локальної моделі машинного навчання щодо захисту конфіденційної інформації у відкритому програмному коді

УДК 004.056.55

Даніїл Драгін

Національний університет «Одеська політехніка», 9480561@stud.op.edu.ua

В сучасному цифровізованому світі, ми кожного дня використовуємо велику кількість різних застосунків, які використовують, зберігають або передають конфіденційну інформацію. Безпека цих даних з кожним роком стає все більш важливим питанням і розглядається не тільки, як проблема особистої безпеки або компанії, а інколи може досягати загальносвітового рівня. Загалом, добре побудова інформаційна система в технічному плані немає слабких місць, які зловмисник міг би використати для незаконного доступу до конфіденційної інформації, але під час створення застосунку, розробники можуть залишити у відкритому доступі конфіденційну інформацію (API ключі, токени доступу, паролі до баз даних), що робить їх вразливими до автоматизованих сканерів, які

постійно переглядають платформи розробки, такі як GitHub, GitLab, npm або PyPi, у пошуках витоків, для несанкціонованого доступу до персональної інформації користувача або злому системи. Згідно зі звітом GitGuardian за 2023 рік, у публічних репозиторіях було виявлено 12 778 599 нових секретів, з яких 3 698 686 є унікальними, і ця кількість з кожним роком лише зростає. Для порівняння у 2022 році — 10 мільйонів, що на 28% менше, ніж у 2023 році [1].

Для вирішення цієї проблеми було створено багато рішень, але більшість ініціатив в цій проблемі фокусуються вже на аналізі репозиторіїв після завантаження коду, що в деяких випадках може бути запізно. Про що свідчіть дослідження Cybenari, для виявлення та використання чутливої інформації на GitHub треба лише 127 секунд. Набагато гірші результати має менеджер пакетів і репозиторій для JavaScript і Node.js – npm, для якого зловмисникам треба лише 60 секунд [2].

Тому метою цієї роботи є розробка локальної моделі машинного навчання для захисту конфіденційної інформації у відкритому програмному коді для забезпечення превентивного захисту від витоку секретної інформації. Щоб система могла працювати локально, було використано саме модель машинного навчання, хоча нейроні мережі є більш ефективними, але для своєї роботи вони потребують велику кількість ресурсів.

Для побудови цієї моделі використовується логістична регресія, яка була спеціально розроблена для задач класифікації, що дозволяє їй ефективно розподіляти об'єкти між класами на основі ймовірнісного підходу. Для визначення моделі логістичної регресії, вводиться певна випадкова величина Y, що набуває значення від 0 до 1. Найчастіше 0 відповідає за те, що певний об’єкт не відповідає певному класу, а 1 – відповідає. Результатом є ймовірності для кожного класу, що допомагають приймати рішення про класифікацію [3]. Ця величина залежить від певної множини змінних, які впливають на те, яке значення буде приймати змінна Y.

Для того, щоб отримати залежність змінної Y від вектору пояснювальних змінних, вводиться додаткова прихована змінна y*, яка відповідає за лінійний результат.

$$y^*=Tx=0+1x1+\ldots+nxn+\varepsilon, \quad (1)$$

Ця зміна є лінійною комбінацією параметрів , що визначають вплив кожної ознаки x, до яких додається випадкова похибка , що зазвичай є підпорядкованою логістичному розподілу та є випадковою величиною з певним логістичним розподілом ймовірностей. Тому залежність Y від y* має вигляд:

$$Y=\{0,\ y^*\leq 0\ 1,\ y^*>0\ , \quad (2)$$

Для перетворення лінійного результату у вірогідність використовується сигмоїдна функція. Сигмоїдна функція є математичною функцією, яка має S-подібну (sigmoid) форму, що наведено на рис. 1. Її основна мета — перетворення будь-якого дійсного числа в значення в інтервалі від 0 до 1 [3].

$$y^*= 11+e-y^* \quad (3)$$

Додатково ефективність системи можна підвищити за рахунок гібридних підходів, що поєднують методи обробки тексту (TF-IDF, регулярні вирази) з алгоритмами машинного навчання.

Під час тестування системи було виявлено, що для сканування 2000 файлів займає приблизно 5-7 секунд, в залежності від розмірів файлів, а також кількості секретної інформації в них, що є кращим результатом ніж той, що надає GitHub. Повідомлення про наявність секретної інформації в коді надійшла приблизно через 43 секунди після завантаження. GitHub не проводить евристичний аналіз, через що не було знайдено всі паролі в програмному коді, які в свою чергу знайшла локальна модель. Проте вона демонструю певні ознаки надмірності в свої рішеннях, коли рядки які не є конфіденційною інформацію вона помічає такими, що потенційно можуть бути такими. Для вирішення цієї проблеми на перших етапах треба збільшити кількість даних для навчання моделі, а також покращити функції обробки тексту, але вже отримані результати свідчать про певний успіх в розробці моделі.

Таким чином, можна зробити висновок про те, що в сучасних системах увагу треба приділяти не тільки класичним методам захисту інформації, а також шляхам вирішення проблеми людського фактору. Дана модель забезпечує захист та аналіз відкритого програмного коду в умовах обмежених ресурсів, а також з забезпечення потрібної швидкості обробки, за допомогою поєднання різних методів обробки тексту з алгоритмами машинного навчання.

1. The State of Secrets Sprawl Report. *GitGuardian*. 2024.
2. You Have One Minute to Save Your Leaked AWS Credentials *ThreatDown Blog*. 2023.
3. Hastie T., Tibshirani R., Friedman J. The Elements of Statistical Learning: Data Mining, Inference, and Prediction. – Springer, 2001. – 533 p.

Класифікація шкідливої активності в інформаційних системах

УДК 004.056.5:004.08

Володимир Дубровський

Державний університет інформаційно-комунікаційних технологій,
v.dybrovskyi@stud.duikt.edu.ua

Кібератаки відбуваються щодня у більших масштабах, оскільки все більше людей підключаються до Інтернету. Усі користувачі на роботі чи вдома все частіше виходять в Інтернет на сайтах соціальних мереж, таких як X, раніше відомий як Twitter, Facebook, TikTok серед багатьох таких веб-сервісів, доступних сьогодні. Співробітники організацій можуть приділити частину свого часу спілкуванню з колегами-професіоналами, друзями та іншими людьми по всьому світу.

Організації через своїх IT-спеціалістів вживають заходів для своєчасного виявлення спроб зловмисних атак на IT-інфраструктуру та пов’язані з нею дані та системи. Незважаючи на спроби компаній захистити цінні IT-активи, кібератаки все ще відбуваються, хоча бізнес-структури не розголошують ці спроби, побоюючись репутаційної шкоди.

З розвитком інформаційно-комунікаційних технологій і збільшенням доступу до Інтернету організації стають вразливими до різних видів загроз. Проте їхня інформація піддається кібератакам і завдає їм збитків.

Загрози надходять з різних джерел, як від дій співробітників так і від хакерських атак. Фінансові збитки, спричинені порушеннями безпеки, зазвичай не можуть бути точно виявлені, оскільки значна кількість збитків походить від менш масштабних інцидентів безпеки, спричинених недооцінкою ризику безпеки інформаційної системи [1].

Таким чином, менеджери повинні знати про загрози, які впливають на їхні активи і визначити їхній вплив, щоб визначити, що їм потрібно робити, щоб запобігти атакам, вибравши відповідні контрзаходи.

Уразливі місця складаються зі слабких місць у системі, якими можуть скористатися зловмисники, що може призвести до небезпечного впливу. Коли в системі існують уразливості, загроза може проявлятися через агента загрози, який використовує певну техніку проникнення, щоб викликати небажані ефекти [2]. Фінансові втрати для організацій можуть бути значними.

За даними 11-го щорічного дослідження комп'ютерної злочинності та безпеки, 74,3% загальних втрат викликано: вірусами, несанкціонованим доступом, крадіжкою ноутбука або мобільного обладнання та крадіжкою конфіденційної інформації [2].

Для виявлення загроз, необхідно знати джерела і конкретні області системи, які можуть постраждати, щоб активи інформаційної безпеки могли бути захищені заздалегідь. Таким чином, ефективна класифікація безпеки необхідна для розуміння та визначення загроз та їх потенційного впливу [3].

Загрози безпеці можна спостерігати та класифікувати різними способами, враховуючи різні критерії, такі як джерело, агенти та мотиви. Класифікація загроз допомагає ідентифікувати та організовувати загрози безпеці в класи для оцінки та оцінки їх впливу, а також розробки стратегій запобігання або пом'якшення впливу загроз на систему [3].

В роботах видатних вчених є кілька відомих класифікацій і таксономій атак на комп'ютерні системи. Багато дослідників запропонували таксономії, які класифікують атаки на основі передбачуваного ефекту атаки, як атака на відмову в обслуговуванні, а інші включають техніку, за допомогою якої зловмисник досягає цього ефекту, наприклад обхід автентифікації або авторизації [3].

Огляд літератури показує, що слід дотримуватися наступних принципів класифікації інформаційної безпеки. Взаємовиключні: кожна загроза класифікується в одній категорії, виключаючи всі інші, оскільки категорії не збігаються. Кожен зразок має відповідати щонайбільше одній категорії. Вичерпний: Категорії в класифікації повинні включати всі можливості (всі зразки загрози). Однозначність: усі категорії мають бути чіткими та точними, щоб класифікація була надійною [4].

Кожна категорія повинна супроводжуватися однозначними критеріями класифікації, які визначають, які зразки слід віднести до цієї категорії. Повторюваність: повторні застосування призводять до тієї самої класифікації, незалежно від того, хто класифікує. Прийнято: усі категорії є логічними, інтуїтивно зрозумілими та легко сприймаються більшістю. Корисно: його можна використовувати, щоб отримати уявлення про сферу дослідження; його можна адаптувати до різних потреб застосування. Ці принципи можна

використовувати для оцінки класифікації загроз. Хороша класифікація має підтримувати більшість представлених принципів [4].

Інформаційна безпека є критичною проблемою для окремих осіб та організацій, оскільки вона призводить до великих фінансових втрат. Ця робота стосується проблеми класифікації загроз, щоб знайти загальну та гнучку модель, яка дозволяє краще зрозуміти природу загроз, щоб розробити відповідні стратегії та рішення щодо інформаційної безпеки для запобігання або пом'якшення їх наслідків.

1. The Role of Ethical Hacking in Strengthening SOC Operations for Proactive Threat Detection. Hasher Malik, Frank Blaser December, 2024
2. Falowo O.I., Botsyoe L., Koshoedo K., Ozer M. (2024). Enhancing cybersecurity with artificial immune systems and general intelligence: A new frontier in threat detection and response. IEEE Access.
3. Arandjelovic, R., et al. (2017). NetVLAD: CNN architecture for weakly supervised place recognition, IEEE Transactions on Pattern Analysis and Machine Intelligence, 40(6). https://doi.org/10.1109/TPAMI.2017.2711011
4. Grata E. G., Deshpande A., Lopes R. T., Laghari A. A., Khan A. A. (2024). Artificial intelligence for threat anomaly detection using graph Data bases a semantic outlook. Analytics and Cyber Threat Detection, 249-278.

Дослідження використання штучного інтелекту для керування безпілотних літальних апаратів

УДК 621.395.7 (043.2)

Ігор Дюба[1], Юлія Ткач[2]
Національний університет "Чернігівська політехніка",
[1]idyuba@gmail.com, [2]tkachym79@gmail.com

Українська оборонна промисловість розробляє автономне програмне забезпечення на основі штучного інтелекту, яке можна інтегрувати в різні платформи для збільшення автономності на полі бою [1-4]. Відокремимо основні види програмного забезпечення та систем управління, які розроблені та використовуються в Україні для підвищення автономності безпілотних літальних апаратів (БПЛА) з використанням штучного інтелекту (ШІ).

1. Автономна навігація та програмне забезпечення для польотів: це програмне забезпечення дозволяє БПЛА самостійно орієнтуватися, слідувати заздалегідь визначеним маршрутам, уникати перешкод та виконувати польотні завдання без постійного нагляду оператора. Штучний інтелект можна використовувати для покращення планування маршруту в середовищі, що динамічне змінюється.
2. Системи керування корисним навантаженням з елементами штучного інтелекту: програмне забезпечення, що відповідає за керування датчиками (камерами, радарами тощо) та зброєю (якщо є) на БПЛА. Штучний інтелект може використовуватися для автоматичного виявлення, розпізнавання та відстеження цілей, а також для прийняття рішень щодо використання зброї (за участю людини або автономне , залежно від протоколів).

3. Програмне забезпечення для обробки та аналізу даних у реальному часі (на борту): алгоритми штучного інтелекту, які працюють безпосередньо на борту БПЛА для обробки інформації, що надходить від датчиків. Це може включати розпізнавання образів, виявлення аномалій, класифікацію об'єктів та інші завдання, які вимагають швидкої обробки даних без затримки, пов'язаної з передачею на наземну станцію.

4. Системи планування місій на основі штучного інтелекту: програмне забезпечення для автоматизованого планування польотних місій на основі різних факторів, таких як місцевість, місцезнаходження ворога, зони протиповітряної оборони та доступні ресурси. Штучний інтелект може оптимізувати плани місій для максимальної ефективності.

5. Програмне забезпечення для управління групою БПЛА (роєм) з елементами штучного інтелекту: системи, які дозволяють координувати кілька автономних БПЛА для виконання складних завдань. Штучний інтелект можна використовувати для розподілу ролей, синхронізації дій та прийняття колективних рішень.

6. Системи машинного зору (комп'ютерного зору на основі штучного інтелекту): програмне забезпечення для обробки зображень та відеопотоків з камер БПЛА. Штучний інтелект використовується для автоматичного виявлення, розпізнавання та класифікації об'єктів, людей, обладнання та інших елементів навколишнього середовища.

7. Системи прийняття рішень на основі штучного інтелекту: програмні модулі, які на основі оброблених даних і заданих правил можуть пропонувати або навіть самостійно приймати рішення в певних ситуаціях (наприклад, вибір цілі для атаки, зміна маршруту при виявленні загрози).

8. Інструменти навчання та розгортання моделей штучного інтелекту: програмне забезпечення та фреймворки, що використовуються для розробки, навчання та інтеграції моделей машинного навчання в бортові системи БПЛА. У статті наголошується на підході України до навчання малих моделей на обмежених наборах даних.

Аналіз і розвиток вище згаданих наукових задач сприяє збільшення автономності на полі бою та відповідно зменшує вплив кількісних переваг в особовому складі на полю бою тому він є актуальним та першочерговим при проведенні наукових досліджень.

1. M. Bondar, “Advancing Ukrainian Unmanned Systems with Autonomy and AI,” *Center for Strategic and International Studies*, Mar. 06, 2025. [Online]. Available: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-03/250306_Bondar_Autonomy_AI.pdf?VersionId=E2h8uqROea77udoc_og82HWsrfgfJRTZ. [Accessed: Apr. 30, 2025].

2. Constantin-Adrian CIOLPONEA, "THE INTEGRATION OF UNMANNED AIRCRAFT SYSTEM (UAS) IN CURRENT COMBAT OPERATIONS," Land Forces Academy Review Vol. XXVII, No 4(108), 2022 [Online]. Available: [https://www.researchgate.net/publication/367055350_The_Integration_of_Unmann

ed_Aircraft_System_UAS_in_Current_Combat_Operations]. [Accessed: Apr. 30, 2025].

3. Ren, M., Wang, B., Liu, J. (2024). Conception of Foreign Heterogeneous Electronic Warfare UAV Cross Domain Cooperative Operations. In: Qu, Y., Gu, M., Niu, Y., Fu, W. (eds) Proceedings of 3rd 2023 International Conference on Autonomous Unmanned Systems (3rd ICAUS 2023). ICAUS 2023. Lecture Notes in Electrical Engineering, vol 1171. Springer, Singapore. https://doi.org/10.1007/978-981-97-1083-6_2

4. Yang ZHANG, Guangya SI, Yanzheng WANG, Wenbin HAN. (2023). Modeling and simulation of UAVs swarm electromagnetic operation. Systems Engineering and Electronics ›› 2023, Vol. 45 ›› Issue (7): 2121-2130. doi: 10.12305/j.issn.1001-506X.2023.07.23

5. Ren, M., Wang, B., Liu, J. (2024). Conception of Foreign Heterogeneous Electronic Warfare UAV Cross Domain Cooperative Operations. In: Qu, Y., Gu, M., Niu, Y., Fu, W. (eds) Proceedings of 3rd 2023 International Conference on Autonomous Unmanned Systems (3rd ICAUS 2023). ICAUS 2023. Lecture Notes in Electrical Engineering, vol 1171. Springer, Singapore. https://doi.org/10.1007/978-981-97-1083-6_2

Приватність та інформаційна безпека у соціальних медіа

УДК 004.056.5(043.2) Микола Жмурак[1], Геннадій Шаповалов[2]

Національний університет «Одеська політехніка»,
[1]*9480576@stud.op.edu.ua*, [2]*shapovalov@op.edu.ua*

У XXI столітті соціальні медіа стали не лише засобом комунікації, а й платформою для ведення бізнесу, поширення новин і формування громадської думки. Проте широке використання соціальних мереж, таких як Facebook, Instagram, TikTok, Twitter/X та ін., супроводжується зростанням кількості загроз, що стосуються конфіденційності та інформаційної безпеки користувачів.

Серед ключових проблем – несанкціонований збір, обробка та передача персональних даних третім сторонам, поширення фішингових посилань, використання даних для створення психологічних профілів, а також втручання з боку державних або комерційних структур.

Метою дослідження є аналіз актуальних кіберзагроз у соціальних медіа, оцінка ефективності існуючих механізмів захисту приватності, а також розробка рекомендацій щодо захисту особистих даних користувачів

Аналіз кіберзагроз показує, що найпоширенішими з них є соціальна інженерія (виманювання паролів, маніпуляції), фішинг через повідомлення або посилання, витоки баз даних, стеження через cookies, пікселі та трекери, а також поширення deepfake-контенту та маніпулятивної реклами на основі поведінкових моделей.

Методи захисту включають використання двофакторної автентифікації, розширення браузера для блокування трекерів (Privacy Badger, uBlock, Origin), псевдомінімізацію та шифрування даних, застосування VPN і TOR для

збереження анонімності, а також відмову від «умовно-безкоштовних» сервісів із сумнівною політикою конфіденційності. Також запропоновано використання моделей математичного моделювання для передбачання поширення персональної інформації у соцмережах, що дозволяє виявляти «вразливі» вузли в інформаційному просторі.

У межах дослідження було застосовано адаптовану SIR-модель (Susceptible-Informed-Recovered), яка дозволяє формалізувати динаміку поширення інформації у соціальних медіа. В рамках цієї моделі користувачі поділяються на три категорії:

- S (непоінформовані) – користувачі, які ще не отримали повідомлення;
- I (поінформовані) – користувачі, які ознайомились із повідомленням і активно його поширюють;
- R (неактивні) – користувачі, які більше не поширюють інформацію.

Математично модель описується системою диференціальних рівнянь:

$$\begin{cases} \frac{dS}{dt} = -\beta SI + \mu - \delta S \\ \frac{dI}{dt} = \beta SI - \gamma I - \delta I \\ \frac{dR}{dt} = \gamma I - \delta R \end{cases} \quad (1)$$

де β – швидкість поширення повідомлення, γ – швидкість втрати інтересу до нього, μ – приплив нових користувачів, δ – середня швидкість втрати активності. Отримані результати показують, що поширення інформації досягає піку за умови $\beta > \gamma$, а зростання μ значно підсилює віральність контенту. Це дозволяє ідентифікувати критичні вузли у мережі, через які можливе масове поширення персональних даних. Виявлення таких вузлів є надзвичайно важливим при побудові стратегій протидії дезінформації, оскільки дає змогу цілеспрямовано впливати на поширення контенту.

Крім того, моделювання поширення інформації дозволяє оцінити ефективність обмежувальних заходів , таких як затримка публікацій, модерація коментарів, а також алгоритмічне зниження пріоритетності певного контенту. Наприклад, виявлено, що навіть незначне зменшення коефіцієнта передачі інформації (β) за рахунок вчасного маркування підозрілого контенту може суттєво знизити загальний рівень охоплення.

Також доцільним є дослідження впливу структури мережі на динаміку поширення – зокрема, аналіз ролі центральних та периферійних учасників, щільності зв'язків та ступеня довіри між користувачами. Результати таких досліджень можуть лягти в основу системи раннього попередження про потенційні витоки персональних даних або кампанії з маніпулятивним впливом.

Практичні рекомендації передбачають використання складних паролів і менеджерів паролів, регулярну перевірку налаштувань приватності, мінімізацію обсягу особистої інформації, яку публікують користувачі, а також навчання цифровій гігієні та критичному мисленню.

У результаті дослідження виявлено, що підвищення кіберграмотності, використання сучасних технологій і прозора політика конфіденційності є ключовими факторами у зниженні ризиків втрати приватності у соціальних мережах

1. Solove D.J. Understanding Privacy. Harvard: Harvard University Press, 2008. 256 p.
2. Kokolakis S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security. – 2017. – Vol. 64. – P. 122-134.
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. General Data Protection Regulation (GDPR).
4. Махней О.В. Математичне моделювання. Івано-Франківськ, 2015. 23 с.

Кількісна оцінка безпеки інтернет-магазину OWASP Juice Shop

УДК 004.056

Наталія Загородна[1], Олександр Ревнюк[2], Руслан Козак[3]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]revo0708@gmail.com, [2]zagorodna_n@tntu.edu.ua, [3]ruslank@tntu.edu.ua

Сьогодні інтернет-магазин є не просто торговим майданчиком, а стратегічним інструментом розвитку бізнесу у цифрову епоху. Електронна торгівля через інтернет дозволяє бізнесу ефективніше взаємодіяти з покупцями, збирати аналітику про поведінку користувачів, автоматизувати процеси замовлень та логістики, а також зменшити витрати на фізичну інфраструктуру.

Використання інтернет-магазинів відкриває нові можливості для розвитку, але, водночас, робить компанію більш вразливою до кіберзагроз: хакерських атак, витоку даних та фінансових шахрайств. Тому, розвиваючи електронну комерцію, бізнес повинен паралельно інвестувати в надійні системи захисту, щоб зберегти довіру клієнтів і уникнути потенційних втрат.

Безпека вебдодатків регулюється стандартом OWASP Application Security Verification Standard (ASVS) [1]. Це один із ключових документів, розроблених OWASP, що встановлює чіткі критерії для перевірки безпеки вебзастосунків.

ASVS охоплює широкий спектр аспектів безпеки і складається з 14 розділів, які охоплюють такі теми, як автентифікація, управління сесіями, криптографія, обробка помилок, доступ до даних тощо. У версії ASVS 4.0.3, яка є актуальною станом на 2024 рік, міститься 286 вимог, розподілених за цими розділами.

Хоча OWASP ASVS є потужним інструментом для оцінки безпеки вебдодатків, варто зазначити, що він не передбачає чисельної оцінки для кожної окремої вимоги. Документ формулює вимоги як контрольні пункти — вони або виконані, або ні, без шкали градації (наприклад, частково виконано). У ASVS, також, відсутні формалізовані метрики, які б дозволяли кількісно оцінити загальний рівень безпеки. Це означає, що стандарт не забезпечує автоматичної або універсальної методики для порівняння безпеки між різними вебдодатками чи відстеження динаміки покращення. Крім того, використання стандарту передбачає вибір спектру вимог в залежності від типу вебдодатку, доступу до

інформації щодо етапів його розробки та експлуатації, що в свою чергу, є далеко непростим завданням навіть для досвідченого користувача.

В [2] було запропоновано адаптивну методологію розрахунку кількісного показника стану захищеності вебзастосунків на основі побудованої системи кількісних оцінок кожної з вимог та системи вагових коєфіцієнтів. Розроблена методика передбачає обчислення інтегральної оцінки *m*-ої вимоги в межах *n*-го розділу Rm,n, як зваженої суми відповідних оцінок критеріїв за цією вимогою. Оцінку безпеки *n*-го розділу можна обчислити схожим чином з врахуванням особливостей структури сайту та індивідуального підходу:

$$Qn=k=1mnRm,nRm,n, \quad (1)$$

де Rm,n - нормалізований ваговий коефіцієнт *m*-ої вимоги *n*-го розділу.

Кількісну інтегровану оцінку безпеки сайту запропоновано обчислювати, як середню оцінку безпеки всіх розділів:

$$Q=i=1NQnN \quad (2)$$

Хоч в [2] було запропоновано методику, проте не було наведено прикладу її застосування. В іншій публікації [3] авторів було здійснено спробу кількіоцінки безпеки інтернет-магазину на прикладі OWASP Juice Shop. OWASP Juice Shop – це навчальний вебдодаток з відкритим кодом, спеціально створений для практики тестування безпеки. Він містить навмисні вразливості всіх категорій OWASP Top 10 і слугує безпечним полігоном для етичного хакінгу.

Автори [3] побудували систему оцінок кожного з критеріїв за принципом:

- 1 бал – критерій повністю виконано,
- 0.5 бала – частково виконано або є обмеження,
- 0 балів – не виконано.

Абсолютні показники кожного розділу було обчислено, як суму набраних балів за всіма критеріями розділу, а відносні показники – як відношення набраної суми балів за розділом до максимально можливого балу. Даний підхід дає часткове розуміння ситуації, проте не враховує важливість вимог та не дає можливість обчислити інтегральну оцінку безпеки інтернет-магазину.

Використавши за основу множину відібраних вимог для оцінки безпеки інтернет-магазину на етапі експлуатації, авторами було запропоновано систему вагових коєфіцієнтів важливості кожного критерію та вимоги в межах розділу. На основі підходу запропонованого в [2] виконано обчислення значення захищеності за кожним розділом, які наведено в таблиці 1.

Таблиця 1

Кількісна оцінка захищеності інтернет-магазину OWASP Juice Shop за розділами

Розділ	Значення захищеності
Authentication	0.21
Session Management	0.43
Access Control	0.35
Validation, Sanitization and Encoding	0.52
Data Protection	0.28
Files and Resources	0.39
Configuration	0.47

Тоді загальний показник захищеності вебсайту, обчислений на основі формули (2) буде рівний 0,38. Невисокий показник обумовлений наявністю навмисно спроєктованих вразливостей в об'єкті дослідження.

1. OWASP Foundation. OWASP Application Security Verification Standard [Електронний ресурс] // OWASP. — Режим доступу: https://owasp.org/www-project-application-security-verification-standard/ (дата звернення: 03.05.2025)
2. Ревнюк, О. А. Адаптивна методологія розрахунку кількісного показника стану захищеності вебзастосунків / О. А. Ревнюк, Н. В. Загородна, О. С. Улічев // Центральноукраїнський науковий вісник. Технічні науки : зб. наук. пр. - Кропивницький : ЦНТУ, 2024. - Вип. 10(41). - Ч. 2. - С. 3-10.
3. Ревнюк О. А., Загородна Н. В. Методологія кількісної оцінки захищеності вебдодатку електронної комерції на етапі експлуатації // Scientific Bulletin of Ivano-Frankivsk National Technical University of Oil and Gas. — 2024. — № 2(57). — С. 107–119.

Культура безпеки як детермінанта вразливості до соціоінженерних атак у корпоративному середовищі

УДК 004.056
Михайло Запорожченко[1], Сергій Голобородько[2]
Державний університет інформаційно-комунікаційних технологій,
[1]m.zaporozhchenko@duikt.edu.ua, [2]s.holoborodko@duikt.edu.ua

У сучасних умовах соціоінженерні атаки залишаються одним із найефективніших інструментів компрометації корпоративної інформаційної безпеки (ІБ), оскільки орієнтовані на людський фактор – найменш формалізований та найменш захищений елемент будь-якої інформаційної інфраструктури. На відміну від технічних вразливостей, що підлягають автоматизованому виявленню й усуненню, людська вразливість формується у процесі взаємодії з організаційним середовищем, у тому числі – через культуру безпеки.

Культура безпеки у сфері ІБ трактується як сукупність колективних цінностей, норм поведінки, установок і практик, що визначають ставлення працівників до вимог безпеки та впливають на їхню готовність діяти відповідно до внутрішніх політик організації в умовах ризику. Саме низький рівень культури безпеки часто стає основою для успішної реалізації соціоінженерних впливів, оскільки знижує рівень критичності мислення, послаблює увагу до аномальних комунікацій та формує толерантність до несанкціонованої передачі інформації.

Проблема полягає в тому, що у більшості організацій культура безпеки не розглядається як стратегічний актив, не підлягає системному оцінюванню чи розвитку і зазвичай обмежується формальним ознайомленням із політиками або одноразовими тренінгами, які не формують стійких моделей поведінки. Відсутність послідовної програми формування культури ІБ підвищує організаційну вразливість до різних форм фішингу, маніпулятивної поведінки в комунікаціях та несанкціонованого фізичного доступу, що імітує легітимну взаємодію.

З практичної точки зору культура безпеки виконує роль регулятора поведінкових реакцій персоналу, впливаючи на імовірність того, що працівник розпізнає загрозу, повідомить про інцидент або діятиме згідно з протоколами. Таким чином, вона є опосередкованим, але критичним чинником у моделях оцінювання ризику успішності соціоінженерних атак.

Недостатньо сформована культура безпеки в організації виявляється через низку стійких поведінкових і організаційних проявів, які підвищують ймовірність успішної реалізації соціоінженерних сценаріїв. До основних індикаторів низької культури безпеки можна віднести такі:

відсутність практики верифікації аномальних запитів, наприклад, у разі отримання нетипових або невідповідних контексту вимог (зокрема, звернень, що імітують директиви керівництва, але суперечать усталеним процедурам), працівники часто діють за інерцією, не перевіряючи джерело або повноваження;

- недовіра або байдужість до каналів зв'язку з підрозділами ІБ, що проявляється в тому, що співробітники або не знають, як повідомити про підозрілі дії, або не вважають це за доцільне. Це призводить до зниження оперативності реагування та до невиявлених інцидентів, які залишаються поза увагою відповідальних осіб;
- нечітко виражена персональна відповідальність за дотримання вимог безпеки, що призводить до формування культури толерантності до відхилень. Це руйнує дисципліну виконання процедур і стимулює спрощення або ігнорування заходів захисту;
- низький рівень залученості або відсутність демонстрації належної поведінки з боку менеджменту знижує цінність норм ІБ в очах персоналу та розмиває легітимність політик безпеки.

Ефективне управління культурою безпеки потребує не разових дій, а створення цілісної системи організаційних і поведінкових механізмів, спрямованих на довгострокове закріплення бажаних моделей поведінки. Основні напрями цього процесу включають:

- побудову системи безперервного навчання, що виходить за межі формальних інструктажів і передбачає регулярне оновлення навчального контенту, використання імітаційних атак, сценарного моделювання та гейміфікованих методів для підвищення рефлексивного сприйняття ризиків;
- впровадження зворотного зв'язку як інструменту корекції поведінки, наприклад, формування двосторонніх каналів комунікації між співробітниками та підрозділом ІБ, що дозволить не лише виявляти слабкі місця, а й створювати атмосферу залученості, де безпека розглядається як спільна відповідальність;
- інтеграція показників (метрик) поведінкової безпеки у систему оцінювання результативності персоналу – у процеси атестації, преміювання чи внутрішнього аудиту – посилює суб'єктивне значення безпеки для співробітників і підвищує їхню мотивацію до дотримання встановлених норм;
- інтеграція принципів безпеки у повсякденну діяльність, зокрема, підтвердження чутливих запитів кількома каналами, обов'язкове використання захищених каналів комунікації, перевірка контексту при передачі

конфіденційної інформації, реалізація принципу нульової довіри (Zero Trust) на індивідуальному рівні тощо.

У цьому контексті культура безпеки не є лише похідною від технічної захищеності або нормативної відповідності – вона формується як організаційна компетенція, що дозволяє запобігати атакам, знижувати вразливість до маніпуляцій і підвищувати загальну стійкість системи. Її розвиток має здійснюватися як через впровадження чітко визначених процедур, так і через зміну підходів до управління, у яких людський чинник розглядається не як вразливість, а як ключовий об'єкт цілеспрямованого формування поведінки та навичок.

1. Security-first culture: defending against social engineering. URL: https://www.venzagroup.com/security-first-culture-defending-against-social-engineering (дата звернення: 24.04.2025)
2. Defending against social engineering: a proactive approach. URL: https://privacymatters.ubc.ca/news/defend-against-social-engineering (дата звернення: 24.04.2025)
3. 8 ways organisations prevent social engineering attacks. URL: https://blogs.stickmancyber.com/cybersecurity-blog/8-ways-organisations-prevent-social-engineering-attacks (дата звернення: 24.04.2025)

Структурна модель системи оцінювання стану кіберзахисту хмарних сервісів

УДК 004.056.5

Євгенія Іванченко[1], Євгеній Педченко[2], Марі Петровська[3], Ігор Іванченко[4]
State University of Information and Communication Technologies,
[1]evivancenko@gmail.com
State Non-Commercial Company «State University «Kyiv Aviation Institute»,
[2]ympedchenko@gmail.com, [3]pmarisha2004@gmail.com,[4]igor-p-l@gmail.com

Оцінювання рівня інформаційної безпеки постачальників хмарних сервісів є актуальним завданням для будь-якої організації, що планує або вже здійснила міграцію своїх ресурсів до хмарних середовищ, проте не володіє повною інформацією щодо їхньої кіберзахищеності [1]. Дослідження провідних світових компаній, зокрема Proofpoint [2], CrowdStrike [3] та Check Point [4], підтверджують, що проблема забезпечення безпеки хмарних платформ має пріоритетне значення, а організації, які застосовують хмарні технології, постійно стикаються з низкою ризиків, загроз та викликів у сфері кібербезпеки.

На сьогоднішній день, виділяються такі ключові проблеми оцінювання стану кіберзахисту хмарних сервісів: невиявлені та невиправлені вразливості, проведення перевірки налаштувань відповідно до кращих практик та належна побудова відповідного рівня захищеності на всіх рівнях роботи хмарних сервісів. З огляду на зазначене, проблема оцінювання стану кіберзахисту хмарних сервісів є комплексною та потребує системного підходу, що враховує інтереси та відповідальність як користувачів, так і постачальників хмарних послуг. Важливим аспектом цього процесу є постійний моніторинг і

впровадження відповідних інструментів, спрямованих на ефективне управління ризиками й ідентифікацію потенційних вразливостей [5].

Метою даної роботи є розробка структурної моделі системи оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури.

Новизною є розроблена структурна модель системи оцінювання, яка за рахунок розроблених модулів оцінювання дозволяє оцінити стан кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури [6].

Структурна модель системи оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури зображена на Рис. 1 та складається з наступних компонентів:

- база даних результатів оцінювання (БДРО);
- база даних загальних запитань (БДЗЗ);
- база даних запитань мережевого модуля (БДЗММ);
- база даних запитань модуля збереження даних (БДЗМЗД);
- база даних запитань серверного модуля (БДЗСМ);
- база даних запитань модуля віртуалізації (БДЗМВ);
- база даних запитань модуля операційної системи (БДЗОС);
- база даних запитань модуля контейнеризації (БДЗМК);
- база даних запитань модуля безперервної роботи (БДЗМБР);
- база даних запитань модуля додатків (БДЗМД);
- база даних запитань модуля обробки даних (БДЗМОД);
- база даних рекомендацій (БДР);
- база даних еталонних значень (БДЕЗ);
- модуль ініціалізації оцінювання (МІО);
- модуль отримання загальних даних (МОЗД);
- модуль оцінки мережі (МОМ);
- модуль оцінки зберігання даних (МОЗіД);
- модуль оцінки серверного обладнання (МОСО);
- модуль оцінки системи віртуалізації (МОСВ)
- модуль оцінки операційної системи (МООС);
- модуль оцінки системи контейнеризації (МОСК);
- модуль оцінки безперервної роботи (МОБР);
- модуль оцінки додатків (МОД);
- модуль оцінки обробки даних (МООД);
- модуль запису результатів оцінювання в базу даних (МЗРОБД);
- модуль візуалізації результатів оцінювання (МВРО) [5].

Структурна модель оцінювання стану кіберзахисту хмарних сервісів працює за наступним алгоритмом:

1. Робота системи починається із запуску модуля МІО для ініціалізації оцінювання та формування підмножини CSP.
2. Наступний модуль МОЗД із базою БДЗЗ визначає тип сервісу (IaaS, PaaS, CaaS, FaaS, SaaS [7]) та параметри оцінювання.
3. Модуль МОМ разом із базою БДЗММ оцінює захищеність мережевого рівня.

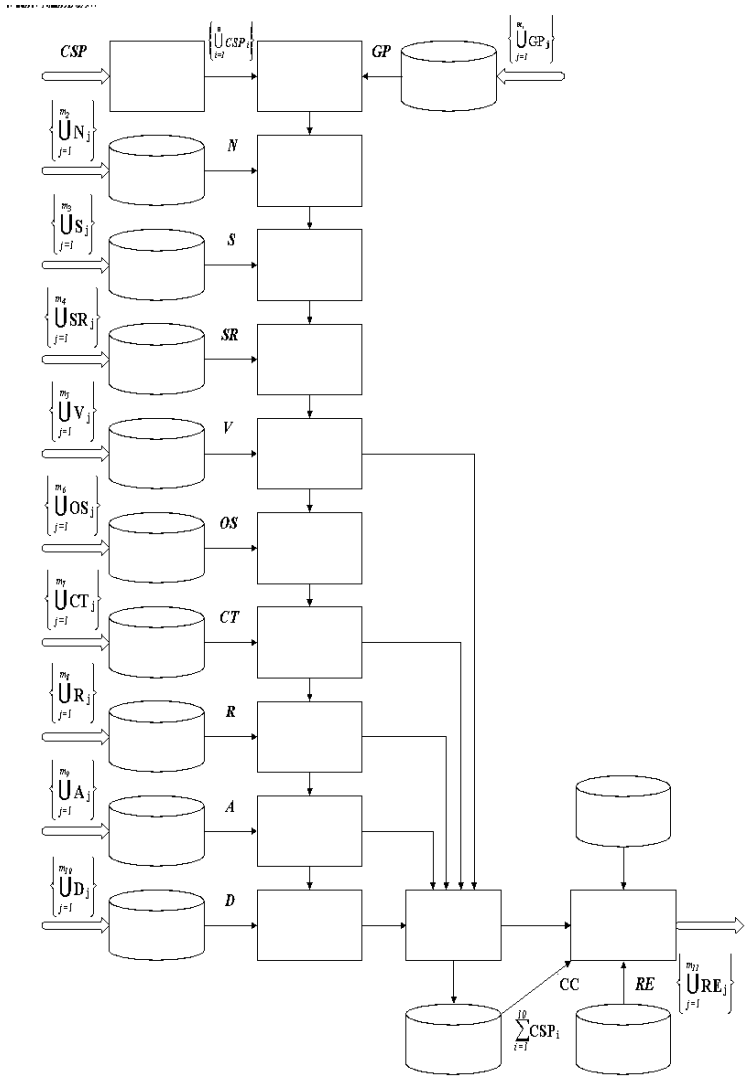


Рис. 1. Структурна модель системи оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури

4. Модуль МОЗіД із базою БДЗМЗД аналізує стан захисту середовища зберігання даних.

5. Модуль МОСО із базою БДЗСМ оцінює фізичну захищеність серверного обладнання.
6. Модуль МОСВ із базою БДЗМВ аналізує безпеку середовища віртуалізації VPC/VDS.
7. Модуль МООС з базою БДЗОС перевіряє захищеність підтримуваної операційної системи.
8. Модуль МОСК із базою БДЗМК здійснює оцінювання безпеки середовища контейнеризації.
9. Модуль МОБР з базою БДЗМБР визначає захищеність безперебійності роботи сервісу.
10. Модуль МОД з базою БДЗМД аналізує безпеку запропонованого хмарного застосунку.

Після завершення оцінки всіх параметрів запускається модуль МЗРОБД, який підраховує результати й записує їх у базу БДРО. Визначається загальна сума балів, обчислюється коефіцієнт СС та вводиться параметр **RC** для надання рекомендацій щодо подальшого використання сервісу у середовищі компанії.

В роботі представлено розроблену структурну модель системи оцінювання стану кіберзахисту хмарних сервісів об'єктів інформаційної інфраструктури, що базується на запропонованих моделі та методі оцінювання стану кіберзахисту хмарних сервісів. Для побудови структурної моделі було використано 11 параметрів оцінювання, визначених у відповідній моделі оцінювання. Кожному етапу оцінювання відповідають методичні напрацювання, які передбачають виставлення балів за відповіді аудитора під час проведення оцінюваня стану кіберзахисту хмарного сервісу. У структурній моделі продемонстровано взаємодію параметрів оцінювання з відповідними базами даних. За результатами оцінювання здійснюється підрахунок набраних балів, після чого приймається рішення щодо доцільності використання хмарного сервісу в продуктивному середовищі компанії. Розроблену систему оцінювання в подальшому буде використано для розробки програмного застосунку оцінювання стану кіберзахисту хмарних сервісів об’єктів інформаційної інфраструктури.

1. Cloud Adoption and Risk Report, *McAfee*. 2019, 14 p. URL: https://files.constantcontact.com/e4d8c81b001/d093e39a-1795-4f0b-928d-c5bb25a3a4b7.pdf
2. Stephen L. Cloud Security Posture Management (CSPM), *HyperGlance*. 2023. URL: https://www.hyperglance.com/blog/cloud-security-posture-management-cspm/
3. Shared responsibility in the cloud, *Microsoft*. 2024. URL: https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
4. ISO/IEC 27001. Information security management systems, *ISO*. 2022, 19 p. URL: https://www.iso.org/standard/27001
5. Педченко Є.М., Іванченко І.С. Структурна модель системи оцінювання кібербезпеки хмарних сервісів об’єктів інформаційної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 2024. Том 1, № 25. С.

505-515. URL: https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/667 . DOI: https://doi.org/10.28925/2663-4023.2024.25.505515

6. Педченко Є.М. Іванченко І.С. Метод оцінювання кіберзахищеності хмарних сервісів об'єктів інформаційної інфраструктури. *Сучасний захист інформації*. 2024, Том 59, № 3, 75-84 с. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2999/2897

7. Roger S. IaaS vs. CaaS vs. PaaS vs. FaaS vs. SaaS — What's the difference? *Medium*. 2021. URL: https://stample.com/link/stamples/5ff3d43b60b2acfb9eb5ceb6/iaas-vs-caas-vs-paas-vs-faas-vs-saas-whats-the-difference

Інструменти динамічного аналізу шкідливого програмного забезпечення

УДК 621.395.7 (043.2)

Степан Івасьєв[1], Віталій Кобиця[2]

Західноукраїнський національний університет,

[1]isv@wunu.edu.ua, [2]kobutsia.v.v@gmail.com

Розвиток шкідливого програмного забезпечення зумовлений постійною кібервійною призводить до постійної необхідності в засобах динамічного та статичного аналізу ШПЗ. Важливим елементом є боротьба з засобами виявлення віртуальних машин та методами їх протидії, що застосовуються в ШПЗ для унеможливлення їх динамічного аналізу.

Поширеними інструментами для аналізу ШПЗ є відкриті засоби доступні онлайн такі, як VirusTotal, Joe Sandbox Cloud, Hybrid Analysis, Any.Run, Intezer Analyze.

Проте враховуючи широкий набір засобів боротьби з віртуальними машинами окрему увагу потрібно приділити налаштуванню власної віртуальної машини, для боротьби з методами виявлення віртуалізації.

Для ефективного динамічного аналізу шкідливого програмного забезпечення доцільно використовувати такі віртуальні машини, які здатні протидіяти методам виявлення віртуалізації, які активно застосовують зловмисники. З цією метою слід обирати рішення, що забезпечують гнучке налаштування, можливість маскування віртуального середовища та максимально наближені до умов реального комп'ютера. Процес динамічного аналізу програмного забезпечення можна представити у вигляді схеми, що на рис. 1.

Для динамічного аналізу досить часто використовують гіпервізори VMware Workstation або VMware ESXi. Ці платформи мають відносно низький рівень виявлення, оскільки дозволяють детально налаштувати параметри віртуальної машини. Завдяки цим можливостям VMware часто використовується для ручного або напівавтоматизованого аналізу зразків шкідливого ПЗ.

Ще одним поширеним рішенням є VirtualBox, який завдяки відкритому вихідному коду зручно модифікувати. Проте в базовому стані VirtualBox часто виявляється шкідливими програмами через типові драйвери, службові процеси та пристрої з характерними назвами. Щоб зменшити ймовірність детектування, слід вручну видалити ознаки віртуального середовища, змінити системні назви

пристроїв, а також забезпечити імітацію справжніх користувацьких дій. Проте навіть за умови серйозного тюнінгу VirtualBox поступається VMware у здатності маскувати свою присутність.

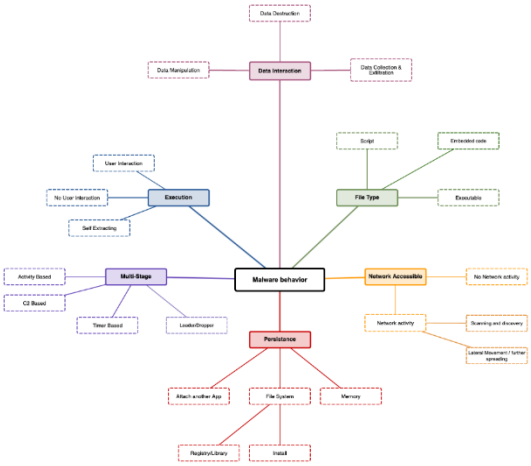


Рис.1. Схема динамічного аналізу програмного забезпечення

Для досвідчених користувачів хорошу альтернативу становить поєднання KVM та QEMU на базі Linux. Завдяки повній емуляції обладнання QEMU дозволяє створювати дуже реалістичне середовище, майже не відмінне від фізичного комп'ютера. Це значно ускладнює виявлення віртуалізації. KVM/QEMU часто використовуються у складних лабораторіях аналізу зразків зі складним захистом.

При динамічному аналізі для віртуальних машин часто застосовують набори засобів дослідження поведінки програмного забезпечення, таких як: Cuckoo Sandbox, REMnux, Sysinternals Suite, фреймворки DynamoRIO, Intel PIN або Frida. Для дослідження мережевої взаємодії широко застосовуються: Wireshark, Netcap або FakeNet-NG.

Методи протидії віртуальним машинам постійно вдосконалюються, тому сучасні системи динамічного аналізу застосовують техніки маскування або часткової емуляції, щоб обійти виявлення. Конкуренція засобів протидії віртуальним машинам та інструментів для динамічного аналізу ПЗ лише загострюється та обумовлює актуальність досліджень та нових розробок в даній сфері.

1. Saurabh, "Advance Malware Analysis Using Static and Dynamic Methodology," *2018 International Conference on Advanced Computation and Telecommunication (ICACAT)*, Bhopal, India, 2018, pp. 1-5, doi: 10.1109/ICACAT.2018.8933769.

2. S. Jadhav, T. T. Oh, J. P. Jeong, Y. H. Kim and J. N. Kim, "An Assistive System for Android Malware Analysis to Increase Malware Analysis Efficiency," *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, Taipei, Taiwan, 2017, pp. 370-374, doi: 10.1109/WAINA.2017.26.

3. A. K. Sinha and S. Sai, "Integrated Malware Analysis Sandbox for Static and Dynamic Analysis," *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Delhi, India, 2023, pp. 1-5, doi: 10.1109/ICCCNT56998.2023.10306805.

Підвищення надійності та захисту збору даних у вебзастосунках засобами конструкторів форм

УДК 621.395.7 (043.2)

Юрій Івков[1], Геннадій Шаповалов[2]
Національний університет "Одеська Політехніка",
[1]9480556@stud.op.edu.ua, [2]shapovalov@op.edu.ua

В умовах розвитку інформаційних технологій обсяг даних в обороті зростає, посилюються і вимоги стосовно їх захисту й обробки. Цифровізація потребує рішень які дозволять забезпечити їхню цілісність, конфіденційність і доступність. Однією з проблем сучасної IT-інфраструктури у вебсфері є ненадійність механізмів збору й обробки даних, їх контролю [1].

Метою дослідження є аналіз проблем надійності збору та обробки даних у вебсередовищі, а також вивчення можливостей використання конструкторів вебформ як засобу для підвищення безпеки, стандартизації та ефективності цих процесів та розробки за результатами дослідження ефективного конструктора захищених веб-форм.

Практично всі сервіси "спілкуються" із користувачем через вебформи, які своєю чергою різняться у складності та різноманітності від реєстраційних і контактних до багаторівневих опитувальників. Вебформи використовуються на комерційних сайтах, в електронному урядуванні, медичних системах, освітніх платформах. Помилки в їх обробці чи захисті мають реальні наслідки, тому розв'язання проблем в цих областях має прикладне значення. Варто поставити питання – чи є вебформи достатньо надійними та чи підготовлені вони для розширення або швидких змін? До того ж, потрібні технічні знання для реалізації та підтримки постійного рівня якості, адже розробку треба вести як на клієнтському, так і на серверному рівнях, що може бути поза можливостями менших бізнесів [2].

Конструктори вебформ можуть допомогти розв'язати ці проблеми – такі застосунки-інструменти мають вбудовані механізми для створення, редагування та вбудовування у будь-які вебзастосунки, гарантуючи централізовану обробку всіх форм без винятків. Важливим є і те, що перевірка виконується як на клієнтській, так і на серверній частині. Такі інструменти можуть одразу "з коробки" підтримувати методи захисту вебформ, такі як, наприклад, honeypot-поля для боротьби зі спамом, автоматично додавати CSRF-маркери, вводити CAPTCHA, та забезпечувати перевірку і фільтрацію введених

даних як на клієнтському, так і на серверному рівнях [3]. Узагальнена схема принципу роботи конструкторів форм представлена на рис. 1.

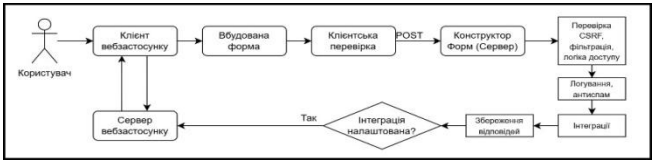


Рисунок 1 – “Узагальнена схема принципу роботи конструкторів форм”

Конструктори вебформ є зручними завдяки можливості додавати інтеграції – відправлення заповнень форм на пошту, аналіз даних, зв’язок із зовнішніми API та сервісами аналітики. Так вони забезпечують не лише збір, а й первинну обробку даних [2]. Ба більше, сучасні дослідження у сфері кібербезпеки призводять до розробки нових способів виявлення загроз, які можуть бути інтегровані як модулі в конструктори форм. Це дозволить швидко реагувати на нові загрози й оновлювати механізми захисту. Хоча це ще не універсальним рішенням, конструктори вебформ є кроком у вирішенні проблеми доступності для людей з обмеженими можливостями. Якщо конструктор відповідає стандартам WCAG, це значно спрощує реалізацію вимог доступності і підвищує ймовірність їхнього впровадження.

Як показав аналіз сучасних аналогів в ході дослідження, більша частина основного функціоналу такий як інтеграції, кількість відправлень форм, контроль доступу в межах самого конструктора форм, є платним. Також популярні конструктори форм які потенційно можуть бути повністю інтегровані в інші вебзастосунки можуть потребувати для цього корегувань коду (якщо це інструменти із відкритим кодом), що теж є недоліком. Пропонується впровадити гнучку систему контролю доступу для самого конструктора форм; гнучке налаштування форм (готові шаблони, користувацькі поля тощо); ввести основні методи захисту; дозволити зручну інтеграцію API із власними сервісами. Те, що все це може бути реалізовано в межах одного застосунку, мінімізує ризики, пов’язані із обробкою даних, помилками при інтеграції форм які були створені власноруч.

Таким чином, в результаті дослідження було розроблено ефективний засіб для створення веб-форм з урахуванням безпеки та засобів боротьби з фрагментацією обробки інформації, передбачено швидку адаптованість до змін у вимогах безпеки, покращено шифрування, валідацію, методи захисту від атак. Конструктор вебформ загалом розв’язує одразу кілька завдань: стандартизацію збору і обробки даних, централізоване впровадження політик безпеки і формалізацію процесу валідації та збереження інформації, що може стати кроком у перетворенні вебсервісів на більш інклюзивні, сприяти відповідності сучасним нормам цифрової етики та законодавства.

1. IBM. What Is Data Reliability. IBM - United States. URL: https://www.ibm.com/think/topics/data-reliability (Дата звернення: 08.04.2025).

2. Dr Sarita Simaiya, Muskan Singh, Makul Swami, Dudekula Sabaa Farheen. Formcraft: Empowering Dynamic Online Forms. International Journal of Engineering Research & Technology (IJERT), 2023. URL: https://www.ijert.org/research/formcraft-empowering-dynamic-online-forms-IJERTV12IS110188.pdf?utm_source=chatgpt.com

3. Толокнов Анатолій Арнольдович. Огляд методів захисту вебформ. Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень : матеріали Міжнар. наук.-практ. конф., м. Одеса 19 травня 2023 р. с.599-602. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/268a770e-1ea1-4a29-9bf5-e45440f41a2a/content

Програмна реалізація перевірки автентичності та шифрування даних у мобільному середовищі

УДК 621.395.7 (043.2)

Владислав Ілінчук
Національний університет «Одеська політехніка»
9480554@stud.op.edu.ua

У сучасних умовах стрімкого переходу користувачів зі стаціонарних пристроїв на мобільні, а також зростання обсягів оброблюваної та збереженої особистої інформації, смартфони стають все більш привабливою мішенню для кіберзлочинців. Проблема забезпечення цілісності та конфіденційності даних потребує глибокого аналізу існуючих механізмів захисту. Перевірка хеш-сум файлів та використання криптографічного шифрування відіграють ключову роль у протидії несанкціонованим змінам і витоку інформації.

Метою роботи є розробка програмного застосунку та аналіз інструментів , які забезпечують надійний захист мобільних пристроїв. Основна ціль застосунку є здійснення локальних перевірок хеш-сум APK-файлів, виявляючи розбіжності з так званою «еталонною базою», що забезпечує захист даних шляхом виявлення змінених або підроблених APK-файлів. Крім того, в застосунку реалізовано функціонал симетричного шифрування та дешифрування будь-якого обраного файлу за допомогою алгоритму AES , що дозволяє надійно захищати інформацію користувача. Основні функції застосунку представлені на інтерфейсі, що показано на рис. 1.

Також у межах практичного дослідження було проведено тести на двох пристроях з різними версіями Android (Kyivstar Aqua — Android 2.3.4 та OPPO A17k — Android 12). За допомогою інструмента ADB (Android Debug Bridge) перевірено наявність шифрування, можливість доступу до системних файлів, а також вивчено статус SELinux. В доповнення , для демонстрації потенційних загроз було створено тестовий Android-додаток, який без root-доступу збирає технічну інформацію про пристрій (модель, версію ОС, Android ID) та надсилає її на зовнішній сервер, імітуючи атаку.

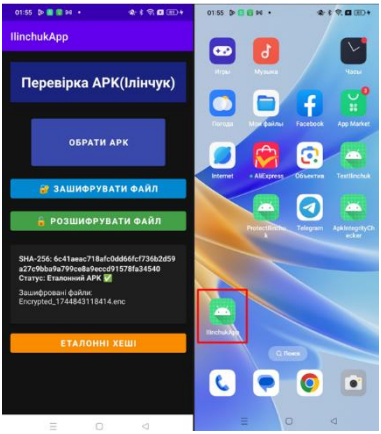


Рис.1. Інтерфейс застосунку

В результаті цього дослідження проведено порівняння пристроїв з Android 2.3.4 та 12, що підтвердило перевагу сучасної ОС завдяки наявності розширених механізмів захисту, зокрема шифрування та SELinux.

Наукова новизна роботи полягає у поєднанні методів перевірки цілісності (SHA-256) з еталонною базою, а також у реалізації локального шифрування/дешифрування файлів алгоритмом AES у рамках одного застосунку. У розробленій програмі користувач може обрати APK-файл, перевірити його хеш, зашифрувати або розшифрувати будь-який інший файл, а також ознайомитися зі списком зашифрованих елементів. Розробка застосунку здійснена у середовищі Android Studio з використанням мови програмування Java.

Розроблений застосунок може використовуватись як у корпоративному середовищі, так і для особистого захисту. У компаніях, що розповсюджують власні APK-додатки, він дозволяє перевірити автентичність файлів перед встановленням завдяки порівнянню з еталонними хешами, що знижує ризик розповсюдження модифікованого або шкідливого ПЗ. Для індивідуальних користувачів застосунок стане корисним інструментом при встановленні програм з неофіційних джерел, а також для локального шифрування конфіденційних документів без залучення хмарних сервісів.

1. Ahmed A., Uk I. Analysis of Most Common Encryption Algorithms. *Empirical Research Press Ltd.*, 2022.

2. Gotzfried J., Müller T. Analysing Android’s Full Disk Encryption Feature. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications.* – 2013. – Т. 5, №1. – С. 84–100.

3. Zangana H. M., Omar M. Threats, Attacks, and Mitigations of Smartphone Security. *Academic Journal of Nawroz University (AJNU).* – 2020. – Т. 9, №4. – С. 324–331.

Multicollision attacks on tree-based hash functions

UDC 004.056.55:004.032.26
Vitalii Kazmirevskyi[1], Yurii Baryshev[2]
Vinnytsia National Technical University,
[1]kazmirevskiy1999@gmail.com, [2]yuriy.baryshev@vntu.edu.ua

Tee-based hash functions are increasingly adopted across a wide range of practical applications: ensuring and verifying data integrity in blockchain systems, optimization of electronic document workflow, structured hashing of complex objects (such as JSON or XML), digital signature schemes etc. This approach allows reduced complexity of hash values updating due to ability of processing only an updated part of the hashed message. However, tree structure exhibits internal non-uniformity, which creates new attack vectors such as subtrees manipulation.

The aim of this research is to improve tree-based hash functions infeasibility be analyzing the structural vulnerabilities of tree-based hash functions in the context of multicollision attacks.

One of the most important attacks is the method proposed by Antoine Joux in 2004 [1], which is schematically illustrated in Figure 1.

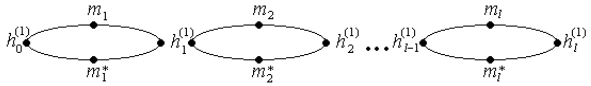


Fig. 1. Schematic representation of Joux's multicollision.

It is based on the ability to combine collisions of the compression function into an exponentially growing set of messages that yield the same hash value [1]. Another significant method is the Colliding subtree attack, which relies on the repeated usage of collisions to construct tree nodes those yield to identical hash values. In the absence of domain separation or positional information within the tree structure, this attack enables the generation of 2^k collisions with the same computational cost as finding k collisions [2]. Another case of efficient attack is the Herding-based tree collision attack [3]. Due to the hierarchical structure of the hash tree, this attack allows an adversary to manipulate not only individual nodes but entire subtrees.

Hash tree grafting attack, which exploits the ability to replace a subtree of the hash tree with an alternative, structurally compatible subtree containing different content, without altering the final hash. This attack is based on the existence of collisions between subtrees that differ in input data but produce the same intermediate hashes [4]. The position-blind multicollision attack constitutes a separate class of attacks those arise when the compression function of the hash does not rely on the position of input blocks within the tree [3]. A further critical threat is posed by the Expand-compress tree attack [5], which is based on alternating phases of tree expansion and compression to create multicollisions between trees of differing topology but with the same resulting hash. A summarized comparative analysis of these attacks is presented in Table 1.

Table 1

Comparative analyses of the multicollision attacks

Attack	Threat	Complexity
Joux's attack	Generation of an exponentially growing number of multicollisions	Decreases with tree height
Colliding Subtree	Possibility of subtree manipulation	Decreases with tree height
Herding-based Tree Collision	Possibility of manipulating subtrees	High complexity; requires manipulation of tree structure
Hash Tree Grafting Attack	Ability to alter the tree structure	Medium complexity; requires finding subtrees collisions
Position-Blind Multicollision	Generation of an exponentially growing number of multicollisions	Decreases with tree height
Expand-Compress Tree Attack	Construction of different trees with the same final hash	Technically complex; effective when structural protections are absent

Tree-based hash functions, despite their advantages, are vulnerable to multicollision attacks. The research findings confirm the critical impact of tree height and the structure of the compression function on the overall resilience of the system. The analyzed attacks highlight the necessity of integrating contextual information, positional encoding, and unique identifiers for nodes and levels in the design of tree-based hash functions.

1. Joux A. Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions. *Advances in Cryptology - CRYPTO 2004*, 2004. p. 306-316. URL: https://link.springer.com/chapter/10.1007/978-3-540-28628-8_19 (application date 23.04.2025).

2. Andreeva E., Bouillaguet C., Dunkelman O., Fouque P., Hoch J., Kelsey J., Shamir A., Zimmer S. New Second-Preimage Attacks on Hash Functions. *Journal of Cryptology*. – 2015. – V. 29 – p. 657-696. (application date 23.04.2025).

3. Andreeva E., Bouillaguet C., Dunkelman O., Kelsey J. Herding, Second Preimage and Trojan Message Attacks Beyond Merkle-Damgard. Selected Areas in Cryptography, 2009. p. 393-414. URL: https://link.springer.com/chapter/10.1007/978-3-642-05445-7_25 (application date 23.04.2025).

4. Castelnovi L., Martinelli A., Prest T. Grafting Trees: A Fault Attack Against the SPHINCS Framework. *Post-Quantum Cryptography*, 2018. p. 165–184. URL: https://eprint.iacr.org/2018/102.pdf (application date 23.04.2025).

5. Blackburn S., Stinson D., Upadhyay J.. On the complexity of the herding attack and some related attacks on hash functions. *Designs, Codes and Cryptography*,

2011. p. 171-193. URL: https://eprint.iacr.org/2010/030.pdf (application date 23.04.2025).

Дослідження ролі машинного навчання та глибоких нейронних мереж у боротьбі з фінансовими злочинами

УДК 004.8

Богдан Калинюк[1], Ірина Замрій[2]
Державний університет інформаційно-комунікаційних технологій,
[1]*b.kalyniuk@duikt.edu.ua*, [2]*i.zamrii@duikt.edu.ua,*

У сучасному фінансовому середовищі кількість та складність шахрайських схем стрімко зростає, що зумовлює необхідність впровадження інтелектуальних систем виявлення загроз.

Класичні методи, що базуються на правилах або статистичних порогах, виявилися обмеженими у виявленні складних і нових форм фінансових злочинів. З огляду на це, особливу увагу привертають підходи машинного навчання (ML) та глибоких нейронних мереж (DNN), які здатні аналізувати великі обсяги даних транзакцій, виявляючи аномалії навіть у складних часових і структурних шаблонах [1].

Мета дослідження — дослідити потенціал сучасних методів машинного та глибокого навчання для виявлення фінансових злочинів, оцінити їхню точність, адаптивність, продуктивність, а також проаналізувати можливості їх практичного впровадження у фінансових установах.

Актуальність дослідження зумовлена необхідністю підвищення ефективності систем протидії шахрайству в умовах динамічного зростання обсягу електронних транзакцій, зниження довіри користувачів до фінансових послуг через часті інциденти шахрайства, а також появи більш витончених атак, які не фіксуються традиційними інструментами [2].

Наукова новизна роботи полягає у порівняльному аналізі продуктивності кількох архітектур DNN — зокрема згорткових нейронних мереж (CNN), довготривалої короткочасної пам'яті (LSTM), автоенкодерів (AE) та графових нейронних мереж (GNN) — у задачах детекції аномалій у транзакційних потоках.

Додатково проаналізовано гібридні моделі, які поєднують навчання з підкріпленням (Reinforcement Learning, RL) з моделями класифікації, що дає змогу адаптуватися до нових шаблонів поведінки моделі в режимі реального часу [3].

Дослідження базується на обробці двох відкритих наборів даних:

1) Credit Card Fraud Detection Dataset (розміщений на Kaggle, містить анонімізовані дані реальних транзакцій з високою диспропорцією між класами) [4];

2) PaySim — симульований набір мобільних грошових переказів на основі даних з M-Pesa (опублікований у Harvard Dataverse) [5].

Було здійснено повний цикл обробки даних: очищення, нормалізація, зменшення дисбалансу класів через SMOTE, побудова та тренування моделей. Нижче подано порівняльну таблицю з результатами основних метрик:

Таблиця 1

Порівняльний аналіз моделей виявлення фінансових злочинів

Модель	F1-міра (%)	Точність (Accuracy, %)	Повнота (Recall, %)	Середній час прогнозу (мс/запис)
Logistic Regression	82.4	91.1	79.3	0.5
XGBoost	91.6	96.3	89.7	1.8
CNN	93.0	97.1	91.5	2.1
LSTM	95.8	97.8	94.2	3.4
Autoencoder (AE)	94.6	96.9	93.1	2.6
GNN	92.2	95.7	90.4	4.0

CNN та XGBoost продемонстрували високі результати на великих масивах даних, однак LSTM та AE показали кращу продуктивність у виявленні складних, часово залежних аномалій. GNN виявили потенціал у виявленні скоординованих атак між пов'язаними користувачами [6], хоча вимагають більше ресурсів для розгортання.

Використання глибокого навчання у фінансовій безпеці дає змогу значно підвищити точність виявлення злочинів порівняно з класичними підходами. Комбінація різних архітектур нейромереж і методів обробки даних дозволяє адаптувати системи до нових викликів. У подальших дослідженнях важливо зосередитися на підвищенні енергоефективності моделей і забезпеченні пояснюваності результатів, що є критично важливим для довіри регуляторів і користувачів.

1. Phua C., Lee V., Smith K., Gayler R. A Comprehensive Survey of Data Mining-based Fraud Detection Research. arXiv:1009.6119. – 2010.

2. West J., Bhattacharya M. Intelligent financial fraud detection: A comprehensive review. Computers & Security. – 2016. – Vol. 57. – P. 47–66.

3. Fiore U., De Santis A., Perla F., Zanetti P., Palmieri F. Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. Information Sciences. – 2019. – Vol. 479. – P. 448–455.

4. Dal Pozzolo A., Boracchi G., Caelen O., Alippi C., Bontempi G. Credit Card Fraud Detection Dataset. Kaggle. https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud

5. Lopez-Rojas E. PaySim: Simulation of Mobile Money Transactions Dataset. Harvard Dataverse. https://doi.org/10.7910/DVN/UU6IDR

6. Dou Y., Liu Z., Sun L., Deng Y., Peng H., Yu P.S. Enhancing Graph Neural Network-based Fraud Detectors against Camouflaged Fraudsters. Proceedings of the 29th ACM SIGKDD Conference. – 2023.

Використання технології цифрового водяного знаку як засобу контролю академічної доброчесності

УДК 004.93+005.33

Владислав Капелюшний[1], Наталія Кушніренко[2], Інна Ярова[3]

Національний університет «Одеська політехніка»,

[1]9480571@stud.op.edu.ua, [2]kushnirenko@op.edu.ua, [3]yarova@op.edu.ua

Академічна доброчесність є фундаментальним принципом, на якому базується довіра до результатів навчання. В умовах впровадження у ВНЗ систем дистанційного навчання, актуальною є потреба у простих та ефективних технічних засобах контролю академічної доброчесності під час складання тестів онлайн. Одним із таких засобів є технологія цифрового водяного знаку (ЦВЗ) – інструмент, який дозволяє не лише унеможливити копіювання тестових завдань, але й забезпечити відстежуваність джерела витоку, легко інтегрується в сучасні освітні платформи та збільшує рівень автоматизації процесів моніторингу академічної доброчесності [1].

Мета: проаналізувати можливості використання технології ЦВЗ як ефективного інструменту контролю академічної доброчесності в умовах дистанційного навчання.

ЦВЗ у контексті освітньої платформи – це прихований або візуально помітний текстовий маркер, що пов'язаний із особистими даними студента на цієї платформі. Певні дані, наприклад, ID користувача, його ім'я, прізвище, електронна пошта, дата народження або дата складання тесту можуть бути об'єднані в унікальний рядок, який хешується криптографічним алгоритмом. Створений хеш розміщується як прозорий текст на сторінку тестування, таким чином роблячи кожну копію тесту унікальною [2].

Використання ЦВЗ дозволяє зменшити ймовірність академічного шахрайства двома ключовими способами: превентивним і доказовим. Превентивний аспект полягає в тому, що студент, який проходить тест, бачить на екрані свій персоналізований ідентифікатор – цифровий водяний знак, сформований на основі його особистих даних, який виводиться у кількох частинах сторінки, зокрема у вигляді прозорого тексту, вбудованого у фон або кути запитання. Наявність такого маркера формує психологічний бар'єр для користувача: він усвідомлює, що кожне завдання містить його цифровий слід і що в разі порушення (наприклад, публікації в мережі або спроби обміну завданнями) відповідальність буде покладена особисто на нього. Доказовий аспект реалізується за умови, коли все ж відбувся витік інформації (тестових завдань). Якщо в інтернеті опиняється скріншот із завданням, достатньо зчитати ЦВЗ, який залишився у зображенні або у фоновому шарі HTML, зіставити його з базою користувачів, і таким чином швидко визначити джерело витоку. Це дозволяє не лише оперативно реагувати на порушення, а й вжити відповідних дисциплінарних заходів. Подібна система надає цінну доказову базу для рішень комісій з академічної доброчесності. У поєднанні ці два механізми забезпечують ефективну систему контролю академічної доброчесності, що працює як запобіжник і одночасно як інструмент для розслідування порушень.

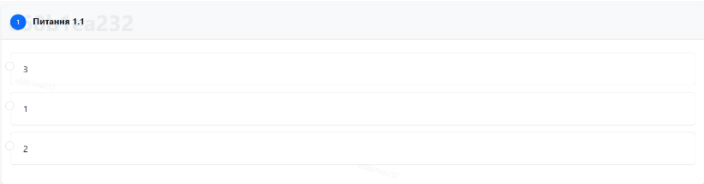


Рис.1. Приклад використання цифрового водяного знаку на сторінці тестування

Приклад вбудовування ЦВЗ на сторінку тестування наведений на рисунку 1. Для створення хешу використано криптографічний алгоритм BLAKE2b, який є сучасною альтернативою SHA-2. Для формування унікального ЦВЗ враховуються особисті дані користувача. Отриманий хеш обрізається до обсягу 10 – 12 символів, що дозволяє виводити його у інтерфейс без візуального перевантаження простору запитання.

Додатковими опціями контролю можуть бути заборона користувачеві відкривати консолі браузера, використання правої кнопки миші, копіювання вмісту або збереження сторінки через клавіші PrintScreen чи Ctrl+P. Реалізація таких обмежень здійснюватиметься через події JavaScript (keydown, contextmenu, copy), які блокуватимуть взаємодію з інтерфейсом тесту. Також можлива реалізація механізмів детекції спроб зробити знімок екрана, наприклад, за допомогою зміни фокусу вікна або зменшення яскравості сторінки при втраті активності. Також система може вести журнал усіх спроб взаємодії з HTML-структурою сторінки через інструменти розробника, що дозволить виявити потенційно підозрілі дії студентів у реальному часі.

Впровадження технології ЦВЗ у системах онлайн-тестування знань підвищує ефективність процесів підтримки академічної доброчесності. Вони поєднують у собі технічну складову з етичним впливом, сприяючи персоналізації та прозорості навчального процесу. Завдяки використанню сучасних криптографічних алгоритмів та гнучкій інтеграції в HTML-інтерфейс, цифрові водяні знаки дають змогу не лише відстежувати витоки інформації, а й запобігати порушенням ще до їх виникнення. У майбутньому подібна система може доповнюватись інтелектуальним аналізом поведінки, автоматичним логуванням підозрілих дій та засобами виявлення спроб обходу захисту. Таким чином, цифрові водяні знаки стають не лише інструментом контролю, а й активним елементом цифрової педагогіки, що сприяє формуванню свідомої та відповідальної академічної спільноти.

1. Barni M., Bartolini F., Cox I. J., Hernandez J., Perez-Gonzalez F. Digital watermarking for copyright protection. *IEEE Communications Magazine*. – 2001. – V. 39, №8. – p. 90-91. DOI: 10.1109/MCOM.2001.940043 (application date 22.04.2025).

2. Allaf A.H., Kbir M.A. A Review of Digital Watermarking Applications for Medical Image Exchange Security. Springer, Cham. 2019. URL: https://doi.org/10.1007/978-3-030-11196-0_40 (application date 22.04.2025).

Алгоритм протидії Cross-Site Scripting атакам на веб додатки

УДК 621.395.7 (043.2)

Дмитро Карпец
Західноукраїнський національний університет,
d.karpets@st.wunu.edu.ua

Cross-Site Scripting (XSS) вразливості, які завжди були широко розповсюджені у веб додатках, залишаються бути такими ж актуальними на сьогоднішній день. Цьому свідчать рейтингові списки популярних веб вразливостей та вразливостей безпеки загалом. Так, MITRE зі своїм щорічним рейтингом “CWE Top 25” віддає XSS атакам першу сходинку [1], а Open Worldwide Application Security Project (OWASP) з рейтинговим списком “OWASP Top Ten”, відносячи XSS вразливості до категорії ін'єкцій, розміщують її на третій позиції [2].

Метою роботи є покращення алгоритму протидії Cross-Site Scripting атакам на веб додатки.

Реалізація XSS атак можлива, коли користувач передає довільні дані, а веб додаток не виконуючи належної валідації та обробки цих даних, безпосередньо виводить їх на своїх веб сторінках [3] (Рис.1).

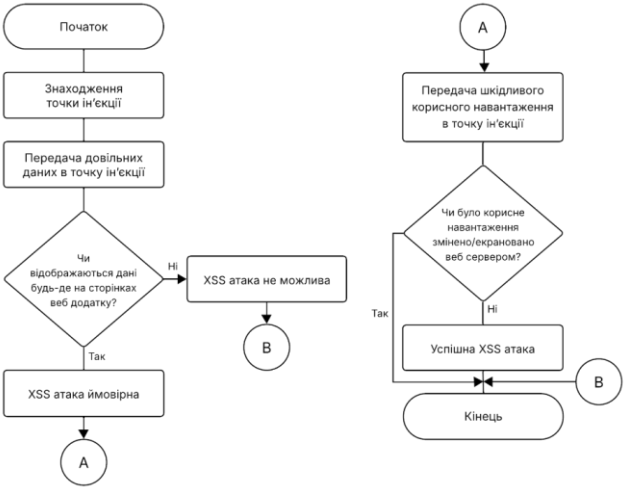


Рис.1. Схема алгоритму XSS атаки

В результаті досліджень запропоновано алгоритм протидії XSS атакам (Рис.2).

У зв'язку з тим, що популярність XSS вразливостей не спадає, створення нових та покращення існуючих алгоритмів протидії XSS атакам є актуальним завданням. На сьогоднішній день, на фоні масштабного прогресу пов'язаного з штучним інтелектом (ШІ), пропонується залучати ШІ до розроблення автоматизованих засобів перевірки коду на наявність XSS вразливостей.

Рис.2. Схема алгоритму протидії XSS атаці

Було розглянуто актуальність XSS вразливостей у веб додатках, алгоритм атаки, алгоритм протидії та запропоновано його покращення.

1. CWE Top 25 Most Dangerous Software Weaknesses 2024. URL: https://cwe.mitre.org/top25/archive/2024/2024_cwe_top25.html (дата звернення: 01.04.2025).
2. OWASP Top Ten Web Application Security Risks. URL: https://owasp.org/www-project-top-ten/ (дата звернення: 01.04.2025).
3. CWE-79: Improper Neutralization of Input During Web Page Generation. URL: https://cwe.mitre.org/data/definitions/79.html (дата звернення: 01.04.2025).

Протидії кіберзагрозам на основі штучного інтелекту

УДК 004.056.5:004.08
Євген Кихтенко[1], Олексій Шкурченко[2]
Державний університет інформаційно-комунікаційних технологій,
[1] kykhtenko@stud.duikt.edu.ua, [2] shkurchenko@stud.duikt.edu.ua

Завдяки значному розвитку інформаційних і комунікаційних технологій з’являються та швидко змінюються нові загрози кібербезпеці. Кіберзлочинці впроваджують нові методи, які роблять їхні атаки швидшими та масштабнішими. Таким чином, існує попит на більш адаптивні та компактні

системи кіберзахисту, які можуть виявляти широкий спектр загроз у реальному часі.

В останні роки впровадження методів штучного інтелекту (ШІ) зросло і продовжує відігравати важливу роль у виявленні та запобіганні кіберзагрозам. Хоча програму штучного інтелекту було запропоновано в 1950-х роках, останніми роками вона швидко розширилася і зараз впливає на всі форми спільнот і професій. Ця тенденція також впливає на сферу кібербезпеки, де штучний інтелект використовується як для нападу, так і для захисту в кіберпросторі [1].

Штучний інтелект приносить користь багатьом сферам, таким як обробка природної мови, ігри, освіта, охорона здоров'я, виробництво тощо. З точки зору атаки, кіберзагрози можуть використовувати штучний інтелект для покращення досконалості та масштабу своїх атак. Вони стають більш гнучкими та ефективними, що передбачає адаптацію до змін у навколишньому середовищі, щоб зменшити впливи, які виникли.

Швидкий розвиток комп'ютерних технологій та Інтернету значно впливає на повсякденне життя та роботу людей, однак це також створило багато нових проблем кібербезпеки: по-перше, поширення даних робить ручний аналіз непрактичним [2]. По-друге, загрози зростають швидкими темпами, що теж означає, що нові, короткоживучі види та високоадаптивні загрози стають цілком нормальним явищем. По-третє, загрози в даний час загрожують різними методами розповсюдження, зараження та уникнення; тому їх важко передбачити та виявити. Для створення та впровадження алгоритму потрібно багато часу, грошей і зусиль.

Крім того, наймати або навчати людей у цій галузі важко і дорого. Багато відхилень і загроз виникають і продовжують поширюватися, тому очікується, що методи на основі штучного інтелекту будуть йти в ногу з цими проблемами кібербезпеки [3].

Розвиток технологій значно полегшує наше життя в майбутньому. Кожна нова технологія, що з'являється, несе з собою величезну кількість переваг, але, на жаль, перш за все в очі впадають недоліки. Така ж ситуація і зі штучним інтелектом.

Область, яка дає нам стільки переваг, є дуже великою проблемою на майбутнє через її недоліки, коли мова йде про конфіденційність. На щастя, потужність цієї технології настільки велика, що вона приносить із собою численні рішення.

Справа в тому, що люди недостатньо поінформовані про ризики залишати свою особисту інформацію в Інтернеті, незважаючи на те, що нас до цього ніхто не змушує. Дуже важливо, щоб кількість людей, які працюють над рішеннями безпеки даних, була більшою, ніж кількість тих, хто намагається ними зловживати, оскільки захист даних є першою стіною захисту від злочинності сучасності.

1. Zhang, S., & Zhao, J. (2021). AI Techniques in Network Security. IEEE Transactions on Information Forensics and Security.

2. Shostak, A. (2019). Artificial Intelligence for Counter-Terrorism. Journal of Security Studies.

3. Grata E. G., Deshpande A., Lopes R. T., Laghari A. A., Khan A. A., Jenice Aroma R., Jumani, A. K. (2024). Artificial intelligence for threat anomaly detection using graph Data bases a semantic outlook. Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection, 249-278.

Гібридний метод виявлення аномального трафіку в інформаційно-комунікаційних системах

УДК 004.056.5

Юрій Кльоц[1], Наталія Петляк[2]
Хмельницький національний університет,
[1]klots@khmnu.edu.ua, [2]npetlyak@khmnu.edu.ua

Виявлення аномального трафіку є важливим компонентом сучасної системи захисту інформаційно-комунікаційної системи (ІКС), оскільки дозволяє своєчасно ідентифікувати нетипову активність, що може свідчити про спроби несанкціонованого доступу, розповсюдження шкідливого програмного забезпечення або витік конфіденційних даних. Своєчасне виявлення аномалій оптимізує використання ресурсів системи безпеки, дозволяючи сфокусувати увагу аналітиків на дійсно критичних інцидентах та скоротити кількість хибнопозитивних спрацювань [1].

У даній роботі запропоновано гібридний метод, який пропонує використання трьох різних підходів до класифікації трафіку, що формують гібридну систему аналізу. Метод класифікація за ознаками базується на порівнянні сигнатури з множинами дозволених (DG), заборонених (DB) та невизначених (DU) сигнатур.

Метод швидкий і ефективний при наявності повної бази відомих зразків, однак не здатен обробити нові аномалії. Метод класифікація на основі самоподібності аналізує поведінкову подібність трафіку до вже відомих зразків. Цей підхід дозволяє виявляти варіації відомих аномалій, зберігаючи чутливість до нових типів, які частково збігаються з наявними шаблонами.

Нечіткий метод виявлення аномалій ґрунтується на нечіткій логіці, що дозволяє моделювати невизначені або нечіткі параметри трафіку. Метод ефективний у випадках, коли трафік не підпадає під чіткі правила, але проявляє аномальні властивості [2].

Вхідними даними для гібридного методу є пакети із вихідного потоку даних, множина вихідних сигнатур (D), множина дозволених сигнатур (DG), множина заборонених сигнатур (DB), множина невизначених сигнатур (DU), часові інтервали опорної вибірки та вибірки для перевірки, перелік правил. Метод реалізується у кілька послідовних етапів.

На початковому етапі до системи підключаються необхідні файли, а також перелік відповідних правил. Після цього із вхідного потоку даних формується сигнатура пакету dj, яка підлягає перевірці. Далі здійснюється класифікація

трафіку за визначеними ознаками. У випадку успішної класифікації система переходить до наступного пакету, і процедура повторюється до завершення аналізу. Якщо ж класифікація за ознаками неможлива, застосовується метод класифікації на основі самоподібності.

За відсутності результату і на цьому етапі, до аналізу підключається нечіткий метод виявлення аномального трафіку. Після класифікації сигнатура вважається або дозволеною, або аномальною, що дозволяє досягти однозначного результату оцінки мережевого трафіку.

Множина вихідних даних (D) виступає джерелом вхідної інформації для методу класифікації трафіку за ознаками. Разом із нею, до вхідних даних цього методу також належать множини дозволених (DG) та заборонених (DB) сигнатур. У результаті виконання класифікації формується множина невизначених сигнатур (DU), до якої відносяться ті сигнатури, що не були чітко ідентифіковані як дозволені чи заборонені.

Далі, для класифікації трафіку на основі самоподібності використовуються множини (DG) та (DU). У процесі роботи цього методу частина сигнатур із (DU), які демонструють подібність до дозволених зразків, може бути перенесена до множини (DG), після чого відповідні записи видаляються з (DU). Якщо подібність недостатня для класифікації, сигнатури залишаються в поточному стані.

На завершальному етапі застосовується нечіткий метод виявлення аномального трафіку. Його вхідними даними є множина невизначених сигнатур (DU)та відповідний набір правил.

Метод виконує нечітку класифікацію сигнатур, які, залежно від результатів аналізу, переносяться або до множини заборонених (DB), або до множини дозволених (DG), з одночасним видаленням цих записів із (DU). Загалом схему взаємодії даних у гібридному методі виявлення аномального трафіку в ІКС зображено на рис.1.

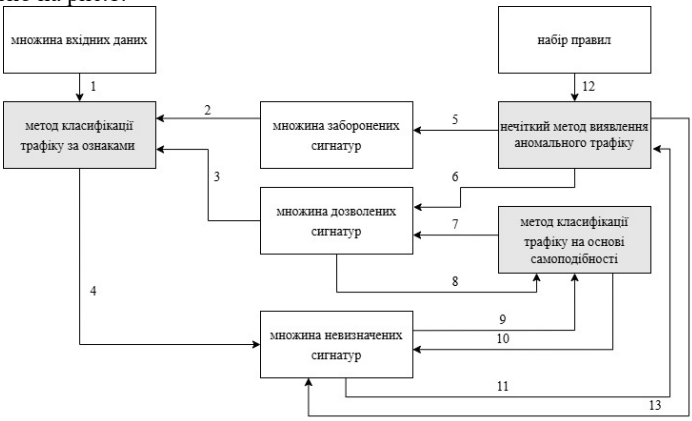


Рис. 1. Схема взаємодії даних у гібридному методі виявлення аномального трафіку в ІКС

1. Кльоц Ю.П., Петляк Н.С.. Виявлення аномального трафіку у загальнодоступних комп'ютерних мережах. Вимірювальна та обчислювальна техніка в технологічних процесах. 2022. № 3. С. 79-86. DOI: 10.31891/2219-9365-2022-71-3-9

2. Petliak N., Klots Y., Titova V., Salem A.-B.M.. Attack detection system based on network traffic analysis by means of fuzzy inference. 1st International Workshop on Advanced Applied Information Technologies (AdvAIT 2024), Khmelnytskyi, 5 December 2024. Vol. 3899. P. 201-213

Сучасні засоби верифікації email адрес

УДК 004.56.5(043.2)

Василь Ковалів

Західноукраїнський національний університет,

vasyl142005@gmail.com

У цифрову епоху, коли інформація стала ключовим ресурсом, інструменти пошуку та верифікації email адрес перетворилися на незамінний компонент професійного OSINT-інструментарію. Вони відіграють вирішальну роль у журналістських розслідуваннях, кібербезпеці та правоохоронній діяльності, надаючи фахівцям можливість ефективно працювати з цифровими слідами та встановлювати достовірні зв'язки між об'єктами дослідження [1].

Мета роботи проаналізувати сучасні засоби верифікації email адрес та оцінити перспективи розвитку інструментів і загроз пов'язаних з нимим.

Необхідність у точних інструментах верифікації email адрес зростає разом із збільшенням обсягів дезінформації та кіберзлочинності. Сучасні дослідження показують, що до 40% публічно доступних email адрес є неактивними або фейковими, що створює серйозні перешкоди для ефективної роботи фахівців [2]. Крім того, близько 60% кібератак починаються саме з фішингових листів, що робить питання верифікації особливо актуальним для забезпечення кібербезпеки [3].

Серед сучасних рішень для пошуку та верифікації email адрес особливо виділяється Hunter.io - інструмент, що поєднує високий рівень точності (до 95%) з потужними функціями верифікації. Його конкуренти, такі як Snov.io, VoilaNorbert та FindThatEmail, пропонують альтернативні підходи, що дозволяє вибирати оптимальне рішення для конкретних завдань. Кожен з цих інструментів має свої унікальні особливості - від глибокої інтеграції з CRM-системами до можливості пошуку через соціальні мережі [4].

У професійній практиці ці інструменти демонструють свою ефективність у різних сферах. Журналісти-розслідувачі активно використовують їх для пошуку та перевірки контактів ключових осіб. Фахівці з кібербезпеки застосовують ці технології для виявлення джерел кібератак та аналізу цифрових слідів. Правоохоронні органи знаходять їх корисними для встановлення зв'язків між підозрюваними та збирання доказової бази. Крім того, ці інструменти стають все більш популярними в корпоративній безпеці та маркетингових дослідженнях. Робота інструменів верифікації та дослідження емайл адрес відповідає алгоритму що приведений на рис.1.

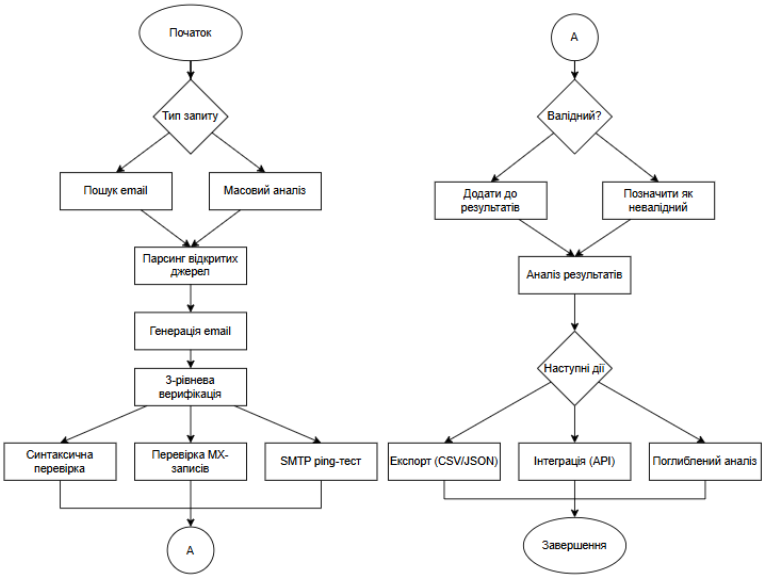


Рис. 1 Схема алгоритму Hunter.io

Сучасні інструменти пошуку та верифікації email адрес стали важливим компонентом OSINT-досліджень, значно підвищуючи ефективність роботи з відкритими джерелами. Їх розвиток йде шляхом вдосконалення алгоритмів, покращення інтеграційних можливостей та впровадження штучного інтелекту. Майбутнє цих технологій пов'язане з подальшим підвищенням точності пошуку та автоматизацією процесів перевірки, що відкриває нові перспективи для аналізу цифрових слідів і боротьби з інформаційними загрозами.

У роботі було проаналізовано можливості використання OSINT у боротьбі з дезінформацією, визначено основні інструменти та етапи аналізу, а також окреслено головні переваги та обмеження даного підходу.

1. Бурлаков, О. В. Сучасні методи OSINT-розслідувань / О. В. Бурлаков // Вісник кібербезпеки 2023 № 4. 45-52 с.

2 Коваленко, І. М. Цифрова криміналістика: інструменти та методи / І. М. Коваленко. - Київ : Видавництво НУ "КПІ" 2024. - 320 с.

3 Smith, J. Advanced Email Verification Techniques / J. Smith // Journal of Digital Investigation 2023. - Vol. 15, No. 2. 78-92 с.

4 Email Intelligence Handbook / ed. by R. Johnson, M. Brown. 2-nd eidition. - London : Security Press, 2024. 280 p.

Розробка системи виявлення фішингових ресурсів на основі інтелектуального аналізу коду

УДК 004.056.53

Андрій Ковальжі
Національний університет «Одеська політехніка»,
9480575@stud.op.edu.ua

Фішингові атаки залишаються однією з найбільших загроз для безпеки інформаційних систем[1], незважаючи на розвиток технологій захисту. Їх еволюція супроводжується використанням обфускації, поліморфізму та методів соціальної інженерії, що значно ускладнює своєчасне виявлення загроз класичними методами, такими як чорні списки чи простий евристичний аналіз. Тому актуальним завданням є розробка нових підходів до автоматизованого виявлення фішингових ресурсів із високою точністю та здатністю до адаптації.

Метою цієї роботи є розробка програмного забезпечення, яке буде здатне правильно виявляти файли, що містять фішингові ознаки. У даній роботі запропоновано новий підхід до виявлення фішингових HTML-ресурсів шляхом візуалізації їх бінарного представлення[2] та подальшого машинного аналізу отриманих векторів ознак. Основна ідея полягає у перетворенні HTML-коду сторінки у байтовий потік із подальшим формуванням зображення у градаціях сірого розміром 128×128 пікселів. Кожен байт представляється як піксель певної яскравості, що дозволяє отримати характерні патерни структури файлу. Цей підхід не залежить від текстового наповнення сторінки та мови вмісту, що робить його стійким до різних способів обфускації коду.

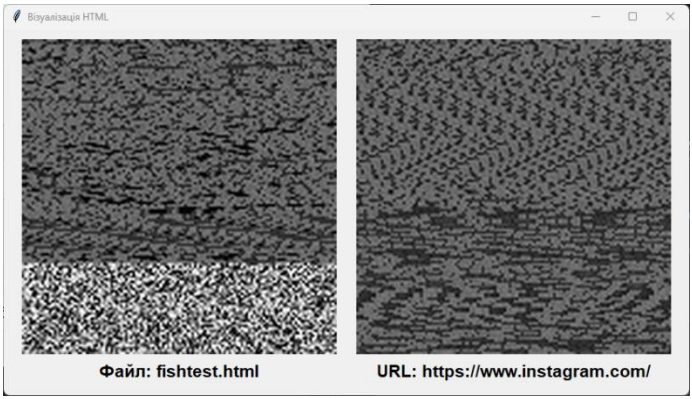


Рис. 1 – Приклад візуалізації фішингового та легітимного файлів

Для підвищення інформативності векторів ознак було розроблено метод поділу зображення на чотири логічні області (верхня, нижня, верхня середня та нижня середня частини). Для кожної області обчислюється нормалізована гістограма яскравості пікселів, що дозволяє зберігати локальні особливості

розподілу даних у структурі файлу. Отримані гістограми об'єднуються у єдиний вектор довжиною 1024 ознаки.

Для класифікації векторів було обрано алгоритм машинного навчання Support Vector Machine із використанням радіальної базисної функції (RBF)[3] як ядра. Процес налаштування гіперпараметрів моделі здійснювався методом GridSearchCV із перехресною валідацією. Навчання проводилося на датасеті, що складався з 3000 легітимних та 1700 фішингових HTML-файлів.

У результаті експериментів було встановлено, що точність класифікації складає 92.45%. Метрики Precision, Recall та F1-міра для обох класів склали близько 0.92, що свідчить про високу збалансованість моделі та її стійкість до помилок першого та другого роду. Було також побудовано матрицю конфузії та візуалізацію T-SNE, які підтвердили роздільну здатність моделі щодо кластеризації фішингових і легітимних векторів.

Розроблений програмний продукт має графічний інтерфейс, що дозволяє користувачеві завантажити локальний HTML-файл або ввести URL-адресу для автоматичної перевірки ресурсу на наявність ознак фішингової активності. У межах тестування система показала високу швидкість обробки запитів та стабільність роботи на реальних даних.

Запропонований підхід довів свою ефективність для задач виявлення фішингових атак за допомогою бінарної візуалізації та машинного навчання. Він демонструє потенціал для подальшого розвитку шляхом інтеграції глибших нейронних архітектур або самонавчальних методів, зокрема автоенкодерів чи контрастивного навчання, що дозволить ще краще пристосовувати систему до змін у природі загроз.

1. Sabillon R., Cano M. J., Serra-Ruiz J., Cavaller V. Cybercrime and Cybercriminals: A Comprehensive Study. International Journal of Computer Networks and Communications Security. 2016. Vol. 4. P. 165–176.

2. Baptista I., Shiaeles S., Kolokotronis N. A Novel Malware Detection System Based on Machine Learning and Binary Visualization : IEEE International Conference on Communications Workshops (ICC Workshops). Shanghai, China, 2019. P. 1–6.

3. Kumar A., Chatterjee J., Díaz V. A novel hybrid approach of SVM combined with NLP and probabilistic neural network for email phishing. International Journal of Electrical and Computer Engineering (IJECE). 2020. Vol. 10, No 1. P. 486–493.

Розробка багаторівневих моделей захисту хмарної інфраструктури з використанням смарт-контрактів

УДК 004.056:343

Назар Козубаль[1], Ігор Пітух[2]
Західноукраїнський національний університет[1,2]
i.pitukh@wunu.edu.ua

Стрімкий розвиток хмарних обчислень спричинив значне зростання обсягів переданих та оброблюваних даних, а також масштабування інфраструктур IT-сервісів. Попри очевидні переваги хмарної моделі – гнучкість, масштабованість,

економічність – її безпекова архітектура залишається вразливою через централізований характер керування, що породжує ризики несанкціонованого доступу, втрати даних, модифікацій або саботажу на рівні сервісних провайдерів. Крім того, відсутність прозорості та складність аудиту дій у хмарному середовищі унеможливлюють повноцінний контроль за дотриманням політик безпеки[1].

Інтеграція блокчейн-технологій до хмарної інфраструктури розглядається як перспективний підхід до усунення або зниження впливу вказаних вразливостей. Блокчейн забезпечує децентралізацію зберігання, незмінність записів та автоматизовану перевірку транзакцій, що дозволяє створити довірчі середовища навіть за відсутності центрального адміністратора.

Розроблена модель поєднує стохастичний аналіз вразливостей хмарних систем із адаптивною теорією графів Маркова[2], в якій ваги змінюються в реальному часі залежно від активності загроз. Це дозволяє системі динамічно реагувати на зміну векторів атак, перерозподіляти ресурси захисту та оптимізувати використання обчислювальних потужностей.

В основі моделі лежить метод динамічного розподілу довіри, який враховує часову складову через механізм експоненційного затухання[3]. Математично рівень довіри до транзакції в момент часу t описується формулою:

$$Trust(t) = Trust_0 \times e^{(-\lambda t)} \quad (1)$$

де:

- Trust(t) – рівень довіри до транзакції в момент часу t;
- $Trust_0$ – початковий рівень довіри (при t = 0);
- e – основа натуральних логарифмів (число Ейлера);
- – коефіцієнт затухання (швидкість зниження довіри)
- t – час, що минув з моменту транзакції

Запропонована модель має важливі аналітичні властивості:

- період напіврозпаду довіри (час, за який довіра знижується вдвічі) дорівнює:

$$t_{1/2} = \ln(2)/\lambda \quad (2)$$

- швидкість зміни довіри виражається похідною:

$$dTrust(t)/dt = -\lambda \times Trust(t)$$

- при $\lambda = 0$ затухання відсутнє, а при збільшенні швидкість затухання зростає;
- експоненційна залежність забезпечує плавне зниження рівня довіри, яке з часом сповільнюється.

Важливим аспектом моделі є квантування транзакцій, що дозволяє здійснювати диференційоване оцінювання рівня довіри. Транзакції розбиваються на кванти з часовими мітками, що забезпечує більш точний аналіз та оцінку їхньої надійності в контексті загальної системи безпеки.

Смарт-контракти є автономними програмними агентами, що забезпечують:

- Автоматизацію безпекових політик;
- Розподіл прав доступу;
- Контроль транзакцій;

- Перевірку відповідності дій користувачів встановленим правилам.

Ключовими перевагами використання смарт-контрактів є прозорість, незмінність та самовиконання умов, що особливо важливо в розподілених гетерогенних системах.

Смарт-контракти інтегруються у всі рівні хмарної інфраструктури:

- Фізичний рівень;
- Мережевий рівень;
- Інфраструктурний рівень;
- Прикладний рівень;
- Рівень даних.

Це забезпечує формування багаторівневої системи захисту без необхідності централізованого керування.

Запропонована модель динамічного розподілу довіри в багаторівневій системі захисту хмарної інфраструктури забезпечує автоматичне зниження рівня довіри до транзакцій з часом, стимулюючи регулярну верифікацію. Використання смарт-контрактів як автономних програмних агентів дозволяє автоматизувати безпекові політики та забезпечити прозорість і незмінність умов у розподіленому середовищі. Інтеграція цієї моделі в різні рівні хмарної інфраструктури формує ефективну систему захисту без централізованого керування.

1. Пономаренко В.С., Листровий С.В. Безпека хмарних обчислень: проблеми та перспективи. Системи обробки інформації. 2022. № 3(170). С. 74-82.

2. Марковський О.П., Великий М.М. Моделювання безпеки інформаційних систем на основі модифікованих ланцюгів Маркова. Наукові записки НаУКМА. Комп'ютерні науки. 2023. Т. 6. С. 55-63.

3. Яцків В.В., Карпінський М.П. Методи експоненційного оцінювання довіри в блокчейн-системах. Кібербезпека: освіта, наука, техніка. 2023. № 2(18). С. 110-123.

4. Wang W., Huang H., Zhang L., Su C. Secure and Efficient Blockchain-Based Authentication for IoT Devices. IEEE Internet of Things Journal. 2022. Vol. 9(11). P. 8002-8011.

Важливість кібербезпеки в російсько-українській війні 2022-2025: аналіз через призму теорії графів

УДК 004.056.5

Юрій Колцун[1], Людмила Бабала[2]
Західноукраїнський національний університет[1]
[1]*yurakoltsun@gmail.com*, [2]*ludaduma7@gmail.com*

Повномасштабна російсько-українська війна, що триває з 2022 року, стала першим великим міжнародним конфліктом XXI століття, де кіберпростір перетворився на повноцінний театр бойових дій. Паралельно з фізичними боями на полі бою, невидима війна розгортається в цифровому просторі, де атаки на критичну інфраструктуру, дезінформаційні кампанії та розвідувальні операції

стали ключовими елементами військової стратегії. Особлива увага в цьому контексті приділяється кібербезпеці як фундаментальній складовій національної безпеки та військової стійкості.

У цьому дослідженні ми застосуємо метод графів для аналізу складної динаміки кіберпротистояння у російсько-українській війні, розглядаючи взаємозв'язки між різними елементами кіберпростору, учасниками конфлікту та типами кібератак.

Теорія графів пропонує потужний інструментарій для моделювання складних взаємозв'язків у кіберпросторі. У нашому аналізіd:

- **Вершини графа** представляють основних акторів (держави, хакерські групи, критичні інфраструктурні об'єкти, інформаційні системи);
- **Ребра графа** відображають взаємодії та впливи між акторами (атаки, захисні заходи, інформаційні потоки);
- **Вага ребер** визначає інтенсивність або значущість відповідних взаємодій;
- **Напрям ребер** показує вектор впливу (атакуючий → ціль).

Аналіз кіберінцидентів у російсько-українській війні через призму теорії графів демонструє еволюцію кіберпротистояння від централізованої структури до розподіленої мережі. Передвоєнний період характеризувався високим ступенем координації атак (WhisperGate, DDoS на банківський сектор, HermeticWiper)[4], що відображалося у графі як концентровані спрямовані ребра від російських кіберпідрозділів до української критичної інфраструктури. У 2022-2023 роках граф суттєво ускладнився через збільшення кількості вершин (нові хакерські групи та міжнародні актори), зростання щільності (інтенсифікація атак) та появу двоспрямованих ребер, що відображали українські контрзаходи. Ключовими вузлами стали енергетична інфраструктура та телекомунікаційні мережі України. Період 2024-2025 років відзначився зростанням ваги ребер, пов'язаних з інформаційними операціями, формуванням кластерів взаємопов'язаних атак та зниженням централізації графа, що свідчить про диверсифікацію джерел кібератак та зростання автономії окремих хакерських груп.

Стратегії кіберзахисту, розроблені на основі аналізу графа, охоплюють три основні напрямки: зменшення центральності критичних вузлів шляхом впровадження надлишкових систем, децентралізації функцій та сегментації мереж, що розпорошує потенційні цілі атак[1]. Посилення вразливих ребер передбачає впровадження багатофакторної автентифікації, посилений моніторинг аномальної активності та регулярний аудит безпеки на ключових з'єднаннях, які визначені як пріоритетні на графі. Підвищення загальної стійкості системи досягається через міжнародну співпрацю з кібербезпеки, яка створює додаткові захисні ребра на графі, розвиток кадрового потенціалу для посилення захисних вершин та цілеспрямовані інвестиції в технології виявлення й реагування на інциденти.

Графовий аналіз дозволяє ідентифікувати найбільш критичні компоненти мережевої інфраструктури та оптимізувати розподіл обмежених ресурсів кіберзахисту, зосереджуючись на вузлах з найвищою центральністю та ребрах

з найбільшою вагою[3]. Таким чином, теорія графів забезпечує математично обґрунтований підхід до пріоритизації заходів кібербезпеки в умовах активного кіберпротистояння у російсько-українській війні, переводячи проблему з технічної площини у стратегічну.

Отже, застосування теорії графів до аналізу кібербезпеки в контексті російсько-української війни демонструє складну, динамічну природу сучасного кіберпротистояння. Ключові висновки:

1. Кіберпростір став невід'ємною складовою сучасної війни, де віртуальні атаки безпосередньо впливають на фізичний вимір конфлікту
2. Критична інфраструктура залишається найуразливішим і найпривабливішим об'єктом для кібератак
3. Ефективний кіберзахист потребує системного підходу, що враховує взаємозв'язки між різними елементами цифрових систем

Методологія графів дозволяє не лише аналізувати поточний стан кібербезпеки, але й прогнозувати майбутні загрози та оптимізувати розподіл ресурсів для захисту найбільш вразливих компонентів. У світлі продовження російсько-української війни, такий аналітичний підхід стає особливо актуальним для розробки проактивних стратегій кіберзахисту та підвищення цифрової стійкості України.

1. Безкоровайний М.М., Татузов А.Л. "Кібербезпека – підходи до визначення поняття" // Питання кібербезпеки. – 2022.
2. Гнатюк С.О. "Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи" // Безпека інформації. – 2023.
3. Microsoft Digital Defense Report 2023-2024. – Microsoft Corporation, 2024.
4. "Ukraine: Timeline of Cyberattacks" // CyberPeace Institute, 2024.
5. Newman M. "Networks: An Introduction". – Oxford University Press, 2022.

Розробка фільтр генератора псевдовипадкових послідовностей на основі хеш функцій

УДК 621.395.7 (043.2)

Роман Корольов[1], Ейюб Аббаскулієв[2], Ірада Рагімова[3], Станіслав Мілевський[4]

Національний технічний університет "Харківський політехнічний інститут", [1]korolevrv01@ukr.net, [4]milevskiysv@gmail.com

Азербайджанський технічний університет, [2]formemaybe23@yahoo.com, [3]ika1402@icloud.com

Генератори псевдовипадкових послідовностей (ГПВП) відіграють ключову роль у сучасних інформаційних технологіях, зокрема в криптографії, моделюванні, статистиці та програмуванні. Їхня важливість зумовлена здатністю створювати послідовності чисел, які здаються випадковими, але генеруються детермінованим алгоритмом із початковим значенням.

Генератори псевдовипадкових послідовностей повинні відповідати певним вимогам, які залежать від їхнього призначення — від простих симуляцій до криптографічних застосувань. До основних вимог які пред'являються до ГПВП можна віднести[1]:

–*статистична випадковість* (числа в сформованій послідовності повинні бути рівномірно розподілені, без видимих закономірностей чи кореляцій між сусідніми значенням);

–*великий період сформованої послідовності* (кількість чисел до повторення послідовності має бути значно більшим за обсяг даних, який потрібно згенерувати);

– *непередбачуваність (* знання частини послідовності чи алгоритму не повинно дозволяти передбачити наступні значення без доступу до початкового стану);

– *криптографічна стійкість (* за наявності значного обсягу вихідних даних неможливо визначити внутрішній стан ГПВП);

– *швидкість генерації* (ГПВП мають працювати достатньо швидко для цільового застосування);

– *простота реалізації* (ГПВП має бути придатним для реалізації на доступних платформах (мікроконтролери, FPGA, процесори)).

– *стійкість до квантових обчислень* (ГПВП має базуватися на задачах, які залишаються складними навіть для квантових алгоритмів).

Безперервне вдосконалення обчислювальних технологій та зростання їхньої потужності, що відповідає закону Мура, а також прогрес у математичних підходах до криптоаналізу вимагають регулярного перегляду розмірів ключових даних.

У цьому контексті особливу важливість набувають ГПВП заснованих використанні на хеш-функціях, які відповідають суворим вимогам криптографічної стійкості[1]. Його значущість полягає у здатності генерувати непередбачувані послідовності з використанням детермінованих алгоритмів, таких як SHA-256, що робить його незамінним для створення ключів і захисту даних в умовах обмежених ресурсів та загроз квантового криптоаналізу.

В NIST SP 800-90A запропонований ГПВП оснований на використанні хеш функції HMAC (Hash_DRBG). Структурна схема даного ГПВП представлена на рисунку 1.

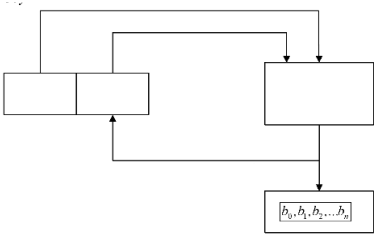


Рис.1. Структурна схема ГПВП на основі хеш функції HMAC

В доповіді пропонується фільтр генератор псевдовипадкових послідовностей на основі хеш функцій з гарантованою довжиною періоду. Структурна схема запропонованого ГПВП представлена на рисунку 2.

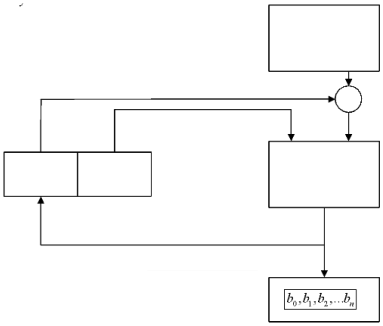


Рис.2. Структурна схема запропонованого фільтр ГПВП на основі хеш функції HMAC

В якості функції *f* можливо використання операцій *xor* або *mod* 2^n. Використання регістра зсуву з лінійним зворотнім (РЗЗЗЗ) зв'язком дає можливість формувати псевдовипадкові послідовності гарантованого періоду, а завдяки хеш-функції (наприклад, SHA-256) запропонований ГПВП забезпечує високу непередбачуваність та легко реалізовується на програмному та апаратному рівні.

1. NIST SP 800-90A Rev.1. URL: https://csrc.nist.gov/pubs/sp/800/90/a/r1/final

Теоретико-множинний підхід до класифікації сучасних методів соціотехнічних атак

УДК 004.056.53(045)

Анна Корченко[1], Кирило Давиденко[2]
[1,2]*Національний технічний університет «Дніпровська політехніка», Україна,*
[1]annakor@ukr.net, [2]kirilldavy@gmail.com,

Постійний розвиток інформаційних технологій і цифрових послуг породжує нові кіберзагрози, зокрема соціотехнічні атаки. Зловмисники застосовують психологічні маніпуляції для отримання несанкціонованого доступу до інформаційних ресурсів, що становить загрозу конфіденційності, цілісності та доступності даних. Особливу небезпеку такі атаки становлять для об'єктів критичної інформаційної інфраструктури (КІІ) та кіберфізичних систем, де наслідки можуть виходити за межі віртуального простору й впливати на реальні технологічні процеси, безпеку життєдіяльності й національну безпеку в цілому.

Відсутність систематизованої класифікації актуальних підходів та відповідних методів реалізації таких атак ускладнює розробку ефективних

заходів протидії, особливо в контексті захисту КІІ. З огляду на це, аналіз, класифікація і розробка сучасних підходів та методів виявлення соціотехнічних атак є важливим і актуальним науковим завданням.

Соціальна інженерія – це метод маніпулювання людьми з метою отримання доступу до конфіденційної інформації або ресурсів. Такі атаки спрямовані на людський фактор, використовуючи довіру, неуважність та недостатню обізнаність користувачів, що особливо критично в умовах, коли ціллю зловмисника є персонал або адміністратори об'єктів КІІ.

Аналізуючи дані провідних досліджень, можна виділити певні методи, які використовуються соціотехніками. Водночас у наявних публікаціях не в повному обсязі сформовані множини ознак, які характеризують підходи до реалізації відповідних атак, що дасть можливість з системних позицій формалізувати процес їх класифікації.

Крім того, соціотехнічні атаки постійно еволюціонують, що зумовлює необхідність їх комплексного аналізу та створення адаптивних методів захисту, що є ключовим для проектування механізмів захисту кіберфізичних об'єктів критичної інфраструктури. Ефективна протидія має базуватися не лише на технологічних рішеннях, а й на підвищенні обізнаності користувачів, впровадженні процедурного контролю та зміцненні організаційних і політичних аспектів кібербезпеки.

Метою роботи є розробка методу побудови моделі класифікації сучасних підходів реалізації соціотехнічних атак для систематизації та інтеграції існуючих класифікацій відповідних підходів [1, 2] з можливістю розширення новими ознаковими характеристиками. Це, в першу чергу, дасть можливість з системних позицій навчити персонал протистояти соціотехнічним загрозам. Для досягнення поставленої мети необхідно на основі теоретико-множинного підходу розробити метод побудови моделі класифікації соціотехнічних атак.

Для цього, з урахуванням запропонованих ознак, критеріїв та підкритеріїв [3] класифікації сучасних підходів до реалізації соціотехнічних атак було розроблено відповідну модель, метод формування якої реалізується в три етапи:

Етап 1 – визначення множини ідентифікаторів ознак ($\mathbf{S}$) класифікації підходів до реалізації соціотехнічних атак $\mathbf{S} = \{\boxtimes_{i=1}^{n} \mathbf{S_i}\} = \{\mathbf{S_1}, \mathbf{S_2}, ..., \mathbf{S_n}\}$, $(i = \overline{1,n})$. Де $\mathbf{S_i}$ i-й ідентифікатор ознак класифікації підходів реалізації соціотехнічних атак, а n – їх кількість.

Етап 2 – визначення множини критеріїв щодо класифікації підходів до реалізації соціотехнічних атак $\mathbf{S_i} = \{\boxtimes_{j=1}^{m_i} \mathbf{C_{ij}}\} = \{\mathbf{C_{i1}}, \mathbf{C_{i2}}, ..., \mathbf{C_{im_i}}\}$, $(j = \overline{1,m_i})$. Де $\mathbf{C_{ij}} \subseteq \mathbf{S_i}$ множина набору критеріїв ($\mathbf{C}$) i-го ідентифікатора j-го критерія класифікації підходів до реалізації соціотехнічних атак, а m_i – їх кількість.

Етап 3 – визначення множини підкритеріїв класифікації підходів реалізації соціотехнічних атак $\mathbf{C_{ij}} = \{\bigotimes_{k=1}^{r_j} \mathbf{SC_{ijk}}\} = \{\mathbf{SC_{ij1}}, \mathbf{SC_{ij2}}, ..., \mathbf{SC_{ijr_j}}\}$, $(k = \overline{1, r_j})$. Де $\mathbf{SC_{ijk}}$ k-й ідентифікатор підкритеріїв j-го критерія i-го ідентифікатора ознак класифікації підходів реалізації соціотехнічних атак, а r_j – їх кількість.

Таким чином, запропоновано метод побудови моделі класифікації соціотехнічних атак в якому за рахунок етапів визначення множин: ідентифікаторів ознак, критеріїв та підкритеріїв класифікації підходів до реалізації соціотехнічних атак, дозволило розробити узагальнену модель теоретико-множинної інтерпретації класифікації сучасних підходів реалізації соціотехнічних атак.

1. Класифікація методів соціального інжинірингу / О.Г. Корченко, Є.В. Паціра, Д.А. Горніцька // Захист інформації. – 2007. – №4 (36). – С.37-45.

2. О. Г. Корченко, Д. А. Горніцька, та А. Ю. Гололобов, «Розширена класифікація методів соціального інжинірингу», Безпека інформації, т. 20, № 2, с. 197-205, 2014.

3. Корченко А. Сучасні методи соціотехнічних атак. Корченко А., Давиденко К. ITSec: Безпека інформаційних технологій: матеріали XIII Міжнар. наук.-техн. конф., м. Львів, 9-11 трав. 2024 р. Л.: ЛНУ ім. І. Франка, 2024, с. 123-125.

Аналіз існуючих підходів, методів та моделей оцінки захищеності систем захисту інформації в корпоративній мережі

УДК 004.056.5:004.08

Віталій Котелянець[1], Денис Трухан[2]

Державний університет інформаційно-комунікаційних технологій,

[1]v.kotelianets@duikt.edu.ua, [2] trukhan@stud.duikt.edu.ua

У сучасному бізнес-середовищі корпоративні мережі є основою для функціонування компаній. Вони зберігають, обробляють та передають величезні обсяги цінної інформації – від фінансових даних та інтелектуальної власності до персональних даних клієнтів та співробітників. Забезпечення безпеки цих мереж є критично важливим завданням, оскільки будь-який інцидент може призвести до значних фінансових збитків, репутаційної шкоди та юридичних наслідків.

У сучасному світі динамічного розвитку інформаційних технологій захист комп'ютерних мереж стає ключовим завданням для забезпечення кібербезпеки.Особливу увагу слід приділяти захисту від атак в різних секторах країни, які можуть паралізувати критично важливу інфраструктуру та фінансовий сектор на тривалий час [1].

Крім того, поява нових фінансових інструментів, таких як альтернативні валюти, стимулює злочинців до подальшої розробки шкідливого програмного забезпечення (ШПЗ) з метою отримання прибутку. При цьому шкідливе програмне забезпечення використовує обчислювальні потужності не тільки

свої, але й інших користувачів, підключених до глобальної мережі. Тому своєчасне виявлення шкідливого програмного забезпечення є нагальним питанням для організацій та бізнесу.

Інформаційна сфера, яка є головною, впливає на стан соціально-політичної, економічної сфери діяльності. Складність процесів, які відбуваються в розподілених інформаційних системах (РІС), постійно зростає. Це призводить до того, що РІС застосовується для обміну інформацією та розв'язання різного типу завдань у всіх сферах людської діяльності, які можуть стати об'єктом зловживань.

В основі сучасної розподіленої інформаційної системи містяться засоби інформації, комунікаційні сервери, сервери вторинної і третинної інформації, різного типу процесори обробки інформації, обчислювальні комплекси системи, пристрої передачі інформації. Кожна розподілена інформаційна система має свої особливості, які обумовлені сферою її застосування [2].

Важливість і відповідальність задач, розв'язуваних за допомогою розподілених систем у реальному масштабі часу, обумовили високі вимоги до надійності цих систем, у яких, найчастіше, неможливо проведення технічного обслуговування під час функціонування і відмова всієї розподіленої інформаційної системи, або її окремих компонентів може привести до негативних наслідків. Крім того, зростає необхідність підвищення ефективності РІС, оскільки помилки, які можуть бути допущені призводять до суттєвих негативних наслідків [3].

Здатність розподіленої інформаційної системи виконувати необхідні функції та їх поведінку характеризується властивістю функціональної стійкості. Це означає, що зі структури виключаються несправні елементи, структура перебудовується, а параметри системи коригуються для пристосування.

Таким чином, аналіз вимог до розподілених інформаційних систем та існуючих наукових методів показує, що на сьогоднішній день загострилось протиріччя між необхідністю забезпечення інформаційної системи властивістю функціональної стійкості в сенсі робастності системи відносно програмних збоїв, відмов, які утворилися в результаті кібернетичних атак з однієї сторони та недосконалістю існуючих наукових та інженерних методів забезпечити захист від кібернетичних загроз.

1. Чабан Б. В., Котенко А. М. (2024). Модель системи захисту інформації від витоку матеріально-речовим каналом на базі ланцюгів Маркова. Сучасний захист інформації, 4(60), 46–52. https://doi.org/10.31673/2409-7292.2024.040005

2. Using the Latest Methods of Cluster Analysis to Identify Similar Profiles in Leading Social Networks. Bohdan Zhurakovskyi, Ihor Averichev and Ivan Shakhmatov. Information Technology and Implementation (Satellite) Conference Proceedings, 21 November, 2023. https://ceur-ws.org/Vol-3646/Paper_12.pdf [in Ukraine]

3. Tevet I. Speed Matters: The Crucial Role of MTTD and MTTR in Cybersecurity [online], 2024 [viewed 2025-04-25]. Available from: https://intezer.com/blog/speed-matters-mttd-and-mttr-in-cybersecurity/

Заповнення буферу обміну псевдовипадковим шумом для захисту функції автозаповнення менеджерів паролів

УДК 004.056.57

Костянтин Кравченко[1], Юлія Козіна[2]
Національний університет «Одеська політехніка»,
[1]kostyantinkravchenko@gmail.com, [2]yuliya.kozina@keenethics.com

На сьогоднішній день парольний захист, незважаючи на його застарілість, залишається найпоширенішим механізмом автентифікації користувачів в інформаційних системах. Парольний захист зазнає різні типи атак, тому сучасний парольний захист вимагає від користувачів прояви власної ініціативи для захисту власних паролів: використання паролів певної довжини, наявність спеціальних символів тощо [1]. Ці рекомендації дійсно є ефективними для забезпечення захисту парольного захисту, але ці методи здійснюють захист за рахунок зручності користувачів. Користувачі, зі свого боку, можуть не усвідомлювати важливість цих вимог, особливо якщо вони заважать зручності отримання доступу до бажаних ресурсів, тому користувачі часто можуть ігнорувати ці поради, що призводить до зниження рівня захисту.

Для вирішення цієї проблеми застосовуються менеджери паролів – програмне забезпечення, яке пропонує компроміс між надійним рівнем безпеки та зручністю користування, через безпечне зберігання паролів користувача та їх автозаповнення до полей вводу облікових даних за потребою користувача [2].

Для забезпечення зручності, менеджери паролів запроваджують функціонал автозаповнення, які автоматично заповнюють поля ідентифікатора та паролю, без потреби власноручного заповнення цих полів користувачем – користувачеві потрібно лише обрати обліковий запис та підтвердити автозаповнення полей.

Для веб-сервісів, менеджери паролів можуть пропонувати використання розширення для веб-браузеру, яке під'єднується до серверу зберігання паролів користувача та, при підтвердженні користувача, заповнює поля облікових даних через безпосереднє вставлення тексту до HTML-елементів. Ця схема змінюється при використанні сервісів, доступ до яких забезпечується не через веб-сторінку, а через безпосереднє програмне забезпечення, наприклад: месенджери, звітні системи, клієнти електронної пошти тощо. Для таких сервісів менеджери паролів або не пропонують функціонал автозаповнення (використувач власноруч копіює пароль до буферу обміну), або забезпечують його за рахунок симуляції натискання клавіш клавіатури.

Проблемою наведених методів є їх вразливість до традиційного шпигунського програмного забезпечення, такого як кейлогери або шпигуни за буфером обміну [3]. Відповідно, метою даної роботи є розробка рішення, яке спроможне протидіяти класичному шпигунському ПЗ при автозаповненні паролів менеджерами паролів.

Розглядуючи існуючі рішення проблеми, однією з пропозицій її вирішення є метод «двох-канальної обфускації авто-друку» від менеджеру паролів Keepass. Сутність методу полягає у випадковому розподілі автозаповненого паролю на дві строки (канали), одна з яких заповнюється через копіювання та вставлення буферу обміну, а інша заповнюється через симуляцію натискання клавіш. Цей метод може захистити автозаповнення окремо від кейлогерів та

шпигунів за буфером обміну, але не за шпигунами, які відстежують обидва канали.

Наше запропоноване рішення, розроблене в цій роботі, передбачає захист за рахунок заповнення буфера обміну псевдовипадковим шумом, який буде приховувати справжні частини паролю при відстеженні буферу обміну шпигунським ПЗ. Сутність рішення полягає у розділі строки уведеного паролю на окремі символи, після кожного якого буде генеруватися послідовність випадкових символів (шум) випадкової довжини, схожих на ті символи, які присутні у паролі. При самому процесі автозаповнення паролю, кожний символ (включаючи як згенерований шум так і пароль) буде послідовно копіюватися в буфер обміну, але лише ті символи, які належать до оригінального паролю, будуть вставлятися до полей вводу. Таким чином зловмисник буде бачити усі збережені символи, але не зможе відрізнити символи уведеного паролю від згенерованого шуму. Для додаткового захисту, шум також додається ще до початку першого символу паролю, щоб зловмисник не міг визначити, чи належить перший символ відстеженої послідовності оригінальному паролю.

Одним з можливих векторів атаки на такий вид автозаповнення є перебір можливих паролів за рахунок випробування усіх можливих комбінацій уведених символів при автозаповненні, доки не будуть знайдені символи, які відповідають оригінальному паролю. Для протидії повному перебору є критичною наявність достатньої довжини згенерованого шуму, із метою ускладнення часу перебору всіх комбінацій. Ми можемо розрахувати час t, який потрібен для повного перебору паролів за формулою:

$$t = i = 0 lj = 1 p - i\mathrm{F}(l+1,\ j)v, \qquad (1)$$

де p – поточна довжина згенерованої послідовності (включаючи шум та пароль), l – максимальна довжина згенерованого шуму між символами паролю (яка може бути відома зловмиснику), v – швидкість перебирання паролів за секунду, а функція $F(n,k)$ розраховує k-ий елемент послідовності Фібоначчі n-го порядку ($n = 2$ для послідовності Фібоначчі, $n = 3$ для трібоначчі тощо).

Для прикладу обрахунку ми можемо обрати пароль користувача довжиною у 8 символів (рекомедована мінімальна довжина паролів), а $v = 100\,000$ паролів за секунду. Значення l є змінним від потреби користувача щодо швидкості алгоритму та потрібного рівню захисту, тому оберемо $l = 50$ для нашого випадку.

Так як максимальна довжина шуму становить 50, і за припущенням використання надійного ГВЧ, середньоарифметичне значення довжини згенерованого шуму буде становити половину максимального значення, тобто 25 символів шуму між кожним символом паролю (та на початку), тому $p = 8 + 8 \cdot 25 = 208$. З цима параметрами ми можемо обрахувати час $t = 139 \cdot 10^{12}$ секунд, або $764{,}2 \cdot 10^9$ років, що підтверджує стійкість алгоритму до перебору. Звісно, що точний час буде коливатися в залежності від довжини згенерованого шуму.

Ще одним з можливих векторів атаки є відстеження моментів, коли менеджер паролів вставляє символ оригінального паролю, а не лише копіює його. Цей метод атаки має більш технічну природу, адже його ефективність буде залежити від конкретної реалізації методу автозаповнення, а також середовища (наприклад операційна система), на якій використовується

менеджер паролів. Природа цього вектора атаки представляє кількісну оцінку методу важкою для реалізації, але ми приведемо можливі схеми реалізації цієї атаки.

Перша атака полягає у відстеженні сигналів, які обробляються при вставленні символу паролів. Якщо конкретна реалізація функції автозаповнення використовує симуляцію клавіш «Ctrl» та «V» для вставлення паролю, то зловмисник може відстежувати натискання цих клавіш, щоб визначити символи, які вставлялися із вмісту буферу обміну. Якщо ж реалізація автозаповнення використовує системні виклики ОС для вставлення вмісту буферу обміну, то спроможність реалізації цієї атаки може залежити від можливості процесу шпигунського ПЗ відстежувати за системними викликами. Як метод протидії є можливість «підробки» сигналів вставлення паролю зі сторони менеджеру паролів. Наприклад, менеджер паролів може вставляти символи із шуму до вікна іншої програми (наприклад самого себе), щоб зловмисник вважав ці символи частиною паролю.

Інший метод атаки полягає у відстеженні затримки при вставленні паролю. Хоч процес вставки вмісту буферу обмену є порівняно швидким для людського ока, навіть номінальна затримка при цьому процесі може бути помічена програмним забезпеченням. Як засіб протидії, менеджер паролів може власноруч імітувати затримку між випадковими символами згенерованого шуму, щоб зловмисник вважав, що подані символи належать паролю.

Узагалом, розроблений підхід автозаповнення паролів для менеджерів паролів спроможний надати деякий ступінь захисту проти класичних типів шпигунського програмного забезпечення. Розроблений метод є стійким до атак перебору, проте має технічні недоліки, ступінь серйозності яких залежить від конкретної реалізації механізму цього методу. У порівнянні із існуючими аналогічними методами захисту, розроблений метод пропонує окремі переваги за рахунок можливості протидії різним імплементаціям шпигунського ПЗ, але також зазнає недоліки при протидії іншим видам шпигунського ПЗ.

Подальшим напрямком розробки алгоритму може виступати його поєднання із іншими методами протидії шпигунського ПЗ, або використання в інших сферах.

1. Кульчицький О. С., Грицюк В. В., Зотова І. Г. Аналіз існуючих підходів при ідентифікації і аутентифікації користувачів в інформаційно-телекомунікаційних системах. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України.* 2016. №3. С. 60–64.

2. Грабовська С. А., Лах Ю. В. Важливість використання менеджерів паролів у сучасному світі. *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення*, м. Тернопіль, 7-8 червня. 2022. С. 14–16.

3. Luevanos C., Hirschi K., Elizarraras J., Yeh J. Analysis on the Security and Use of Password Managers. *18th International Conference on Parallel and Distributed Computing, Applications and Technologies*. 2017. P. 17–24.

Вплив реалістичних умов реалізації змагальних атак проти систем виявлення вторгнень на методи захисту

УДК 004.056.5

Олександр Кручінін[1], Дмитро Тимофєєв[2], Сергій Мацюк[3]

Національний технічний університет «Дніпровська політехніка»,

[1]kruchinin.o.v@nmu.one, [2]tymofieiev.d.s@nmu.one, [3]matsiuk.s.m@nmu.one

В умовах зростання складності та обсягів кіберзагроз, системи виявлення вторгнень (англ. Intrusion Detection System, IDS) відіграють критично важливу роль у забезпеченні безпеки мереж. Перспективним напрямком розвитку IDS є інтеграція методів машинного навчання (англ. Machine Learning, ML), що дозволяє виявляти як відомі, так і нові типи атак. Однак, IDS на базі ML є вразливими до змагальних атак. Тому актуальною є задача розвитку методів та засобів протидії таким атакам [1]. Для оптимізації цих методів та засобів протидії є доцільним врахування реалістичних умови реалізації змагальних атак [2].

Метою даної роботи є аналіз реалістичних умов реалізації змагальних атак проти IDS, які використовують ML, із врахуванням моделей загроз та порушника.

Окремі методи протидії змагальним атакам проти IDS, як правило, адаптовані до конкретного виду атак. Одним з методом реалізації більш універсального рішення є використання ансамблів моделей, тобто інтеграція кількох моделей машинного навчання та поєднання різних стратегій ідентифікації. Але таке рішення має свої недоліки: складність реалізації порівняно з одиночними моделями; підвищені вимоги до обчислювальних ресурсів та енергоспоживання; збільшення затримки у виявленні та реакції на атаки; збільшення трудомісткості налаштування та оновлення.

Слід зазначити, що для конкретних інформаційно-комунікаційних систем (ІКС) існує обмежена кількість реальних сценаріїв реалізації змагальних атак. Тобто множина таких атак та, відповідно, актуальних методів та засобів протидії є обмеженою.

На сьогодні для класифікації змагальних атак використовується ряд ознак [3]:

1) Рівень знань зловмисника про IDS («біла», «сіра» або «чорна» скриня).

2) Мета атаки (конфіденційність, цілісність, доступність).

3) Стратегія атаки (ухилення, отруєння, оракула).

4) Фаза атаки (із впливом на тренувальні дані, без впливу на тренувальні дані).

5) Простір атаки (ознак, задач).

6) Спрямованість (спрямована, не спрямована)

Частина цих ознак залежить від конкретних умов функціонування ІКС, тобто від моделі загроз та порушника.

Для демонстрації такого впливу можна розглянути декілька сценаріїв реалізації змагальних атак проти IDS для різних ІКС з різними профілями зловмисників:

1) об’єкт атаки: веб-сервер. Зловмисник, не маючи інформації про внутрішню роботу IDS на базі ML, що захищає веб-сервер, намагається обійти його захист. Для цього він використовує автоматизовані інструменти для сканування веб-сервера з метою виявлення вразливостей, таких як SQL injection або Cross-Site Scripting (XSS). Зловмисник поступово змінює параметри своїх запитів, наприклад, кодує шкідливі SQL-команди або змінює структуру XSS-скриптів, щоб обійти правила IDS. Оскільки зловмисник не знає, які саме ознаки використовує IDS для виявлення атак, він намагається внести невеликі зміни у велику кількість параметрів, щоб знайти комбінацію, яка дозволить обійти захист. Його кінцевою метою є успішна експлуатація вразливості веб-сервера, не будучи виявленим IDS. Ця атака за рівнем знань зловмисника про IDS – «чорна» скриня, без впливу на тренувальні дані, націлена на зміну або пошкодження даних або моделі машинного навчання, не спрямована;

2) об’єкт атаки: промислове обладнання. Інсайдер, маючи повний доступ до інформації про IDS на базі ML, яка контролює роботу промислового контролера (PLC) технологічного обладнання, планує диверсію. Він знає архітектуру IDS, має доступ до тренувальних даних та алгоритму навчання. Використовуючи ці знання, він розробляє змагальні приклади, які маніпулюють вхідними даними контролера, наприклад, значеннями тиску, температури та швидкості обертання.

Мета маніпуляцій - змусити контролер працювати в небезпечному режимі, не викликаючи при цьому підозри у IDS. Кінцевою метою є спричинення аварії промислового обладнання, залишаючись непоміченим системою захисту. Ця атака за рівнем знань зловмисника про IDS – «біла» скриня, без впливу на тренувальні дані, націлена на зміну роботи контролера та обхід захисту для саботажу.

Таким чином, на основі аналізу моделі загроз та порушника можна визначити реалістичні умови та результати реалізації змагальних атак проти IDS, а значить сфокусувати увагу на обмеженому переліку таких атак. Це дозволить оптимізувати ефективність застосування методів та засобів протидії таким атакам за умови мінімізації вимог до обчислювальних потужностей та затримки у виявленні та реакції на атаки.

1. Liu, H., & Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. applied sciences, 9(20), 4396. – URL: https://www.mdpi.com/2076-3417/9/20/4396. (дата звернення: 25.04.2025).

2. Ennaji, Sabrine & Benkhelifa, Elhadj & Mancini, Luigi. (2025). Toward Realistic Adversarial Attacks in IDS: A Novel Feasibility Metric for Transferability. – URL: https://arxiv.org/abs/2504.08480. (дата звернення: 25.04.2025).

3. Alotaibi, A.; Rassam, M.A. Adversarial Machine Learning Attacks against Intrusion Detection Systems: A Survey on Strategies and Defense. Future Internet 2023, 15, 62. – URL: https://doi.org/10.3390/fi15020062. (дата звернення: 25.04.2025).

Принципи застосування цифрової криміналістики в Україні

УДК 004.056

Сергій Кулина[1], Олександр Дзівак[2]
Західноукраїнський національний університет,
[1]sersks@gmail.com, [2]ole.dzvk@gmail.com

У сучасному світі, підтвердження автентичності даних є ключовим пріоритетом, як при встановленні права власності на цифрові об’єкти, так і при розслідуванні цифрових злочинів [1].

Сучасні технології дають нові можливості криміналістам для розкриття злочинів, проте це вимагає глибокої адаптації та постійного вдосконалення. Цифрові докази можуть мати вирішальне значення для підтвердження фактів, що мають суттєве значення для кримінальної справи, а також для ефективного розслідування правопорушень, особливо в умовах, коли традиційні методи збору доказів є менш ефективними [2].

Як зазначалося в попередніх публікаціях [3] всі інструменти для цифрової криміналістики згідно їх ключових завдань поділяються на інструменти зв’язані з типом завданням (збору, аналізу та відновлення) та інструменти зв’язані з місцем застосування (робота на хмарах, мобільних пристроях і в мережі). Для експертів цифрової криміналістики найдоступнішими та найпоширенішими джерелами інформації є фізичні пристрої, а саме домашні комп’ютери, ноутбуки та смартфони.

Проте, не зважаючи на поширеність цілей дослідження різноманітність сфер поширення цифрових технологій вимагає від дослідників глибокого аналізу та правильного поводження з даними, що до них надходять. Дослідження пристроїв з подальшим використанням даних розміщених на них в якості цифрових доказів вимагає дотримання існуючих стандартів щодо поводження з цифровими доказами[4].

В Україні принципи застосування цифрової криміналістики базуються на міжнародному стандарті ISO/IEC 27037 [5].

Цей стандарт передбачає чотири етапи роботи з цифровими доказами:

1) ідентифікація (Identification). Етап ідентифікації включає в себе не лише пошук та документування потенційних доказів, але й визначення обсягу інциденту, типу залучених даних та потенційних джерел доказів. Його можна вважати процесом первинного огляду та оцінки ситуації;

2) збір (Collection/Acquisition). Другий етап включає в себе збір даних з різних джерел (комп'ютери, сервери, мобільні пристрої, хмарні сховища тощо) із використанням спеціалізованих апаратних та програмних засобів;

3) експертиза (Examination). Третій етап включає детальне дослідження зібраних даних для виявлення, вилучення та аналізу релевантної інформації. Це включає відновлення видалених файлів, аналіз журналів, пошук за ключовими словами тощо;

4) збереження (Preservation). Четвертий етап полягає в забезпеченні цілісності та збереженні цифрових доказів протягом усього процесу розслідування, включаючи створення резервних копій та контроль доступу.

Ці процеси є ключовими під час слідства та для підтримання цілісності цифрових доказів, а прийнятна методологія їх отримання забезпечує їхню

допустимість при законодавчих або дисциплінарних судових процесах та в інших інстанціях.

Проте, під час роботи з цифровими доказами, для повнішого опису процесу роботи з ними, перед етапом збереження даних вводяться два додаткові етапи, а саме аналіз та звітність.

Аналіз забезпечує інтерпретацію знайдених під час експертизи даних для встановлення фактів, послідовності подій, мотивів та зв'язків. Це включає реконструкцію подій, атрибуцію дій та підготовку висновків.

У свою чергу звітність включає в себе документування всіх виконаних дій, знайдених доказів, зроблених висновків та їхнє представлення у чіткій формі, яка може бути використана в юридичних процедурах.

Таким чином, дотримання розширеної методології роботи з цифровими доказами гарантує, що вони не просто зібрані, а й належним чином опрацьовані, проаналізовані та представлені, що значно підвищує їхню доказову силу та сприяє більш справедливому та обґрунтованому правосуддю.

1. Кріцак, І., & Рось, А. (2024). Проблема електронних доказів у кримінальному провадженні / electronic evidence in criminal proceedings: Наукометричний зріз. Члени організаційного комітету, 290.

2. Петрик, В. В. (2025). Використання електронних доказів у кримінальному провадженні: проблеми їх збору, перевірки та оцінки. Науковий вісник Ужгородського національного університету. Серія: Право, 4(87), 119-123.

3. Кулина С. В. (2024). Цифрова криміналістика в умовах сьогодення. Збірник матеріалів науково-практичного симпозіуму «Захист інформації», 30.11. 2024, Тернопіль, с.64-67.

4. Онищук, О. (2024). Криміналістичні дослідження мобільних пристроїв: порівняння апаратно програмних засобів шифрування мобільного зв'язку. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2 (26), 246-257.

5. ISO/IEC 27037:2012 Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html (дата звернення: 22.04.2025).

Розробка застосунку для фільтрації листів електронної пошти

УДК 004.056.5

Микита Курганов-Попозогло[1], Лідія Тимошенко[2]

Національний університет «Одеська політехніка»,
[1]9560993@stud.op.edu.ua, [2]l.m.timoshenko@op.edu.ua

Розглядаються актуальні питання кібербезпеки в контексті електронної пошти, яка сьогодні є одним із найуразливіших і водночас найпоширеніших каналів комунікації. Незважаючи на значний розвиток технологій, електронна пошта продовжує бути ціллю атак у сучасному кіберпросторі. Через неї поширюються шкідливі програми, фішингові листи, спам-повідомлення та

методи соціальної інженерії, спрямовані на обман користувачів та отримання несанкціонованого доступу до інформаційних систем [1].

У зв'язку з постійним зростанням кількості, складності та витонченості кіберзагроз виникає нагальна потреба у створенні надійних програмних систем фільтрації електронної пошти, що і є метою даної розробки. Особливої актуальності набуває здатність таких систем до швидкої адаптації до нових загроз, автоматичного навчання та самостійного вдосконалення з урахуванням актуальних тенденцій у сфері кібербезпеки [2].

У межах роботи розроблено програмний застосунок, який виконує функції виявлення, блокування та фільтрації потенційно небезпечних електронних повідомлень. Цей застосунок орієнтований на захист як окремих користувачів, так і корпоративного середовища, де загроза витоку даних або порушення цілісності інформаційної інфраструктури може мати серйозні наслідки.

Частина функціоналу реалізована за допомогою евристичного аналізу, сигнатурного сканування, механізмів репутаційної оцінки відправників та елементів машинного навчання. Репутаційна оцінка базується на історії взаємодій з конкретним відправником, поведінковому аналізі листів, наявності шаблонів фішингових повідомлень, підозрілих редиректів, вкладень зі шкідливим вмістом або прихованих гіперпосилань.

До класичних методів належать чорні (blacklist) та білі (whitelist) списки, які зберігають інформацію про відомі джерела загроз або надійні контакти. Дані списки регулярно оновлюються через API авторитетних аналітичних платформ (SpamCop, SURBL, Barracuda, Spamhaus тощо), що забезпечує оперативну реакцію системи на появу нових загроз. [3].

Впроваджено механізми перевірки автентичності повідомлень: використання технологій DKIM, SPF та DMARC дозволяє ефективно виявляти підроблені адреси відправників та запобігати атакам - спуфінгу електронної пошти.

Застосунок функціонує як фоновий сервіс, що інтегрується із поштовими серверами через протокол IMAP, що забезпечує його сумісність з різними актуальними платформами. Користувацький інтерфейс дозволяє переглядати результати аналізу, отримувати миттєві сповіщення аналізувати історію спрацювань фільтрів.

У таблиці 1 описана архітектура програми, яка базується на багаторівневому підході до аналізу електронної пошти, що дозволяє комбінувати класичні методи із сучасними технологіями.

Таблиця 1

Логіка роботи застосунку

№	Етап/Блок	Тип	Умова/Дія
1	Початок	Початок	
2	Завантаження `.env`	Процес	Завантаження Email, Password, IPQS_API_KEY
3	Перевірка змінних середовища	Рішення	Якщо відсутні- помилка, зупинка

4	Загрузка *whitelist.txt/blacklist.txt*	Процес	
5	Запуск нескінченного циклу	Цикл	
6	Підключення до IMAP-сервера	Процес	
7	Вибір папки FOLDER (INBOX)	Процес	
8	Пошук непрочитаних листів	Процес	
9	Для кожного листа	Цикл	
10	Отримання адреси відправника	Процес	
11	Чи є у білому списку?	Рішення	Так-дозволити, лог “білий список”
12	Чи є у чорному списку?	Рішення	Так-заборонити, перемістити в Spam
13	Перевірка через IPQS API	Процес	
14	Результат “погана репутація”?	Рішення	Так - додати в blacklist.txt, заборонити, перемістити в Spam
15	Результат “добра репутація”?	Рішення	Так -додати в whitelist.txt, дозволити
16	Інакше	Рішення	Дозволити, лог помилку API
17	Очікування 30 секунд	Процес	
18	Повернення до кроку 5	Перехід	

Для підвищення безпеки система підтримує ведення детального журналу дій (аудиту), який включає записи про дії адміністратора та всі автоматичні процеси. Журнали подій зберігають у зашифрованому вигляді із застосуванням алгоритмів шифрування AES-256. Реалізовано функціонал резервного копіювання налаштувань та баз даних, доступ до чутливої інформації обмежується системою багаторівневого контролю доступу (RBAC).

Програмний продукт розрахований на широкий спектр користувачів - від приватних до представників малого, середнього бізнесу, які прагнуть захистити поштову інфраструктуру від атак. Таким чином, розроблений застосунок виступає як комплексне рішення для фільтрації небезпечних електронних повідомлень. Його впровадження здатне значно знизити ризики витоку конфіденційної інформації, зараження систем шкідливим програмним забезпеченням та фінансових втрат, пов’язаних із діяльністю кіберзлочинців.

1. Cloud and Threat Report 2025. Netskope Threat Labs. URL: https://www.netskope.com/netskope-threat-labs/cloud-threat-report/cloud-and-threat-report-2025
2. Огляд ринку кібербезпеки в Україні. URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf
3. Singh R. Social Engineering Attacks. 2022. 298 p. URL: https:// www.researchgate.net/publication/389359499_Social_Engineering_Attacks

Цифрове профілювання кіберзлочинців на основі криміналістичних артефактів

УДК 004.02

Марина Ларченко
Національний університет «Чернігівська політехніка», Ніжинський державний університет імені Миколи Гоголя,
urlinka2006@gmail.com

Зростання кіберзлочинності супроводжується ускладненням методів вчинення злочинів та зменшенням ефективності традиційних підходів до кримінального розслідування. Формується новий напрям цифрової криміналістики – цифрове профілювання кіберзлочинців. Його сутність полягає у реконструкції поведінки, мотивів і характеристик злочинця на основі цифрових слідів, які залишаються в інформаційно-комунікаційних системах після інциденту. Особливу роль у цьому процесі відіграють криміналістичні артефакти, тобто технічні залишки діяльності зловмисника, що підлягають аналізу для ідентифікації особи або групи [1].

Профілювання кіберзлочинця – це міждисциплінарна діяльність, яка об'єднує методи криміналістики, поведінкової аналітики, інформаційної безпеки та машинного навчання. На відміну від традиційного профілювання, цифрове профілювання ґрунтується на технічних характеристиках поведінки зловмисника в кіберсередовищі. Такий профіль може включати: 1) рівень технічної обізнаності (наявність авторських скриптів, складність експлойтів); 2) стиль програмування (ідентифікація почерку коду – стилометрія); 3) часові рамки активності (час доби, частота дій); 4) регіональну прив'язку (мовні патерни, часовий пояс, IP-адреси); 5) особливості використаних інструментів (тип шкідливого ПЗ, засоби шифрування або обфускації) [4]. Ці ознаки дозволяють не лише встановити потенційну особу, причетну до кіберзлочину, а й виявити спільні риси з іншими інцидентами, що сприяє виявленню серійних дій або зв'язків між групами [2].

Профілювання неможливе без ретельного збору та аналізу цифрових артефактів. До них, як правило, відносять: 1) системні журнали подій (event logs) – фіксують акти входу, помилки, запуск програм; 2) дампи пам'яті (memory dumps) – містять фрагменти активних процесів, ключі шифрування, залишки повідомлень; 3) мережеві артефакти – пакети трафіку, лог-файли проксі та VPN, адреси з'єднань; 4) метадані файлів – дата створення/модифікації, авторські атрибути; 5) залишкові сліди діяльності – кеші браузерів, списки відкритих документів, тимчасові файли; 6) шкідливі

скрипти і програми – вивчення їх структури, взаємодії з системою, механізмів самозахисту.

Комплексна обробка таких об'єктів дозволяє ідентифікувати «почерк» зловмисника. Наприклад, навіть після видалення шкідливого ПЗ, залишаються ознаки його активності, тобто записи в системному журналі, артефакти в реєстрі Windows, фрагменти у вільних блоках пам'яті. Профілювання потребує інструментального аналізу з використанням спеціалізованого програмного забезпечення. Збір та обробка даних виконуються за стандартною схемою: ідентифікація – вилучення – аналіз – інтерпретація.

З огляду на складність злочинів, актуальним є застосування методів машинного навчання. Наприклад: класифікація зразків коду за схожістю до відомих шкідливих програм (малварей); кластеризація поведінкових патернів на основі логів; побудова моделей аномалій для виявлення нетипових дій; стилометричний аналіз коду для виявлення авторства або стилю програмування. Ці підходи дозволяють автоматизувати формування профілів та прискорити ідентифікацію повторних злочинців або груп, що діють під різними прикриттями.

Серед головних викликів цифрового профілювання варто відзначити анонімізацію діяльності зловмисників, використання обфускації та шифрування в коді для ускладнення атрибуції. Організаційні проблеми зводяться до правових обмежень щодо використання персональних даних при аналізі, відсутності уніфікованих підходів до класифікації артефактів, обмеженості якісних навчальних вибірок для моделей ШІ. Іноді частина артефактів втрачається або пошкоджується через дії самого зловмисника або через неправильне вилучення даних на етапі реагування на інцидент.

Отже, ефективність цифрового профілювання визначається якістю збору криміналістичних артефактів, рівнем автоматизації аналізу та міждисциплінарною інтеграцією знань. У поєднанні з методами машинного навчання цифрове профілювання відкриває нові можливості не лише для ретроспективного розслідування кіберзлочинів, а й для прогнозування загроз та раннього виявлення організованих злочинних груп у кіберпросторі. Актуальним є розвиток правових засад використання цифрових профілів та розбудова міжнародної співпраці у сфері обміну профільною інформацією.

1. Степанюк, Р. Л. & Перлін, С. І. (2023). Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник Луганського навчально-наукового інституту імені Е.О. Дідоренка*, (3), 283–294. https://doi.org/10.33766/2524-0323.99.283-284

2. Sutter, Owen. (2020). The Cyber Profile -Determining human behavior through cyber-actions. 157 p. https://www.researchgate.net/publication/361655413_The_Cyber_Profile_-_Determining_human_behavior_through_cyber-actions

3. Зачек, О. І. & Дмитрик, Ю. І. (2020). Застосування профайлінгу для протидії кіберзлочинності. *Соціально-правові студії,* 4 (10). 94-100. https://doi.org/10.32518/2617-4162-2020-4-94-100

Розробка моделі системи оцінки негативних наслідків втрати персональних даних

УДК 004.056.5:005.8

Ірина Лозова[1], Олександр Корченко[2]

[1]ДУ «Київський авіаційний інститут», iryna.lozova@npp.kai.edu.ua
[2]Державний університет інформаційно-комунікаційних технологій, o.korchenko@duikt.edu.ua.

Актуальність розробки моделі оцінки наслідків втрати персональних даних (ПД) відповідно до GDPR зумовлена вимогами ЄС щодо захисту ПД. Регламент зобов'язує організації оцінювати ризики для прав осіб у разі витоку, а стандартизована система допомагає своєчасно ухвалювати рішення щодо інформування та мінімізувати ризики штрафів, репутаційних і правових втрат.

Метою роботи є розробка моделі системи, що забезпечить організаціям дотримання вимог безпеки ПД, зниження ймовірності порушення конфіденційності та зменшення негативних наслідків втрати ПД.

Сучасні системи оцінки наслідків втрати ПД у контексті GDPR мають низку недоліків. Серед них – низький рівень автоматизації, складність інтеграції в бізнес-процеси, неврахування особливостей конкретних організацій, відсутність ефективного моніторингу та прозорої звітності, а також складність впровадження для малого та середнього бізнесу через високу вартість і складність алгоритмів.

На основі кортежної GDPR-моделі параметрів ПД [1] та методу визначення негативних наслідків порушення конфіденційності ПД [2] сформовано структурну модель системи для оцінювання наслідків втрати ПД (див. рис. 1), до складу якої входять: блок формування та зберігання даних (БФЗД); блок ідентифікації та визначення рівня порушення (БІВРП); блок формування експертної інформації (БФЕІ); блок обробки експертних даних (БОЕД).

БФЗД призначений для підготовки даних (суджень експертів) і складається з: бази даних (БД) групи питань (БДГП) – питання для аналізу ризиків; БД результатів опитувань (БДРО) – зібрані відповіді експертів; БД рекомендацій (БДР) – зберігає пропозиції щодо мінімізації ризиків.

БІВРП складається з: модуля визначення загального глобального річного обігу (ЗГРО) – компонента T^{φ} формується шляхом визначення експертом річного обігу в €; модуля визначення показника рівня порушення (ПРП) – $P^{\varphi}_{Гп}$ обчислюється на основі множини визначених рівнів порушень, відносно яких формується коефіцієнт максимально можливого збитку.

БФЕІ – складається з модулів оцінювання та вибору певних характеристик порушення (специфіка порушення (СП), характер порушення (ХП), зниження шкоди (ЗШ), ступінь відповідальності (СВ), рецидив порушення (РП), рівень співпраці (РС), категорії даних (КД), спосіб виявлення (СПВ), відповідність заходам (ВЗ), дотримання кодексів (ДК), визначаючий чинник (ВЧ)), що засновується на конкретних оцінках діяльності підприємства, які в результаті сформують значення показників P^{φ}_{i} $(i = \overline{1,11})$, що в подальшому буде використано для обчислення сумарного збитку φ-го підприємства.

БОЕД складається з: модуля вибору рекомендацій (ВР) – рекомендації RE^{φ} для БФЕІ, відповідно до суджень експерта та своєї належності до певної категорії; модуля визначення коефіцієнта суми набраних балів (КСНБ) – TMC^{φ} (коефіцієнт обчисленої кількості отриманих балів); модуля визначення максимального штрафу (МШ) – MF^{φ} (обрахунок максимального збитку для підприємства); модуля визначення максимально наближеного штрафу (МНШ) – AF^{φ} (максимально наближений штраф з урахування КСНБ).

Розроблена структурна модель системи оцінки негативних наслідків втрати персональних даних є ефективним засобом підвищення рівня інформаційної безпеки організацій. Завдяки впровадженню блоків формування та зберігання даних, ідентифікації та визначення рівня порушення, формування експертної інформації, обробки експертних даних дозволяє створити автоматизовану систему підтримки прийняття рішень для аналізу витоків персональних даних і зниження пов'язаних фінансових ризиків.

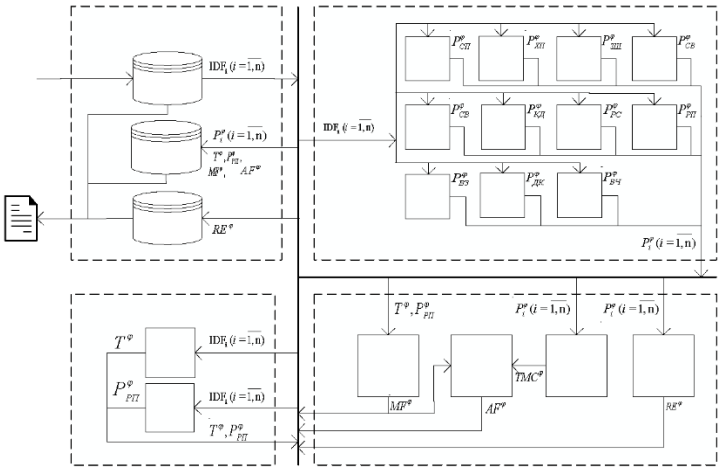


Рис.1. Структурна модель системи оцінки негативних наслідків втрати персональних даних

1. Теоретико-множинна GDPR-модель параметрів персональних даних / О. Г. Корченко та ін. Ukrainian Information Security Research Journal. 2020. Т. 22, № 2. С. 120–141. URL: https://doi.org/10.18372/2410-7840.22.14871.

2. Метод оцінювання негативних наслідків від порушення конфіденційності персональних даних / В. Шульга та ін. Ukrainian Information Security Research Journal. 2023. Т. 25, № 4. С. 254–268. URL: https://doi.org/10.18372/2410-7840.25.18232.

Алгоритми та програмний засіб для дослідження модулярного експоненціювання в асиметричних криптосистемах

УДК 004.41

Анжеліна Максим'юк[1], Михайло Касянчук[2]
Західноукраїнський національний університет,
[1]maksymjukanjelina@gmail.com, [2]kasyanchuk@ukr.net

Асиметричні криптосистеми є фундаментальним елементом сучасної криптографії, які забезпечують конфіденційність, цілісність та доступність даних [1]. Однак ефективність цих систем значною мірою залежить від продуктивності операцій модулярного експоненціювання, що лежать в основі алгоритмів шифрування та розшифрування. Існуючі підходи до оптимізації модулярного експоненціювання характеризуються різними показниками ефективності, що вимагає детального порівняльного аналізу.

Метою роботи є розробка програмного засобу для дослідження та порівняльного аналізу алгоритмів модулярного експоненціювання в асиметричних криптосистемах RSA та Ель-Гамаля, визначення їх ефективності за критеріями часової та обчислювальної складності, а також формування практичних рекомендацій щодо їх застосування.

Наукова новизна та практичне значення дослідження полягає у розробці та реалізації програмного засобу на основі мови програмування Python, який дозволяє досліджувати ефективність різних алгоритмів модулярного експоненціювання (зокрема векторно-модулярного методу, методу виділення квадрату, методу виділення кубу та прямого піднесення до степеня) у контексті практичного застосування в асиметричних криптосистемах.

Для досягнення поставленої мети було розроблено програмний засіб на мові Python, що реалізує основні алгоритми модулярного експоненціювання та забезпечує їх порівняльний аналіз. У рамках дослідження:

1) проаналізовано теоретичні основи асиметричних криптосистем та модулярного експоненціювання;
2) реалізовано криптосистеми RSA та Ель-Гамаля з використанням різних методів модулярного експоненціювання;
3) розроблено архітектуру програмного засобу, що дозволяє оцінювати часову та обчислювальну складність алгоритмів;
4) проведено порівняльний аналіз ефективності реалізованих методів модулярного експоненціювання.

У результаті дослідження було реалізовано програмний інструмент для вивчення особливостей модулярного експоненціювання в асиметричних криптосистемах. Проведений аналіз продемонстрував, що вибір алгоритму експоненціювання істотно впливає на продуктивність криптографічних операцій. Отримані результати можуть бути використані для оптимізації криптографічних рішень у реальних інформаційних системах.

1. Nykolaychuk Ya.M., Yakymenko I.Z., Vozna N.Ya., and Kasianchuk M.M. Residue Number System Asymmetric Cryptoalgorithms. Cybernetics and Systems Analysis. 2022, Vol. 58, No. 4, P.611-618.

Приватність та інформаційна безпека у соціальних медіа

УДК 004.02

Євгеній Машегіров[1], Олексій Стопакевич[2]
Національний університет «Одеська політехніка»,
[1]9480555@stud.op.edu.ua [2]stopakevych@op.edu.ua

Постановка проблеми. Соціальні медіа збирають величезні обсяги персональних даних, що робить їх привабливими цілями для кіберзлочинців. Основні загрози включають: 1) несанкціонований доступ до даних; 2) фішинг та соціальна інженерія; 3) витоки даних; 4) дезінформація; 5) шкідливе програмне забезпечення. Ці загрози можуть призвести до крадіжки особистих даних, фінансового шахрайства, порушення приватності та інших негативних наслідків.

Мета дослідження. Метою роботи є аналіз основних загроз приватності та інформаційної безпеки в соціальних медіа та розробка інноваційних методів їх подолання з використанням новітніх технологій, зокрема машинного навчання та блокчейну, для створення безпечнішого цифрового середовища.

Актуальність. Зі зростанням кількості користувачів соціальних медіа (понад 4,4 мільярда у 2025 році) та обсягу оброблюваних даних питання захисту приватності набуває критичної важливості [5]. Скандали, такі як Cambridge Analytica, підкреслили вразливість централізованих платформ [6]. В Україні, де 84% громадян отримують новини з соціальних мереж, дезінформація та кіберзагрози становлять додаткові ризики [7]. Дослідження показують, що багато українців не ознайомлюються з політиками конфіденційності, що підвищує їхню вразливість [2].

Наукова новизна. Наукова новизна полягає в запропонованому інтегрованому підході, який поєднує аномальне виявлення на основі машинного навчання з атрибутним контролем доступу (ABAC) для динамічного управління дозволами та виявлення порушень приватності в реальному часі [1]. Крім того, досліджується потенціал блокчейн-технологій для створення децентралізованих соціальних медіа, де користувачі мають повний контроль над даними, що є новим напрямком порівняно з традиційними централізованими платформами [3]. Цей підхід вирізняється від попередніх робіт, які зосереджувалися переважно на окремих аспектах безпеки, таких як шифрування чи освіта користувачів [2].

Розв'язок поставленої задачі. Для подолання загроз пропонується комплексне рішення, яке включає: 1) система аномального виявлення на основі машинного навчання для моніторингу поведінки користувачів і виявлення підозрілих активностей, таких як несанкціонований доступ чи аномальні патерни взаємодії [1]; 2) атрибутний контроль доступу (ABAC), що керує правами доступу на основі атрибутів користувачів (роль, місцезнаходження, час доступу); 3) децентралізовані соціальні медіа на базі блокчейну [3].

Інноваційні пропозиції: 1) ШІ-помічник, який аналізує пости перед публікацією, попереджаючи користувачів про потенційні ризики розкриття особистих даних; 2) біометрична автентифікація із застосуванням гомоморфного шифрування для захисту даних; 3) стимулювання кіберграмотності за рахунок гейміфікованих систем, де користувачі отримують

токени чи бали за використання безпечних налаштувань приватності. Ці рішення є реалістичними завдяки сучасним технологіям, таким як Ethereum для блокчейну та доступним бібліотекам машинного навчання, і можуть бути впроваджені платформами чи сторонніми розробниками.

Висновки. Інтеграція машинного навчання та блокчейн-технологій пропонує ефективний підхід до підвищення приватності та безпеки в соціальних медіа. Запропонована система аномального виявлення та ABAC забезпечує реальний захист від загроз, тоді як децентралізовані платформи та інноваційні інструменти, такі як ШІ-помічники та біометрична автентифікація, відкривають нові можливості для безпечного цифрового середовища. Впровадження цих рішень може значно знизити ризики та підвищити довіру користувачів до соціальних медіа.

1. Randa Aljably, "Preserving Privacy in Multimedia Social Networks Using Machine Learning Anomaly Detection." Security and Communication Networks, 2020. URL: https://www.hindawi.com/journals/scn/2020/5874935/ (дата звернення 29.04.2025)
2. Мельник К.С. Обробка та захист персональних даних в соціальних мережах. Київ: Інститут інформації, безпеки і права Національної академії правових наук України, 2014. URL: https://ippi.org.ua/sites/default/files/14mksdsm.pdf (дата звернення 29.04.2025)
3. Top 7 Blockchain Social Media Platforms In 2024. Flying V Group, 2024. URL: https://www.flyingvgroup.com/blockchain-social-media/ (дата звернення 29.04.2025)
4. Витік даних Facebook: що сталося і як захистити себе. *Українська правда*, 2021. URL: https://www.pravda.com.ua/news/2021/04/4/7288929/ (дата звернення 29.04.2025)
5. Blockchain Social Media - Towards User-Controlled Data. *LeewayHertz*, 2019. URL: https://www.leewayhertz.com/blockchain-social-media-platforms/ (дата звернення 29.04.2025)
6. How Blockchain Can Solve Social Media Privacy. *Investopedia*. 2018. URL: https://www.investopedia.com/news/ethereum-blockchain-social-media-privacy-problem-linkedin-indorse/ (дата звернення 29.04.2025)
7. Дослідження медіаспоживання українців: третій рік повномасштабної війни. Київ: ОПОРА, 2024. URL: https://www.oporaua.org/viyna/doslidzhennya-mediaspozhivannya-ukrayinciv-tretiy-rik-povnomasshtabnoyi-viyni-25292 (дата звернення 29.04.2025)

Застосування ML-моделі для виявлення SQL-ін'єкцій у веб-додатках на Flask та Node.js

УДК 004.056.5:004.75:004.738.5

Іванна Мелько[1], Ігор Ігнатєв[2]
[1,2]*Західноукраїнський національний університет*
[1]*ivannamelko59@gmail.com*, [2]*iiv@wunu.edu.ua*

У роботі розглянуто можливість виявлення SQL-ін'єкцій за допомогою алгоритмів машинного навчання. Подано приклад реалізації простої моделі, яка

класифікує запити як легітимні або потенційно шкідливі. Система може бути інтегрована у веб-додатки, створені з використанням Flask або Node.js[4]. Запропоноване рішення забезпечує високу точність та швидкість реагування при мінімальних ресурсних витратах, що дозволяє використовувати його навіть у невеликих проєктах.

SQL-ін'єкції залишаються однією з найпоширеніших загроз у веб-додатках. Вони дозволяють зловмиснику маніпулювати запитами до бази даних, обходити автентифікацію або зчитувати конфіденційну інформацію. Звичайні методи фільтрації не завжди встигають адаптуватись до нових видів атак, особливо zero-day[1]. Саме тому машинне навчання стає перспективним напрямом для побудови більш гнучких та інтелектуальних захисних механізмів.

Мета дослідження — розробити та продемонструвати підхід до виявлення SQL-ін'єкцій у HTTP-запитах на основі машинного навчання, з можливістю інтеграції в веб-додатки на Flask і Node.js.

Рис.1. Схема обробки HTTP-запиту з ML-детектором SQL-ін'єкцій

Для формалізації процесу прийняття рішення можна скористатись наступною формулою класифікації:

$$P(SQLi \mid x) = (1 / N) \sum f_i(x) \quad (1)$$

де: x — векторизований HTTP-запит, $f_i(x)$— рішення і-го дерева у випадковому лісі, N — загальна кількість дерев, P(SQLi|x)— ймовірність, що запит є SQL-ін'єкцією.

Приклад обчислення:

Тобто модель визначає запит як SQLi з ймовірністю 60%, згідно вимог я правильно написати 1. Підписи до рисунків і таблиць

$$P(SQLi \mid x) = 1/5(1 + 1 + 1 + 0 + 0) = 0.6 \quad (2)$$

Таблиця 1

Ефективність моделей

Модель	**Точність**	**Час реакції**
Logistic Regression	92.4%	2.1 мс
Decision Tree	94.3%	3.0 мс
Random Forest	**96.8%**	3.4 мс

Запропонована модель на основі машинного навчання демонструє високу ефективність у виявленні SQL-ін'єкцій у веб-запитах. Вона працює швидко, не потребує великих обчислювальних ресурсів і легко інтегрується у популярні фреймворки, зокрема Flask та Node.js[3].

Модель стабільно розпізнає типові форми шкідливих запитів, а її адаптивність дозволяє враховувати нові сценарії атак. Такий підхід можна розширити й на інші типи загроз, зокрема на бот-активність, аномальні дії користувачів або zero-day атаки.

Нижче наведено приклад реалізації простої ML-моделі для виявлення SQL-ін'єкцій з використанням Python, бібліотек scikit-learn та Flask. Модель аналізує HTTP-запити та класифікує їх як легітимні або SQL-ін'єкційні[1].

– Збір навчальних даних з прикладами запитів (SQLi та OK).

– Побудова моделі з використанням TF-IDF та Random Forest.

– Тестування моделі на нових запитах.

– Збереження моделі у форматі .pkl (joblib)[2].

– Створення Flask-сервера, що приймає запит і повертає результат (SQLi або OK).

Такий підхід дозволяє легко вбудувати інтелектуальний захист у будь-який REST API та проводити перевірку запитів у реальному часі. Рішення підходить як для Flask, так і для Node.js через HTTP-запити.

1. OWASP Foundation. SQL Injection. URL: https://owasp.org/www-community/attacks/SQL_Injection

2. Scikit-learn documentation. URL: https://scikit-learn.org/stable/

3. Géron A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow. O'Reilly, 2019.

4. RFC 7231. URL: https://datatracker.ietf.org/doc/html/rfc7231

Розробка застосунку для підвищення рівня кібербезпеки від атак методами соціальної інженерії

УДК 62

Маргарита Мельник[1], Денис Завадський[2]

[1]SET University, [2]Національний університет, "Одеська Політехніка"

[1] m.melnyk@setuniversity.edu.ua [2]9560447@stud.op.edu.ua

Соціальна інженерія є особливо небезпечною ще через те, що вона не потребує високотехнологічних інструментів. Атаки в соціальній інженерії часто спрямовані на виявлення слабких місць у людському мисленні або поведінці, що робить їх особливо важкими для виявлення і нейтралізації. Тому навіть найсучасніші технології захисту не можуть гарантувати повну безпеку, якщо користувачі не навчені реагувати на ці загрози.

Успіх соціальної інженерії значною мірою базується на нестачі обізнаності серед користувачів. Люди не завжди розпізнають потенційну загрозу в листі, дзвінку чи особистій розмові. Захист від такого виду атак передбачає впровадження різноманітних методів навчання користувачів у кіберпросторі.

Своєчасне виявлення та попередження спроб соціальної інженерії значною мірою знижує ризики витоку даних. Захист починається з людини - найслабшого, але й наважливого елементу інформаційної безпеки. У час стрімкого розвитку цифрових технологій для протидії таким методам атак важливе значення має систематичне навчання користувачів. Необхідно впроваджувати комплексні програми з підвищення кіберграмотності. Існують різні програми навчання, які орієнтовані на формування у користувачів навичок критичного мислення та обережності у взаємодії з цифровими технологіями. Одним з найбільш ефективних підходів є створення навчальних курсів та

тренінгів, що зосереджені на реальних прикладах атак, що дозволяє користувачам на власному досвіді оцінити можливі небезпеки і навчитися швидко реагувати на них. Однак, як показує практика, багато з цих методів не завжди є на 100% ефективними, оскільки зловмисники постійно адаптуються до нових технологій і стратегій навчання.

Також важливим аспектом є розвиток інструментів для автоматичної перевірки наявності ознак соціальних інженерії у повсякденних операціях користувачів. В таких випадках комбінування людських навичок і технологічних засобів може стати оптимальним підходом для забезпечення кібербезпеки.

Тому, вважаю, що розробка застосунку для підвищення рівня кіберграмотності від атак методами соціальної інженерії є дієвим інструментом для ефективного підвищення обізнаності користувачів щодо загроз соціальної інженерії та формування навичок цифрової безпеки.

Крім того, застосунок є масштабованим і доступним, що дає змогу адаптувати його під різні цільові аудиторії, додавати нові сценарії атак, навчальні модулі та інтегрувати сучасні технології гейміфікації.

Кожна кнопка містить заголовок (назву рівня) та тематичне зображення у форматі PNG. Натискання на кнопку викликає відповідну JavaScript-функцію (lvl1(), lvl2() тощо), яка виконує перенаправлення на іншу HTML-сторінку (наприклад, PhishingA.html, Vishing.html), де реалізований відповідний сценарій

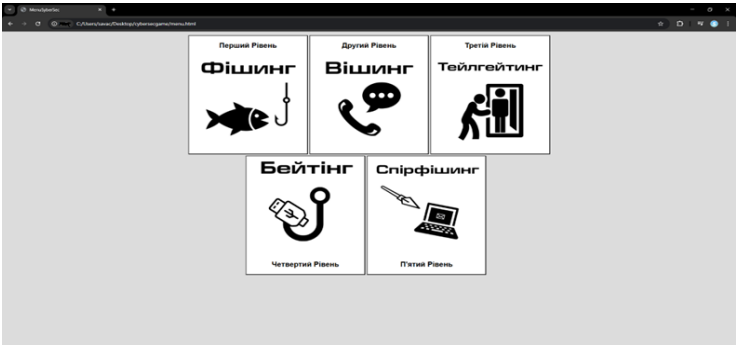


Рис.1. Інтерфейс застосунку

Простота реалізації дозволяє легко масштабувати застосунок, додавати нові блоки запитань, адаптувати інтерфейс для мобільних пристроїв або інтегрувати його в освітні платформи. Таким чином, розроблений інструмент має потенціал для подальшого розвитку як частина більшої системи цифрового навчання або корпоративного тренінгу.

Програмне забезпечення було протестовано в умовах максимально наближених до реального використання, і успішно пройшло всі технічні випробування. Це підтвердило його стабільність, коректність роботи і готовність до впровадження в освітні середовища, компанії або для індивідуального користування. Таким чином, даний вебзастосунок є

ефективним інструментом для підвищення рівня кібербезпеки серед звичайних користувачів шляхом формування критичного мислення та стійкості до соціальних маніпуляцій, і підтверджує доцільність використання гейміфікованих підходів у сфері кібергігієни.

1.Венгерський П.С., Вишневська Н.С., Хохлачова Ю.Є., Хорошко В.О., Чобаль О.І., Кількісна оцінка кіберзахищеності інформації. *Захист інформації*. – 2023. – Т. 25, №2. – С. 53-61.

2. S.Yevseev, S.Pogasiv O.Shmatko, M. Melnyk Cybersecurity:security of linux operating system / Laboratory workshop, Kharkov, 2021

3.Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. *Вісник Національного університету «Львівська політехніка». Серія: "Юридичні науки".* –2024 Том 11, № 1(41), С. 314-320.

Архітектура інформаційної технології інтелектуального моніторингу мережевого трафіку

УДК 004.056.55:004.93’1

Вадим Мєшков
Національний технічний університет «Дніпровська політехніка», mieshkov.v.i@nmu.one

Одним із ключових викликів у сфері кібербезпеки є необхідність своєчасного виявлення атак, які маскуються під звичайну користувацьку активність. Сучасні загрози все частіше використовують динамічні стратегії, зокрема зміну поведінкових характеристик, приховане сканування або доступ до мережі через легітимні сервіси [1]. Така активність ускладнює процес виявлення, особливо в масштабних корпоративних мережах, де обсяг переданого трафіку постійно зростає, а структура взаємодії між вузлами має високий рівень складності. Ефективне виявлення вторгнень вимагає моніторингу мережевих потоків у реальному часі з урахуванням не лише технічних параметрів протоколів, а й поведінкових ознак, характерних для користувачів і пристроїв.

Проблема обмеженої ефективності сигнатурних систем виявлення загроз залишається актуальною [1]. Такі системи орієнтовані на фіксацію заздалегідь відомих шаблонів атак і не здатні реагувати на невідомі чи змінені варіанти вторгнень, зокрема zero-day атаки. За умов появи атак нового покоління, що динамічно змінюють характеристики та обходять традиційні засоби захисту, зростає потреба в адаптивних, інтелектуально керованих підходах до аналізу трафіку. Методи машинного навчання та поведінкового моделювання надають можливість виявляти відхилення від типових моделей взаємодії навіть без попередньої інформації про конкретні реалізації загроз.

Метою дослідження є розробка інформаційної технології для інтелектуального аналізу трафіку комп’ютерної мережі, здатної до автоматичного виявлення атак у режимі реального часу.

Запропоноване рішення реалізовано у вигляді дворівневої архітектури (рис. 1), що поєднує модуль попередньої фільтрації та модуль глибокого аналізу.

Перший з них виконує високошвидкісну первинну обробку вхідного трафіку, спрямовану на зменшення навантаження на систему шляхом оперативного виокремлення підозрілих потоків. Дані структуровано за ознаками сесій, IP-адрес, портів і часових параметрів. На основі агрегованих статистичних характеристик – таких як середній розмір пакету, частота запитів, баланс між вхідними та вихідними потоками – виконується базова класифікація трафіку. У модулі застосовуються алгоритми з низькою обчислювальною складністю, що дозволяє реалізувати його на рівні прикордонних пристроїв або мережевої інфраструктури. Потоки, що класифікуються як потенційно аномальні, передаються для подальшої обробки.

Другий модуль архітектури здійснює глибокий поведінковий аналіз трафіку з використанням інструментів інтелектуальної обробки даних. Ключовим елементом є класифікатор, побудований на основі алгоритму Random Forest, що демонструє стійкість до варіативності параметрів і забезпечує високу достовірність розподілу мережевої активності за класами. У процесі аналізу враховуються складні ознаки, зокрема ентропія пакетів, часові затримки, динаміка створення сесій і характер змін у міжвузлових взаємодіях. Для підвищення точності виявлення в модель інтегровано контекстуальні фактори: часові шаблони активності, типові дії користувачів і сценарії доступу до ресурсів. Навчання моделі проводилося на базі відкритих наборів даних (наприклад, CIC-IDS2017) [2], що дало змогу здійснити повноцінну перевірку ефективності розробленого підходу. Отримані результати передаються до систем візуалізації або інтегруються з SIEM-рішеннями для подальшого реагування на інциденти.

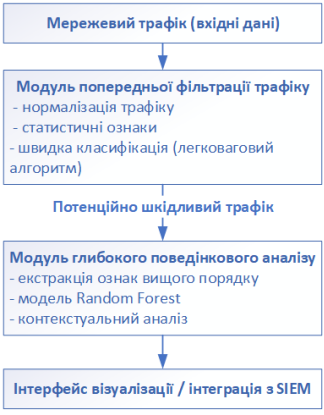


Рис 1. Дворівнева архітектура моніторингу трафіку комп'ютерної мережі

Наукова новизна полягає в побудові багаторівневої системи аналізу, яка об'єднує статистичні та поведінкові характеристики трафіку в єдину аналітичну структуру, орієнтовану на роботу в реальному часі. Під час експериментальної перевірки було зафіксовано зростання ключових показників [3] якості

класифікації – точності, повноти та F1-міри – на 8-12 % порівняно з базовими одношаровими моделями, що підтверджує практичну ефективність запропонованої інформаційної технології в умовах високонавантаженого середовища.

1. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy, 2010. – P. 305-316.

2. Moustafa N., Slay J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). Military Communications and Information Systems Conference (MilCIS), 2015. – P. 1-6.

3. Венгерський П.С., Вишневська Н.С., Хохлачова Ю.Є., Хорошко В.О., Чобаль О.І. Кількісна оцінка кіберзахищеності інформації. Захист інформації. – 2023. – Т. 25, №2. – С. 53-61.

Розвідка емерджентних ризиків інформаційної безпеки

УДК 004[738.5::(056.53+413.4)]

Володимир Мохор[1], Олександр Бакалинський[1], Ярослав Дорогий[2], Василь Цуркан[1,3]

[1]ІПМЕ ім. Г.Є. Пухова НАН України, v.mokhor@gmail.com, baov@meta.ua

[2]ДонНТУ, argusyk@gmail.com

[3]КПІ ім. Ігоря Сікорського, v.v.tsurkan@gmail.com

Емерджентний ризик інформаційної безпеки (англ. emerging information security risk) характеризується новизною і, як наслідок, високим впливом невизначеності на забезпечування непорушності властивостей інформації [1, 2]. Такий вплив може призводити до настання серйозних негативних наслідків. Насамперед втрати конфіденційності (приватності), цілісності, доступності інформації і, загалом, припинення діяльності організації [1]. Тож розвідування емерджентних ризиків інформаційної безпеки є актуальним.

Розвідка ризиків інформаційної безпеки (англ. information security risk intelligence) визначається як результат збирання, аналізування, інтерпретування даних, інформації, знань про вразливості інформаційних активів, загрози, наслідки реалізування загроз, заходи та засоби обробляння [1, 2]. Дана діяльність обумовлюється перш за все існуванням двох факторів – емерджентністю (новизною), високим впливом невизначеності. До того ж цим обгрунтовується необхідність задоволення потреби в наявності якісної інформації для приймання рішень про обирання заходів, засобів обробляння інформаційних ризиків від стратегічного до операційного рівнів. Процес їх розвідування визначається двома взаємозалежними циклами [2]. Зовнішній цикл пов’язаний з досліджуванням навколишнього середовища діяльності організації насамперед виявляння його змінень. Внутрішній цикл складається з чотирьох етапів, виконання яких в кінцевому випадку орієнтоване на отримання розвідувальних даних про емерджентні ризики інформаційної безпеки. З одного боку, так зменшується вплив невизначеності на забезпечення непорушності

властивостей інформації. Тоді як з іншого – підвищується якість приймання рішень про обирання відповідних заходів і засобів [1].

Отже, розвідування перш за все орієнтоване на отримання інформації про емерджентні ризики інформаційної безпеки. Її використання дозволить зменшити вплив невизначеності на забезпечування непорушності властивостей інформації організації. І, як наслідок, підвищити якість приймання рішень про обирання заходів і засобів обробляння емерджентних ризиків інформаційної безпеки.

1. Мохор В. В., Бакалинський О. О., Дорогий Я. Ю., Цуркан В. В. Парадигма нових ризиків кібербезпеки. *Кібербезпека енергетики* : матеріали науково-практичної конференції (Київ, 29 травня 2024 р.). Київ : ІПМЕ ім. Г.Є. Пухова НАН України, 2024. С. 116–117. DOI: https://doi.org/10.5281/zenodo.14601760.

2. ISO/TS 31050:2023. Risk management. Guidelines for managing an emerging risk to enhance resilience. [From 2023-10-27]. URL: https://www.iso.org/standard/54224.html (accessed on: 28.04.2025).

Застосування технологій штучного інтелекту в біометричних системах

УДК 004.056:343

Іван Мудрий[1]
Роман Іваницький[2]
[1]*Західноукраїнський національний університет*
[2]*Тернопільський національний педагогічний університет імені Володимира Гнатюка*
[1]*ludaduma7@gmail.com*, [2]*romikiv@ukr.net*

Інтеграція технологій ШІ в біометричні системи відкриває нові перспективи для підвищення безпеки та ефективності ідентифікації особи. Розглянемо детальніше ключові напрямки розвитку та інноваційні підходи у цій галузі. Штучний інтелект кардинально змінив підхід до розробки та впровадження біометричних систем. Сучасні рішення використовують складні нейромережеві архітектури для досягнення безпрецедентної точності та надійності. Зокрема, згорткові нейронні мережі (CNN) продемонстрували значні результати в обробці візуальних біометричних даних, а рекурентні нейронні мережі (RNN) та трансформери ефективно аналізують часові послідовності, що важливо для голосової біометрії та аналізу поведінкових патернів.

Розпізнавання обличчя: нові горизонти

Системи розпізнавання обличчя на основі глибокого навчання досягли вражаючої точності, що перевищує 99% у контрольованих умовах. Ключові інновації включають:

- **Аналіз мікроміміки**: ШІ здатен ідентифікувати унікальні особливості міміки обличчя, що використовується для перевірки "живості" під час автентифікації.

- **Стійкість до маскування**: Сучасні алгоритми можуть розпізнавати обличчя навіть при частковому закритті масками, окулярами чи іншими елементами.
- **Емоційний аналіз**: Додаткова верифікація через аналіз емоційних реакцій, що важко підробити під час спроби несанкціонованого доступу.

Одним з найперспективніших напрямків є розробка мультимодальних біометричних систем, що поєднують різні біометричні характеристики для підвищення надійності ідентифікації:

- Комбінація відбитків пальців з розпізнаванням обличчя зменшує ймовірність помилкового допуску в 100-1000 разів порівняно з одномодальними системами.
- Інтеграція голосової біометрії з аналізом руху губ забезпечує додатковий рівень захисту від підробок.
- Використання ШІ для динамічного визначення оптимальної комбінації біометричних характеристик залежно від ситуації та доступних даних.

Інноваційні біометричні технології включають поведінкову біометрію, яка аналізує динаміку набору тексту, особливості руху та когнітивні патерни для ідентифікації особи.

Сучасні ШІ-системи адаптуються до різних умов, автоматично регулюючи параметри залежно від освітлення та шуму, а також динамічно вибирають оптимальні біометричні характеристики у конкретних ситуаціях. Впровадження цих технологій викликає етичні проблеми, зокрема потенційну дискримінацію через незбалансованість тренувальних даних та необхідність посиленого захисту чутливих біометричних даних. Для покращення безпеки використовуються шифрування, локальна обробка даних та технології гомоморфного шифрування.

Перспективними напрямками розвитку є квантова біометрія, що забезпечує високий рівень захисту через квантове шифрування та квантово-стійкі протоколи. Неінвазивна глибока біометрія відкриває нові можливості для ідентифікації через аналіз мозкової активності та характеристик кровоносних судин. У фінансовому секторі біометричні системи застосовуються для автентифікації та запобігання шахрайству при здійсненні платежів. У медицині такі системи забезпечують надійну ідентифікацію пацієнтів та захист доступу до медичних даних. Впровадження біометричних технологій у міську інфраструктуру дозволяє оптимізувати пасажиропотоки та підвищити рівень громадської безпеки через системи контролю доступу на основі розпізнавання обличчя.

Однак, поряд з технологічними інноваціями, необхідно приділяти особливу увагу етичним аспектам та питанням захисту приватності. Балансування між безпекою, зручністю та дотриманням прав людини залишається ключовим викликом для розробників та регуляторів у цій сфері.

Майбутнє біометричних систем на основі ШІ передбачає подальшу інтеграцію з іншими передовими технологіями, такими як Інтернет речей, 5G-

мережі та розподілені обчислення, що відкриває нові можливості для безпечної та надійної ідентифікації у все більш цифровому світі.

1. Wang, M., & Deng, W. (2023). Deep face recognition: A comprehensive survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, 45(4), 1-20.
2. Johnson, A., & Smith, B. (2024). Multimodal biometric systems: Challenges and opportunities. Journal of Cybersecurity, 12(3), 245-267.
3. Петренко О.В., Іваненко С.М. (2023). Проблеми конфіденційності в сучасних біометричних системах. Інформаційна безпека, 18(2), 45-59.
4. Zhang, L., et al. (2024). Quantum-resistant biometric template protection: A review. ACM Computing Surveys, 56(4), 1-34.
5. Коваленко Т.І., Бондаренко М.П. (2024). Інтеграція штучного інтелекту в системи контролю доступу: український досвід. Кібербезпека України, 9(1), 78-92.

Цілі захисту критичної інфраструктури відповідно до Національної стратегії кібербезпеки США

УДК 004.056

Тетяна Мужанова[1], Світлана Легомінова[2], Тетяна Капелюшна[3]

Державний університет інформаційно-комунікаційних технологій
[1]t.muzhanova@duikt.edu.ua, [2]s.legominova@duikt.edu.ua, [3]t.kapeliushna@duikt.edu.ua

В умовах постійного зростання обсягів протиборства держав у цифровому просторі, в тому числі із залученням до здійснення кібератак різноманітних злочинних кіберугрупувань, забезпечення кібербезпеки об’єктів критичної інфраструктури набуває особливого значення.

Національна стратегія кібербезпеки США 2023 року [1] визнає захист систем і активів, які становлять критичну інфраструктуру, життєво важливим для національної і суспільної безпеки, економічного процвітання США. Стратегічні цілі щодо захисту критичної інфраструктури, окреслені у документі, показані на рис. 1.

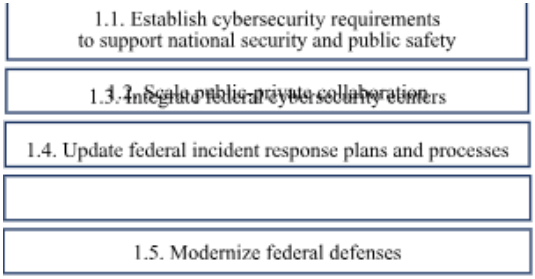


Рис. 1. Стратегічні цілі забезпечення захисту критичної інфраструктури

Розглянемо основні положення кожної із перелічених вище цілей.

1.1. Встановлення вимог кібербезпеки для служб, критично важливих для національної та суспільної безпеки. Федеральний уряд планує розбудувати сучасну динамічну й узгоджену нормативно-правову базу для кібербезпеки, адаптовану до ризиків кожного критичного сектора, спрямовану на зменшення дублювання й посилення державно-приватної співпраці. Основою для цього є вітчизняні рамкові документи з кібербезпеки, добровільні узгоджені стандарти й настанови, зокрема Агенції з кіберзахисту (CISA) [2] і Національного інституту стандартів і технологій (NIST) [3], а також гармонізовані нормативні акти з кібербезпеки США, інших держав та міжнародних організацій.

Важливим завданням є створення умов для власників і розпорядників об'єктів критичної інфраструктури, зокрема й тих, які мають обмежені фінансові можливості, забезпечити належний рівень кібербезпеки шляхом державного регулювання, стимулювання інвестицій через процес встановлення ставок, податкові структури чи інші механізми.

1.2. Поглиблення державно-приватної співпраці. Уряд США прагне посилити партнерство між CISA, що виконує функції національного координатора з питань безпеки і стійкості критичної інфраструктури, секторальними агенціями з управління ризиками (SRMA) й іншими державними органами, з одного боку, й окремими власниками, операторами критичних об'єктів, які відповідають за захист критичних систем і активів, з іншого.

Метою такої співпраці є визначення потреб конкретного сектору, оцінка прогалин у наявних можливостях федеральних органів, використання технологічних рішень для обміну даними, координації захисних зусиль тощо.

1.3. Інтеграція федеральних центрів кібербезпеки. Федеральний уряд в особі Офісу національного кібердиректора (ONCD) буде координувати повноваження й можливості департаментів і агенцій, які спільно відповідають за підтримку захисту критичної інфраструктури, зокрема й федеральних центрів кібербезпеки, які служать вузлами співпраці й покликані об'єднати зусилля правоохоронних, розвідувальних, оборонних, дипломатичних, економічних і військових урядових агенцій.

1.4. Оновлення федеральних планів і процесів реагування на інциденти. З огляду на те, що приватний сектор здатний самостійно пом'якшити більшість кіберінцидентів, допомога з боку федерального уряду має полягати в наданні єдиного й узгодженого Національного плану реагування на кіберінциденти (NCIRP) [4].

Планується чітко встановити, до яких державних установ і з яких питань можуть звернутися партнери з приватного сектору для отримання підтримки згідно з принципом «дзвінок одному є дзвінком усім».

1.5. Модернізація федерального захисту. Адміністрація докладатиме довгострокових зусиль для захисту федеральних підприємств критичної інфраструктури та модернізації федеральних систем відповідно до принципів нульової довіри, зробивши їх зразком для наслідування приватним сектором. Федеральний уряд також поглиблюватиме оперативну та стратегічну співпрацю

з постачальниками програмного й апаратного забезпечення, керованих послуг, які зможуть змінити кіберландшафт на користь більшої безпеки та стійкості.

Отже, Національна стратегія кібербезпеки США представила бачення федерального уряду щодо забезпечення стабільного й надійного захисту критичної інфраструктури шляхом встановлення вимог кібербезпеки для критично важливих служб, поглиблення державно-приватної співпраці, інтеграції федеральних центрів кібербезпеки, оновлення федеральних планів і процесів реагування на інциденти, модернізації системи федерального захисту.

1. National cybersecurity strategy. March 2023. *The White House.* URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
2. Cybersecurity Performance Goals (CPGs). October 2022. *CISA*. URL: https://www.cisa.gov/cybersecurity-performance-goals-cpgs
3. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. April 16, 2018. *NIST*.
4. National Cyber Incident Response Plan. Update Public Comment Draft. December 2024. *CISA*. URL: https://www.cisa.gov/sites/default/files/2025-01/NCIRP%20Update%20Public%20Comment%20Draft%20508c__0.pdf

Проєктування нейромережевого фільтра фішингових повідомлень

УДК 004.056.55

Владислав Назаров
Національний університет «Одеська політехніка,
tasknavigator@stud.op.edu.ua

З розвитком месенджерів і збільшенням електронної кореспонденції традиційні спам-фільтри неефективні від складних фішингових атак. Статистичні й SVM-фільтр втрачають лінгвістичні ознаки, не враховуючи зовнішні посилання [1], нейромережеві моделі вимагають значних ресурсів, мають затримки [2].

Метою роботи є розробка розподіленої мікросервісної архітектури фільтра, інтегрованого в месенджери та поштові сервіси, для швидкого й безперервного виявлення фішингу з мінімальною затримкою.

Запропонована система поєднує NLP-аналіз, ранжування чинників ризику і нейромережеву класифікацію. Конфіденційність забезпечується завдяки виключенню втручання людини та аналізу повідомлень лише в оперативній пам’яті, без збереження їх змісту.

Система реалізована як комплекс автономних мікросервісів, що взаємодіють через асинхронну чергу RabbitMQ (таб.1).

Вхідні повідомлення надходять через REST-шлюз та послідовно обробляються NLP-модулем, сервісом формування чинників ризику і нейромережевими класифікаторами.

Таблиця 1

Опис компонентів системи та їх функціональні взаємодії

Компонент	Опис та функціональні взаємодії	Технологія	Продуктивність
Інтеграційний шлюз API	Приймає повідомлення (месенджери, SMTP/IMAP), встановлює SSL/TLS, передає запити в чергу RabbitMQ.	FastAPI, Docker, SSL/TLS	500 запитів/с
Брокер повідомлень	Асинхронна передача даних між контейнерами, гарантія доставки («at least once»),горизонтальнемасштабування	RabbitMQ 3.x, Docker	SLA ≤ 50 мс на доставку
NLP-модуль	NLP-аналіз тексту (токенізація, шаблони, URL), формування ознак аналізу ризиків.	Python 3.8+, spaCy, regex	1 000 повідомлень/с; 98% точн
Модуль ранжування ризиків	Перетворення ознак на числовий вектор (Rm, Tm, Ez, Rz), кешування Redis,підготовка даних для класифікації	C++17, PyBind11, Redis	< 1 мс на повідомлення
Сигмоїдна нейромережа	Одношарова модель (MSE-втрати), класифікація ймовірності фішингу, GPU-прискорення,передача рез-ів моніторингу	TensorFlow 2.x, CUDA-GPU	Помилка ≤ 10^{-3}; 200 ітерацій ≈ 5 хв
Порогова модель	Лінійна порогова модель, адаптивне оновлення Rz, швидка класифікація, передача результатів	NumPy 1.22+, C++	< 0,1 мс на класифікацію; похибка ≈ $0{,}5 \cdot 10^{-3}$
Моніторинг та логування	Збір метрик продуктивності, затримок та помилкових спрацьовувань; зворотний зв'язок	ELK Stack, Prometheus, Grafana	Затримка збору метрик ≤ 200 мс

1. Khamis S.A., Foozy C.F.M., Ab Aziz M.F., Rahim N. Header based email spam detection framework using Support Vector Machine (SVM) technique. *Advances in Intelligent Systems and Computing*. 2020. P. 57–65.

2. Petliak N., Bezkorovalnyi Y. Analysis of modern methods of detection of phishing e-mails.Herald of Khmelnytskyi National University.2024.Issue 5

Побудова довірчих IoT-мереж на основі lightweight-хешування з урахуванням ротації вузлів

УДК 621.395.7 (043.2)

Сергій Науменко[1], Інна Розломій[2]
Черкаський національний університет імені Богдана Хмельницького,
[1]naumenko.serhii1122@vu.cdu.edu.ua,
Черкаський державний технологічний університет, [2]inna-roz@ukr.net

Інтернет речей (IoT) активно впроваджується в критичні сфери – від розумного міста до медицини й оборони. Однією з головних умов надійного функціонування таких мереж є формування довіри між пристроями, що взаємодіють у гетерогенному середовищі з обмеженими ресурсами. Використання традиційних криптографічних засобів і методів ідентифікації часто є неприйнятним через високі обчислювальні витрати [1]. У роботі пропонується підхід до формування довірчих IoT-мереж на основі полегшеного хешування з урахуванням ротації вузлів.

Під час функціонування IoT-мереж часто спостерігається ротація вузлів: частина пристроїв тимчасово втрачає зв'язок, деякі – приєднуються або виходять із мережі через переміщення, завершення циклу живлення чи енергозбереження. У таких умовах ключовим викликом є забезпечення постійного рівня довіри між учасниками взаємодії без значних затримок на повторну автентифікацію. Зважаючи на обмежені ресурси пристроїв (обчислювальні потужності, енергозабезпечення, пам'ять), актуальним є створення механізму полегшеної верифікації нових та повторно приєднаних вузлів [2].

У запропонованій моделі кожному вузлу призначається lightweight-хеш-ідентифікатор, який формується з урахуванням поточного часу, контексту використання (тип даних, пріоритет обміну, роль вузла), а також унікального ключа пристрою. Для цього використовуються хеш-функції класу PHOTON, SPONGENT або інші, оптимізовані під IoT.

Мережа підтримує таблицю довіри, яка містить останні хеш-ідентифікатори активних пристроїв. При приєднанні нового вузла система порівнює його хеш-контекст з шаблонами, доповнюючи довірчу таблицю або позначаючи вузол як потенційно підозрілий. Таким чином формується адаптивна модель довіри, яка враховує не лише статичні ідентифікатори, а й динамічний контекст комунікації.

Архітектура довірчої IoT-мережі включає множину вузлів, кожен з яких генерує власний контекстуальний lightweight-хеш-ідентифікатор на основі унікального ключа, ролі пристрою та мітки часу. Центральним компонентом є таблиця довіри, в якій зберігаються останні актуальні хеші активних пристроїв. У випадку приєднання нового або повторно активованого вузла система виконує перевірку його ідентифікатора за шаблонами у таблиці. Вузол додається до довіреного пулу або позначається як потенційно підозрілий залежно від результату перевірки.

Модель підтримує ротацію вузлів: при виході пристрою його запис деактивується, а при повторному з'єднанні виконується оновлення з урахуванням нового контексту.

Основною перевагою підходу є можливість швидкої перевірки повторно приєднаних вузлів без повного перерахунку ключів або ініціалізації заново. В основі побудови хеш-ідентифікаторів у запропонованій моделі використано обчислення контекстуального значення на основі поєднання унікального ключа пристрою, контексту його взаємодії та мітки часу, що відображено у формулі (1).

$$Ti=HKi|Ci|tmod\ M \quad (1)$$

де Ti – поточний хеш-ідентифікатор вузла i, H – вибрана полегшена хеш-функція, Ki – унікальний ключ пристрою, Ci – контекстна інформація (роль, тип даних, сценарій), t – часовий слот або мітка часу, M – модуль обмеження для TTL (time-to-live). Кожен хеш-ідентифікатор має обмежений час життя (TTL), після чого автоматично оновлюється. Завдяки цьому знижується ризик атак повторного відтворення (replay attack).

Для оцінки ефективності запропонованої схеми проведено порівняння з типовими підходами до довірчої автентифікації в IoT-середовищах. У таблиці 1 наведено ключові показники обчислювального навантаження, пам’яті та стійкості до атак.

Таблиця 1

Порівняння витрат ресурсів у різних схемах довірчої перевірки

Параметр	Традиційна схема з ключами	Запропонована lightweight-схема
Час автентифікації, мс	120–300	20–35
Пам'ять для зберігання ключів, КБ	8–16	2–4
Ступінь адаптивності	Низький	Високий
Захист від replay-атак	Обмежений	Вбудований механізм TTL

В роботі також враховано імовірні сценарії: приєднання пристрою після тривалої відсутності, підміна ідентифікатора, нестабільне з'єднання. Алгоритм хеш-перевірки з використанням контексту дозволяє заздалегідь прогнозувати поведінку вузла і приймати рішення про рівень довіри.

Запропонована модель забезпечує баланс між обчислювальними витратами та рівнем безпеки для IoT-мереж з динамічною топологією. Використання контекстуального полегшеного хешування дозволяє знизити затрати на автентифікацію, зберігаючи надійність взаємодії в умовах ротації пристроїв.

1. Розломій, І., Фауре, Е., & Науменко, С. (2025). Методи аутентифікації у вбудованих системах з обмеженими обчислювальними ресурсами. *Вимірювальна та обчислювальна техніка в технологічних процесах*, (1), 29-35. https://doi.org/10.31891/2219-9365-2025-81-4

2. Ganeshkumar, P., & Albalawi, T. (2022). A Locality-Sensitive Hashing-Based Jamming Detection System for IoT Networks. *Computers, Materials & Continua*, *73*(3).

Концепція безпекових токенів як інструменту підтвердження легітимності операцій у гібридних хмарних середовищах

УДК 004.056.5:004.75:004.738.5

Дмитро Небесний[1], Володимир Драпак[2]

Західноукраїнський національний університет[1,2]

[1]dima.neb5343@gmail.com, [2]v.drapak@wunu.edu.ua

Сучасні гібридні хмарні середовища поєднують переваги приватних і публічних хмар, проте супроводжуються високим рівнем складності щодо забезпечення прозорості, керованості та безпеки транзакцій. Традиційні підходи до контролю доступу та аудиту часто виявляються недостатніми в умовах розподілених систем. У цьому контексті перспективним є використання безпекових токенів, створених на основі блокчейн-технологій, як інструменту легітимізації операцій та забезпечення довіри між компонентами гібридної інфраструктури.

Дана робота пропонує інтегрований підхід, що поєднує концептуальне розуміння безпекових токенів з математичною моделлю оцінки їх ефективності. Таке поєднання дозволяє не тільки теоретично обґрунтувати переваги використання токенів, але й надати кількісні методи для оцінки та оптимізації системи безпеки в різних конфігураціях гібридних хмарних середовищ.

Безпековий токен — це цифровий об'єкт, який містить ідентифікатор транзакції, часову мітку, підпис користувача та динамічний рівень довіри[1]. Рівень довіри зменшується з часом, що спонукає до регулярної перевірки актуальності транзакцій. Такий підхід забезпечує адаптивність системи та дозволяє враховувати часовий контекст для підтвердження легітимності операцій. Токени зберігаються у блокчейн-структурі, яка гарантує незмінність даних та децентралізовану верифікацію.

Інтеграція токенів у хмарну інфраструктуру здійснюється за допомогою багаторівневої моделі захисту:

- Рівень доступу: Токен підтверджує автентичність запиту та дозволяє доступ лише при відповідному рівні довіри[2].
- Рівень транзакцій: Кожна операція супроводжується токеном, що містить дані про ініціатора, ціль операції та параметри узгодження[4].
- Рівень аудиту: Журнал дій формується з токенів, що дозволяє відслідковувати ланцюг подій з високою точністю[2].

Модель поєднує теорію графів Маркова[3] для динамічного аналізу ризиків і смарт-контракти як виконавчий механізм безпекових політик.

Ефективність системи безпекових токенів E визначається як функція від декількох ключових параметрів:

$$E = f(S, P, L, T, R) \quad (1)$$

де:

- S - рівень захисту $S = \alpha_1 \cdot E\_c + \alpha_2 \cdot A\_m + \alpha_3 \cdot I\_v$;
- P - продуктивність системи $P = N\_t/(t \cdot R\_u)$;
- L - латентність авторизації $L = T\_req + T\_proc + T\_resp$;
- T - термін дії токенів $T = 1/((V\_s \cdot R\_r) + C\_s$;
- R - стійкість до різних типів атак $R = \Sigma\ w\_i \cdot r\_i$.

Загальна ефективність системи безпекових токенів визначається як:

$$E = \beta_1 \cdot S + \beta_2 \cdot 1/L + \beta_3 \cdot P + \beta_4 \cdot T + \beta_5 \cdot R \quad (2)$$

Де, β_1, β_2, β_3, β_4 , β_5 - вагові коефіцієнти, що відображають відносну важливість кожного компонента для конкретної гібридної хмарної інфраструктури. Для гібридного середовища вводиться додатковий параметр гібридності:

$$H = \gamma_1 \cdot C\_p + \gamma_2 \cdot O\_p + \gamma_3 \cdot I\_c \quad (3)$$

Тоді кінцева формула ефективності з урахуванням специфіки гібридного середовища:

$$E\_hybrid = E \cdot (1 + \delta \cdot H) \quad (4)$$

де, - коефіцієнт впливу гібридності (зазвичай від 0.1 до 0.3).

Запропонована математична модель оцінки ефективності безпекових токенів у гібридних хмарних середовищах дозволяє формалізувати підхід до забезпечення безпеки в розподілених системах. Поєднання концепції безпекових токенів на базі блокчейн-технологій із кількісною оцінкою їх ефективності надає потужний інструментарій для проєктування, розгортання та оптимізації систем безпеки в гібридних середовищах.

Результати імітаційного моделювання підтверджують високу адаптивність моделі до різних сценаріїв використання та дозволяють знаходити оптимальні конфігурації безпекових механізмів відповідно до конкретних вимог організації.

1. Kumar, R., & Tripathi, R. (2024). Security and Privacy in Hybrid Cloud Computing. Springer.
2. Li, J., et al. (2023). "Blockchain-based security token framework for distributed systems." IEEE Transactions on Cloud Computing, 11(3), 1245-1260.
3. Smith, A., & Brown, B. (2024). "Dynamic trust models in hybrid environments." Journal of Cybersecurity, 8(2), 189-204.
4. Zhao, X., et al. (2024). "Performance analysis of security token mechanisms in enterprise environments." Cloud Computing Journal, 15(4), 412-429.

Смарт-контракти як інструмент контролю доступу до персональних даних у корпоративному блокчейн-середовищі

УДК 004.056.5(043.3)
Софія Новік
Державний університет інформаційно-комунікаційних технологій, sonnovik@gmail.com

У сучасних корпоративних мережах зростає потреба у прозорих і стійких до модифікації механізмах контролю доступу до персональних даних. В умовах

стрімкого розвитку цифрових сервісів та інтеграції хмарних рішень, традиційні моделі управління доступом втрачають свою ефективність. Дослідження можливостей застосування смарт-контрактів як основного механізму контролю доступу до персональних даних у корпоративному середовищі з використанням блокчейн-технологій є актуальним завданням для науковців [1].

Смарт-контракт дозволяє формалізувати правила доступу у вигляді умов, що автоматично перевіряються при кожному запиті, та забезпечує прозорість і незмінність політик. Для кращого розуміння переваг запропонованого підходу порівняльну характеристику традиційних моделей управління доступом та смарт-контрактів наведемо в Таблиці 1 [2].

Таблиця 1

Порівняльна характеристика підходів до управління доступом

Параметр оцінювання	*Традиційна модель*	*Модель на основі смарт-контрактів*
Архітектура	Централізована: єдина точка контролю	Децентралізована: відсутність центрального елемента
Прозорість управління	Часткова: залежить від внутрішніх механізмів системи	Повна: логіка доступна для перевірки в смарт-контракті (on-chain)
Незмінність політик доступу	Відсутня: можливі несанкціоновані зміни	Гарантована: політики фіксуються у блокчейні та не можуть бути змінені
Механізм аудиту	Обмежений: потребує зовнішніх інструментів	Вбудований: автоматичне логування дій у блокчейн-реєстрі
Гнучкість налаштування правил	Висока: підтримка складної логіки через рольові моделі	Середня: обмежена логікою смарт-контракту
Продуктивність (швидкодія)	Висока: без додаткових накладних витрат	Залежить від обраної блокчейн-мережі та складності перевірок

Таким чином, впровадження смарт-контрактів у корпоративні системи дозволяє підвищити рівень довіри між підсистемами, забезпечити прозорий контроль доступу до персональних даних та підвищити відповідність сучасним вимогам регуляторів у сфері інформаційної безпеки [3].

Завдяки використанню незмінного журналу подій та автоматизованого механізму прийняття рішень, смарт-контракти значно знижують ризики людського фактору та несанкціонованого втручання в політики доступу.

1. Christidis K., Devetsikiotis M. Blockchains and Smart Contracts for the Internet of Things. IEEE Access. — 2016. — Vol. 4. — P. 2292–2303.

2. Венгерський П.С., Вишневська Н.С., Хохлачова Ю.Є., Хорошко В.О., Чобаль О.І. Кількісна оцінка кіберзахищеності інформації. Захист інформації. — 2023. — Т. 25, №2. — С. 53–61.

3. Zhang Y., Xue R., Liu L. Security and Privacy on Blockchain. ACM Computing Surveys. — 2019. — Vol. 52, No. 3. — Article 51.

Використання нейронних мереж для запобігання загроз SQL-ін’єкцій у клієнт-серверних застосунках

УДК 004.056.5

Орест Онищенко[1], Петро Венгерський[2], Ярина Коковська[3]

Львівський національний університет імені І. Франка,
[1]orest.onyshchenko@lnu.edu.ua, [2]petro.venherskyy@lnu.edu.ua,
[3]yaryna.kokovska@lnu.edu.ua

У сучасному цифровому середовищі бази даних є критично важливим елементом будь-якого вебзастосунку. Через активну інтеграцію користувацького вводу у вебінтерфейси, запити до бази даних часто будуються динамічно. Якщо не впроваджено відповідного захисту, це створює потенційно небезпечне середовище, яке може бути використане зловмисниками для SQL-ін'єкцій. [1].

SQL-ін'єкція (SQLi) це один із видів атак на вебзастосунки, який дозволяє зловмисникам змінювати структуру SQL-запитів, що надсилаються до серверу бази даних, вставляючи у поля вводу користувача спеціально сконструйований код. Метою такого втручання є отримання несанкціонованого доступу до даних, зміна або видалення інформації, а також обхід механізмів автентифікації.

Цей тип атак виникає через недостатню обробку або фільтрацію вхідних даних. Уразливий застосунок трактує введені користувачем дані як частину SQL-запиту, а не як звичайний текст.

```
SELECT * FROM users WHERE username = 'admin' AND password = '1234' OR '1
   '='1';
```

Рис.1. Приклад класичної ін’єкції

Запит на рисунку 1 завжди буде істинним, оскільки умова '1'='1' виконується завжди. У результаті зловмисник отримує доступ до облікового запису без надання правильного пароля.

Традиційні методи захисту від SQL-ін’єкцій застосовуються як перша лінія оборони та можуть значно знизити ймовірність успішної атаки. Нижче подано найбільш поширені з них: 1) Валідація та санітизація вводу. 2) Параметризовані запити (Prepared Statements) і ORM. 3) Web Application Firewall (WAF). 4) Обмеження привілеїв користувача БД.

На відміну від класичних методів сигнатурного виявлення, нейронні мережі здатні виявляти і нетипові загрози, які відхиляються від нормального шаблону поведінки — саме завдяки здатності аналізувати контекст і структуру запитів. Це дозволяє ефективно боротися навіть із тими загрозами, що ще не описані в сигнатурних базах.

Використання нейронних мереж для виявлення SQL-ін'єкцій забезпечує новий рівень адаптивного захисту, якого складно досягти за допомогою традиційних підходів. Однією з головних переваг є адаптивність: модель може бути легко перенавчена на нових даних без потреби змінювати її архітектуру або логіку інтеграції. Це дає змогу оперативно реагувати на появу нових форм атак шляхом оновлення датасету і повторного навчання, що значно підвищує стійкість системи до Zero-Day загроз. Ще однією критично важливою перевагою є висока точність класифікації запитів. Наприклад, моделі типу LSTM або CNN здатні ефективно виявляти складні шаблони у вхідних SQL-запитах.

У реальних тестуваннях модель, створена за допомогою TensorFlow, досягала точності понад 95% при класифікації запитів як «шкідливих» або «безпечних». [2].

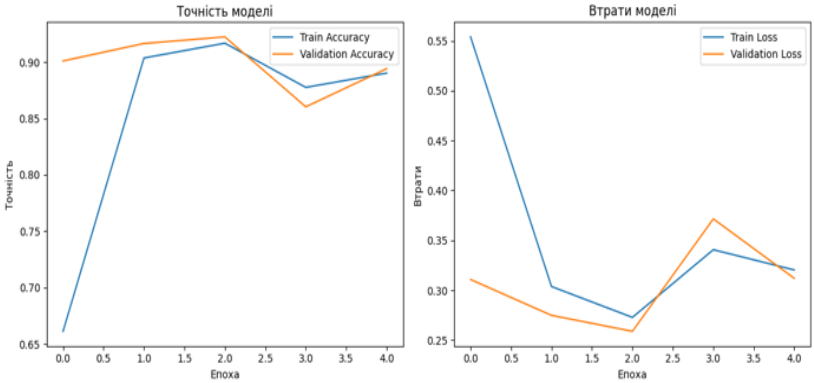


Рис.2. Графіки точності та втрат моделі під час навчання.

На рисунку 2 зображено результати тренування моделі для виявлення загроз SQL-ін'єкцій. Незважаючи на незначне коливання втрат, модель демонструє високу точність класифікації SQL-запитів та придатна для використання в реальному застосунку для попередження SQL-ін'єкцій. Для покращення стабільності результатів у майбутньому варто розглянути: 1) застосування регуляризації (dropout, L2); 2) збільшення об'єму навчального датасету; 3) використання більш глибоких або комбінованих моделей (наприклад, CNN + LSTM).

У таблиці 1 наведено порівняння ефективності трьох основних підходів до виявлення SQL-ін'єкцій: регулярних виразів, фаєрволів вебзастосунків (WAF) та нейронних мереж. Порівняння здійснено за трьома критеріями: точність, здатність виявляти Zero-Day загрози та рівень автоматизації.

Таблиця 1

Порівняння підходів

Метод	Точність	Zero-Day виявлення	Автоматизація
Regex-фільтри	~70%	Немає	частково
WAF (фаєрволи)	~ 85%	Обмежено	Середня
Нейронна мережа	>90%	Так	Повна

1. Li, X., Wang, Z., Xu, M. (2021). A Neural Network-Based Approach for SQL Injection Detection. *Journal of Network and Computer Applications*, 178, 102988. Hilpisch Y. Financial Theory with Python. A Gentle Introduction. Sebastopol: O`Reilly, 2021. 201 p.
2. Kaggle.com SQL Injection Dataset

Розробка системи аналізу вторгнень на основі логів веб-серверу

УДК 004.056.53 Анастасія Піддубровська
Національний університет «Одеська політехніка»,
9480567@stud.op.edu.ua

За даними Verizon DBIR 2024 веб-додатки залишаються головним «шляхом-у» для зловмисників: торік шаблон Basic Web Application Attacks утворив понад 8 % підтверджених зламів і посів перше місце серед векторів початкового проникнення. У середньому організації витрачають 194 дні на виявлення та ще 64 дні на локалізацію інциденту, тож зловмисник місяцями може залишатися непоміченим.

Паралельно з цим високонавантажені сайти генерують десятки або навіть сотні гігабайт HTTP-логів щодоби, що унеможливлює ручний аналіз і вимагає автоматизованих методів обробки. Незважаючи на стрімкий розвиток таких методів, проблема створення ефективних систем аналізу вторгнень на основі логів серверів на сьогодні залишається відкритою.

Метою роботи є підвищення рівня кібербезпеки веб-серверів шляхом розробки системи аналізу вторгнень на основі логів веб-серверу.

Для повноти розгляду матеріалу коротко наведемо характеристики систем аналізу вторгнень. Сучасні дослідження щодо систем аналізу вторгнень можна умовно згрупувати у три взаємопов’язані напрями.

По-перше, застосування глибинного навчання: моделі типу LogEDL (2024) поєднують Transformer-кодери з evidential loss-функцією та демонструють найвищий F1-показник на наборах HDFS, BGL і Thunderbird; новітня архітектура LogLLM (2024/2025) будує двонапрямну зв’язку BERT ↔ Llama і перевершує попередні DL-підходи на чотирьох публічних датасетах.

По-друге, традиційні та гібридні ML-методи: емпіричне дослідження ICSE 2024 засвідчило, що звичайний k-NN навчається у 1000 разів швидше за CNN і водночас підвищує F1 на 6 п.п., а робота Web Traffic Anomaly Detection Using Isolation Forest (Informatics 2024) досягає Precision 95 % і F1 92 % без складного препроцесингу .

По-третє, передобробка та інженерія ознак: велике дослідження в Empirical Software Engineering (2024) показало, що якість парсингу логів слабо корелює з точністю детектування, а вирішальним є коефіцієнт distinguishability шаблонів .

Така еволюція методів підкреслює прагнення спільноти знайти баланс між обчислювальною вартістю, інформативністю ознак і здатністю моделей адаптуватися до нових типів трафіку.

У цьому контексті активно розвиваються самонавчальні та контрастивні підходи**.** Метод Contrastive Log Learning for Unsupervised Anomaly Detection (CLLAD, 2025) істотно знижує залежність від маркованих даних: автори повідомляють про зростання F1-міри на 7–10 п.п. порівняно з LogBERT, зберігаючи час навчання в межах однієї години на наборі OpenHAB .

Ключовою ідеєю є формування позитивних і негативних пар шаблонів запитів та навчання моделі максимізувати інформаційний розрив між нормальними та аномальними подіями.

Нарешті, індустріальні кейси підтверджують практичну ефективність описаних рішень. Упровадження Elastic 8.13 SIEM у трафіку онлайн-ритейлера з середнім навантаженням 350 000 HTTP-запитів за хвилину дозволило виявити та заблокувати 83 % бот-сканувань ще на рівні периметра, скоротивши середній час реакції SOC з 18 до 4 хвилин без помітного впливу на продуктивність кластера . Цей результат демонструє, що грамотне поєднання потокового парсингу, евристичної фільтрації та ML-моделей робить систему придатною для протидії атакам у реальному часі навіть під високими навантаженнями.

Враховуючи окреслені у попередньому абзаці тенденції — стрімке зростання обсягів HTTP-логів, високу тривалість «невидимості» зловмисників і суперечливі результати новітніх DL- та ML-підходів — постає потреба у практичному рішенні, що поєднує дві риси: масштабованість під реальний трафік і прозорість для фахівців SOC. Саме на цей баланс спрямована розроблена у даній роботі гібридна система аналізу логів веб-серверів. Її ядром слугує комбінація Isolation Forest (швидке безнаглядне виявлення рідкісних патернів) і Decision Tree (інтерпретація причин тривоги у вигляді зрозумілих правил), що дозволяє зберегти високу точність без глибокої залежності від маркованих даних — ключове обмеження для більшості «важких» DL-моделей.

На відміну від чисто трансформерних підходів, система реалізує повний конвеєр «лог → інцидент», де модулі збору (Filebeat/Logstash), парсингу й нормалізації одразу готують дані до машинного аналізу, а блок пояснень на базі Decision Tree видає оператору перелік конкретних аномальних ознак — наприклад, нестандартний HTTP-метод чи вибухове зростання запитів із однієї IP-адреси. Така прозорість, підтверджена внутрішніми тестами, суттєво скорочує час ручної валідації й підвищує довіру до автоматичних сповіщень.

Крім того, модульна архітектура розробленого рішення дозволяє нарощувати пропускну здатність кластера або підмінювати окремі компоненти (наприклад, додати контрастивний препроцесинг чи LLM-класифікатор) без переробки всієї системи. У тестовій інфраструктурі з навантаженням понад 300 000 запитів/хв. рішення зберегло стабільний час реакції, а кількість хибнопозитивів залишилася нижчою, ніж у класичних сигнатурних або чисто частотних методів. Таким чином, запропонована система відповідає сучасним вимогам до реального сектору: швидке розгортання, пояснювані результати й можливість поступово інтегрувати більш складні ML-та DL-модулі у міру розвитку загроз.

1. Verizon. 2024 Data Breach Investigations Report. New York : Verizon, 2024. 114 p.
2. Cost of a Data Breach Report 2024. USA : IBM Security, 2024. 87 p.
3. Barr J. Access Logs for Elastic Load Balancers [Electronic resource]. AWS News Blog. 2014. Access mode: https://aws.amazon.com/blogs/aws/access-logs-for-elastic-load-balancers/ (date of access: 22.04.2025).

Використання NetLogo для моделювання кібератак на IoT системи

УДК 004.2

Юрій Підлісний
Національний університет «Чернігівська політехніка», ypodlesny@ukr.net

Інтернет речей (IoT) є однією з найбільш перспективних технологій сучасності, що знаходить застосування у розумних містах, промислових системах та охороні здоров'я. Проте зростаюча кількість IoT-пристроїв робить їх привабливою ціллю для зловмисників. Одним з ефективних методів аналізу вразливостей IoT-мереж є мультиагентне моделювання, яке дозволяє досліджувати динаміку атак і механізми їхнього виявлення.

У цій статті розглядається використання NetLogo для моделювання кібератак на IoT [1].

Модель у NetLogo створена для симуляції взаємодії між різними агентами в мережі IoT, зокрема пристроями, хакерами та захисниками [2]. Вона включає три основних *типи агентів:*

- *Пристрої (devices)* – елементи IoT-мережі, які можуть бути вразливими до атак.
- *Хакери (hackers)* – атакувальні агенти, що намагаються інфікувати пристрої.
- *Захисники (defenders)* – агенти, які виявляють і нейтралізують загрози.

Агенти мають наступні властивості:

Пристрої (devices):

- infected? – статус пристрою (інфікований чи ні).
- security-level – рівень безпеки (від 0 до 100).
- update-readiness – готовність до оновлень, що покращують захист.

Хакери (hackers):

- attack-power – потужність атаки, що визначає ефективність зламування пристроїв.
- preferred-target – стратегія вибору цілі, яка може бути спрямована на пристрої з низьким рівнем захисту або на критично важливі елементи мережі.

Захисники (defenders):

- detection-radius – радіус виявлення загроз.
- response-time – час реакції на атаку.

Візуалізація моделі представлена на Рисунку 1:

1) *Пристрої (Devices):*Вони відображаються як зелені квадрати (або прямокутники).
2) *Хакери (Hackers):*Хакери відображаються як червоні фігури людини.
3) *Захисники (Defenders):*Захисники відображаються як блакитні кола.

Опис взаємодії агентів: Пристрої можуть рухатися по мережі (повертатися і рухатися вперед, а хакери здійснюють атаки на пристрої з низьким рівнем безпеки або пристрої, що мають високу цінність. Захисники намагаються знайти інфіковані пристрої в радіусі своєї виявлення і відновити їх.

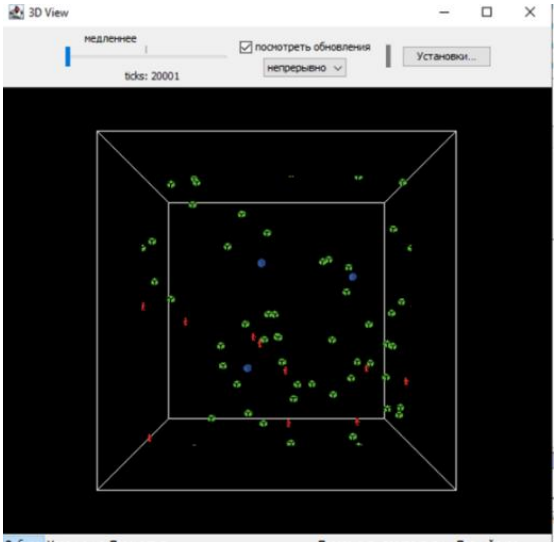


Рис 1. Візуалізація кібератаки на мережу IoT за допомогою NetLogo

Зміни в кольорі:

- *Зелені пристрої* — це здорові пристрої, які не інфіковані.
- *Червоні пристрої* — це пристрої, які були інфіковані хакерами.
- *Червоні хакери* — ці агенти здійснюють атаки на пристрої.
- *Сині захисники* — вони працюють на відновлення пристроїв.

У процесі симуляції ми бачимо як хакери атакують пристрої, як захисники реагують на ці атаки, і як пристрої можуть оновлюватися, щоб підвищити свій рівень захисту. Така 3D візуалізація допомагає краще уявити, як ці агенти працюють в реальному часі, спостерігаючи за змінами в мережі і рухами агентів, що дає вам наочне розуміння того, як працює механізм атаки та захисту.

1. Alrawi, C. Lever, M. Antonakakis, F. Monrose, Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures. November 2019IEEE Communications Surveys & Tutorials 22(1):616-644 DOI:10.1109/COMST.2019.2953364

2. Seth Tisue, Uri Wilensky. NetLogo: Design and Implementation of a Multi-Agent Modeling Environment. Center for Connected Learning and Computer-Based Modeling Northwestern University, Evanston, Illinois,

Розробка алгоритму детекції шкідливого програмного забезпечення на основі поведінкового аналізу

УДК 004.056.5 (043.2)

Артем Повозніков[1], Наталья Козаченко [2]

Національний університет «Одеська Політехніка»,

[1]9560415@stud.op.edu.ua, [2]kozachenko.n.h@op.edu.ua

В умовах стрімкого зростання кількості та складності кіберзагроз традиційні антивірусні рішення стають менш ефективними. Це обумовлює потребу у впровадженні нових методів виявлення шкідливого програмного забезпечення (ШПЗ), зокрема заснованих на поведінковому аналізі.

Мета роботи – розробка алгоритму детекції ШПЗ, який базується на аналізі аномальної поведінки програм, а не лише на сигнатурних базах.

Сигнатурні антивірусні системи залежать від оновлення баз даних загроз і часто не здатні розпізнати нові або модифіковані варіанти шкідливих програм. Натомість поведінковий аналіз орієнтується на виявлення відхилень у звичних сценаріях роботи програм, таких як аномальні зміни реєстру, нетипові запити до мережі або небажаний доступ до критичних системних ресурсів. У рамках дослідження розглянуто існуючі методи детекції шкідливого ПЗ(таблиця 1).

Таблиця 1

Порівняння методів детекції шкідливого програмного забезпечення

Критерій/ Метод	**Сигнатурний аналіз**	**Евристичний аналіз**	**Поведінковий аналіз**	**Машинне навчання**
Виявлення нових загроз	Низьке	Середнє	Високе	Високе
Рівень хибних спрацьовувань	Низький	Середній	Середній	Може бути високим

Швидкість виявлення	Висока	Висока	Залежить від реалізації	Залежить від моделі
Необхідність оновлення баз	Часте	Менш часте	Не потребує	Не потребує
Вимоги до ресурсів	Низькі	Середні	Високі	Високі
Складність реалізації	Низька	Середня	Висока	Висока

Таким чином, використання поведінкового аналізу та методів машинного навчання дозволяє істотно підвищити ефективність виявлення нових загроз у порівнянні з традиційними підходами.

Було розроблено та протестовано власний алгоритм, що включає:

1) збір даних про поведінку програм у контрольованому середовищі (sandbox),

2) екстракцію ключових поведінкових ознак,

3) навчання моделі машинного навчання для класифікації нормальної та шкідливої активності.

Для тренування моделі використовувались відкриті датасети поведінкових логів, зокрема зі спільнот VirusTotal та Cuckoo Sandbox.

Результати експериментальної перевірки показали, що запропонований алгоритм досягає точності виявлення понад 95% при мінімальному рівні хибних спрацьовувань, що свідчить про його перспективність для реального впровадження.

Таким чином, поведінковий аналіз відкриває нові можливості для раннього виявлення невідомих та складно маскованих шкідливих програм, що є важливим кроком для підвищення рівня кібербезпеки.

1. Saxe, J., Berlin, K. Deep neural network-based malware detection using two-dimensional binary program features // Proceedings of the 10th International Conference on Malicious and Unwanted Software (MALWARE), IEEE, 2015.

2. Anderson, H. S., Roth, P. Ember: An open dataset for training static PE malware machine learning models // arXiv preprint arXiv:1804.04637, 2018.

3. Gandotra, E., Bansal, D., Sofat, S. Malware analysis and classification: A survey // Journal of Information Security, 2014.

4. Mohaisen, A., Alrawi, O., Mohaisen, M. AMAL: High-fidelity, behavior-based automated malware analysis and classification // Computers & Security, 2015.

5. VirusTotal. [Електронний ресурс]. URL: https://www.virustotal.com/ (дата звернення: 05.05.2025).

6. Cuckoo Sandbox. [Електронний ресурс]. URL: https://cuckoosandbox.org/ (дата звернення: 05.05.2025).

7. Stiborek, J., Rehák, M., Pevný, T. Anomaly-based network intrusion detection: Techniques, systems and challenges // Computers & Security, 2018.

8. Kolosnjaji, B., Zarras, A., Webster, G., Eckert, C. Deep learning for classification of malware system call sequences // Australasian Joint Conference on Artificial Intelligence, Springer, 2016.

9. Yuan, B., Lu, X., Xie, M. Malware detection based on deep learning of behavior graphs // Journal of Computer Virology and Hacking Techniques, 2020.

10. Ucci, D., Aniello, L., Baldoni, R. Survey of machine learning techniques for malware analysis // Computers & Security, 2019.

Застосування нейронних мереж для аналізу побічних каналів (side-channel attacks)

УДК 004.4:056.57

Олександр Полевод
Національний університет «Чернігівська політехніка»,
oleksandr.polevod23@gmail.com

Актуальність досліджень у галузі інформаційної безпеки зумовлена стрімким розширенням використання криптографічних засобів захисту конфіденційних даних. Попри стабільність теоретичних моделей сучасних криптоалгоритмів, їх реальні програмно-апаратні реалізації нерідко зазнають загроз, пов'язаних із побічними каналами (side-channel)[1]. Побічні канали можуть надавати додаткову інформацію про внутрішній стан системи внаслідок вимірювання часових затримок, електромагнітного випромінювання, енергоспоживання, шуму тощо. Застосування методів глибинного навчання дозволяє суттєво підвищити ефективність атак на основі побічних каналів, адже нейронні мережі добре справляються з масивними та «зашумленими» даними, виявляючи приховані закономірності.[2]

Основна мета роботи полягає у дослідженні можливостей застосування глибинних нейронних мереж для проведення атак на основі побічних каналів та оптимізації методів виявлення криптографічних витоків. Зокрема, робота має на меті визначити найефективніші архітектури нейронних мереж і методи обробки сигналів, які б дозволили зменшити обсяг необхідних вимірювань, підвищити точність відновлення секретних ключів та сприяти розробці нових методів захисту від подібних атак.

Класичні методи аналізу побічних каналів ґрунтуються на використанні статистичних чи кореляційних підходів (Differential Power Analysis, Correlation Power Analysis тощо)[1]. Вони вимагають ретельної підготовки наборів даних та візуального/евристичного пошуку оптимальних характеристик сигналу. Проте з ускладненням апаратних реалізацій (наприклад, систем на кристалі, які поєднують декілька криптографічних ядер одночасно) та суттєвим зростанням рівня шуму ці підходи стають дедалі менш ефективними. Натомість, використання нейронних мереж надає змогу автоматично виявляти найінформативніші ознаки (features) у сигналах, що дає змогу успішно відтворювати секретні ключі або інші конфіденційні дані з меншими вимогами до попередньої обробки.[3]

Дослідження базується на застосуванні різних підходів машинного навчання. Зокрема, найефективнішими виявилися згорткові (Convolutional Neural Networks, CNN) та рекурентні нейронні мережі (Recurrent Neural

Networks, RNN) у поєднанні з блоками довготривалої короткочасної пам'яті (LSTM)[4]. Для аналізу часових рядів сигналів енергоспоживання (power traces) або електромагнітних коливань пропонується використовувати наступні кроки:

1) Збір та нормалізація сигналів. Здійснюється фіксація сигналів при виконанні криптографічних операцій (наприклад, шифрування блочним алгоритмом AES). Одержані часові ряди підлягають фільтрації для видалення високочастотного шуму та вирівнювання амплітуди.[1] 2) Розмітка даних (labeling). На етапі експерименту відомі ключі або їхні бітові фрагменти, що слугує «підказкою» (ground truth) для supervised-навчання. Кожний сегмент сигналу відповідає певному підключу (subkey). 3) Підбір архітектури нейронної мережі:

- При використанні CNN зручно захоплювати локальні патерни в сигналах, що повторюються;
- RNN/LSTM корисні для відстеження більш тривалих залежностей у часовому ряді;
- Поряд із цим можуть застосовуватися автоенкодери (Autoencoder) для попереднього зменшення шумів та формування стислих репрезентацій сигналу.[3]

4) Навчання і валідація. Навчання здійснюється на наборі сигналів, після чого виконується тестування для оцінки точності відтворення ключа або його фрагментів. Як метрики використовуються точність класифікації, середньоквадратична помилка або середній час на відновлення секретної інформації.[4] 5) Аналіз результатів та оптимізація. Порівняння різних моделей дає змогу визначити найефективнішу для конкретних умов (наприклад, різний тип криптоалгоритму, рівень шуму, апаратна реалізація).

Експерименти свідчать, що при достатньо великому обсязі навчального набору даних глибинні нейронні мережі можуть виявляти закономірності у сигналах з високим рівнем шуму, які лишаються непомітними або слабо помітними для класичних методів кореляційного аналізу.[2] Зокрема, якщо в традиційних методиках потрібно зібрати десятки тисяч вимірювань для надійного відновлення частини ключа, то навчена модель CNN чи RNN здатна досягти бажаних результатів зі значно меншою кількістю вибірок. Застосування нейронних мереж для аналізу побічних каналів посилює загрози для криптографічних систем, оскільки підвищує точність та швидкість відновлення секретної інформації з обмежених або зашумлених даних. Це відкриває шлях до якісно нових контрзаходів: вивчення модельованих нейронними мережами патернів сигналів дає змогу проектувати більш захищені апаратні та програмні рішення.[4] У підсумку, поєднання криптографічних методів із інструментами штучного інтелекту є одним із найважливіших напрямів досліджень у сучасній інформаційній безпеці. Завдяки нейронним мережам аналіз побічних каналів виходить на новий рівень, вимагаючи від розробників складнішої і водночас більш системної протидії потенційним атакам.

1. Kocher P. et al. Differential Power Analysis. Advances in Cryptology — CRYPTO '99, 1999.

2. Peeters E., Standaert F.-X., Quisquater J.-J. Power and electromagnetic analysis: Improved model, consequences and comparisons. Integration, the VLSI Journal, 40(1), 52–60, 2007.
3. Zaid G. et al. Ranking Key Hypotheses in Side-Channel Attacks through Deep Learning. Cryptographic Hardware and Embedded Systems — CHES, 2020.
4. Kim D., Ryu C., Lee K. Efficient Power Analysis Attack Using Deep Learning.

Автоматизоване реагування на кіберінциденти за допомогою ШІ: міф чи реальність сучасних SOC?

УДК 004.056.5:004.08
Петро Поночовний
Державний університет інформаційно-комунікаційних технологій,
petja9186@gmail.com

Інтеграція штучного інтелекту (ШІ) в операційні центри безпеки (SOC) перетворює реагування на інциденти з рутинного процесу на автоматизовану систему, здатну нейтралізувати загрози в реальному часі. Проте ефективність таких рішень залежить від точності алгоритмів, етичних норм та адаптації до динаміки кібератак.

До основних аспектів кібератак належать:

- автоматизація як драйвер ефективності;
- сценарії автоматизованого реагування;
- виклики та обмеження сьогодення.

Давайте розглянемо більш детальніше кожен із цих аспектів. До автоматизації так би мовити драйвера ефективності відносять такі особливості:

- проаналізовані ШІ лог-файли, мережевий трафік та поведінку користувачів для виявлення аномалій (напр., DDoS, фішинг);

- системи на основі машинного навчання, які прогнозують вектори атак, використовуючи історичні дані інцидентів які раніше відбувались (наприклад, аналіз шаблонів атак zero-day) [1].

До сценаріїв автоматизованого реагування відносять такі особливості:

- карантин інфікованих пристроїв, ШІ ізолює вразливі вузли мережі без участі людини;

- блокування IP-адрес, система ідентифікує та блокує підозрілі джерела на основі аналізу трафіку;

- відновлення даних, використання AI для автоматичного відновлення шифрованих файлів після ransomware-атак.

Виклики та обмеження, які постають сьогодні перед фахівцями кібербезпеки:

- помилки алгоритмів, ризик хибних спрацьовувань, що призводять до блокування легальних процесів;

- етична дилема, делегування рішень ШІ порушує питання відповідальності за наслідки;

- адаптація до нових загроз, необхідність постійного оновлення моделей машинного навчання [2].

Щоб більш детальніше зрозуміти автоматизоване реагування та блокування аномалій за участі людини, розглянемо схему Рис. 1 Схема автоматизованого реагування на кіберінциденти з інтеграцією ШІ [3].

Рис. 1 Схема автоматизованого реагування на кіберінциденти з інтеграцією ШІ.

Оглянувши дану схему ми бачимо, що вона складається з наступних блоків, та розгалужень. Першим блоком є збір даних, який в собі уособлює:

- джерела, мережеві логи, дані з EDR/XDR, інформація про загрози (Threat Intelligence);
- інструменти, SIEM-системи (напр., Splunk, IBM QRadar).

Наступним блоком є аналіз та виявлення аномалій (ШІ), який уособлює в собі наступні процеси:

- машинне навчання, класифікація інцидентів (DDoS, фішинг, ransomware);
- аналіз поведінки (UEBA), виявлення відхилень від нормальних шаблонів;
- прогнозування, використання історичних даних для упередження векторів атак.

Наступним блоком є блок прийняття рішень в якому більшу частину роботи виконує ШІ. а саме:

- блокування IP/доменів;
- ізоляція інфікованих пристроїв;
- відновлення backup-даних після атак.

Якщо рівень впевненості ШІ < 90%. то дане рішення перенаправляється до експертів, таким чином вирішуються більш складні та незрозумілі сценарії кіберінцидентів, які іще не відомі для ШІ яка використовується в системі.

Наступним блоком є реагування та відновлення в якому відбувається автоматтизація (SOAR), а саме:

- запуск сценаріїв реагування (напр., видалення шкідливого ПО);
- корекція, оновлення правил фаєрволу на основі аналізу ШІ.

Наступним кроком схеми є зворотній зв'язок та навчання до якого належить:

- оцінка ефективності та аналіз помилок (false positive/negative);
- оновлення моделей ШІ, перетренування алгоритмів на нові дані для ШІ.

Наступним кроком є імітація атак (Red Team), генеративна ШІ (наприклад, GPT-4) для тестування системи. Після чого дані про навчання передаються до блоку аналізу та виявлення аномалій (ШІ) де беруть участь у наступному циклі кіберінцидентів.

Ключовими елементи схеми є:

- гібридний підхід, взаємодія ШІ з аналітиками SOC;
- етичний фреймворк, обмеження для ШІ (наприклад, заборона самостійних контратак);
- безперервний цикл, Дані → Аналіз → Дії → Навчання.

Прикладом використання є сценарій Ransomware-атака, яка протікає за наступним сценарієм:

- ШІ виявляє аномальне шифрування файлів;
- система автоматично ізолює інфікований пристрій та відновлює дані з backup;
- експерт отримує сповіщення для аналізу логів та перевірки ефективності дій;
- модель ШІ оновлюється з урахуванням нових даних про атаку.

Автоматизоване реагування на інциденти — це не міф, а еволюційний крок для SOC. ШІ дозволяє зменшити час реакції з годин до секунд, але його успіх залежить від балансу між технологіями, етикою та людським фактором. Майбутнє належить гібридним системам, де ШІ і фахівці працюють синергійно.

Схема яка представлена в даній тезі підкреслює, що автоматизація на основі ШІ — це не заміна людей, а інструмент для підвищення швидкості та точності роботи SOC.

Рекомендації для впровадження:

- гібридний підхід, комбінувати автоматизацію з аналізом експертів для критичних інцидентів;
- розробка етичних стандартів, чіткі правила для ШІ у сфері кібербезпеки (наприклад, заборона на самостійні контратаки).
- використання генеративних моделей (на кшталт GPT-4) для імітації атак і тренування систем.

1. Ponochovny P. LOW-SPEED HTTP DDOS ATTACK PREVENTION MODEL FOR END USERS. Cybersecurity: Education, Science, Technique. 2024. Vol. 2, no. 26. P. 291–304. URL: https://doi.org/10.28925/2663-4023.2024.26.695

2. Redbooks I. Understanding SOA Security Design and Implementation: February 2007. Vervante, 2007. 408 p.

2. Swapnil Chawande. AI-driven threat modeling for critical infrastructure. World Journal of Advanced Engineering Technology and Sciences. 2024. Vol. 13, no. 1. P. 1142–1155. URL: https://doi.org/10.30574/wjaets.2024.13.1.0476

Етичний хакінг як інструмент проактивної оцінки захищеності

УДК 004.056.5:004.08

Денис Поршнев
Державний університет інформаційно-комунікаційних технологій,
d.porshnev@stud.duikt.edu.ua

У сучасному середовищі кіберзагроз, що швидко розвивається, організації стикаються з дедалі складнішими проблемами щодо захисту своїх цифрових активів від складних кібератак. Операційні центри безпеки (SOC) служать передовою обороною від цих загроз, використовуючи вдосконалені механізми моніторингу, виявлення та реагування для захисту критично важливих систем і даних.

Однак одних тільки традиційних заходів безпеки недостатньо проти сучасних ворогів, які постійно вдосконалюють свої методи атаки. Етичне хакерство, також відоме як тестування на проникнення або хакерство білих капелюхів, яке стало вирішальним підходом до зміцнення операцій SOC шляхом активного виявлення слабких місць у безпеці до того, як зловмисники зможуть ними скористатися.

Однією з головних переваг етичного хакерства в операціях SOC є його здатність виявляти вразливі місця системи безпеки до того, як ними скористаються зловмисники. Традиційні заходи кібербезпеки часто зосереджуються на реагуванні на кіберінциденти, але етичне хакерство зміщує підхід до проактивного виявлення загроз.

Виявляючи вразливості на ранній стадії, організації можуть виправити недоліки безпеки, посилити захист і зменшити ризики до того, як станеться фактична кібератака. Цей проактивний підхід підвищує загальну безпеку та значно знижує ймовірність витоку даних, атак програм-вимагачів і несанкціонованого доступу до системи [1].

Імітуючи кібератаки в реальному світі, етичні хакери допомагають організаціям виявити слабкі місця до того, як зловмисники зможуть ними скористатися, тим самим підвищуючи загальні можливості виявлення загроз і реагування на інциденти.

Етичне хакерство відіграє життєво важливу роль у підвищенні ефективності SOC, надаючи командам безпеки практичну інформацію про потенційні вектори атак. Завдяки оцінці вразливості, вправам для об'єднання червоних команд і безперервному тестуванню безпеки етичні хакери допомагають аналітикам SOC у визначенні пріоритетів ризиків і зміцненні критичних активів [2].

Інструменти етичного хакерства на основі штучного інтелекту ще більше покращують виявлення загроз, автоматизуючи сканування вразливостей, аналізуючи мережевий трафік і виявляючи аномалії в реальному часі. Інтеграція штучного інтелекту та автоматизації в етичне хакерство революціонізувала спосіб виявлення та пом'якшення вразливостей безпеки.

Інструменти тестування на проникнення на основі ШІ можуть аналізувати величезні обсяги даних, виявляти аномалії та автоматизувати повторювані завдання безпеки, скорочуючи час, необхідний для оцінки вразливості.

Крім того, керовані ШІ інструменти етичного хакерства можуть проводити безперервне тестування безпеки, забезпечуючи захист організацій від нових загроз. Використовуючи AI-керований автоматизації, команди SOC можуть оптимізувати зусилля з етичних хакерів, покращити видимість загроз і підвищити загальну стійкість кібербезпеки.

Незважаючи на свої переваги, етичне хакерство створює проблеми, зокрема юридичні та етичні міркування, дотримання нормативних вимог і ризик ненавмисних збоїв під час тестування на проникнення. Організації повинні впроваджувати структуровані програми етичного хакерства з чіткими вказівками, авторизованими середовищами тестування та співпрацею між етичними хакерами та командами SOC.

Крім того, безперервне навчання та обмін інформацією про загрози є важливими для того, щоб спеціалісти з безпеки випереджали нові кіберзагрози [3].

Таким чином, роль етичного хакерства в операціях SOC продовжуватиме розвиватися, інтегруючи передові технології, такі як штучний інтелект (ШІ), машинне навчання та автоматизація, щоб покращити можливості тестування безпеки. Інструменти етичного хакерства на основі штучного інтелекту забезпечать безперервну оцінку безпеки, виявлення аномалій у реальному часі та прогнозування загроз, що ще більше зміцнить захист SOC.

Оскільки кіберзагрози стають все більш витонченими, етичне хакерство залишатиметься наріжним каменем стійкості кібербезпеки, надаючи можливість організаціям передбачати, виявляти і нейтралізувати загрози до того, як вони завдадуть значної шкоди. Взявши етичне хакерство як важливу практику безпеки, організації можуть побудувати міцнішу та адаптивнішу структуру кібербезпеки, яка захищає їхні критично важливі активи у все більш цифровому та взаємопов’язаному світі.

1. The Role of Ethical Hacking in Strengthening SOC Operations for Proactive Threat Detection. Hasher Malik, Frank Blaser December, 2024

2. Falowo O. I., Botsyoe L., Koshoedo K., Ozer M. (2024). Enhancing cybersecurity with artificial immune systems and general intelligence: A new frontier in threat detection and response. IEEE Access.

3. Grata E. G., Deshpande A., Lopes R. T., Laghari A. A., Khan A. A., Jenice Aroma R., Jumani, A. K. (2024). Artificial intelligence for threat anomaly detection using graph Data bases a semantic outlook. Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection, 249-278.

Дослідження відеореєстраторів в рамках судової комп'ютерно-технічної експертизи

УДК 343.983

Роман Пташкін[1], Володимир Палагін[2]
[1]Черкаський науково-дослідний експертно-криміналістичний центр Міністерства внутрішніх справ України, [2]Черкаський державний технологічний університет,
[1]ptashkin@ndekc.ck.ua, [2]palahin@ukr.net

Судова комп'ютерно-технічна експертиза за експертною спеціальністю 10.9 «Дослідження комп'ютерної техніки та програмних продуктів» належить до класу інженерно-технічних експертиз і охоплює дослідження апаратного та програмного забезпечення цифрових пристроїв. Її об'єктом є електронні носії інформації, комп'ютери, портативні пристрої, мережеве обладнання та програмні продукти, що використовуються для збирання, обробки, зберігання або передавання цифрових даних. Метою експертизи є встановлення обставин, що мають значення для кримінального, цивільного або адміністративного провадження, зокрема фактів наявності, змісту, способу обробки чи видалення інформації, що зберігалася або передавалася за допомогою відповідних засобів [1]. Підготовка та проведення таких експертиз здійснюється відповідно до вимог законодавства України, методичних матеріалів Експертної служби МВС та інших суб'єктів судово-експертної діяльності, із дотриманням принципів законності, об'єктивності та повноти.

Метою цього дослідження є узагальнення відомостей, отриманих у ході експертної практики при дослідженні відеореєстраторів, для їх подальшого використання під час підготовки методичних матеріалів, розробки алгоритмів дослідження носіїв інформації та підвищення ефективності виявлення цифрових доказів у судовій практиці.

Відеореєстратори, які підлягають дослідженню у межах цієї експертизи, є пристроями цифрового запису відеоінформації, які часто використовуються в автомобілях, охоронних системах або побутовому спостереженні. У практиці судової експертизи об'єктом дослідження вважається не стільки сам відеореєстратор, скільки його носій інформації – флеш-карта, жорсткий диск або вбудована пам'ять [2]. Основною цінністю відеореєстратора є саме накопичувач даних, де зберігається відеоінформація про зафіксовані події, що можуть мати доказове значення.

У процесі дослідження носіїв інформації, вилучених з відеореєстраторів, судовий експерт насамперед стикається з особливостями використаних файлових систем. Більшість сучасних відеореєстраторів використовують власні або спеціалізовані файлові системи. Однією з найпоширеніших є DHFS, яка застосовується в пристроях компаній, що спеціалізуються на виробництві обладнання для відеоспостереження [2,3]. Ця файлова система не підтримується операційними системами загального призначення, що ускладнює доступ до відеозаписів без використання спеціалізованого програмного забезпечення. Окрім DHFS, існує низка подібних пропрієтарних форматів, зокрема PFS (Private File System), MODD, а також адаптовані версії стандартних структур із модифікаціями. Тобто пропрієтарні файлові системи становлять окрему

складність, адже вони не документовані, їх структура закрита, що унеможливлює прямий доступ без використання спеціалізованого програмного забезпечення.

Оскільки більшість відеореєстраторів працюють у циклічному режимі запису, старі файли автоматично видаляються для звільнення простору під нові. У результаті цього можуть бути втрачені критично важливі відеофрагменти. Експерт повинен ураховувати, що після вилучення пристрою будь-які подальші спроби його використання можуть призвести до часткового перезапису інформації, що зменшує обсяг відновлюваних даних.

Під час аналізу накопичувачів інформації з відеореєстраторів використовуються як традиційні методи файлового дослідження, так і інструменти глибокого аналізу структури даних. Для автоматизованого виявлення та вилучення відеозаписів із носіїв інформації, що використовуються у відеореєстраторах, судові експерти широко застосовують спеціалізоване програмне забезпечення.

Одним із найефективніших інструментів є Magnet DVR Examiner. Це програмне забезпечення дозволяє досліджувати накопичувачі навіть у випадках, коли сам пристрій недоступний або несправний. Перевагою DVR Examiner є можливість роботи з понад 70 типами пропрієтарних файлових систем, зокрема DHFS, PFS та іншими, які типовими методами операційні системи не розпізнають [2,3]. Програма здійснює автоматичне сканування носія, виявляє фрагменти відеофайлів, метадані, часові мітки та дозволяє здійснювати експорт відео у форматах, придатних для перегляду.

Для аналізу вмісту звичайних файлових систем, зокрема exFAT, які зустрічаються на microSD-картах, ефективним інструментом залишається FTK Imager від AccessData. Хоча FTK Imager не підтримує пропрієтарні файлові системи відеореєстраторів, його використання доцільне у випадках, коли накопичувач формально сумісний із файловими системами, які розпізнаються традиційними засобами.

Таким чином, дослідження відеореєстраторів у межах судової комп'ютерно-технічної експертизи базується на сучасних принципах цифрової криміналістики, що включають ідентифікацію, збереження, аналіз і представлення електронних доказів. Основною цінністю таких пристроїв є інформація, зафіксована на носіях, яка у разі правильного поводження з цифровими доказами може бути відновлена, ідентифікована та використана у судовому процесі.

1. Шепітько В. Ю., Шепітько М. В., Латиш К. В., Демидова Є. Є., Капустіна М. В. Вступ до цифрової криміналістики. Харків: Право, 2025. 124 с.;

2. Handbook of Digital Forensics of Multimedia Data and Devices / Ed. Anthony T. S. Ho. – Wiley, 2020. – 670 p.;

3. Forensic Video Analysis: A Complete Guide – 2021 Edition. – The Art of Service, 2021. – 304 p.

Роль OSINT у виявленні та нейтралізації інформаційної зброї

УДК 327.8:004.056.55
Дмитро Рабчун[1], Діана Примаченко[2]
Державний університет інформаційно-комунікаційних технологій,
[1]rabchundima92@gmail.com, [2]d.prymachenko@duikt.edu.ua

Інформаційне протиборство стало невід'ємною складовою гібридних конфліктів. Одним із ключових інструментів у боротьбі з інформаційною агресією є OSINT (Open Source Intelligence) — розвідка на основі відкритих джерел. Цей підхід дозволяє ефективно виявляти, аналізувати та нейтралізувати дезінформацію та інші форми інформаційної зброї. OSINT охоплює збір та аналіз інформації з відкритих джерел, таких як соціальні мережі, новинні ресурси, супутникові знімки та інші публічні дані. Цей метод став особливо актуальним у контексті сучасних конфліктів, де інформація відіграє стратегічну роль.

Під час війни в Україні OSINT відіграв ключову роль у викритті та спростуванні російської дезінформації. Наприклад, організація Bellingcat використовувала відкриті джерела для розслідування обставин збиття рейсу MH17 та інших інцидентів, пов'язаних з агресією Росії. Також українська волонтерська спільнота InformNapalm активно застосовує OSINT для ідентифікації російських військових та документування воєнних злочинів. Їх робота демонструє, що навіть без доступу до секретної інформації можна встановити факти та відповідальність агресора [1].

Сучасні технології значно розширили можливості OSINT. Платформи на кшталт DISINFOX дозволяють структурувати та аналізувати інциденти дезінформації, використовуючи стандарти STIX2 та DISARM TTPs. Крім того, використання супутникових знімків, аналізу трафіку в реальному часі та інших цифрових інструментів забезпечує оперативне реагування на інформаційні загрози [2].

Такі технології перетворюють OSINT на системну аналітичну практику, яка може застосовуватись як у військових структурах, так і в журналістиці та правозахисній діяльності.

В Україні використання OSINT стало особливо масовим після 2014 року, коли почалась російська агресія проти Криму та Донбасу. Добровольці, журналісти, ІТ-фахівці та аналітики об'єднали зусилля, щоб викривати фейки, документувати військову присутність РФ, спростовувати ворожу пропаганду. Одним з яскравих прикладів стало використання геолокації знімків, метаданих, соціальних профілів для підтвердження пересування техніки, ідентифікації солдатів та виявлення їх участі у бойових діях.

Поширення фейкової інформації є одним із ключових методів ведення інформаційної війни. Зокрема, Росія активно використовує багаторівневу мережу сайтів, телеграм-каналів та ботів для впливу на свідомість як українських громадян, так і західної аудиторії.

У таких умовах OSINT відіграє роль своєрідного щита — інструменту швидкої верифікації новин, перевірки джерел та виявлення аномалій у наративі. Це дозволяє не тільки виявляти фейки, а й відслідковувати шляхи їх поширення, джерела фінансування та організаторів інформаційних кампаній.

Серед інструментів OSINT, які використовуються як у професійному, так і у волонтерському середовищі, варто відзначити Maltego, SpiderFoot, Shodan, а також сервіси аналізу метаданих та відкритих супутникових зображень (табл.1). Їх поєднання дозволяє створити комплексний портрет об'єкта розслідування — від IP-адрес і цифрових слідів до географічного положення та зв'язків між учасниками інформаційних атак. Такі дані нерідко стають підґрунтям для кримінальних справ або офіційних звітів міжнародних організацій [3].

Таблиця 1

Порівняння OSINT-інструментів

Назва	**Призначення**	**Джерела**	**Сфера використання**
Maltego	Візуалізація зв'язків	WHOIS, DNS, соцмережі	Кіберрозвідка, OSINT
SpiderFoot	Автоматизований збір OSINT	IP, домени, email	Автоматизований моніторинг
Shodan	Сканування пристроїв	IP-адреси, порти	Кібербезпека

Особливої уваги заслуговує взаємодія між OSINT-спільнотами та державними структурами. У багатьох випадках волонтерські OSINT-ініціативи виявляють загрози раніше, ніж це роблять офіційні служби. Однак така взаємодія вимагає правових механізмів, які б регулювали передачу та обробку даних, захищали джерела інформації та гарантували її використання винятково в законний спосіб. Україна, наприклад, поступово впроваджує відповідні механізми співпраці між СБУ, Мінцифри, ЗСУ та громадськими OSINT-групами.

Окрім безпосередньої протидії фейкам, OSINT застосовується і в стратегіях контрнаративу — формування альтернативних, правдивих інформаційних потоків, що спростовують ворожі наративи. Це можуть бути як візуальні кейси з доказами, так і мультимедійні формати, які легко поширюються у соцмережах.

Ефективне використання OSINT можливе лише за умов високої цифрової грамотності користувачів. Це ставить перед державою і громадянським суспільством завдання з навчання, просвітництва та підвищення загальної інформаційної культури.

1. Akhgar B. OSINT as an integral part of the national security apparatus. Open source intelligence investigation. Cham, 2016. P. 3–9. URL: https://doi.org/10.1007/978-3-319-47671-1_1

2. Korystin O. E., Svyrydiuk N. P. Foreign Experience in the Anti-Terrorist Use of OSINT. *Uzhhorod national university herald. series: law*. 2024. Vol. 2, no. 82. P. 177–181. URL: https://doi.org/10.24144/2307-3322.2024.82.2.28

3. Staniforth A. Open source intelligence and the protection of national security. *Open source intelligence investigation*. Cham, 2016. P. 11–19. URL: https://doi.org/10.1007/978-3-319-47671-1_2

Використання OSINT для захисту персональних даних

УДК 004.056.5:004.738.5:342.7

Михайло Різак[1], Олександр Котик[2]
ДУ «Київський авіаційний інститут»,
[1]mykhailo.rizak@npp.kai.edu.ua, [2]kotyk.oleksandr.81@gmail.com

У сучасному цифровому середовищі персональні дані стали об’єктом постійних загроз з боку кіберзлочинців. Одним із ефективних методів як атак, так і захисту є OSINT (Open Source Intelligence) – розвідка на основі відкритих джерел. Технології OSINT широко застосовуються не лише злочинцями, а й фахівцями з інформаційної безпеки для виявлення витоків даних, оцінки цифрового сліду користувачів та посилення кіберзахисту. В умовах зростаючих вимог GDPR щодо конфіденційності персональної інформації особливо актуальним є використання OSINT для превентивного виявлення ризиків і зменшення потенційних загроз.

Метою даної роботи є дослідження можливостей використання інструментів OSINT для виявлення вразливостей, які можуть призвести до втрати або витоку персональних даних, а також демонстрація їх потенціалу в підвищенні рівня захисту інформації в організаціях та у приватному секторі.

Питання використання OSINT в інформаційній безпеці активно обговорюється в науковій та прикладній літературі. Зокрема, у роботі [1] розглядаються практичні аспекти використання OSINT для збору інформації з відкритих джерел, підкреслюючи важливість анонімності та правових аспектів. Інше дослідження [2] акцентує увагу на ризиках, пов'язаних із використанням OSINT зловмисниками для збору персональних даних та доксингу. Окрема увага приділяється питанням інтеграції OSINT в системи кіберзахисту підприємств, зокрема, через виявлення цифрового сліду, ризиків соціальної інженерії та витоків даних. У публікаціях останніх років також аналізується досвід застосування OSINT у військовій сфері, зокрема під час повномасштабної агресії проти України, що підтверджує ефективність інструментів відкритої розвідки як для оборони, так і для безпеки цивільного сектору.

OSINT – це метод збору та аналізу інформації з відкритих джерел: вебсайтів, соціальних мереж, форумів, даркнету тощо. Для захисту персональних даних OSINT використовується в кількох напрямках:

1) виявлення витоків інформації. Наприклад, за допомогою сервісу Have I Been Pwned [3] можна перевірити, чи були зламані облікові записи або електронна пошта;

2) аналіз цифрового сліду. Інструменти на кшталт Maltego або SpiderFoot дозволяють зібрати дані про особу або організацію та виявити потенційно небезпечну інформацію, що публічно доступна [4,5];

3) оцінка ризиків соціальної інженерії. Google Dorking дає змогу знайти відкриті конфіденційні файли, логіни, бази даних, які не були належним чином захищені;

4) інформаційна обізнаність. Демонстрація даних, зібраних OSINT-інструментами, використовується під час навчання персоналу щодо цифрової безпеки;

5) автоматизація. Recon-ng та SpiderFoot автоматизують збір OSINT-даних та можуть бути інтегровані у внутрішні системи моніторингу загроз [6].

Окрему увагу у межах OSINT слід приділити аналізу метаданих документів. Метадані – це службова інформація, яка автоматично додається до файлів (текстових документів, PDF, зображень тощо) і може містити імена авторів, геолокацію, час створення, шляхи збереження файлу. Нерідко саме ці дані дозволяють ідентифікувати особу чи організацію, що створила документ. Наприклад, зображення з вбудованими EXIF-даними можуть містити GPS-координати зйомки. Такі метадані є об'єктом першочергової уваги як з боку атакуючих, так і фахівців із захисту. Видалення метаданих перед публікацією або передаванням документів, а також використання спеціального ПЗ (ExifTool, MAT2 тощо) значно знижує ризики витоку персональних даних.

Застосування OSINT у контексті захисту дозволяє організаціям:

- моніторити витоки персональних даних у реальному часі;
- виявляти сторонні ресурси, де згадуються співробітники чи клієнти;
- оцінювати рівень ризику, пов’язаний із відкритими джерелами інформації;
- вдосконалювати політики конфіденційності та інформування.

Однак важливо підходити до збору даних етично й відповідно до чинного законодавства, зокрема статей 5 і 6 Регламенту GDPR.

OSINT є потужним інструментом не лише для атак, але й для побудови ефективної стратегії захисту персональних даних. Його грамотне застосування дозволяє організаціям своєчасно виявляти витоки, аналізувати цифрову експозицію та формувати обґрунтовану відповідь на потенційні інциденти безпеки. Розширене використання OSINT-інструментів сприяє реалізації принципу превентивного захисту, що є основою сучасного підходу до конфіденційності.

1. Використання інструментів та методів OSINT для отримання пошукової інформації :практичний порадник / Зоренко Д. С., Лех Р. В., Кулик Д. О., Червяков О. І. Х.: ІПЮК для СБУ, 2023. 36 с.

2. Главацька, А., Ангельська , О., Опірський, І. Дослідження технології використання OSINT як нової загрози з деанонімізації особи в інтернет просторі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024, 1(25), С. 19–50. URL: https://doi.org/10.28925/2663-4023.2024.25.1950.

3. Have I Been Pwned. URL: https://haveibeenpwned.com (дата звернення: 20.04.2025).

4. Maltego. URL: https://www.maltego.com/ (дата звернення: 20.04.2025).

5. SpiderFoot. OSINT Automation Tool. URL: https://www.spiderfoot.net (дата звернення: 20.04.2025).
6. GitHub-репозиторій Recon-ng. URL: https://github.com/lanmaster53/recon-ng (дата звернення: 20.04.2025).

Ключові технології кібербезпеки хмарного середовища

УДК 004.056.5:004.08
Артем Роженко[1], Ігор Аверічев[2]
Державний університет інформаційно-комунікаційних технологій,
[1]a.rozhenko@stud.duikt.edu.ua, [2]iaverichev19@gmail.com

З розвитком цифрових технологій та збільшенням доступу до Інтернету, організації стають вразливими до різних видів кібератак та мережевим вторгненням. Поширені проблеми включають складність розуміння, обмеження в роботі з масивними наборами даних, тривалий час обробки, значні вимоги до зберігання та підвищений рівень помилок.

Хмарні обчислення в Інтернеті речей (IoT) виникли як революційна парадигма, яка глибоко вплинула на безліч сфер, включаючи системи охорони здоров'я, військові програми, освіту тощо. Його привабливість походить від притаманної йому економічності та надзвичайної надійності, що дозволяло організаціям масштабувати свої операції з безпрецедентною гнучкістю. Однак із зростанням залежності від хмарної інфраструктури виникла зловісна та постійна загроза кібератак [1]. Постійні кібератаки та мережеві вторгнення на цифрову інфраструктуру порушують нормальну роботу системи, здійснюючи зловмисні дії, що порушують цілісність даних, конфіденційність, доступність і конфіденційність.

У відповідь на цю зростаючу загрозу посилення безпеки хмарних мереж стало першорядним. Зважаючи на ці виклики, у центрі уваги цього дослідницького заходу – сприяти розробці оптимізованої, зручної стратегії захисту хмарних систем від кіберзагроз. Використовуючи силу інновацій, мета полягає в тому, щоб подолати розрив між зростаючою складністю сучасних кіберзагроз і потребою в ефективних, зрозумілих і ефективних рішеннях безпеки для хмарних екосистем [2].

Крім того, хмарні обчислення надають послуги в Інтернеті, які стали широко використовуваною технологією. Модель хмарних обчислень розвинулась із технології віртуалізації, розподілених обчислень, службових обчислень та інших комп'ютерних технологій, щоб забезпечити функції доступності та масштабованості для великих програм корпоративного рівня. Він також пропонує послуги для віртуальних машин, призначених через значний пул фізичних ресурсів.

Хмарні обчислення пропонують кілька переваг для різних хмарних моделей на основі тенденцій безпеки та проблем. А саме включаючи зниження витрат, спільне використання та налаштування обчислювальних ресурсів, обслуговування на вимогу, а також високу гнучкість і масштабованість, швидке керування, економічна продуктивність, велика ємність пам'яті та переваги швидкого доступу до кінцевих пристроїв у будь-який час і всюди [3].

Перелічимо п’ять життєво важливих особливостей хмарних обчислень включають самообслуговування на вимогу, розширений доступ до мережі, об’єднання ресурсів, високошвидкісну відмовостійкість і вимірювані послуги. Ці переваги спонукають великі компанії переносити свою IT-інфраструктуру в хмарне середовище [4].

Для надійних послуг хмарні обчислення мають бути захищені для даних користувачів. Хмарні обчислення стикаються з кількома типовими хмарними ризиками, такими як зловживання даними, зловмисники, незахищені інтерфейси, точки доступу, спільні технологічні проблеми, втрата даних і викрадення. Тому точне розуміння хмарної безпеки є фундаментальною вимогою для успішного розгортання хмарних обчислень.

Різні типи атак ускладнюють хмарним провайдерам і адміністраторам розгортання можливих рішень, необхідних клієнтам [4]. Це пояснюється тим, що різні атаки пов’язані з різними загрозами, де важливість ризиків змінюється залежно від потреб безпеки інших клієнтів, які використовують хмарні служби.

Таким чином, адміністратори безпеки оцінять і впровадять механізми безпеки, щоб відповідати основним вимогам безпеки як постачальників послуг. Однак безпеку можна покращити, оскільки на практиці практично неможливо налаштувати повністю безпечну систему [5]. Отже, необхідно знайти загрози безпеці, а потім відповідні рішення, такі як підзвітність, автентифікація та збереження конфіденційності.

Однак багато питань безпеки заважають прийняттю хмарних обчислень. Тому існує гостра потреба в рішеннях безпеки для боротьби з різними загрозами безпеці в хмарних обчисленнях.

1. Halim, Z.; Sulaiman, M.; Waqas, M.; Aydın, D. Deep neural network-based identification of driving risk utilizing driver dependent vehicle driving features: A scheme for critical infrastructure protection. J. Ambient. Intell. Humaniz. Comput. 2023, 14, 11747–11765. [Google Scholar] [CrossRef].

2. Butt, U.A.; Amin, R.; Mehmood, M.; Aldabbas, H.; Alharbi, M.T.; Albaqami, N. Cloud security threats and solutions: A survey. Wirel. Pers. Commun. 2023, 128, 387–413. [Google Scholar] [CrossRef].

3. Falowo O.I., Botsyoe L., Koshoedo K., Ozer M. (2024). Enhancing cybersecurity with artificial immune systems and general intelligence: A new frontier in threat detection and response. IEEE Access.

4. Nafea, R.A.; Almaiah, M.A. Cyber security threats in cloud: Literature review. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 779–786. [Google Scholar].

5. Alotaibi, A.F. A comprehensive survey on security threats and countermeasures of cloud computing environment. Turk. J. Comput. Math. Educ. (TURCOMAT) 2021, 12, 1978–1990. [Google Scholar].

Створення криптографічного ключа на основі протоколу BIP-39

УДК 621.395.7 (043.2)

Кирило Росінський[1], Олена Головачова[2]
Національний університет «Одеська політехніка»,
[1]9560425@stud.op.edu.ua, [2]holovachova@op.edu.ua

Криптографічний ключ – базове поняття у криптографії, яке відіграє важливу роль у забезпеченні конфіденційності та цілісності інформації. Його можна розглядати як унікальну послідовність символів або бітів, яка використовується в процесах шифрування та дешифрування даних. Метою дослідження є створення міцного криптографічного ключа на основі протоколу BIP-39, який хоч і орієнтований на захист криптогаманців, проте сам алгоритм створення криптографічного ключа може використовуватися і у інших системах.

Головна його мета перетворити випадкову послідовність бітів у мнемонічну фразу для легшого запам'ятовування людиною.

Загальна схема алгоритму створення ключа через BIP-39 наведена на рисунку 1.

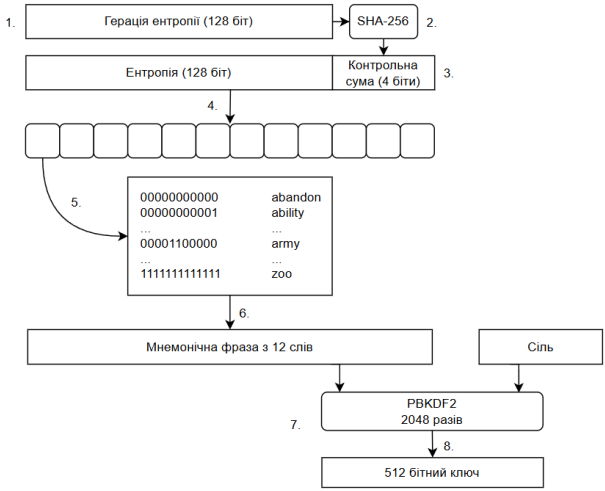


Рис 1. Загальна схема алгоритму створення ключа через BIP-39

Створення ключа за протоколом BIP-39 відбувається наступним чином:

1) Створюється випадкова послідовність з 128 до 256 біт з кроком у 32 біти.

2) Використовується хеш-алгоритм SHA-256 на випадковій послідовності для генерації хеш-значення та беруться перші N біт цього хеш-значення, які є результатом ділення довжини ентропії на 32, як контрольну суму ентропії.

3) Додається контрольна суму до кінця випадкової послідовності.

4) Розділюється випадкова послідовність на 12 сегментів розміром 11 біт.

5) За спеціальним словником, який покриває усі можливі значення сегментів, обираються слова відповідно значенню кожного сегменту.

6) Кінцева група слів згенерована у послідовності є мнемонічною фразою.

7) Отримана мнемонічну фразу використовується як пароль у алгоритмі PBKDF2 та як «сіль» – значення, яке додається до пароля, змінюючи процес генерації хешу – фразу, комбіновану з «mnemonic» та мнемонічної фрази.

8) У результаті виходить ключ розміром у 512 біт.

Для забезпечення підвищеного захисту є варіант додатково обробити ключ за допомогою алгоритму Argon2 – сучасної функції похідного ключа, яка спеціально розроблена для протидії атакам типу грубої сили та захищає від атак з використанням високопродуктивних обчислювальних пристроїв, таких як GPU та FPGA, враховуючи обсяг оперативної пам'яті, тривалість обчислень і ступеня паралелізму, що дозволяє чітко налаштувати рівень захисту відповідно до можливостей системи.

Створення криптографічного ключа за допомогою Argon2

1) Алгоритм спочатку створює початковий блок, використовуючи вхідні значення, отримані від користувача, такі як пароль і сіль. Цей початковий блок заповнює послідовність блоків, використовуючи пам'ять.

2) Алгоритм заповнює ці блоки пам'яті до встановленого обсягу пам'яті. Обчислення кожного блоку залежить від попередніх блоків, що робить цей етап залежним від даних.

3) Після заповнення всіх блоків алгоритм вибирає один блок як останній.

4) Алгоритм передає останній блок хеш-функції для генерації остаточного хешу пароля.

Припустимо, обладнання для злому виконуватиме один хеш за 10^{-6} секунди.

Мнемонічна фраза, яка складається з 24 слів, матиме ентропію у 256 бітів, отже матиме наступну кількість комбінацій:

$$N = \frac{2^{256}}{2} = 2^{255} \approx 5,79 \cdot 10^{76} \quad (1)$$

Час, який знадобиться на обробку такої кількості комбінацій, наведений у наступному обчисленні:

$$T_{роки} = \frac{N \cdot t}{t_{рік}} \approx \frac{5,79 \cdot 10^{76} \cdot 10^{-6}}{3,154 \cdot 10^{7}} \approx \frac{5,79 \cdot 10^{70}}{3,154 \cdot 10^{7}} \approx 1,84 \cdot 10^{63} \text{ років}, \quad (2)$$

де N – кількість комбінацій, t – час обчислення на один хеш,

$t_{рік}$ – кількість секунд у році.

Отже, для злому мнемонічної фрази, яка складається з 24 слів та оброблена алгоритмом Argon2, знадобиться $1,84 \cdot 10^{63}$ років, що є практично неможливим.

1. Palatinus M., Rusnak P., Voisine A., Bowe S., Mnemonic code for generating deterministic keys. *Github*. URL: https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki.

2. Eum S., Kim H., Song M., Seo H. Optimized Implementation of Argon2 Utilizing the Graphics Processing Unit. *Applied Sciences*. 2023; 13(16):9295. URL: https://doi.org/10.3390/app13169295.

Протидія засобам радіоелектронної боротьби у логістичних безпілотних апаратах шляхом застосування когнітивного радіо

УДК 621.396

Сергій Семендяй
Національний університет "Чернігівська політехніка",
serhiisemendiai@icloud.com

Стрімкий розвиток виробництва безпілотних літальних апаратів (БпЛА), спровокований війною в Україні, став одним із ключових чинників трансформації сучасного поля бою. Використання БпЛА значною мірою змінює хід бойових дій, впливаючи на значення традиційних родів військ та зумовлюючи перегляд доктрин застосування артилерії, розвідки, засобів протиповітряної оборони тощо.

Одночасно спостерігається стрімкий розвиток засобів радіоелектронної боротьби (РЕБ), призначених для виявлення, пригнічення та перехоплення каналів управління дронами [1]. Проте, наявні військові комплекси РЕБ демонструють вразливість до новітніх тактик, включно із використанням маневрових БпЛА та автономних роїв [2]. На практиці все більше застосовуються малі мобільні комплекси, пристосовані до роботи в умовах позиційної війни – так звані «окопні РЕБ» [3].

Однією з найперспективніших загроз стає застосування РЕБ-дронів – спеціалізованих безпілотних платформ, здатних наближатися до цільових дронів-жертв на мінімальну відстань для глушіння їх каналів зв'язку за допомогою низькопотужних завад, що ускладнює їх виявлення навіть сучасними системами радіотехнічної розвідки.

Метою цього дослідження є обґрунтування необхідності впровадження технологій когнітивного радіо (CR) та програмно визначеного радіо (SDR) в логістичні БпЛА з метою забезпечення високої стійкості каналів керування до впливу засобів РЕБ, зокрема у випадках атак із використанням РЕБ-дронів.

Актуальність проблематики зумовлена не лише воєнними потребами. Передбачається, що після закінчення активної фази війни набуті технології та досвід боротьби з дронами будуть використані кримінальними структурами у всьому світі для здійснення крадіжок цінних логістичних БпЛА або їх пограбування. Застосування мініатюрних РЕБ-дронів дозволить зловмисникам легко нейтралізувати канали керування дронів-жертв, при цьому залишаючись непомітними для правоохоронних органів.

Наукова новизна роботи полягає у розробці концептуально нових підходів до забезпечення стійкості радіоканалу керування (РКК) безпілотних літальних апаратів в умовах активного застосування засобів РЕБ. Запропоновано адаптивні алгоритми динамічного вибору параметрів РКК, що передбачають автоматичне коригування частоти, ширини смуги пропускання, типу модуляції, структури кадру та часових характеристик сигналу на основі безперервного моніторингу радіочастотного середовища в зоні польоту БпЛА. Такі алгоритми поєднуються з використанням технологій SDR та CR, що забезпечує гнучкість та інтелектуальне переналаштування параметрів каналу в реальному часі.

Особливістю підходу є повторне використання радіочастотного спектра відповідно до погодженої сітки частот, дозволеної для використання в умовах

надзвичайних ситуацій, загроз або активного застосування засобів РЕБ. Така сітка має бути попередньо узгоджена з відповідними уповноваженими органами у сфері управління спектром радіочастот. У поєднанні з вбудованими засобами спектрального аналізу та базою пріоритетів, адаптивна система приймає рішення щодо вибору або зміни робочого частотного каналу, з урахуванням інтенсивності завад, правового статусу частоти, рівня потенційної загрози та ризику втрати керування.

Застосування розроблених підходів дозволяє реалізувати принцип «радіоспектрової маневровості» логістичних БпЛА, що значно підвищує їхню живучість і ускладнює ефективне придушення зі сторони засобів РЕБ, зокрема малопотужних РЕБ-дронів, які діють приховано на близькій відстані. У процесі дослідження запропоновано архітектуру модульної системи радіоелектронного захисту логістичних БпЛА (рис. 1).

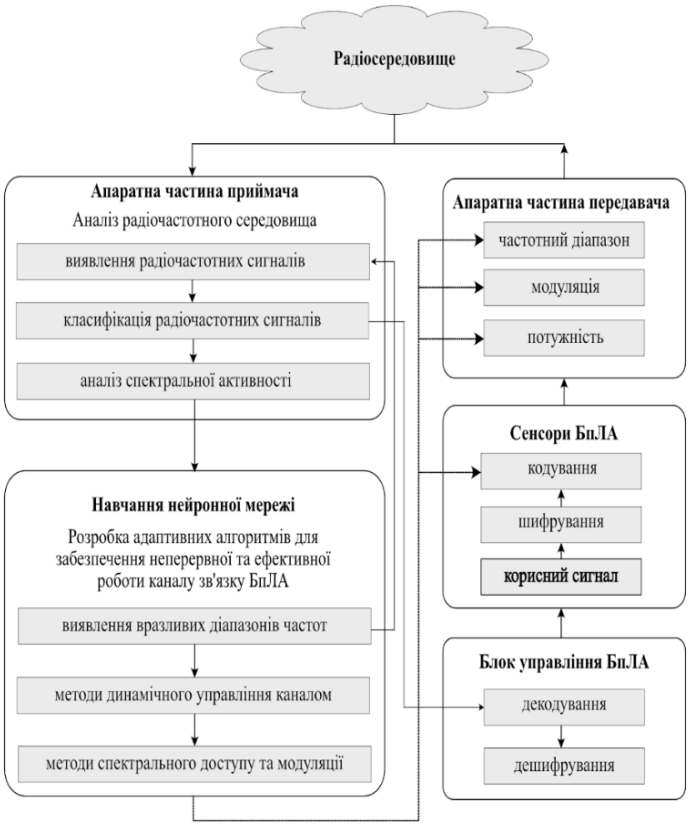


Рис.1. Система радіоелектронного захисту БпЛА

Вона включає: блоки спектрального моніторингу, когнітивного аналізу ризиків, прийняття рішень на основі машинного навчання та блоки динамічного переналаштування радіопараметрів. Проведене комп'ютерне моделювання сценаріїв атаки показало, що застосування когнітивного управління забезпечує суттєве зменшення ймовірності втрати керування дроном під час активного застосування засобів РЕБ.

Висновки дослідження дозволяють стверджувати, що впровадження когнітивного та програмно визначеного радіо в комерційні та військові логістичні БпЛА значно підвищить їхню стійкість як у воєнний, так і в післявоєнний період. Це стане вагомим чинником у захисті критичної інфраструктури доставки та забезпеченні безпеки логістичних операцій.

1. COGINT. Russian Electronic Warfare Systems: Analytic Insight Report. – 3GIMBALS, 7 червня 2023. – 82 с.

2. Українські військові знищили вже третій за тиждень РЕБ «Борисоглебск-2» [Електронний ресурс] // Мілітарний. – 2023. – 25 червня. – Режим доступу: https://militarnyi.com/uk/news/ukrayinski-vijskovi-znyshhyly-vzhe-tretij-za-tyzhden-reb-borysoglebsk-2/ – Назва з екрана.

3. Окопна РЕБ проти БпЛА [Електронний ресурс] // АрміяInform. – 2023. – 15 липня. – Режим доступу: https://armyinform.com.ua/2023/07/15/okopna-reb-proty-bpla/ – Назва з екрана.

Ринок VPN-рішень: Проблеми конфіденційності

УДК 004.056.5 (043.2)

Тетяна Сеніч[1], Олександр Сиропятов[2]

Національний університет «Одеська Політехніка»,

[1]9480723@stud.op.edu.ua, [2]o.a.syropiatov@op.edu.ua

В умовах зростання ризиків приватності та посилення інтернет-цензури користувачі дедалі частіше шукають інструменти для захисту персональних даних і контролю над власною онлайн-активністю. Мета роботи – проаналізувати сучасний ринок VPN-рішень з точки зору конфіденційності, оцінити основні ризики для користувачів та сформулювати практичні рекомендації щодо вибору безпечних сервісів.

Активне просування VPN-послуг через онлайн-рекламу, зокрема інфлюенсерів, сприяє їх популяризації серед широкого кола користувачів. Проте багато сервісів не здатні гарантувати належний рівень безпеки, незважаючи на заявлені «політики нульового логування».

VPN-ринок насичений комерційними рішеннями різної якості, що часто рекламуються без реального розкриття пов’язаних з ними ризиків. Така інформаційна асиметрія формує у користувача хибне уявлення про повну безпечність послуги.

Дослідження показують, що рекламні матеріали нерідко містять перебільшення або спрощення: наприклад, твердження, що VPN повністю виключає загрози в мережі. За даними Лін К. та ін., загальна кількість переглядів VPN-реклами на платформі YouTube перевищує 4,5 млрд [1].

Окрему загрозу становлять безкоштовні VPN, які у 2021 році виявилися причетними до витоків даних обсягом понад 1,2 ТБ, включно з IP-адресами, логінами, історією переглядів [2].

Це підкреслює особливу вразливість безкоштовних VPN-рішень, де відсутність належного захисту даних створює серйозні ризики для приватності користувачів.

У рамках дослідження сучасного ринку VPN-рішень було проведено порівняння трьох основних типів сервісів: комерційних VPN (наприклад, NordVPN, ExpressVPN), корпоративних VPN (Cisco AnyConnect, Fortinet) та open-source VPN (OpenVPN, WireGuard).

Аналіз базувався на критеріях, що безпосередньо стосуються забезпечення конфіденційності користувачів та оцінки потенційних ризиків, пов'язаних із використанням цих рішень.(табл.1).

Таблиця 1

Таблиця порівняння VPN-рішень

Критерій / Тип VPN	**Комерційні VPN (NordVPN, ExpressVPN)**	**Корпоративні VPN (Cisco AnyConnect, Fortinet)**	**Open-source VPN (OpenVPN, WireGuard)**
Юрисдикція	Часто офшорні (Панама, БВО та ін.)	Залежить від компанії, зазвичай у країні діяльності	Не прив'язані до юрисдикції (самостійне управління)
Шифрування та протоколи	AES-256, WireGuard, OpenVPN	IPSec, SSL, OpenVPN	OpenVPN, WireGuard
Незалежний аудит безпеки	Зазвичай проводиться	Внутрішній аудит	Залежить від спільноти та розробників
Ризики передачі даних третім особам	Можливі (особливо у безкоштовних версіях)	Мінімальні, дані залишаються в компанії	Відсутні при правильній конфігурації
Вартість	Підписка від $2-10 на місяць	Ліцензія, корпоративні тарифи	Безкоштовно, витрати на інфраструктуру
Зручність використання	Висока, готові додатки	Середня, потребує адміністрування	Потребує технічних знань
Додаткові функції	MultiHop, Tor-over-VPN, блокування реклами	Інтеграція з корпоративними системами безпеки	Гнучке налаштування, кастомізація

Таким чином, кожен тип VPN-рішень має свої переваги і недоліки з точки зору конфіденційності та безпеки.

Комерційні VPN пропонують зручність і додаткові функції, але іноді можуть бути ризики, пов'язані з юрисдикцією та політикою логування.

Корпоративні VPN забезпечують контроль і безпеку в межах організації, але вимагають адміністративних ресурсів.

Open-source VPN забезпечують максимальну прозорість і контроль, проте потребують технічних знань для налаштування і підтримки.

З огляду на численні проблеми, пов'язані з приватністю та надійністю VPN-сервісів, побудова власного VPN-рішення є найбільш ефективним шляхом для забезпечення конфіденційності та контролю над власними даними. Створення власного VPN на базі поширених технологій (наприклад, OpenVPN чи WireGuard) дозволяє повністю керувати інфраструктурою, мінімізуючи ризики витоку даних та забезпечуючи прозорість роботи системи.

Mazurek, "Investigating influencer vpn ads on youtube,"
in IEEE Symposium on Security and Privacy (SP), 2022
O. Akgul, R. Roberts, M. Namara, D. Levin, and M. L.
Mazurek, "Investigating influencer vpn ads on youtube,"
in IEEE Symposium on Security and Privacy (SP), 2022
O. Akgul, R. Roberts, M. Namara, D. Levin, and M. L.
Mazurek, "Investigating influencer vpn ads on youtube,"
in IEEE Symposium on Security and Privacy (SP), 2022

1. Lin K., Xiao Y., Chen J. As Advertised: Understanding the Impact of Influencer VPN Ads [Електронний ресурс]. ResearchGate, 2024. URL: https://www.researchgate.net/publication/381579245_As_Advertised_Understanding_the_Impact_of_Influencer_VPN_Ads (дата звернення: 15.04.2025).

2. vpnMentor. Report: Free VPNs Leak Data [Електронний ресурс]. 2021. URL: https://www.vpnmentor.com/blog/report-free-vpns-leak/ (дата звернення: 15.04.2025).

Розробка алгоритму для криптографічного захисту текстових та графічних даних

УДК 004.056.5:004.4

Катерина Сирбу

Національний університет «Одеська політехніка», 9480559@stud.op.edu.ua

У роботі представлено програмний застосунок для криптографічного захисту текстових і графічних даних, що поєднує шифрування за алгоритмом AES, цифровий підпис RSA, аналіз ентропії та статистичних характеристик файлів. Метою дослідження є забезпечення високого рівня конфіденційності оброблених файлів через багаторівневе шифрування та зменшення ймовірності ідентифікації початкового типу даних на основі залишкових статистичних характеристик після шифрування. Реалізована система дозволяє не лише шифрувати, а й виявляти потенційно вразливі структури у файлах. Ефективність застосунку підтверджено тестуванням на різних форматах даних.

Зростання обсягів переданої та збереженої цифрової інформації супроводжується ускладненням методів несанкціонованого доступу. Стандартні схеми шифрування, як правило, забезпечують конфіденційність змісту, але можуть залишати статистичні ознаки, за якими зловмисник здатен зробити припущення про тип вихідних даних. Це створює ризики витоку метаінформації, у разі використання засобів автоматизованого виявлення структурних закономірностей у зашифрованих даних. У таких випадках потрібні підходи, що не лише шифрують дані, а й унеможливлюють визначення їхнього початкового формату.

Захист конфіденційної інформації у цифровому середовищі вимагає застосування надійних криптографічних методів. Текстові файли часто мають статистично передбачувану структуру, графічні – містять метадані та просторові кореляції, що знижує ефективність базового шифрування [2]. Робота спрямована на подолання цих недоліків шляхом створення застосунку, здатного одночасно шифрувати дані та оцінювати ступінь їхньої криптостійкості.

Для досягнення цієї мети у застосунку реалізовано багаторівневу систему криптографічного захисту, яка забезпечує комплексну обробку даних на основі сучасних методів симетричного шифрування та структурного ускладнення зашифрованого потоку. Основу захисту файлів у застосунку становить модуль багаторівневого шифрування, реалізований у класі Encryptor. Він поєднує три послідовні етапи:

1) AES у режимі CBC — виконується базове шифрування з використанням ключа key1, отриманого через похідну функцію від пароля й солі [1];

2) перестановка блоків — за допомогою key2 (16 байт), що виступає насінням генератора випадкових чисел, зашифровані 16-байтні блоки перемішуються у псевдовипадковому порядку;

3) AES у режимі GCM — застосовується до результату перестановки з ключем key3, забезпечуючи як конфіденційність, так і автентичність даних (генерується тег перевірки цілісності).

Фінальний зашифрований файл містить службовий заголовок з усіма необхідними параметрами для розшифрування (сіль, вектор ініціалізації (IV), тег, розмір блоків, розширення файлу тощо) і тіло зашифрованих даних. Розшифрування відбувається у зворотному порядку з перевіркою цілісності та відновленням початкової структури файлу.

З метою оцінки ефективності шифрування та подальшого виявлення структурних закономірностей, у застосунку реалізовано модуль аналізу файлів, який досліджує як початкові, так і оброблені шифруванням дані. Цей модуль дозволяє виявити залишкові ознаки структури у зашифрованих файлах, а також порівняти властивості даних до і після криптографічної обробки. У межах аналізу враховуються такі характеристики:

- обчислення загальної та блочної ентропії (метод Шеннона);
- частотний аналіз символів, біграм і триграм у текстових файлах;
- аналіз розподілу каналів RGB у зображеннях з побудовою гістограм;

- вилучення метаданих (наприклад, EXIF з графічних файлів або службової інформації з документів);
- побудова порівняльних графіків частот до та після шифрування;
- обчислення статистичних метрик — тести Колмогорова–Смирнова та хі-квадрат, серійна кореляція та KL-дивергенція [3].

Для реалізації зазначених функцій було створено повнофункціональний програмний застосунок, написаний мовою Python із використанням сучасних бібліотек PyCryptodome для криптографічних операцій, NumPy та Pandas для обробки даних, а також з графічним інтерфейсом, реалізованим засобами Tkinter.

Для кількісного підтвердження ефективності реалізованого шифрування було проведено статистичний аналіз текстового файлу до та після криптографічної обробки. За результатами дослідження спостерігається зростання загальної ентропії з 4.46 до 7.98 біт/байт, що свідчить про значне зростання випадковості даних [4]. Значення p за критерієм χ^2 зросло з 0.0000 до 0.9538, що демонструє вирівнювання розподілу байтів до рівномірного — характерного для шифрованих даних.

KL-дивергенція зменшилась у понад 200 разів (з 3.5351 до 0.0163), що підтверджує втрату схожості із початковим розподілом. Серійна кореляція знизилася до майже нульового рівня, вказуючи на знищення послідовних зв'язків у потоці даних. Отримані зміни свідчать про руйнування впорядкованих структур і формування байтового розподілу, близького до випадкового, що суттєво ускладнює проведення частотного аналізу та реалізацію атак, заснованих на виявленні візуальних або статистичних закономірностей. У таблиці 1 наведено ключові характеристики оригінального текстового файлу та його зашифрованої версії.

Таблиця 1

Порівняльний аналіз статистичних характеристик файла до та після шифрування

Показник	Оригінальний файл (text.txt)	Зашифрований файл (text.enc)
Розмір файлу (байт)	9540	9632
Перші 16 байтів (hex)	50 6f 6c 69 74 69 63 61 6c 20 73 63 69 65 6e 63	d0 15 1c 60 75 6b 32 8c 3f 86 8f 18 5d e8 c3 af
Загальна ентропія (біт/байт)	4.4649	7.9837
Середня блочна ентропія (1024 байт)	4.3886	7.7838
p-значення Chi-square	0.0000	0.9538
KL-дивергенція	3.5351	0.0163
Серіальна кореляція	0.0455	–0.0068
Тип файлу (за метаданими)	Text file	Encrypted/Binary file (likely encrypted)

Таким чином, було розроблено застосунок, який поєднує багаторівневе шифрування з оцінкою статистичних характеристик даних. На відміну від типових засобів криптографічного захисту, система дозволяє не лише зашифрувати інформацію, а й оцінити ефективність шифрування на основі таких показників, як ентропія, KL-дивергенція, p-значення χ^2 та серійна кореляція. Отримані результати підтверджують, що застосунок забезпечує надійне руйнування структур текстових і графічних даних, знижуючи їхню передбачуваність і вразливість до статистичних атак. Це робить його корисним інструментом для галузей, де важливо не лише зашифрувати, а й верифікувати рівень криптостійкості захищених файлів — зокрема, у цифровій криміналістиці, розробці безпечного програмного забезпечення, аудиті інформаційної безпеки.

1. Gavaskar, K., et al. AES Algorithm using Dynamic Shift Rows, Sub Bytes and Mix Column Operations for Systems Security with Optimal Delay. – 2022.
2. Prajapat S., Thakur R. S. Various approaches towards cryptanalysis // International Journal of Computer Applications. – 2015. – V. 127. – №14. – P. 15-24.
3. Zhou, Xinping, Kexin Qiao, and Changhai Ou. Leakage detection with Kolmogorov-Smirnov test // Cryptology ePrint Archive. – 2019.
4. Zolfaghari B., Bibak K., Koshiba T. The odyssey of entropy: cryptography // Entropy. – 2022. – V. 24. – №2. – P. 266.

Algorithms in Cybersecurity: Encryption and Hashing

UDC 004.056.55
Marharyta Sytnyk[1], Oleksandr Oliinyk[2]
Kharkiv National University of Radio Electronics,
[1]*marharyta.sytnyk@nure.ua*, [2]*oleksandr.oliinyk1@nure.ua*

In the digital age, where information technologies permeate all areas of our lives, data protection has become one of the most important issues. Today, we perform hundreds of actions online every day: sending messages, shopping, accessing banking services, registering on websites. All these operations involve the processing of personal information, which must remain protected from unauthorized access [1].

Information security means a state of data in which their confidentiality, integrity, availability, and resilience to external threats are guaranteed. With the development of global networks, new risks have emerged that complicate security assurance: malware, phishing attacks, data leaks, etc. The Internet is an open environment where confidentiality is not guaranteed without additional control measures. The easier it is to access the network, the higher the risk of data leakage or tampering during transmission [1].

That is why cryptographic algorithms are used to protect information - mathematical methods that ensure data preservation even if an attacker gains access to it. Currently, the most common are open encryption algorithms, which are publicly available so anyone can verify their reliability, while the content remains inaccessible without the appropriate key [1].

Modern cryptography actively uses the concept of public and private keys. In public-key systems, one part of the pair - the public key - can be shared with anyone, while the private key is kept secret. This allows for secure communication between parties without the need for a shared secret beforehand. A key point is that knowing one key does not allow calculating the other, ensuring the reliability of encryption [2].

There are many public-key cryptographic algorithms, but not all are suitable for practical use. The most effective ones are those that provide sufficient security with acceptable performance. These include RSA, ElGamal, and elliptic curve–based algorithms. When properly configured with adequate key length, these methods ensure data confidentiality even in case of hacking attempts [2].

All encryption algorithms are divided into symmetric and asymmetric. In symmetric schemes, the same key is used for both encryption and decryption. This makes them fast and suitable for processing large amounts of data. Asymmetric algorithms, on the other hand, are based on a pair of keys and are used to establish a secure communication channel [3].

Symmetric ciphers are ideal for transmitting large files due to their speed. However, they require prior key exchange, which is not always convenient or secure. Asymmetric methods, in turn, enable secure connections without having to trust the other party, though they are slower and mainly used for initial connection setup or digital signatures. However, even these algorithms are not without risks - for example, they may be vulnerable to "man-in-the-middle" attacks, where an attacker intercepts keys and tampers with messages [3].

Encryption is widely used in various areas. For instance, secure email utilizes protocols that ensure confidentiality and sender authenticity. VPN technologies allow for secure data channels even over public Wi-Fi. Web protocols like SSL/TLS, indicated as "https" in browsers, encrypt communication between users and servers, ensuring safe entry of passwords, banking details, and other sensitive information [8][5].

Another key component of cybersecurity is hashing. This is a process in which any data is converted into a fixed-length sequence of characters - a hash code. Its main characteristic is irreversibility: it is impossible to restore the original data from the hash. Another important feature is the avalanche effect - even a minor change in the input results in a completely different hash. This makes hash functions highly effective for checking data integrity [8].

Hashing is widely used in information systems for:

- storing passwords in databases as hashes with added "salt" (an additional string of characters added before hashing to make the hash unique);
- verifying the integrity of files and data during transmission;
- creating digital signatures to ensure authenticity;
- implementing fast search in hash tables and caching systems [9].

Among the most well-known algorithms are SHA-2 (SHA-256, SHA-384, SHA-512), which provide high security due to resistance to collision and brute-force attacks. SHA-256 is one of the most reliable hash algorithms and is widely used in cryptocurrencies, digital signatures, and data verification in modern security systems [4].

Hashing is also widely used for password storage. Instead of storing plain-text passwords, systems store only their hash codes. To further secure this process, salted hashing algorithms like bcrypt or Argon2 are used. They add a random salt to each password, making even identical passwords appear different in the database. This renders precomputed rainbow tables nearly useless [4][11].

Encryption and hashing differ in nature and application, so it's reasonable to compare them by key criteria [5]:

Table 1

Comparison of Encryption and Hashing by Key Criteria

Feature	Hashing	Encryption
Reversibility	One-way (irreversible)	Two-way (reversible)
Purpose	Data integrity, password storage	Confidentiality and data protection
Output length	Fixed	Variable
Key requirement	No	Yes (encryption and decryption keys)
Confidentiality	Does not ensure confidentiality	Ensures data confidentiality
Data recovery	Original data cannot be restored	Data can be decrypted to original
Example use	Password storage	Protection of sensitive information

In conclusion, it is important to note that modern cryptography faces new challenges. In particular, the development of quantum computing raises concerns about the resilience of classical algorithms. Quantum computers are capable of efficiently breaking algorithms that are currently considered secure - including RSA and ECDSA - using Shor's and Grover's algorithms. This already motivates the search for new cryptographic solutions that are resistant to quantum attacks - the so-called post-quantum cryptography [6].

Encryption and hashing are the core mechanisms of cryptographic protection, but their functionality differs significantly. Hashing performs an irreversible transformation of data, making it ideal for verifying data integrity and storing passwords. In contrast, encryption enables both the encryption and decryption of data, ensuring its confidentiality. Both approaches are widely used in modern digital systems: hash functions in digital signatures, authentication systems, and data storage; encryption algorithms in secure transmission protocols, VPNs, and electronic communication. Despite their differences, these methods share a common goal - to protect information in a digital environment.

Thus, encryption and hashing are fundamental tools in cybersecurity. They enable the protection of personal data, the integrity of digital information, and secure interaction in the online space. However, only their continuous development and adaptation to emerging threats can guarantee the stability of the digital world in the face of rapid technological progress.

1. Zemlianska O.V. et al. *Internet Security and Personal Data Protection*. ELAKPI :: Repository of Igor Sikorsky Kyiv Polytechnic Institute. URL: https://ela.kpi.ua/server/api/core/bitstreams/30caa1e2-2b9b-4d2e-9a9f-67844e4115c1/content
2. Avramenko K.M. *Diploma Project on "Computer System for Information Protection Using Hypercomplex Number Systems"*. ELAKPI :: Repository of Igor Sikorsky Kyiv Polytechnic Institute. URL: https://ela.kpi.ua/server/api/core/bitstreams/3023375f-b592-4108-a8d9-034998d6613c/content
3. Filipieva M., Gvozdecka K. *Comparison of Symmetric and Asymmetric Encryption*. URL: https://openarchive.nure.ua/server/api/core/bitstreams/a47f80d7-cf00-4b39-aba6-31843899f002/content
4. Groza P., Kimachuk T. *Analysis of Information Encoding Algorithms for Personal Data Protection*. Information protection. – 2023. – V. 25, №2. – p. 53–61.
5. *Hashing vs Encryption – JS Communities*. URL: https://javascript.org.ua/heshuvannya-proti-shifruvannya/
6. Koliada A.S., Pavlyshko A.V., Litvinov V.F. *Cryptography Beyond the Quantum Era: New Challenges and Solutions for Information Security*. URL: http://immm.op.edu.ua/files/archive/n3_v14_2024/2024_3(7).pdf
7. Wikimedia contributors. *Hash Function*. Wikipedia. URL: https://uk.wikipedia.org/wiki/Хеш-функція
8. *What is Hashing, Encryption, and Coding*. SSL.com.ua Blog. URL: https://ssl.com.ua/blog/ukr/hashing-coding-encryption/
9. Zhdanova Y.D. et al. *Applied and Methodological Aspects of Using Hash Functions in Information Security*. Institutional Repository of Borys Grinchenko Kyiv University. URL: https://elibrary.kubg.edu.ua/id/eprint/31942/1/Y_Zhdanova_S_Spasiteleva%20_S_Shevchenko_K_Kravchuk_4_8.pdf
10. Wikimedia contributors. *Encryption*. Wikipedia. URL: https://uk.wikipedia.org/wiki/Шифрування
11. *Data Hashing: Methods and Algorithms*. Cyberset.com.ua. URL: https://cyberset.com.ua/encryption/heshuvannya-danykh-metody

Інформаційна безпека на ринку фінансових послуг та особливості її забезпечення

УДК 004.56:336.76

Микола Стецько[1], Василь Стецько[2], Володимир Манжула[3]
[1,3]Західноукраїнський національний університет,
[2]Фаховий коледж економіки, права та інформаційних технологій ЗУНУ,
[1]nsteco6691@gmail.com, [2]vasyastetsko@gmail.com,
[3]v.manzhula@wunu.edu.ua

Інформаційна безпека на ринку фінансових послуг в Україні є критично важливою сферою, що розвивається і яка характеризується ризиками кіберзагроз та регулятивних заходів, котрі спрямовані на захист фінансових

установ. Важливість цієї сфери підкреслюється геополітичним контекстом України, особливо після ескалації воєнних дій з 2022 року та збільшення частоти кібератак, спрямованих на її фінансовий сектор. Все це зумовило необхідність розробки надійних заходів інформаційної безпеки та нормативно-правової бази, яка б відповідала міжнародним стандартам, що робить вивчення практик кібербезпеки важливим для розуміння глобальних тенденцій фінансової безпеки.

Необхідно зазначити, що проблеми, які пов'язані з інформаційною безпекою в цілому, і зокрема, використанням інформації на ринку фінансових послуг (РФП) досліджують вітчизняні і зарубіжні науковці − А. Баранець, С. Бірюк, Я. Гринчишин [1], М. Дубина [2], Н. Зачосова, М. Касянчук, О. Корченко, Д. Пілевич, Н. Холявко [2], І. Якименко, В. Яцків, С. Ратледж, Р. Симондс, М. Уддін [3], Б. Фрончек, Д. Циман.

Питання, котрі пов'язані з вимогами і принципами інформаційної безпеки при наданні фінансових послуг в Україні, на даний час досліджені недостатньо. Причому оцінка чинників та важелів, які впливають на інформаційну прозорість на РФП, здебільшого мають фрагментований та не систематизований характер.

Дослідження показало, що світовий фінансовий ринок стикається з безліччю кіберзагроз, причому різні країни розробили комплексні рамки кібербезпеки задля пом'якшення цих ризиків. Надзвичайні виклики, що стоять перед Україною, включно з протистоянням щодо військової агресії та фінансованою державою кібердіяльністю, спонукали до прискореного вдосконалення її правил та практик кібербезпеки [4; 5].

Спільні зусилля між державними установами та компаніями приватного сектору ще більше зміцнили стійкість України до кіберзагроз, відображаючи модель, яка контрастує з більш централізованими підходами, що спостерігаються в інших країнах. Зокрема, сектор фінансових послуг в Україні повинен орієнтуватися в складному середовищі ризиків, де вразливість посилюється технологічним прогресом і зростаючою залежністю від цифрових операцій. Національне нормативно-правове середовище на РФП, яке контролюється таким відомством, як Національний банк України, вимагає дотримання суворих стандартів кібербезпеки, розроблених для захисту конфіденційних фінансових даних і забезпечення операційної цілісності [6].

Підсумовуючи можна констатувати, що інформаційна безпека на РФП України ілюструє динамічну взаємодію між дотриманням нормативних вимог, технологічною адаптацією та необхідністю стратегічного реагування на кіберзагрози, що активізуються. Оскільки сектор продовжує розробляти свої стратегії кібербезпеки, важливість сприяння державно-приватному партнерству та інвестування в розвиток фахівців залишається першочерговим завданням для створення стійкої фінансової екосистеми, здатної протистояти майбутнім викликам [7].

Маємо підкреслити, що в міру розвитку технологій, їхня роль у формуванні практик безпеки стала більш очевидною. Практика діяльності фінансових установ в Україні засвідчила, що технології відіграють вирішальну роль у захисті цифрових активів, тим самим зумовлюючи необхідність проактивного підходу до кібербезпеки. Водночас складнощі сучасних кіберзагроз вимагають

постійної адаптації заходів безпеки, що в свою чергу впливає на історичну траєкторію практик інформаційної безпеки на ринку фінансових послуг [8].

Безперечно, що сфера кібербезпеки в останні роки в нашій державі вагомо еволюціонувала, особливо в контексті воєнної агресії. Статистичні дані свідчать про значне зростання кібероперацій після початку війни 2022 року, коли частота кіберінцидентів різко зросла, незважаючи на відносно незмінну серйозність порівняно з довоєнною статистикою [9].

Більше того, в Україні спостерігається підвищена вразливість до кібератак, обумовлена рядом специфічних факторів ризику, які можуть серйозно загрожувати інформаційній безпеці організацій та компаній. Ця вразливість означає ймовірність того, що слабкі місця в кіберсистемах будуть використані зловмисниками, що підкреслює важливість впровадження ефективного управління ризиками. У зв'язку з цим компаніям та установам доцільно впроваджувати заходи кібербезпеки на всіх рівнях своєї діяльності − як у ключових операційних процесах, так і в допоміжних функціях − для забезпечення належного захисту та зменшення потенційних ризиків.

Маємо підкреслити, що ефективність кіберзахисту в Україні значною мірою пояснюється міцним приватно-державним партнерством. Ця модель співпраці дозволяє підвищити стійкість національної інфраструктури інформаційно-комунікаційних технологій та швидко реагувати на кіберінциденти.

Результати проведеного дослідження підтверджують, що сфера інформаційної безпеки на РФП в Україні готова до значної еволюції в найближчі роки. Очікується, що в міру прискорення цифрової трансформації кілька ключових тенденцій визначатимуть майбутнє кібербезпеки.

Крім того прогнозується, що майбутні сфери зростання включатимуть вирішення питань безпеки на основі штучного інтелекту, хмарного захисту та надійних стратегій реагування на інциденти. Ці зміни є життєво важливими, оскільки сектор фінансових послуг стає все більш залежним від цифрових технологій, наражаючи установи на більш високі ризики кібератак.

Причому інтеграція штучного інтелекту в практики кібербезпеки покращить можливості виявлення загроз і реагування на них, адаптуючись до тактики кіберзлочинців, котрі також розвиваються.

Очевидним є те, що значні інвестиції після завершення війни ще більше зміцнять позиції України у сфері цифрового захисту. Збільшення підтримки від країн-партнерів не лише підвищить стійкість фінансових установ, але й сприятиме розвитку загальної інфраструктури кібербезпеки країни.

1. Гринчишин, Я. (2024). Роль інформації у зменшенні ризиків споживачів на ринку фінансових послуг. Економіка та суспільство, (65). https://doi.org/10.32782/2524-0072/2024-65-29

2. Дубина, М., Холявко, Н., Попело, О. (2023). Цифровізація ринку фінансових послуг: переваги та ризики для домогосподарств. Науковий вісник Полісся, (2 (25), 160–177. https://doi.org/10.25140/2410-9576-2022-2(25)-160-177

3. Uddin, M.H., Ali, M.H., & Hassan, M.K. (2020). Cybersecurity hazards and financial system vulnerability: A synthesis of literature. Risk Management, 22, 239-309. https://link.springer.com/article/10.1057/s41283-020-00063-2

4. Ukraine's Cyber Market Quadruples in Eight Years (2025). https://digitalstate.gov.ua/uk/news/it-outsourcing/ukrayinskyy-rynok-kiberbezpeky-zris-u-4-razy-za-8-rokiv
5. Ukraine. Jurisdictions. DataGuidance (2022). https://www.dataguidance.com/jurisdictions/ukraine
6. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг (проект) (2025) https://bank.gov.ua/ua/news/all/startuye-obgovorennya-poryadku-organizatsiyi-zahodiv-iz-zabezpechennya-informatsiynoyi-bezpeki-ta-kiberzahistu-nadavachami-finansovih-poslug
7. Кльоба, Л., & Кльоба, Т. (2022). Кіберзагрози банківського сектора в умовах воєнного стану в Україні. Financial and Credit Activity Problems of Theory and Practice, *5* (46), 19–28. https://doi.org/10.55643/fcaptp.5.46.2022.3883
8. Ukraine's Cyberthreat Landscape 2024 (2025). https://cyble.com/blog/ukraine-cyberthreat-landscape-2024/
9. Єгоричева, С., Глушко, А., Худолій, Ю. (2023). Питання інформаційної безпеки фінансового сектору України. управління розвитком, 22(4), 45-52. https://doi.org/10.57111/devt/4.2023.45

Прийняття рішень при виборі UTM-системи бездротового мапування на основі LoRa для передачі геопросторових даних

УДК 004.67

Андрій Сторожко
Національний технічний університет «Харківський політехнічний інститут»

У статті представлено тайл-орієнтовану UTM-систему мапування (Universal Transverse Mercator) для ESP32 з інтегрованим LoRa-комунікацією. Запропонована система дозволяє ефективно зберігати, отримувати та відображати векторні дані мап на пристроях з обмеженими ресурсами, що робить її придатною для реалізації географічних додатків у режимі реального часу. Дані мап зберігаються у ієрархічній структурі тек на SD-карті, де кожен тайл відповідає певній UTM-зоні та динамічно завантажується залежно від навігації користувача. Система підтримує бездротову синхронізацію тайлів за допомогою LoRa, що дозволяє обмінюватися даними мап між кількома вузлами ESP32, забезпечуючи децентралізовані та автономні рішення для мапування. Механізм кешування оптимізує використання пам'яті, забезпечуючи плавне відображення мап на TFT-дисплеях. Запропоноване рішення особливо корисне для віддалених або слабко з'єднаних з мережею середовищ, де традиційні мережеві сервіси мапування недоступні. У статті розглянуто архітектуру, реалізацію та оцінку продуктивності системи, виділивши її потенціал для геопросторових застосувань у навігації БПЛА, екологічному моніторингу та операціях швидкого відгуку.

Запропонована система інтегрує тайл-орієнтоване UTM-мапування з LoRa-бездротовим зв'язком для децентралізованого, енергоефективного та реального часу обміну геопросторовими даними для пристроїв на базі ESP32.

Система складається з трьох основних компонентів: зберігання геопросторових даних, LoRa-комунікації та інтелектуального кешування. Тайли мап структуровано ієрархічно на SD-карті, що дозволяє швидке та ефективне отримання даних. Технологія LoRa забезпечує довгодійний, низькопотужний зв'язок між пристроями, сприяючи реальному часу обміну даними без традиційної мережевої інфраструктури. Механізм кешування оптимізує використання пам'яті, динамічно завантажуючи та видаляючи тайли мап в залежності від руху користувача та навігаційних шаблонів. Система особливо корисна для застосувань мапування на базі БПЛА, де реальний час передачі геопросторових даних критичний для навігації, розвідки та екологічного моніторингу.

Таблиця 1

Порівняння пакетної комутації

Параметри	**LoRa**	**Sigfox**	**LTE-M**	**NB-CPS**	**EC-GSM-CPS**
Метод мультип-лексування	Мультиплек-сування з часовим розділенням	Статистичне мультиплек-сування	Мультиплек-сування з часовим розділенням	Поділ портів	Часове розділення та поділ портів
Поділ портів	Не застосовується	Не застосовує-ться	Не застосовуєть ся	Має свій унікальний порт	Статичний динамічний розділ портів
Продукти-вність	Залежить від інтеграції з алгоритмами передачі даних та управління мережею	Залежить від оптимізації протоколу та мережевої інфраструк-тури	Висока завдяки використанн ю широкого діапазону часових інтервалів	Залежить від ефективно-сті алгоритмів доступу до каналу та управління мережею	Залежить від ефективності алгоритмів доступу до каналу та управління мережею
Затримка	висока	низька	низька	низька	низька

Проект пропонує UTM-систему LoRa-мапування для ESP32, розроблену для ефективного управління геопросторовими даними у середовищах з низькою з'єднаністю. Запропонована система інтегрує зберігання тайлів мап, бездротову LoRa-комунікацію та реальний час синхронізації даних, що робить її високо придатною для застосувань, таких як навігація БПЛА, віддалене мапування та операції швидкого відгуку. Система має кілька ключових переваг, включно з автономною роботою, енергоефективністю, масштабованістю, децентралізованим управлінням даними та легковаго, швидкого відображення. Проект підтверджує, що високочутливі, низькопотужні GPS-приймачі є критичними для надійного трекингу, особливо в застосуваннях БПЛА, де обмеження потужності є ключовою умовою. Порівняльний аналіз різних технологій бездротового передавання даних виділяє LoRa як найбільш придатну для довгодійного, низькопотужного обміну геопросторовими даними.

1. Semtech Corporation, "LoRa and LoRaWAN: A Technical Overview," 2021.

2. Espressif Systems, "ESP32 Series Datasheet," 2022.
3. A. Augustin, J. Yi, T. Clausen, and W. M. Townsley, "A Study of LoRa: Long Range & Low Power Networks for the Internet of Things," Sensors, vol. 16, no. 9, 2016.
4. U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low Power Wide Area Networks: An
5. Overview," IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 855–873, 2017.

Верифікація резервного копіювання бази даних

УДК 621.395.7 (043.2)
Максим Теліга[1], Олена Головачова[2]
Національний університет «Одеська політехніка»
[1]9480545@stud.op.edu.ua, [2]holovachova@op.edu.ua

Безпека та цілісність даних набувають вирішального значення для забезпечення стабільної роботи інформаційних систем в наш час. Особливо це актуально у контексті резервного копіювання баз даних, що є одним із ключових елементів захисту даних від втрати чи пошкодження.

Резервні копії баз даних забезпечують можливість відновлення інформації у разі збоїв, однак ризик пошкодження копій або втрати частини даних під час їх створення залишається. Метою дослідження є алгоритм перевірки цілісності резервних копій шляхом порівняння контрольних хеш-сум. Цей підхід дозволяє ефективно виявляти будь-які розбіжності між оригінальними даними та їх резервною копією.

Щоб обрати алгоритм хешування, порівняємо два методи: SHA-256, MD5. Для тесту було обрано MD5 [1] через його простоту, швидкість, але низьку безпеку, в той же час SHA-256 [2] є дуже надійний, менш швидкий, але це може компенсувати підтримка апаратного прискорення (табл. 1). Нами було взято текстовий файл на 20 МБ, який було зашифровано через програмну платформу Node.js за допомогою бібліотеки crypto.

Таблиця 1

Оцінка часу обробки алгоритмів

Алгоритм	20Мб	100Мб
MD5	66.296 мс	312.383 мс
SHA-256	42.284 мс	196.16 мс

Виходячи із даних з таблиці ми оберемо за алгоритм хешування SHA-256, через те що він більш швидкий для нашої системи, але для старих систем, де немає підтримки апаратного прискорення MD5 буде краще.

Алгоритм для перевірки цілісності даних:

1) отримання контрольної хеш-суми з бази даних. На етапі аналізу даних у базі використовується запит (рисунок 1), що обчислює хеш-суму за вибраними полями та забезпечує сортування даних для уникнення впливу порядку записів;

2) створення дампа бази даних. Виконується повне резервне копіювання бази з подальшим збереженням у файл;

3) обчислення хеш-суми дампа. Хешування вмісту файлу резервної копії забезпечує можливість його порівняння з вихідною базою (рисунок 2);

4) порівняння отриманих хеш-сум. Порівняння результатів дозволяє виявити розбіжності між базою даних та резервною копією.

```
SELECT
  SHA2(GROUP_CONCAT(
    CONCAT('INSERT INTO `', table_name, '` VALUES (', col1, ',', col2, ');')
    ORDER BY table_name, id SEPARATOR '\n'), 256 ) AS database_hash
FROM users;
```

Рис.1. Запит на отримання хеш-суми резервної копії

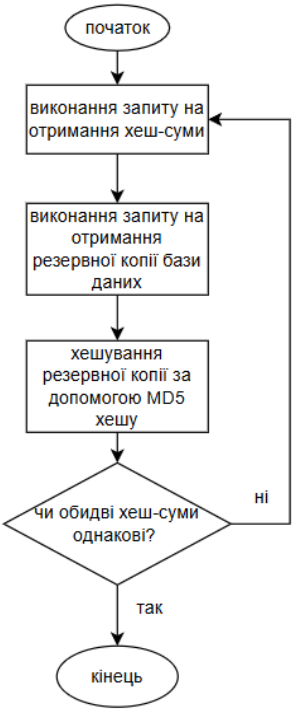


Рис.2. Алгоритм перевірки контрольних хеш-сум

Запропонований алгоритм дозволяє перевірити, чи всі дані з бази даних потрапили до резервної копії, та чи не були вони пошкоджені під час процесу створення резервної копії, звісно є дуже малий шанс того, що під час обчислення обох хеш сум резервні копії будуть пошкоджені однаково і перевірка буде успішною. Використання алгоритму MD5 забезпечує високу швидкість обчислень, однак він має обмеження в контексті криптографічної стійкості. Наприклад, MD5 уразливий до атак типу "зіткнення", що може бути критичним для деяких застосувань. Однак для цілей перевірки цілісності резервних копій цей алгоритм є прийнятним завдяки своїй ефективності.

Для перевірки методу було проведено тестування на реальних даних. У результаті було підтверджено, що метод здатний виявляти навіть незначні розбіжності між вихідними даними та резервними копіями. Крім того, запропонований підхід є універсальним і може бути адаптований для інших баз даних та форматів резервного копіювання.

Метод перевірки хеш-сум забезпечує ефективний механізм контролю цілісності резервних копій баз даних. Запропонована методологія дозволяє виявляти втрати чи пошкодження даних під час резервування, що підвищує загальну надійність системи.

1. Смарт Н. Криптографія пер. с англ. / Н. Смарт – М.: Техносфера, – 2005 – 528с.
2. Борд Р.В., Лозовська Л.І., «Методологічний вибір хеш-функції для оптимальної синхронізації бази даних національних парків Хорватії». – 2016. , – С. 25-27.

Виявлення та запобігання витоку даних у реальному часі за допомогою систем моніторингу мережевого трафіку

УДК 004.056.5 (043.2)
Іван Тихонов[1], Олександр Сиропятов[2]
Національний університет «Одеська Політехніка»,
[1]9560414@stud.op.edu.ua, [2]o.a.syropiatov@op.edu.ua

У сучасних інформаційних середовищах захист конфіденційних даних набуває особливої актуальності: лише у 2024 році кількість інцидентів витоку даних у світі зросла на 25% порівняно з попереднім роком. Збільшення складності кібератак, поява нових векторів проникнення, а також використання зловмисниками штучного інтелекту та машинного навчання вимагають переходу від класичних методів безпеки до систем, що аналізують мережевий трафік у реальному часі. Мета роботи – розробити методику виявлення та запобігання витоку даних у режимі реального часу шляхом кореляції даних DLP і IDS.

Сигнатурний аналіз (IDS/IPS) забезпечує високу точність у виявленні відомих атак, наприклад SQL-ін’єкцій чи експлойтів SMB, проте не здатний реагувати на нові зразки загроз без оновлення сигнатур.

Аномалійний аналіз із використанням моделей машинного навчання дозволяє виявляти нетипові патерни поведінки, такі як раптове зростання вихідного трафіку чи зміна структури запитів.

Гібридні моделі, що комбінують сигнатурний та аномалійний підходи, створюють баланс між швидкістю реагування і адаптивністю до нових загроз. Такий багаторівневий конвеєр забезпечує низький рівень хибних спрацьовувань та здатність адаптуватися до еволюції загроз, що особливо важливо в середовищах із високими вимогами до DLP та NGFW [1, 2].

На основі цього аналізу запропоновано методику, яка корелює події DLP із виявленими IDS аномаліями.

Для практичного впровадження рекомендується:

- інтегрувати DLP та IDS у SIEM-платформу (Splunk, QRadar) для централізованої кореляції подій і автоматизації реагування;
- налаштувати автоматичне оновлення сигнатурних баз із перевірених джерел та періодично проводити аудит правил;
- забезпечити регулярне навчання аналітиків моделюванню інцидентів і користувачів – базовим принципам інформаційної безпеки, а також впроваджувати періодичне тестування та адаптацію моделей машинного навчання відповідно до появи нових типів загроз [3].

Запропонована методика є універсальною та може бути адаптована для різних галузей, що робить її перспективною для широкого впровадження у сучасних корпоративних інформаційних системах.

1. Бурячок В. Л., Толубко В. Б., Хорошко В. О. Інформаційна та кібернетична безпека: підручник. Київ: ДУТ, 2018. 456 с.

2. Шерстюк В. І., Жуков С. О. Кібербезпека інформаційних систем: монографія. Київ: НАУ, 2020. 320 с.

Darktrace. AI-Powered Network Security [Електронний ресурс]. URL: https://www.darktrace.com/products/network

Використання ШІ для виявлення інформаційних операцій у медіапросторі

УДК04.8:316.774.3

Віталій Тищенко[1], Олександр Дьячук[2]

Державний університет інформаційно-комунікаційних технологій,

[1]v.tyshchenko@duikt.edu.ua, [2]realjewua@gmail.com

Інтеграція штучного інтелекту (ШІ) у виявлення інформаційних операцій у медіа-просторі стала критично важливою через зростання дезінформації та її соціальних наслідків. Дезінформація, навмисно оманливий контент для завдання шкоди, поширюється цифровими платформами, вимагаючи передових методів протидії. Технології ШІ, зокрема машинне навчання (ML) і обробка природної мови (NLP), автоматизують виявлення, але проблеми етики, алгоритмічної упередженості та зловживань залишаються.

Автоматизовані системи перевірки фактів використовують алгоритми ML для аналізу даних з перевірених джерел, застосовуючи семантичний аналіз і синтаксичне розпізнавання шаблонів. Інтеграція блокчейну забезпечує незмінні записи, покращуючи верифікацію в реальному часі [1]. Ефективність залежить від якісних наборів даних, що ускладнено динамікою тактик дезінформації та дефіцитом маркованих даних для маловивчених мов.

Лінгвістичний аналіз та аналіз настроїв виявляють стилістичні аномалії та емоційні сигнали. Моделі NLP аналізують лексику й синтаксис, аналіз настроїв виокремлює емоційну поляризацію. Проте контекстуальні нюанси (сарказм, культурні референції) вимагають використання фреймворків «людина в циклі» (HITL). Напівкероване навчання підвищує точність, зберігаючи масштабованість.

Вороже використання ШІ для створення синтетичних медіа (глибокі фейки, текст від GAN) ускладнює боротьбу. Державні операції використовують ці технології для маніпуляцій, дискредитації журналістів, посилення пропаганди. Гендерно зумовлена дезінформація експлуатує алгоритми платформ, поширюючи шкідливий контент.

Етичні проблеми включають алгоритмічну упередженість через спотворені дані та недостатнє лінгвістичне розмаїття. Моделі NLP для мов з низькими ресурсами неефективні. Непрозорість алгоритмів і відсутність аудиту загрожують підзвітності. Ініціативи на кшталт принципів надійного ШІ від IBM акцентують на справедливості та пояснюваності, але комерціалізація дезінформаційних послуг вимагає регуляторного втручання [2].

Журналістика залишається ключовою: ШІ допомагає аналізувати дані, але людський нагляд незамінний для контекстуалізації та етичних рішень. Системи HITL поєднують масштабованість ШІ з критичним мисленням. Націленість на журналістів дезінформації підриває довіру, вимагаючи кібербезпеки та міжнародної співпраці [3].

Рис.1.ШІ-антидезінформація

Запропоновані рішення включають розвиток багатомовного NLP, спільні хеш-бази для синтетичних медіа, прозорість алгоритмів. Регуляторні заходи

мають охоплювати суворіший нагляд за політичною рекламою, підзвітність платформ. Підвищення медіаграмотності та підтримка незалежної журналістики посилять стійкість суспільства [3].

Ефективність ШІ залежить від подолання етичних, технічних і геополітичних викликів. Збереження цілісності медіа-простору вимагає комплексного підходу, що поєднує технології, людський досвід і надійну нормативну базу.

1. Santos F. C. C. Artificial Intelligence in Automated Detection of Disinformation: A Thematic Analysis. *Journalism and Media*. 2023. Vol. 4, no. 2. P. 679–687. URL: https://doi.org/10.3390/journalmedia4020043

2. Kubrak Y., Plechystyy D., Romanishyn V. Принципи формування мультиагентної системи штучного інтелекту. Computer-integrated technologies: education, science, production. 2022. № 48. С. 76–82. URL: https://doi.org/10.36910/6775-2524-0560-2022-48-12

3. Sančanin B., Penjišević A. Use of artificial intelligence for the generation of media content. Social informatics journal. 2022. Vol. 1, no. 1. P. 1–7. URL: https://doi.org/10.58898/sij.v1i1.01-07

Використання методу FRAM (Functional Resonance Analysis Method) в процесі управління ризиками кібербезпеки пов'язаними з людським фактором

УДК 004.77

Ірина Удовик[1], Дмитро Тимофєєв[2], Олександр Кручінін[3]
Національний технічний університет «Дніпровська політехніка»,
[1]udovyk.i.m@nmu.one, [2]tymofieiev.d.s@nmu.one, [3]kruchinin.o.v@nmu.one

В рамках реалізації процесу управління ризиками кібербезпеки комплексний підхід до їх аналізу і оцінки є складною багатокомпонентною і багаторівневою проблемою. Контекст процесу охоплює вплив зовнішнього та внутрішнього середовища, апаратне та програмне забезпечення, людський фактор. В рамках постійних зусиль зі створення моделей оцінки, характеристика людського фактору, що включає в себе поведінку людини, навколишнє середовище і необхідна для того, щоб зрозуміти, як дії стейкхолдерів, менеджменту, користувачів, захисників і зловмисників впливають на ризики кібербезпеки.

Метою даної роботи є підвищення ефективності аналізу та оцінки ризиків кібербезпеки пов'язаних з впливом людського фактору в соціотехнічних системах.

Традиційно до забезпечення захисту інформації, інформаційної та кібербезпеки в інформаційно-комунікаційних системах (ІКС) підходили з програмно-технічної або технологічно-центричної точки зору, з незначним урахуванням когнітивних процесів, потреб і мотивації кінцевих користувачів. Відповідно, використовуючи широко розповсюджені фреймворки, методи та засоби захисту традиційно приділяють велику увагу програмно-технічним рішенням для побудови системи забезпечення безпеки. Останні дослідження в галузі кібербезпеки засвідчують, що для забезпечення резильєнтності потрібно

запроваджувати комплексний соціотехнічний підхід, а не лише окремі організаційні чи програмно-технічні рішення. Це особливо стосується організацій та ІКС в таких галузях, як наука і освіта, державне управління та самоврядування, охорона здоров'я, а також у напрямах пов'язаних з розробкою та використанням передових технологій, таких як штучний інтелект, хмарні обчислення та в цілому забезпечення безпеки об'єктів критичної інформаційної інфраструктури. Відповідно до цього, стверджується [1], що забезпечення інформаційної та кібербезпеки є системним питанням і що для вирішення цього явища слід брати до уваги цілісний підхід з урахуванням людського фактора.

Враховуючи результати численних науково-практичних досліджень вітчизняних та зарубіжних авторів, на поточний момент неможливо визначити єдиний підхід до управління, аналізу або оцінки ризиків інформаційної та кібербезпеки. Динамічність та багатофакторність процесу забезпечення кібербезпеки з урахуванням людського фактора вимагає поєднання комплексу методів та підходів заснованих, як на статистично-ймовірнісному так і на поведінковому аналізі [2].

Метод аналізу функціонального резонансу (Functional Resonance Analysis Method – FRAM) використовується для вивчення складних соціотехнічних систем. Теоретичні засади методу розроблено і обґрунтовано Е. Холнагелєм, суть полягає в тому, що складні технічні системи містять велику кількість підсистем і компонентів, мінливість продуктивності яких зазвичай поглинається системою з мінімальним впливом на загальну систему. Основними джерелами цієї мінливості є людський, технологічний та організаційний фактори, які забезпечують стале функціонування системи в цілому.

Наявність всієї сукупності означених факторів є характерною ознакою кіберфізичних систем, що дає суттєві переваги в застосуванні методу FRAM в процесі аналізу ризиків, як системи в цілому, так і її окремих складових та компонентів; процесів безпечної розробки програмного забезпечення, впровадження моделей штучного інтелекту, підвищення освіченості персоналу з кібербезпеки та інших.

Для прикладу, можна розглянути процес управління інформаційною/кібербезпекою в організації в цілому, як сукупність функцій, пов'язаних між собою, для кожної з яких визначаються шість найбільш впливових аспектів (характеристик, параметрів): I – вихідні дані; T – час; C – контроль; R – ресурс; P – передумови; O – вихідні дані. Схематично функція відображається у вигляді функціонального шестикутника. Всі функції розглядаються у взаємодії між собою так, що компоненти або результат однієї функції можуть бути вхідними параметрами, передумовою, контрольним аспектом іншої функції, або ж її базовим елементом. Застосування методу FRAM для аналізу системи і оцінювання ризику виникнення інцидентів проводиться у чотири кроки: 1 - визначення та опис функцій за елементами - встановлюємо, що є вхідним елементом, який запускає функцію, передумовою для її роботи та необхідними ресурсами для її виконання; 2 - визначення потенційної мінливості функцій - визначаємо за вихідними результатами, які можуть бути змінними в часі та точності виконання; 3 - визначення

функціонального резонансу - вирішуємо задачу з оцінки ризику відмови кожної з функцій і впливу такої мінливості на інші складові процесу; 4 - управління змінами - виявляємо найбільш впливові (резонансні) фактори, обираємо контролі (механізми безпеки) як складові обробки ризиків.

Використання методу FRAM дає можливість поєднати переваги статистично-ймовірнісного та поведінкового аналізу, та має перспективи реалізації із застосуванням моделей штучного інтелекту.

1. Pollini, A., Callari, T.C., Tedeschi, A. et al. Leveraging human factors in cybersecurity: an integrated methodological approach. Cogn Tech Work 24, 371–390 (2022). https://doi.org/10.1007/s10111-021-00683-y

2. Тимофєєв Д.С., Совенко А.С. Оцінка ризиків в процесі управління ризиками кібербезпеки пов'язаними з людським фактором. Проблеми використання інформаційних технологій в освіті, науці та промисловості: XVIII міжнар. конф. (24 лист. 2023 р., м. Дніпро): зб. наук. пр. Дніпро: НТУ «ДП», 2023. – № 8. – 219 с., с. 173-176

Аналіз існуючих систем контролю та управління доступом користувача

УДК 004.056.5:004.08

Євген Філімончук[1], Ігор Аверічев[2]

Державний університет інформаційно-комунікаційних технологій,

[1]st7348081@stud.duikt.edu.ua , [2]iaverichev19@gmail.com

У сучасному середовищі кіберзагроз, що швидко розвивається, організації стикаються з дедалі складнішими проблемами щодо захисту своїх цифрових активів від складних кібератак. Операційні центри безпеки (SOC) служать передовою обороною від цих загроз, використовуючи вдосконалені механізми моніторингу, виявлення та реагування для захисту критично важливих систем і даних.

В епоху цифровізації, забезпечення безпеки систем і програм є першорядним. Управління ідентифікацією, контроль доступу та авторизація разом утворюють наріжний камінь захисту конфіденційних даних і ресурсів у цифровій сфері. Ці три основні процеси відіграють важливу роль у визначенні того, хто має до чого доступ, які дії він може виконувати та за яких обставин їм надаються такі привілеї.

Управління ідентифікацією охоплює складне завдання керування та контролю ідентифікаційних даних користувачів у екосистемі інформаційних технологій. Це передбачає створення, підтримку та керування профілями користувачів, призначення ролей і регулювання рівнів доступу. Контроль доступу, з іншого боку, обертається навколо практики диктування того, кому дозволено входити в систему чи програму, і в якій мірі вони можуть взаємодіяти з доступними ресурсами. Це передбачає формулювання та застосування політики доступу, аутентифікацію користувачів і розподіл прав доступу на основі попередньо визначених ролей і дозволів [1].

Авторизація, третій стовп цієї тріади, отримує дозволи, отримані від контролю доступу і визначає конкретні дії, які користувач може виконувати в системі. В цифрову епоху, коли межі між фізичним і цифровим середовищем розмиваються, управління ідентифікацією, контроль доступу та авторизація стають незамінними в різних секторах.

Управління ідентифікацією разом із контролем доступу та авторизацією є одним із трьох основних процесів забезпечення безпеки системи чи програми. Управління ідентифікацією — це процес управління та контролю ідентифікаційних даних користувачів і привілеїв доступу до системи або програми. Це передбачає встановлення та підтримку ідентифікаційних даних користувачів, призначення ролей і рівнів доступу, а також забезпечення доступу користувачів лише до тих ресурсів, які їм необхідні для виконання своїх завдань.

Управління ідентифікацією стосується процесів і технологій, які використовуються для керування цифровими ідентифікаторами користувачів, які отримують доступ до IT-системи чи програми. Воно включає створення та керування обліковими записами користувачів, призначення ролей і дозволів, а також підтримку точної інформації про користувачів. Керування ідентифікацією має важливе значення для забезпечення того, щоб лише авторизовані користувачі мали доступ до IT-системи чи програми, а також для відстеження дій користувачів у системі [2].

Розглянемо контроль доступу — це процес керування тим, хто може отримати доступ до системи чи програми та до яких ресурсів вони можуть отримати доступ. Він передбачає визначення та застосування політик доступу, автентифікацію користувачів і авторизацію користувачів для доступу до певних ресурсів на основі їхніх ролей і дозволів.

Контроль доступу відноситься до механізмів, які використовуються для обмеження або дозволу доступу до IT-системи або програми. Контроль доступу може приймати різні форми, включаючи фізичний контроль доступу (наприклад, ключ-картки, біометричні сканери), логічний контроль доступу (наприклад, облікові записи користувачів, паролі) і контроль доступу до мережі (наприклад, брандмауери, системи виявлення вторгнень). Контроль доступу має вирішальне значення для забезпечення конфіденційності, цілісності та доступності конфіденційних даних і ресурсів.

З іншого боку, авторизація — це процес визначення того, які дії дозволено виконувати користувачеві в системі чи програмі. Він передбачає визначення та застосування дозволів і рівнів доступу на основі ролі користувача та ресурсів, до яких вони мають доступ.

Авторизація зазвичай реалізується за допомогою політик і механізмів контролю доступуб. Авторизація означає процес надання або заборони певних дій або привілеїв користувачеві або групі користувачів у IT-системі чи додатку. Авторизація зазвичай базується на ідентифікації користувача, ролі та дозволах. Наприклад, авторизованому користувачеві може бути надано можливість переглядати або редагувати певні дані, тоді як неавторизованому користувачеві може бути повністю заборонено доступ до цих даних.

Авторизація є важливим компонентом контролю доступу та необхідна для забезпечення виконання політик безпеки та запобігання несанкціонованому доступу до конфіденційних даних. Вона визначає, які дії користувачеві дозволено виконувати в системі на основі його ідентифікації, ролі та дозволів.

Авторизація необхідна для забезпечення виконання політики безпеки та запобігання несанкціонованому доступу до конфіденційних даних. Деякі поширені технології авторизації включають системи контролю доступу на основі ролей (RBAC), які призначають дозволи користувачам на основі їхніх ролей в організації, і системи контролю доступу на основі атрибутів (ABAC), які використовують такі атрибути, як місцезнаходження користувача, час доби або посадова функція для визначення привілеїв доступу. Політики авторизації також можна застосовувати за допомогою програмних і апаратних механізмів, таких як облікові записи користувачів, паролі та дозволи.

Методи управління ідентифікацією, контролю доступу та авторизації відіграють вирішальну роль у забезпеченні безпеки державних і приватних установ. Ці процеси допомагають забезпечити безпеку, конфіденційність і цілісність конфіденційних даних і ресурсів, керуючи ідентифікаторами користувачів, правами доступу та діями та контролюючи їх. Управління ідентифікацією передбачає встановлення та підтримку ідентичності користувачів і рівнів доступу, тоді як контроль доступу передбачає визначення та застосування політик доступу та автентифікацію користувачів.

Впроваджуючи методи ефективного керування ідентифікацією, контролю доступу та авторизації, організації можуть зменшити ризик витоку даних і кібератак, а також захистити свої системи та програми від несанкціонованого доступу чи зловживання.

Деякі поширені технології керування ідентифікацією включають системи єдиного входу (SSO), які дозволяють користувачам входити в декілька програм за допомогою єдиного набору облікових даних, а також рішення Identity and Access Management (IAM), які забезпечують централізований спосіб керування ідентифікацією користувачів і привілеями доступу [3].

Управління ідентифікацією включає створення, підтримку та контроль цифрових ідентифікацій для користувачів системи або програми. Це включає визначення ролей користувачів і рівнів доступу, створення облікових записів користувачів і керування ними, а також забезпечення точності та актуальності ідентифікаційних даних користувачів. Керування ідентифікацією має важливе значення для забезпечення автентифікації користувачів перед наданням доступу до системи чи програми, а також для відстеження дій користувачів у системі.

Наші висновки мають на меті служити ресурсом для посилення заходів кібербезпеки в умовах сучасного середовища кіберзагроз та складних кібератак, що швидко розвивається.

1. Mollakuqe E, Dimitrova V, Popovska-Mitrovikj A: Data classification based on sensitivity in public and private institutions,14th ICT Innovations Conference 2022. ICT Innovations 2022, Skopje, North Macedonia.

2. Mollakuqe E: Comparative analysis of identity management, access control, and authorization practices in public and private universities. [Dataset], 2024. http://www.doi.org/10.17605/OSF.IO/5P9KE.

3. Grata E. G., Deshpande A., Lopes R. T., Laghari A. A., Khan A. A., Jenice Aroma R., Jumani, A. K. (2024). Artificial intelligence for threat anomaly detection using graph Data bases a semantic outlook. Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection, 249-278.

Штучний інтелект у сфері відеоспостереження

УДК 004.056.5:004.08

Марк Хіленко[1], Максим Фесенко[2]

Державний університет інформаційно-комунікаційних технологій,

[1]markhilenko@gmail.com

Постановка задачі. На сьогоднішній день безпека є одним із пріоритетних напрямків для громадян та організацій. Неодмінною складовою у сфері безпеки та охорони є системи відеоспостереження зі штучним інтелектом.

Один із ключових аспектів систем відеоспостереження із штучним інтелектом є їх можливість аналізувати великі обсяги даних у реальному часі. Нейронні мережі та інші алгоритми машинного навчання можуть обробляти величезні потоки інформації з камер відеоспостереження, датчиків руху, систем виявлення вторгнень та інших джерел, що дозволяє виявляти аномалії та надзвичайні ситуації в реальному часі.

Дослідники постійно працюють над створенням більш точних та ефективних моделей, які можуть розпізнавати нові типи загроз та адаптуватися до змінних умов навколишнього середовища. Отже, зростання потенціалу виявлення загроз завдяки використанню штучного інтелекту є ключовою тенденцією, яка сприяє покращенню безпеки та ефективності охоронних систем [1].

Мета дослідження. Дослідити дані щодо застосування технологій штучного інтелекту в сучасних системах відеоспостереження та визначити практичну їх реалізацію.

Результати дослідження. У роботі проведено аналіз сфер застосування сучасних безпекових та охоронних систем із штучним інтелектом.

• Виявлення загроз.

Системи відеоспостереження зі штучним інтелектом здатні виявляти підозрілу поведінку, залишені предмети, зброю та інші потенційні загрози, що дозволяє оперативно реагувати на інциденти. Наприклад, компанія Bosch Security Systems використовує AI-аналітику для виявлення блокування аварійних виходів, неправильного паркування та інших порушень безпеки [2].

• Розпізнавання обличчя та номерних знаків.

Інтеграція алгоритмів розпізнавання обличь та номерних знаків дозволяє ідентифікувати осіб та транспортні засоби, що сприяє ефективному розслідуванню правопорушень. Наприклад, компанія Flock Safety пропонує автоматизовані системи розпізнавання номерних знаків, які використовуються

в понад 5000 громадах США для виявлення викрадених автомобілів та інших правопорушень [3].

• Прогнозування інцидентів.

Використання штучного інтелекту дозволяє прогнозувати можливі інциденти на основі аналізу поведінки та історичних даних, що підвищує превентивні заходи безпеки. Наприклад, компанія Knightscope розробляє автономні роботи для патрулювання, які можуть виявляти аномальні звуки, зміни температури та інші показники, що свідчать про потенційні загрози [4].

Висновки та перспективи. В результаті дослідження, було виявлено, що використання систем відеоспостереження з штучним інтелектом демонструє значну продуктивність та здатність виявляти загрози. Приклади компаній Bosch Security Systems, Flock Safety та Knightscope показують, що впровадження нейронних мереж та інтеграція з відеоспостереженням значно підвищують ефективність виявлення загроз та зменшує кількість хибних спрацювань.

Подальші дослідження мають бути зосереджені на підвищенні точності, зменшенні помилок та захисті персональних даних.

1. Тенденції у використанні штучного інтелекту для покращення реагування охоронних систем на загрози. URL: https://mindscope.biz.ua/tendenczіyi-u-vykorystanni-shtuchnogo-intelektu-dlya-pokrashhennya-reaguvannya-ohoronnyh-system-na-zagrozy (дата звернення 16.0.2025).

2. Javier Finance, Artificial Intelligence for video surveillance (Use cases). URL: https://javierfinanc e.com/blog/ai-video-surveillance-use-cases/ (дата звернення 16.0.2025).

3. Louise Matsakis, Flock Safety Says Its License Plate Readers Reduce Crime. It's Not That Simple. URL: https://www.wired.com/story/flock-safety-license-plate-readers-crime/ (дата звернення 16.0.2025).

4. How Autonomous Robots are Revolutionizing Public Safety**.** URL: https://knightscope.com/blog/autonomous-security-robots-upgrading-public-safety (дата звернення 16.0.2025).

Аналіз елементів класичної моделі передачі інформації

УДК 519.72

Юрій Хлапонін[1], Володимир Вишняков[2]

Київський національний університет будівництва та архітектури,

[1]y.khlaponin@gmail.com, [2]volodymyr.vyshniakov@gmail.com

Класична модель процесу передачі інформації (запропонована в 1948 році засновником теорії інформації Клодом Шенноном) показана на рис. 1.

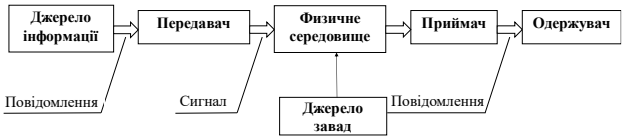


Рис. 1. Модель системи передачі інформації

З цієї моделі ми бачимо, що у разі передачі інформації надсилаються повідомлення та сигнали, а також існує вплив завад у фізичному середовищі, які можуть пошкодити інформацію. Визначення поняття інформації в [1] наведено в наступному вигляді. Інформація – це суть (значення, зміст, сенс, сутність) повідомлення, яка викликає відповідну реакцію системи без інтелекту та впливає на обране рішення інтелектуальною системою. Таке визначення має просте логічне пояснення. Якщо одержувач повідомлення не міг сприйняти його значення (або суть), то інформація не може вважатися прийнятою. Інформацію можна визнати прийнятою лише за умови сприйняття суті повідомлення. З чого витікає, що інформація – це суть повідомлення, а не саме повідомлення чи сигнал. Під інтелектуальними розуміємо системи, які здатні виконувати дії під впливом раніше накопиченої інформації.

Розглянемо процес передачі інформації на прикладі агентів часів Другої світової війни. Горщик з квітами у вікні був обраний сигналом небезпеки для агентів, які прямували до конспіративної квартири. У разі небезпеки агент, який перебував у квартирі, мав поставити цей горщик на вікно. З цього прикладу ми бачимо, що розробник системи передачі інформації повинен обрати якийсь носій інформації (наприклад, горщик з квітами). Також необхідно обрати інформаційну ознаку носію з її значенням. Інформацію про це необхідно передати кожній зі сторін системи передачі. Це означає, що для створення системи передачі необхідно перед цим передати деяку інформацію, а для цього, у свою чергу, також необхідно створити систему передачі інформації. Іншими словами, виходить нескінченний цикл. Цю проблему можна усунути, якщо сторони мають спільне походження з однієї й тієї ж інформаційної системи, де вони повинні отримати знання про те, як обмінюватися інформацією. Уточнимо, як відбувається передача інформації про небезпеку в даній системі. Ця інформація формується агентом у секретній квартирі на основі його спостережень. Через систему передається лише характеристика носія, а саме місцезнаходження горщика з квітами. Щоб отримати інформацію, агент, який прямує до секретної квартири, повинен володіти знаннями про носій інформації і значення його характеристик. Таким чином, ми бачимо, що через систему передається не повна інформація, а лише деяка її частина. Для аналізу процесу передачі інформації в живій природі нзгадаємо дослідження, проведене в 2010 році в Інституті JCVI (Інститут Дж. Крейга Вентера). Це дослідження довело, що інформація, необхідна для забезпечення існування бактерії, зосереджена виключно в послідовності нуклеотидів молекули ДНК. Для цього в пам'ять комп'ютера вводили послідовність символів A, G, C, T, яка відповідала

послідовності нуклеотидів молекули ДНК бактерії Mycoplasma genitalium (A – аденін, G – гуанін, C – цитозин, T – тимін). Штучну ДНК синтезували з пам'яті комп'ютера. Заміна природної ДНК штучною в живій бактерії не вплинула на життєдіяльність бактерії [2]. Це свідчить про те, що дана послідовність містить достатньо інформації для забезпечення життя та розмноження бактерії. Передача інформації в бактеріальній клітині починається з дії біологічного механізму РНК-полімерази, яка створює копії ділянок молекули ДНК у вигляді ланцюгів РНК, як показано на рис. 2..

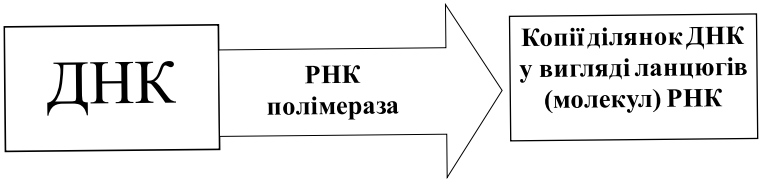


Рис. 2. Процес копіювання ділянок ДНК у ланцюги РНК.

РНК-полімераза аналізує послідовність нуклеотидів у молекулі ДНК з метою виявлення комбінації TATAAT, суть якої полягає в тому, що слід розпочинати процес копіювання. Під час копіювання аналіз нуклеотидної послідовності продовжується для виявлення комбінації AAAA, яка означає, що слід завершити копіювання та повернутись до пошуку наступної комбінації TATAAT. Утворені копії ДНК у вигляді ланцюгів РНК є носіями інформації для побудови всіх біологічних механізмів живої клітини [3]. З цього прикладу витікає, що механізм РНК-полімерази містить інформацію про значення комбінацій TATAAT та AAAA, без яких процес передачі керуючої інформації від ДНК до РНК-полімерази був би неможливим. Важливу роль у живих системах передачі інформації відіграє джерело завад. Через завади відбуваються випадкові зміни в молекулі ДНК. Якщо ці зміни не призводять до втрати здатності до розмноження, то випадково може утворитися істота, більш придатна для виживання. Такі зміни називаються мутаціями. Вони можуть відбуватися як поза життєвим циклом, так і в його межах. При цьому нові знання отримуються та впроваджуються в систему методом спроб та помилок. Цей метод передбачає, що для досягнення успіху слід мати змогу зробити значну кількість помилкових спроб. Саме так відбувається розвиток живих істот.

Необхідною вимогою до учасників процесу передачі інформації є знання значень параметрів носія. Без цього передача інформації між учасниками неможлива. Оскільки для отримання цих знань також необхідно передати інформацію, то утворюється нескінченний цикл. Щоб уникнути нескінченому циклу, необхідно, щоб учасники мали спільне походження з єдиної інформаційної системи, від якої надаються знання щодо обміну інформацією. Це означає, що всі системи, які здатні спілкуватися одна з одною, походять з єдиної батьківської системи. Іншого варіанту забезпечення обміну інформацією не існує.

1. Хлапонін, Ю., Вишняков, В. (2024). Визначення поняття інформації для живих і штучних інформаційних систем. Підводні технології, 2(15), 78–89. https://smarttech.knuba.edu.ua/.

2. Gibson D.G., Glass J.I. & et al. (2010). Creation of a bacterial cell controlled by a chemically synthesized genome. Science (New York, N.Y.). 2010-07-02; 329.5987: 52-6. https://www.jcvi.org/publications/creation-bac-terial-cell-controlled-chemically-synthesized-genome

3. Вишняков В. . (2024). Аналіз інформаційних процесів у живих клітинах. Грааль науки, (35), 181–184. https://doi.org/10.36074/grail-of-science.19.01.2024.032

Аналіз сучасних методів виявлення атак на великі мовні моделі

УДК 004.056.5

Ігор Хоменко

НТУ Харківський Політехнічний Університет,
Ihor.Khomenko@cs.khpi.edu.ua

Метою дослідження є порівняльний аналіз ефективності двох сучасних методів захисту Великих Мовних Моделей (ВММ) – SmoothLLM та Erase-and-Check – у протидії поширеним адверсаріальним атакам типу джейлбрейк (наприклад, GCG та PAIR). Наразі є потреба у розробці та оцінці надійних захисних механізмів для забезпечення безпечного розгортання та використання ВММ[1]..

У ході дослідження було проведено експериментальну оцінку методів SmoothLLM та Erase-and-Check. SmoothLLM, використовує техніку згладжування через множинні пертурбації вхідного запиту та агрегацію відповідей для виявлення аномалій, характерних для адверсаріальних промптів[2]. Erase-and-Check ідентифікує шкідливі елементи шляхом систематичного видалення частин промпту та перевірки отриманих підпослідовностей за допомогою фільтра безпеки [3].

Обидва методи були протестовані проти відомих атак GCG та PAIR. Ефективність оцінювалася за показником зниження частоти успішних атак (Attack Success Rate, ASR) на таких моделях, як Vicuna, Llama2, GPT-3.5 та GPT-4.

Таблиця 1

Ефективність захисту від атак на великі мовні моделі за допомогою SmopthLLM

Тип атаки	Велика мовна модель	Фактор зниження показнику успіху атаки (ASR)
GGG	Vicuna	<1%
GGG	Llama2	<1%
GGG	GTP-3.5	<1%
GGG	GPT-4	<1%
PAIR	Vicuna	2x

PAIR	GPT-4	2x
PAIR	GPT-3.5	29x
Swap, N>6	Llama2	50x
Swap, N>6	Vicuna	100x
N=2, q=10%	Vicuna	2.5-7.0x
N=2, q=10%	Llama2	5.7-18.6%

Ефективність Erase-and-Check може сильно залежати від конкретної моделі LLM, типу атаки, розміру пертурбації, що аналізується, а також якості та конфігурації фільтра безпеки, який використовується для перевірки підпослідовностей. Автори дослідження про метод Erase-and-Check заявляють про те, що за певних умов метод може гарантувати, що шкідливий промпт не буде помилково класифікований як безпечний. Застосування рандомізованої версії Erase-and-Check (RandEC) або версій, що використовують градієнтну інформацію (GradEC), також показує ефективність у зниженні ASR проти автоматичних атак типу GCG.

Як зазначають автори методу Erase-and-Check, використання різних версій методів, таких як RandEC та GradEC, хоч і дозволяють пришвидшити процес пошуку вразливостей, але вони менш точні за Erase-and-Check. Також ефективність цих методів пов'язана з тим, як LLM захищена за замовчуванням.

Таблиця 2

Ефективність захисту від атак на великі мовні моделі за допомогою Erase-and-Check

Тип атаки	Велика мовна модель	Фактор зниження показнику успіху атаки (ASR)
GGG	Vicuna	3.6%
PAIR	Vicuna	16.4%
Різні типи (суфіксні, вставки, інфузія)	GTP-3.5	Можливість отримання сертифікованої безпеки для шкідливих промптів

Результати демонструють, що обидва методи здатні суттєво знизити ефективність адверсаріальних атак. SmoothLLM показав особливо високу ефективність проти GCG-атак, досягаючи зниження ASR до <1% для низки досліджуваних моделей при оптимальних параметрах. Erase-and-Check також продемонстрував значне зниження ASR, особливо ефективно виявляючи приховані шкідливі інструкції, хоча його показники можуть сильніше залежати від конфігурації фільтра безпеки та типу атаки.

Незважаючи на ефективність проаналізованих підходів, існує потреба у подальших дослідженнях. Еволюція тактик атак, специфічність різних архітектур ВММ, обчислювальна складність існуючих рішень та поява нових векторів загроз вимагають розробки більш адаптивних, універсальних та обчислювально ефективних методів захисту ВММ.

1. OWASP Top 10 for LLM Applications 2025. URL: https://tinyurl.com/579xcepd (дата звернення: 22.04.2025).
2. Alexander Robey, Eric Wong, Hamed Hassani, George J. Pappas., SMOOTHLLM: Defending Large Language Models Against Jailbreaking Attacks, 2024. p 8-13.
3. Aounon Kumar, Certifying LLM Safety against Adversarial Prompting, 2025. 18p.

Моделі оцінювання залишкового ризику в інформаційних системах

УДК 004.056.53
Юлія Хохлачова
Державний торговельно-економічний університет,
yuliiahohlachova@gmail.com

Оцінювання залишкового ризику передбачає аналіз взаємодії кіберзагроз із засобами захисту інформації. Основні підходи до моделювання залишкового ризику включають [1, 2]:

- ймовірнісні моделі, які визначають ризик як ймовірність успішної реалізації загроз при існуючих механізмах захисту;
- детерміновані моделі, що базуються на аналізі вразливостей системи та рівня її захисту;
- гібридні моделі, які поєднують ймовірнісні підходи та експертні оцінки.

Доступність інформаційних ресурсів є критичною характеристикою безпеки ІС. Запропонована модель оцінює рівень ризику шляхом аналізу [3, 4]:

- інтенсивності атак типу DoS/DDoS;
- надійності механізмів розподілу навантаження;
- швидкості виявлення та реагування на інциденти.

Ймовірність порушення доступності (P) визначається як сукупність впливу атак (A), ефективності механізмів захисту (Z) та часу відновлення (T):

P=AZ×TP = \frac{A}{Z \times T}.

Чим більша величина P, тим вищий рівень залишкового ризику для доступності ІС.

Практичне застосування розроблених моделей:

1. Оцінювання моделі забезпечення доступності функціонування інформаційних систем на основі залишкового ризику

Модель оцінювання залишкового ризику використовується для аналізу загроз доступності інформаційних ресурсів у системах, зокрема для визначення ймовірності порушення доступності через різні атаки або збої. Основна мета — оцінити залишковий ризик та сформувати стратегії його мінімізації.

2. Оцінювання моделі забезпечення цілісності ресурсів інформаційних систем на основі залишкового ризику. Ця модель оцінювання залишкового ризику використовується для аналізу загроз цілісності інформації в інформаційних системах (ІС). Вона дозволяє визначити ймовірність порушення цілісності даних через несанкціоновану модифікацію, знищення або спотворення інформації.

3. Оцінювання моделі забезпечення конфіденційності ресурсів інформаційних систем на основі залишкового ризику. Ця модель оцінювання залишкового ризику використовується для аналізу загроз конфіденційності інформації в інформаційних системах (ІС). Вона дозволяє оцінити ймовірність порушення конфіденційності через несанкціонований доступ, витік даних або подолання криптографічного захисту.

Для оцінки ефективності запропонованих моделей було проведено тестування на прикладі корпоративної інформаційної системи. Експериментальні результати показали:

- використання моделі оцінювання залишкового ризику дозволило виявити критичні точки у системі безпеки;
- оптимізація механізмів захисту знизила залишковий ризик доступності на 30%, цілісності – на 25%, конфіденційності – на 40%.

Запропоновані моделі можуть бути використані для підвищення ефективності систем кіберзахисту в державних установах, комерційних компаніях та критичних інфраструктурах.

Було представлено нові моделі оцінювання залишкового ризику в інформаційних системах, які дозволяють більш точно визначати рівень загроз та оптимізувати заходи кібербезпеки. Практичне застосування моделей демонструє їхню ефективність для оцінки стану захищеності інформаційних ресурсів та розробки стратегії кіберзахисту. Перспективи подальших досліджень включають удосконалення методик оцінювання ризику та інтеграцію запропонованих моделей у системи моніторингу інформаційної безпеки.

1. ISO/IEC 27005:2018. Information security risk management.
2. NIST Special Publication 800-30. Guide for Conducting Risk Assessments.
3. Ransbotham S., Mitra S., Ramsey J. "Security risk management: frameworks and best practices." Journal of Cybersecurity, 2022.
4. ENISA Threat Landscape Report 2023.

Аналіз безпеки коду веб додатку за допомогою великих мовних моделей

УДК 004.056:004.415.3:004.89

Тарас Цаволик[1], Лукаш Остап[2]
Західноукраїнський національний університет,
[1]calisto2292@ukr.net, [2]oslukash@gmail.com

Веб-додатки є важливими складовими сучасної цифрової інфраструктури, але їхня складність призводить до поширення уразливостей у коді (XSS, SQL-ін’єкції, небезпечне використання eval тощо). Тому автоматизований аналіз

коду для виявлення таких уразливих патернів стає дедалі актуальнішим. Це відкриває нові можливості для автоматизованого пошуку вразливостей, оскільки великі мовні моделі (LLM) можуть використовувати своє “розуміння” контексту коду та виводити здогадки на основі вивчених прикладів [4].

На рисунку1 наведено фрагмент коду з небезпечним використанням *eval* який може призвести до XSS-атаки.

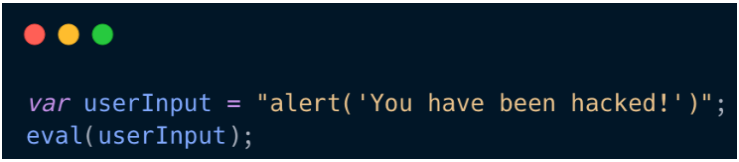


Рис.1. Приклад виконання шкідливого коду

Тут вміст *userInput* не проходить валідацію, тож будь-який скрипт (наприклад, виклик *alert*) буде виконано. Такі прийоми широко відомі як XSS-вразливості, якщо дані користувача не фільтруються перед *eval*, зловмисник може впровадити і виконати довільний JS-код [1, 2].

LLM надають новий підхід, де їх запитують проаналізувати фрагмент коду. Моделі, навчанні на великій кількості відкритого коду (включно з прикладами вразливостей), здатні розпізнавати характерні ознаки небезпечних патернів. Так, LLM «вчаться» знаходити шаблони небезпечного коду (наприклад, незахищені eval чи вставки HTML) і можуть використовувати логічні аналогії та аналіз контексту [3]. Модель може проаналізувати блок коду і дати пояснення, чи містить він уразливість.

Наприклад, задавши ChatGPT або Bard запит «Чи є в цьому коді вразливість?» разом із фрагментом, модель детально аналізує код і видає зрозуміле пояснення вразливості. Таким чином, LLM використовують семантичний аналіз і «зв’язність» програмного контексту, що значно полегшує знаходження складноформульованих вад.

Результати різних досліджень свідчать, що LLM-методи часто перевершують традиційні підходи. Наприклад, GPT-4 за експериментальними даними дав точність виявлення уразливостей, значно вищу за попередні алгоритми. Натомість звичайні SAST-інструменти (статичні аналізатори) мають низьку продуктивність: їх показник виявлення становить лише близько 11–26% у стандартних наборах тестів. Класичні ML-моделі (наприклад, на основі репрезентацій коду та SVM/нейромереж) демонструють проміжні результати (приблизно 50–60%).

Таблиця 1

Оцінка точності виявлення вразливостей в коді

Метод	Точність виявлення, %
LLM (наприклад, GPT-4)	≈85
Класичний ML	≈60
Правило (статичний аналіз)	≈25

У таблиці наведено приблизний рівень точності виявлення вразливостей для різних підходів.

Великі мовні моделі можуть охоплювати широкий спектр уразливостей без жорсткої прив'язки до заздалегідь визначених правил. Завдяки потужним когнітивним здібностям вони краще розуміють семантику коду і можуть надавати пояснення (chain-of-thought) щодо своїх висновків. LLM добре працюють на помірних за розміром фрагментах коду і мають потенціал навчатися на нових патернах атак.

У великих чи складних кодових базах їх точність може знижуватися, зростає ризик «галюцинацій» та хибних спрацьовувань. Деякі тонкі багатофункціональні уразливості LLM досі виявляють ненадійно. Крім того, результати залежать від якості запиту/контексту, а моделі можуть генерувати помилкові або неповні пояснення, що потребує верифікації людиною.

Підходи на основі LLM мають низку переваг у аналізі безпеки коду веб-додатків: висока гнучкість у розумінні контексту, можливість обробляти складні умови та різні мови програмування, а також здатність до природномовного пояснення ризиків. Водночас вони потребують значних обчислювальних ресурсів і можуть давати помилкові результати при погано підібраному prompt. Також показано, що спеціальне донавчання LLM додатково покращує результати виявлення. Таким чином, LLM можуть доповнювати традиційні rule-based та ML-підходи, проте не замінюють їх цілком.

1. OWASP Foundation. Direct Dynamic Code Evaluation – Eval Injection. OWASP. 2024. URL: https://owasp.org/www-community/attacks/Direct_Dynamic_Code_Evaluation_Eval%20Injection (дата звернення: 12.05.2025).
2. Mozilla Developer Network (MDN). Cross-site scripting (XSS). 2024. URL: https://developer.mozilla.org/en-US/docs/Glossary/Cross-site_scripting (дата звернення: 12.05.2025).
3. Tamberg K., Bahsi H. Harnessing Large Language Models for Software Vulnerability Detection: A Comprehensive Benchmarking Study. arXiv. 2024. URL: https://arxiv.org/abs/2405.15614 (дата звернення: 12.05.2025).
4. Ding Y., Fu Y., Ibrahim O., Sitawarin C., Chen X., Alomair B., Wagner D., Ray B., Chen Y. Vulnerability Detection with Code Language Models: How Far Are We? arXiv. 2024. URL: https://arxiv.org/abs/2403.18624 (дата звернення: 12.05.2025).

Можливості та обмеження OSINT у боротьбі з дезінформацією

УДК 004.56.5(043.2)
Олександр Цубера[1] Олександра Чорна[2]
Західноукраїнський національний університет,
fcitcyber25@zoom.wunu.edu.ua

У сучасному інформаційному суспільстві стрімке поширення дезінформації становить суттєву загрозу як для окремих осіб, так і для національної безпеки загалом. Одним із ключових інструментів боротьби з цим явищем є OSINT (Open Source Intelligence) — технологія збору, аналізу та інтерпретації

відкритих джерел інформації. OSINT дає змогу виявляти неправдиві наративи, перевіряти факти, здійснювати атрибуцію джерел та проводити незалежні розслідування, що робить його важливим інструментом у кібербезпеці та журналістиці розслідувань [1]. Метою роботи є аналіз можливостей та обмежень застосування OSINT у виявленні та протидії дезінформації.

На рис.1 подано загальну схему використання OSINT у контексті перевірки достовірності інформації. Вона передбачає багатоступеневу роботу з відкритими джерелами: пошук даних (вебсайти, соціальні мережі, фото, відео), аналіз їхньої автентичності, перевірка часу та місця зйомки, порівняння з іншими відкритими даними.[2]

Рис.1. Схема алгоритму OSINT розслідування

На рис.2 зображено приклад практичного використання OSINT для викриття дезінформації у соціальних мережах. Такий аналіз дозволяє ідентифікувати фейкові акаунти, боти, штучно роздмухані інформаційні кампанії.

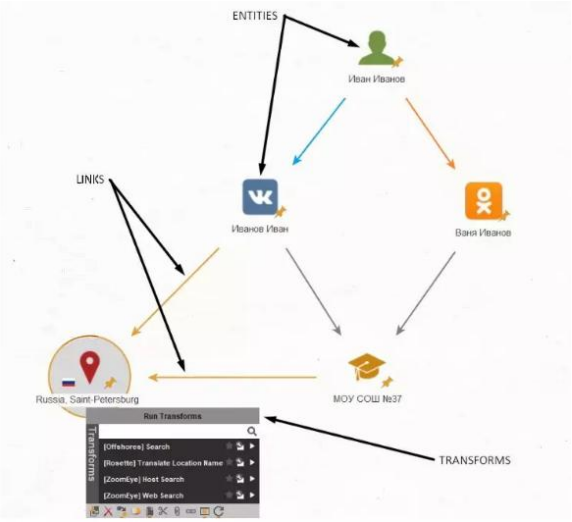


Рис.2. OSINT інструмент Maltego

Попри значні переваги, OSINT має низку обмежень. Зокрема, доступ до деяких джерел може бути обмеженим або піддаватися цензурі, а інтерпретація даних — суб'єктивною. Також існують юридичні та етичні аспекти, пов'язані з обробкою особистої інформації. Проте навіть з цими обмеженнями, OSINT залишається потужним інструментом для протидії інформаційним загрозам.[3]

У роботі було проаналізовано можливості використання OSINT у боротьбі з дезінформацією, визначено основні інструменти та етапи аналізу, а також окреслено головні переваги та обмеження даного підходу.

1. Higgins, A. (2023). Bellingcat and the Rise of Open-Source Investigations. The New York Times. URL: https://www.nytimes.com/bellingcat-osint (дата звернення: 01.04.2025).
2. OSINT Framework. URL: https://osintframework.com/ (дата звернення: 01.04.2025).
3. NATO StratCom COE. Detecting Disinformation: Best OSINT Practices. URL: https://stratcomcoe.org (дата звернення: 01.04.2025).

Розробка алгоритму вбудовування цифрових водяних знаків у відео

УДК 004.056

Ксенія Чабаненко[1], Наталія Кушніренко[2]
Національний університет «Одеська політехніка»,
[1]chabanenkoksenia3@gmail.com, [2]kushnirenko@op.edu.ua

Традиційні методи захисту, такі як криптографія чи контроль доступу, не гарантують збереження авторства або джерела походження після публікації

контенту у відкритих середовищах. У зв'язку з цим цифрові водяні знаки виступають ефективним засобом вирішення задач ідентифікації, верифікації та відстежування цифрових ресурсів. Особливої актуальності набуває розробка таких алгоритмів вбудовування, які забезпечують баланс між високою стійкістю до атак (наприклад, перекодування, фільтрація, стиснення), непомітністю для користувача та достатньою ємністю для передавання службової інформації [1].

У роботі представлено алгоритм вбудовування цифрових водяних знаків у частотну область з використанням дискретного косинусного перетворення. Запропонований підхід передбачає розподіл інформації водяного знака між аудіодоріжкою та кадровими складовими відео. Метою дослідження є створення ефективного алгоритму захисту авторських прав на мультимедійний контент шляхом вбудовування цифрового водяного знака. Реалізований алгоритм забезпечує підвищену стійкість водяного знака до атак і високий рівень непомітності.

Для досягнення зазначеної мети запропонований алгоритм використовує такі елементи:

- вбудовування у частотні коефіцієнти відео- та аудіофрагментів;
- розподіл цифрового водяного знака між аудіодоріжкою та відеокадрами;
- використання ключа для псевдовипадкової вибірки елементів.

Алгоритм використовує дискретне косинусне перетворення (ДКП) для переведення вхідних даних — кадрів та аудіосемплів — у частотну область і вбудовування водяного знака за методом Коха, що ґрунтується на модифікації співвідношення між парою середньочастотних коефіцієнтів [2]. Даний метод вбудовування передбачає розділення вхідного зображення на блоки розміром 8*8 пікселів та застосуванням ДКП до кожного окремого блоку, при цьому вбудовування відбувається з урахуванням того, що один блок придатний для запису одного біта інформації.

У більшості випадків, вбудовування цифрових водяних знаків у відео передбачає його представлення у вигляді послідовності зображень (кадрів), в які вбудовується знак [3].

У запропонованому алгоритмі відео розглядається як сукупність паралельних послідовностей: відеокадрів та відповідних фрагментів аудіодоріжки. Для вибірки кадрів, семплів та блоків, до яких вбудовується знак, використовується числовий ключ. Запропонований алгоритм забезпечує високий рівень надійності та стійкості ЦВЗ завдяки розподілу інформації між кадрами та аудіокомпонентами сигналу. Такий підхід дозволяє зменшити ступінь модифікації кожного окремого носія, що підвищує непомітність, порівняно з методами, які використовують виключно кадри в якості вхідних даних.

З метою забезпечення індивідуального та непередбачуваного розподілу водяного знака у відео застосовується генерація псевдовипадкових чисел. Текстовий ключ K використовується для ініціалізації генератора

псевдовипадкових чисел (ГПВЧ), який формує значення за наступною формулою:

$$R = min + (Nmod(max - min + 1)), \quad (1)$$

де *R*– псевдовипадкове число в межах діапазону [min,max], *N* – ціле число, отримане з хешу повідомлення-ключа, а *min, max* – мінімальне та максимальне значення діапазону, в якому генерується число. Отже, процес вбудовування включає наступні етапи:

1) розподіл відео на аудіодоріжку та кадрові складові;
2) ініціалізація генератора псевдовипадкових чисел за текстовим ключем;
3) вибір кадрів/семплів та блоків на основі псевдовипадкової вибірки;
4) перетворення обраних фрагментів у частотну область методом ДКП;
5) вбудовування ЦВЗ за методом Коха у середньочастотні коефіцієнти.

Таким чином, запропонований алгоритм забезпечує підвищену стійкість до атак завдяки розподілу водяного знаку між відео- та аудіоскладовими. Використання псевдовипадкового числа як основи для ключової вибірки забезпечує варіативність і непередбачуваність структури вбудовування. Описаний алгоритм був розроблений з метою реалізації у веб-застосунку для захисту мультимедійних даних. Програмна реалізація здійснюється з використанням сучасних бібліотек для обробки медіаданих, що забезпечують доступ до окремих кадрів відео та аудіофрагментів. Такий підхід дозволяє забезпечити зручність використання та масштабованість рішення в реальних умовах.

1. Мартинюк Г. В., Мелешко Т. В., Бичков В. В. Огляд існуючих задач, які можна вирішувати за допомогою стеганографії. Забезпечення кібербезпеки та захисту інформації: Колективна монографія. Київ: Європейський університет, 2023. с. 159–168.
2. Fridrich, J. Digital image steganography using stochastic modulation / Fridrich J., Goljan M. // Department of Electrical and Computer Engineering; SUNY Binghamton, Binghamton, NY, USA.
3. Шостак Н. В., Безрук В. М., Астраханцев А. А. Вибір переважного алгоритму вбудовування цифрових водяних знаків в відеофайли. Радіоелектроніка, інформатика, управління. 2018. № 3. с. 167-173.

ITSM-рішення як інструмент підвищення ефективності реагування на інциденти інформаційної безпеки

УДК 621.395.7 (043.2)
Максим Чмель[1], Геннадій Шаповалов[2]
Національний університет «Одеська політехніка»,
[1]9480565@stud.op.edu.ua, [2]shapovalov@op.edu.ua

У сучасному цифровому середовищі, де бізнес-процеси нерозривно пов’язані з інформаційними технологіями, стійкість компанії залежить не лише від технічного рівня захисту, а й від здатності організовано й оперативно реагувати на інциденти інформаційної безпеки. Витоки даних, збої в роботі

сервісів або спроби несанкціонованого доступу можуть завдати суттєвої шкоди – як фінансової, так і репутаційної. Тому управління інцидентами ІБ сьогодні розглядається не як вузько технічна задача, а як комплексна управлінська функція, що вимагає системного підходу.

Одним із таких підходів є впровадження систем управління IT-сервісами (ITSM), які дозволяють перейти від реактивного реагування до чітко структурованого процесу. Вони забезпечують єдину точку входу для фіксації інцидентів, дозволяють їх класифікувати, автоматично призначати відповідальних, вести хронологію дій, формувати супровідну документацію та здійснювати моніторинг ситуації в реальному часі. Такий підхід дозволяє значно зменшити час реакції, уникнути дублювання завдань, покращити якість розслідувань і накопичувати статистику для подальшого аналізу.

Особливу роль ITSM-рішення відіграють у побудові комунікації між користувачами та службами підтримки через концепцію єдиної точки контакту (SPOC). Це забезпечує швидке виявлення потенційних загроз і зменшує навантаження на команди ІБ. Крім того, системи дозволяють інтегрувати політики безпеки в загальний процес сервіс-менеджменту, автоматизуючи ескалацію інцидентів відповідно до рівня ризику.

У цьому контексті окрему увагу варто приділити власній розробці – ITSM-рішенню, створеному з урахуванням сучасних викликів у сфері інформаційної безпеки. В його основі – поєднання гнучкої логіки обробки подій, автоматизації рутинних завдань та прозорої взаємодії між усіма учасниками процесу (рис. 1)

Рис. 1. Принцип роботи розробленої системи

Система дозволяє швидко визначати критичність інциденту, розподіляти відповідальність з урахуванням навантаження та компетенцій, інтегруватися з SIEM, службами сповіщення (Slack, Microsoft Teams), а також функціонує як у хмарному середовищі, так і на локальних серверах – що є критично важливим для компаній, які прагнуть повного контролю над своїми даними.

Ключова особливість рішення – фокус на зручності для кінцевого користувача. Інтерфейс та логіка системи інтуїтивно зрозумілі навіть для співробітників без спеціалізованої IT-підготовки, що сприяє залученню всього персоналу до формування культури кібербезпеки та зниженню ризиків людського фактору.

Результати дослідження свідчать про практичну ефективність запропонованого підходу. Під час моделювання інцидентів (спроби доступу, витоки, порушення політик доступу) середній час реагування скоротився на 42% порівняно з традиційними підходами. Кількість інцидентів, які не були ескальовані або залишились без відповіді, знизилася майже вдвічі. Крім того, автоматизація рутинних задач дозволила зменшити навантаження на IT-відділ і прискорити процес звітності. Це особливо важливо в умовах кризових ситуацій або аудиторських перевірок.

Таким чином, ITSM-системи – і зокрема розроблене рішення – демонструють свою ефективність не лише в технічному, а й в управлінському вимірі. Упровадження таких рішень дозволяє підвищити загальний рівень кіберстійкості організації, мінімізувати наслідки інцидентів та формувати культуру інформаційної відповідальності на всіх рівнях.

Упровадження таких систем, за певних умов, може сприяти зниженню впливу людського фактора та формуванню культури інформаційної відповідальності на всіх рівнях організації. Крім того, наявність єдиної точки контакту, автоматизованого розподілу завдань і можливості інтеграції з іншими інструментами (SIEM, служби сповіщень тощо) відкриває можливості для підвищення загального рівня кіберстійкості.

1. Клімович І. М., Подобєд Т. В. IT-аудит як один з перспективних напрямків інформаційної перевірки підприємств. Вісник Хмельницького національного університету. Економічні науки, 2016. – № 5 (1). – С. 89–93.URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Vchnu_ekon_2016_5(1)__21.pdf

2. Дядечко А., Даценко І., Головченко О. Концептуальні аспекти технологічної підтримки інформаційної інфраструктури Міністерства оборони України. Сучасні інформаційні технології у сфері безпеки та оборони, 2024. – Т. 51, № 3. – С. 96–107. URL: https://sit.nuou.org.ua/article/view/311034/310285 (дата звернення: 08.04.2025).

3. Galup S. D., Dattero R., Quan J. J., Conger S. An overview of IT service management. Communications of the ACM, 2009. – Vol. 52, No. 5. – P. 124–127. URL: https://dl.acm.org/doi/fullHtml/10.1145/1506409.1506439 (дата звернення: 08.04.2025).

Адаптивні нейромережі у боротьбі з веб-спамом

УДК 004.8:004.02

Іван Шахматов[1], Ірина Замрій[2]
Державний університет інформаційно-комунікаційних технологій,
[1]i.shahmatov@duikt.edu.ua, [2]i.zamrii@duikt.edu.ua

Зростання кількості веб-сервісів та інтерактивних форм, що використовуються на сайтах, супроводжується активізацією різноманітних спам-атак, які загрожують безпеці, перевантажують сервери і погіршують взаємодію користувачів із сайтами. Традиційні методи боротьби зі спамом, які

базуються на статичних правилах або простих фільтрах, стають неефективними через постійне вдосконалення технологій, що використовуються спамерами. Запропонована графова нейронна мережа, яка забезпечує автоматизоване виявлення та класифікацію спаму, знижує необхідність ручної модерації, а також має механізми самонавчання й адаптації до нових видів загроз.

Створення гібридних систем на основі поєднання алгоритмів машинного навчання, таких як Decision Tree, Support Vector Machine та Naive Bayesian Classifier, дозволяє здійснювати ефективну поетапну фільтрацію користувачів у соціальних мережах, виявляючи аномалії у їхній поведінці та контенті. Використання такого каскадного підходу демонструє значне підвищення точності виявлення шкідливих або небезпечних активностей порівняно з традиційними моделями [1]. Перспективним є також застосування методів, що аналізують семантичну структуру URL-запитів, виділяючи «вразливі» компоненти, які часто змінюються атакувальниками. Реалізація патерн-дерев і врахування "скелетної структури" URL дозволяє суттєво підвищити точність класифікації HTTP-запитів і знизити кількість помилкових спрацювань при виявленні нових видів атак [2].

Загальний огляд наукових публікацій показує поширеність використання штучних нейронних мереж (ANN), CNN, дерев рішень та ансамблевих моделей для задач кібербезпеки, зокрема виявлення спаму, фішингу та шкідливих посилань. При цьому відзначається потреба у зменшенні складності моделей та підвищенні їхньої адаптивності для забезпечення ефективної боротьби з веб-загрозами [3].

Модель базується на графі G=(V,E),, де V — це вузли, які представляють окремі повідомлення з веб-форм, а E — зв'язки між ними, які можуть грунтуватися на подібності даних або часових характеристиках надсилання. Кожен вузол ініціалізується вектором ознак Xco, які отримуються безпосередньо із заповненої форми. В процесі роботи моделі стан кожного вузла hv(0) оновлюється ітеративно через функцію поширення (1):

$$hvl+1=fXco,Xnb,Hnbl. \quad (1)$$

Цей підхід забезпечує динамічну адаптацію моделі до змін поведінки хакерів (бот-програм). Після завершення ітераційного процесу фінальний стан вузла використовується для класифікації через активаційну функцію (2):

$$ov=g(hv,Xv), \quad (2)$$

де отримується результат про те, чи є повідомлення спамом, підозрілим або легітимним. Важливою особливістю підходу є можливість враховувати ручний зворотний зв'язок адміністратора для покращення точності класифікації.

Для побудови ефективної моделі фільтрації веб-спаму використовуються дані, зібрані з веб-форм, які включають такі поля: IP-адреса, країна, час відправлення, час останнього відправлення з цього IP, повідомлення з форми, ім’я, номер телефону та статус повідомлення (наприклад, "СПАМ", "Не СПАМ", "Не визначено"). На основі цих даних можна ідентифікувати аномальні шаблони поведінки, визначати географічні зони підвищеної спам-активності та виявляти автоматизовані надсилання. Кожне повідомлення представляється як вузол графа, ознаковий вектор якого формується з вищевказаних параметрів.

Зв'язки між вузлами визначаються за критеріями подібності тексту або часової близькості надсилань.

Для програмної реалізації, була запропонована структура системи, яка реалізована через низку класів: Node (вузол графа), Edge (зв'язки між вузлами), Graph (загальна структура графа), та SpamFilterGNN — основний клас нейронної мережі для класифікації. В основі моделі лежать графові конволюційні шари, що дозволяють оновлювати стан вузлів із урахуванням контексту. Система підтримує механізм самонавчання з інтерактивним коригуванням результатів на основі ручної модерації, забезпечуючи постійне вдосконалення точності класифікації. Модель складається з двох графових конволюційних шарів: перший трансформує вхідні ознаки у внутрішній простір розмірністю 16, а другий здійснює остаточну класифікацію. Між шарами використовується функція активації ReLU та Dropout для запобігання перенавчанню. Така структура дозволяє моделі враховувати не лише локальний контекст вузлів, а й інформацію від їхніх сусідів другого порядку, забезпечуючи глибший аналіз графової структури подань.

Для оцінки ефективності моделі було використано реальний набір із 5000 повідомлень, класифікованих вручну на категорії: «спам», «підозріле» та «не спам». Модель навчалась на 70% даних, 15% використано для валідації і 15% — для тестування. Оцінка точності проводилася за метриками: Accuracy (частка правильно класифікованих повідомлень), Precision (точність виявлення спаму серед усіх визначених як спам) Результати моделі: accuracy – 98,2%, precision – 96,7%.

1. Rahman M. S., Halder S., Uddin M. A. An efficient hybrid system for anomaly detection in social networks // Cybersecurity. – 2021. – Vol. 4, Article number: 10. – DOI: https://doi.org/10.1186/s42400-021-00074-w.

2. Cheng Z., Cui B., Qi T., Yang W., Fu J. An improved feature extraction approach for Web anomaly detection based on semantic structure // Security and Communication Networks. – 2021. – Article ID 6661124. – Published: 11 February 2021. – DOI: https://doi.org/10.1155/2021/6661124.

3. Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. IEEE Access, 8, 146598–146612. DOI: https://doi.org/10.1109/ACCESS.2020.3013145.

Методи та засоби виявлення аномалій у децентралізованих транзакціях публічних блокчейн мереж

УДК 004.056 Руслан Шевчук

Західноукраїнський національний університет\University of Bielsko-Biala

rsh@wunu.edu.ua

Блокчейн-технологія є однією з ключових інновацій XXI століття, що забезпечує низку переваг для реалізації децентралізованих систем, зокрема розподілене зберігання даних, одноранговy передачу інформації, високий рівень конфіденційності та ефективне трасування транзакцій [1]. У публічних

блокчейн-мережах, де транзакції є відкритими та незмінними, ці характеристики сприяють створенню прозорих цифрових екосистем без потреби у централізованому контролі.

Однак децентралізований характер таких мереж створює сприятливі умови для зловмисної діяльності, що призводить до зростання кількості аномальних транзакцій та шахрайських схем. Згідно зі звітом Chainalysis Blockchain Scam Report 2024, сума коштів, отриманих незаконними адресами, становила 4,6 мільярда доларів США у 2018 році та зросла до 24,2 мільярда у 2023 році [2]. Незважаючи на вбудовані криптографічні механізми захисту та алгоритми консенсусу, публічні блокчейн-мережі залишаються вразливими до різних видів атак, включно з фішингом, схемами Понці, спам-транзакціями, прихованим майнінгом та зловживанням смартконтрактами [3,4].

Виявлення аномалій у децентралізованих транзакціях є складним завданням через низку факторів: великий обсяг даних, їх високу динамічність, багаторівневу структуру взаємодій між учасниками мережі, а також значний дисбаланс між кількістю легітимних та аномальних транзакцій [4-7]. У зв'язку з цим актуальним є проведення ґрунтовного аналізу та систематизації існуючих методів і засобів, здатних виявляти підозрілі активності на ранніх етапах функціонування блокчейн-мереж, а також визначення перспективних підходів щодо виявлення аномалій у децентралізованих транзакціях.

В рамках даного дослідження проведено аналіз та класифікацію відомих методів (рисунок 1) та засобів виявлення аномалій у децентралізованих транзакціях публічних блокчейн мереж. Виявлено їх переваги, недоліки та оцінено ефективність для виявлення різних типів аномалій.

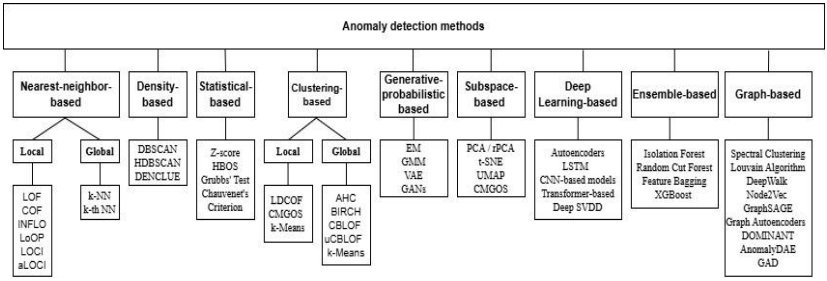


Рис.1. Класифікація методів виявлення аномалій у децентралізованих транзакціях публічних блокчейн мереж

Крім того, в роботі здійснено систематичний огляд та бібліометричне картографування сучасного стану досліджень, пов'язаних із виявленням аномалій у блокчейн-мережах, із використанням програмного забезпечення CiteSpace 6.4.R1. Сформовано та досліджено карти кластерів спільного цитування (рисунок 2), виявлено ключові тренди та визначено перспективні напрями досліджень.

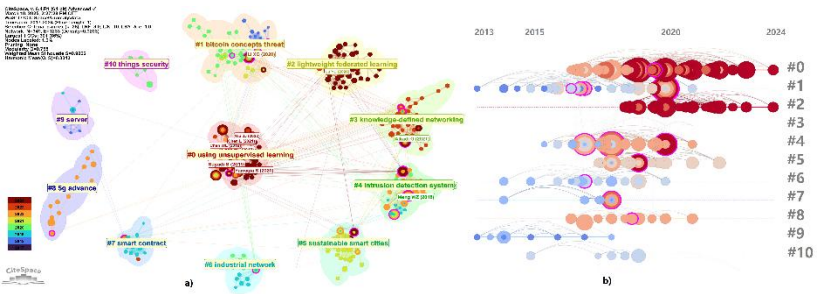


Рис.2. Візуалізація мережевих карт спільних цитувань: а) візуалізація кластерів; б) часова карта

1. Bennet D., Maria L., Sanjaya Y.P.A., Zahra A.R.A. Blockchain technology: Revolutionizing transactions in the digital age // *ADI Journal on Recent Innovation*. – 2024. – Vol. 5, No. 2. – P. 192–199.

2. Chainalysis. 2024 Crypto Crime Report Introduction. – 2024. – URL: https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/ (дата звернення: 28.05.2025).

3. König L., Unger S., Kieseberg P., Tjoa S., Blockchains J.R.C. The risks of the blockchain: a review on current vulnerabilities and attacks // *Journal of Internet Services and Information Security*. – 2020. – Vol. 10, No. 3. – P. 110–127.

4. Cholevas C., Angeli E., Sereti Z., Mavrikos E., Tsekouras G.E. Anomaly Detection in Blockchain Networks Using Unsupervised Learning: A Survey // *Algorithms*. – 2024. – Vol. 17. – P. 201. – DOI: https://doi.org/10.3390/a17050201.

5. Preuveneers D., Rimmer V., Tsingenopoulos I., Spooren J., Joosen W., Ilie-Zudor E. Chained anomaly detection models for federated learning: An intrusion detection case study // *Applied Sciences*. – 2018. – Vol. 8, No. 12. – Article No. 2663.

6. Sayadi S., Rejeb S.B., Choukair Z. Anomaly detection model over blockchain electronic transactions // Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC). – IEEE, 2019. – P. 895–900.

7. Farrugia S., Ellul J., Azzopardi G. Detection of illicit accounts over the Ethereum blockchain // *Expert Systems with Applications*. – 2020. – Vol. 150. – P. 113318.

Вплив штучного інтелекту на сучасну криптографію: виклики та перспективи

УДК 621.395.7 (043.2) Михайло Шелест[1], Юлія Ткач[2] Марина Синенко[3]

Національний університет «Чернігівська політехніка»,
[1]mishel3142@gmail.com, [2]tkachum79@gmail.com [3]mara.a.snnk@gmail.com

З появою штучного інтелекту (ШІ) криптографія зазнала кардинальних змін. У *традиційній криптографії* основна ідея полягала у захисті даних за рахунок

складності криптографічних алгоритмів, при цьому згідно принципу Керкгоффса, криптоалгоритм є публічним. Наразі криптографія виходить з традиційної парадигми «захист даних через алгоритм» у *парадигму захисту користувача, його поведінки та середовища*. Тепер питання стоїть не лише "чи можна зламати шифр", а розглядається питання "чи можна навчити ШІ зламати швидше та ефективніше". ШІ використовується для проведення атак нового покоління, зокрема на криптографічні протоколи, інфраструктуру та кінцевих користувачів. Тепер атакують *не шифр, а користувача*. Таким чином, важливо не тільки *шифрувати*, а й *захищатися від маніпуляцій***.** І тут штучний інтелект одночасно стає як інструментом атаки, так і інструментом захисту.

Розглянемо сучасні вектори атак із застосуванням ШІ, виклики для криптосистем та інфраструктури безпеки, а також перспективи використання ШІ для захисту інформації в умовах зростаючих загроз.

1. *Використання ШІ для атак на криптосистеми.* У сучасному світі розвиток технологій ШІ відкриває нові можливості не лише для захисту інформації, але й для атак на криптосистеми, що ставить перед фахівцями з безпеки серйозні виклики. Зокрема, машинне навчання та інші методи ШІ значно змінюють підходи до криптоаналізу. Однією з головних переваг ШІ у криптоатаках є значне пришвидшення процесу частотного аналізу та пошуку шаблонів у шифрованих даних. У минулому для виявлення слабких місць у шифрограмах використовувались переважно класичні методи, які вимагали значних часових витрат на обробку великих обсягів інформації. Однак, завдяки алгоритмам машинного навчання, ці процеси тепер можна виконувати набагато швидше та ефективніше, дозволяючи знаходити закономірності навіть у складних шифрованих повідомленнях.

Ще однією важливою перевагою використання ШІ є можливість проведення криптоаналізу в режимі реального часу. Алгоритми ШІ можуть миттєво виявляти аномалії, які залишаються непомітними для традиційних методів аналізу. Наприклад, деякі системи ШІ можуть виявляти незначні зміни у структурі шифрованих даних або інші патерни, що вказують на потенційні вразливості у використаних криптографічних схемах.

Але особливо вражаючими є можливості ШІ в області відновлення ключів та іншої конфіденційної інформації. Моделі машинного навчання, які навчаються на великих обсягах злитих відкритих і шифрованих даних, здатні не лише зламувати окремі криптосистеми, а й відновлювати криптографічні ключі, а також відновлювати контекст повідомлення. У деяких випадках ШІ навіть може виявити стиль автора повідомлення, що дозволяє ще точніше ідентифікувати можливі уразливості у системах. Таким чином, розвиток ШІ створює як нові можливості для забезпечення безпеки даних, так і нові загрози для криптосистем.

2. Атаки ШІ на користувача та соціальна інженерія. ШІ змінює не тільки методи шифрування і криптографічної безпеки, а й способи обходу існуючих систем захисту. Однією з таких загроз є використання ШІ в атаках на користувачів, зокрема через соціальну інженерію. Зловмисники можуть застосовувати ШІ для обходу криптографічних захисних механізмів,

маніпулюючи людьми і викрадаючи доступ до ключових даних або самих криптографічних ключів.

Один із найбільш небезпечних методів — це створення дипфейків, які можуть бути використані для фальшування ідентичності. Наприклад, за допомогою ШІ можна згенерувати відео або аудіо повідомлення, яке імітує голос керівника компанії або колеги. В таких випадках криптографічні методи, як-от двофакторна аутентифікація або цифрові підписи, можуть бути обійдені за допомогою соціальної інженерії. Якщо зловмисник успішно підробить голос або обличчя керівника, він може отримати доступ до конфіденційної інформації, навіть якщо система шифрування чи аутентифікації є на найвищому рівні.

Крім того, персоналізовані фішингові атаки, які побудовані на аналізі активності користувача в соціальних мережах та інших публічних джерелах, можуть бути спрямовані на крадіжку приватних криптографічних ключів або інших даних, які використовуються для доступу до захищених систем. Зловмисники можуть створити фальшиве повідомлення, яке виглядатиме як офіційне запитання або повідомлення від банку, постачальника послуг або організації, з якою користувач має справу, щоб примусити його передати важливу інформацію. Це створює серйозну загрозу для систем, що використовують криптографію для захисту даних, адже навіть найсучасніші алгоритми шифрування не зможуть захистити, якщо користувач свідомо передає свій ключ або пароль.

Ще однією небезпекою є здатність ШІ моделювати поведінку користувача, вивчаючи його звички та вподобання. Якщо *зловмисники зможуть підлаштовувати свої атаки під звичний стиль користувача, вони можуть успішно обійти системи* криптографічного захисту, які використовують багатофакторну аутентифікацію або інші заходи безпеки, що засновані на поведінкових патернах. Наприклад, якщо криптосистема враховує типове місце або час входу користувача, зловмисник може здійснити атаку, використовуючи ці дані, щоб пройти автентифікацію.

Отже, навіть найсучасніші методи криптографії можуть бути піддані ризику через маніпуляції людьми, що піддаються соціальній інженерії. Використання ШІ для аналізу поведінки та особистої інформації дозволяє зловмисникам створювати дедалі більш адаптовані й переконливі атаки. Це підкреслює важливість комплексного підходу до безпеки, де разом із криптографією враховуються й фактори соціальної інженерії, адже саме на людському факторі найчастіше ґрунтуються найбільш успішні атаки.

3. Атаки на інфраструктуру, включно з ШІ-моделями. У сучасній інформаційній безпеці все більшого значення набувають атаки, спрямовані на *інфраструктуру криптографічних рішень*, особливо тих, де використовується штучний інтелект. Хоча ШІ активно інтегрується в системи криптозахисту для виявлення аномалій, аналізу трафіку й запобігання кібератакам, водночас він сам стає мішенню зловмисників.

Одним із серйозних викликів є *компрометація моделей штучного інтелекту*, які можуть брати участь у формуванні або захисті криптографічних механізмів. Наприклад, шляхом *атаки типу data poisoning* зловмисники

підсовують шкідливі або викривлені дані на етапі навчання моделі. Уявімо систему, що аналізує криптографічні ключі або автентифікаційні запити: якщо її модель була скомпрометована, то вона може цілеспрямовано допускати фальшиві сертифікати чи дозволяти доступ незареєстрованим користувачам.

Ще один напрям атаки — *model inversion*, коли через доступ до навченої моделі намагаються відновити конфіденційні дані. Це особливо небезпечно в контексті криптографії, де вхідними даними можуть бути *секретні ключі, біометричні шаблони або паролі*, що використовуються для генерації криптографічних секретів. Відновлення таких даних фактично дозволяє зламати криптографічний захист без необхідності атакувати сам алгоритм.

Окрім цього, *extraction attacks* дають змогу зловмисникам викрасти модель ШІ, яка, наприклад, виконує **оцінку** *криптографічної міцності* або забезпечує *динамічне керування ключами*. Після відтворення такої моделі нападник може знайти в ній *вразливості або прогнозувати її поведінку*, щоб обійти системи автентифікації чи дешифрувати трафік.

Не менш небезпечні й *атаки на захисні рішення на базі ШІ*, які вбудовані в *інфраструктуру криптографічного захисту*. Якщо такі рішення мають програмні помилки або впроваджені з порушенням принципів безпечної інтеграції, вони можуть стати вектором атаки.

Наприклад, система управління криптографічними ключами на основі ШІ може бути скомпрометована, що відкриє доступ до ключових сховищ або дозволить маніпулювати процесом генерації ключів, роблячи їх передбачуваними. Таким чином, штучний інтелект, який активно використовується для підсилення криптографічних протоколів та систем захисту, сам по собі стає об'єктом криптографічних атак нового покоління. Забезпечення цілісності, конфіденційності та захищеності моделей ШІ є важливою складовою сучасної криптографічної безпеки.

4. Використання ШІ для захисту криптографії. Сьогодні штучний інтелект відіграє не лише роль потенційної вразливості у криптографічних системах, але й стає потужним інструментом підсилення *їх захисту*. У комплексних рішеннях з інформаційної безпеки дедалі частіше впроваджуються *адаптивні ШІ-системи*, здатні динамічно реагувати на загрози й забезпечувати додатковий рівень криптографічної стійкості.

Одним із практичних застосувань ШІ є інтеграція *адаптивних моделей у системи виявлення вторгнень (IDS)* та *системи поведінкової аналітики користувачів (UBA)*. У таких системах машинне навчання дозволяє виявляти аномальні патерни доступу до зашифрованих даних, які можуть сигналізувати про спроби несанкціонованого отримання криптографічних ключів, атаки на ключову інфраструктуру (PKI) або спроби зламати системи управління ключами (KMS).

Наприклад, якщо користувач починає масово зчитувати зашифровані дані або регулярно змінює запити до KMS, ШІ-система, навчившись на нормальній поведінці, миттєво ідентифікує підозрілу активність. Це дозволяє упередити компрометацію криптографічних протоколів, таких як TLS, IPsec, або Signal, на ранніх стадіях атаки.

Ще одним важливим напрямом є застосування *гомоморфного шифрування (Homomorphic Encryption),* яке дозволяє обробляти зашифровані дані без їх розшифрування. У контексті Federated Learning (федеративного навчання) це означає, що моделі штучного інтелекту можуть навчатися на локальних зашифрованих даних користувачів, не порушуючи їхню приватність і не маючи доступу до відкритої інформації. Гомоморфне шифрування особливо важливе в Secure Multi-Party Computation (SMPC), де кілька учасників виконують спільні обчислення над секретними даними без їх розкриття. Наприклад, у системах спільного управління криптографічними ключами або генерації підписів (дистрибутивний ECDSA), учасники можуть взаємодіяти без ризику втрати контролю над приватними ключами.

Ще один потужний інструмент, що інтегрується у сферу ШІ та криптографії, — це *Zero-Knowledge Proofs (ZKP)*. За допомогою ZKP можливо довести правильність виконання певної операції або цілісність моделі ШІ без необхідності розкривати саму модель або вхідні дані. Це відкриває принципово нові можливості:

- наприклад, можна переконатися, що ШІ-модель у системі керування цифровими підписами виконує валідацію підписів коректно, не розкриваючи деталі алгоритмів або конфіденційних даних.
- у середовищах дистрибутивних криптографічних протоколів, де кілька сторін взаємодіють, ZKP дозволяють кожному учаснику довести правильність дій (генерації частини ключа, підпису тощо), не розкриваючи приватних секретів.

Це особливо актуально для децентралізованих систем та блокчейн-рішень, де забезпечення прозорості та довіри є критичним, наприклад, у протоколах zk-SNARK чи zk-STARK, які активно застосовуються для конфіденційних транзакцій.

5. Перспективи розвитку. У найближчому майбутньому ШІ відіграватиме ще більш важливу роль у розвитку криптографії, особливо з урахуванням викликів, пов'язаних із *настанням епохи квантових обчислень* та зростанням складності кіберзагроз. Одним із ключових напрямів стане розробка постквантових криптосистем, де ШІ забезпечить адаптивність і стійкість до нових типів атак. З появою *квантових комп'ютерів*, традиційні криптографічні алгоритми, зокрема RSA, ECDSA, DH, опиняться під загрозою. Уже сьогодні розробляються постквантові криптографічні алгоритми (CRYSTALS-Kyber, Falcon, Dilithium), які повинні бути стійкими до атак із боку квантових обчислювальних систем. У цьому контексті ШІ може виконувати роль адаптивного механізму генерації ключів і протоколів. Завдяки здатності обробляти великі обсяги даних і навчатися на складних патернах, ШІ може оптимізувати вибір криптографічних параметрів, забезпечуючи динамічну адаптацію системи до різних рівнів ризику та типів середовищ. Наприклад, системи на базі ШІ зможуть аналізувати обчислювальні можливості атакуючих у реальному часі й відповідно підбирати параметри криптографії, які будуть достатньо стійкими в даних умовах.

З розвитком ШІ-рішень у сфері безпеки та криптографії виникає потреба у *чітких етичних стандартах і системах управління AI Governance*, що

гарантують прозорість, відповідальність і безпечність застосування штучного інтелекту. Уже сьогодні NIST пропонує *AI Risk Management Framework (AI RMF)* — підхід до оцінки ризиків і управління ними в системах ШІ. Цей підхід важливий *для захисту криптографічних рішень, що базуються на AI*, адже він забезпечує: прозорість рішень, які приймає ШІ; довіру до моделей, що відповідають за аналіз криптографічних протоколів або виявлення спроб зламу системи шифрування; а також етичні принципи, що регулюють доступ до криптографічних секретів і захист персональних даних у системах із розподіленим доступом.

Разом із AI RMF з'являються і галузеві стандарти безпеки, зокрема *OWASP ML Top 10* — перелік основних ризиків безпеки, притаманних системам машинного навчання. Ці стандарти охоплюють питання цілісності моделей ШІ, контролю доступу до навчальних даних, захисту від атак на конфіденційність тощо.

Висновки. Штучний інтелект відкрив нову еру в розвитку криптографії. Народжується *ШІ-криптографія* - комплексний напрям у сфері інформаційної безпеки, що поєднує традиційні криптографічні методи із технологіями штучного інтелекту (ШІ). ШІ-криптографія - це інтеграція методів штучного інтелекту в процеси проектування, реалізації та захисту криптографічних систем з метою забезпечення адаптивної, стійкої та етично керованої інформаційної безпеки.

1. Троцько, В. В. (2020). Методи штучного інтелекту. Київ. URL: https://library.krok.edu.ua/media/library/category/navchalni-posibniki/trotsko_0001.pdf

Вразливості початкового завантажувача у мікроконтролерах з SPI флеш-пам'яттю

УДК 004.056

Микола Щербина[1], Петро Венгерський[2]

Львівський національний університет імені Івана Франка,
[1]mykola.shcherbyna@lnu.edu.ua, [2]petro.venherskyy@lnu.edu.ua

Впродовж останніх п'яти років на ринку з’явилися мікроконтролери (МК) без внутрішньої флеш-пам’яті, такі як RP2040/RP2350 від Raspberry Pi, LPC18S50/S30/S10 від NXP чи CYW20829 від Infineon Technologies. У них вбудоване програмне забезпечення (ПЗ) зберігається на зовнішньому чипі флеш-пам’яті, на кшталт W25Q128JW від Winbond, що взаємодіє через інтерфейси SPI або QSPI. Спеціалізований периферійний модуль QSPI забезпечує прозору інтеграцію зовнішньої флеш-пам’яті у визначений адресний простір МК, призначений для функціональності XIP (Execute in Place). Завдяки інтегрованому кешу модуль динамічно отримує дані, використовуючи команди швидкого читання SPI Fast Read.

Сьогодні питання кібербезпеки вбудованих систем набуває дедалі більшої актуальності. Перевірка цифрового підпису прошивки стає галузевим стандартом. Особливу важливість має криптографічний захист вмісту

зовнішньої флеш-пам'яті, де розшифрування прошивки здійснюється у реальному часі за допомогою згаданого периферійного блоку «XIP». Розділення МК та флеш-пам'яті забезпечує гнучкість у виборі конкретної моделі мікросхеми зовнішньої пам'яті на етапі передвиробничої підготовки відповідно до остаточного розміру вбудованого ПЗ та вимог до зберігання даних [1]. Метою нашого дослідження є перевірка гіпотези, що таке розділення спричинило появу нових потенційних вразливостей.

Розмістимо «магічний» пристрій у лінії зв'язку між мікроконтролером і зовнішньою флеш-пам'яттю (Рис. 1). З точки зору МК він функціонує як SPI Flash, а з точки зору флеш-пам'яті — як мікроконтролер. Також припустимо, що МК у досліджуваній системі може зазнати атак шляхом введення збоїв [2] (зміна напруги, збої тактового сигналу або електромагнітні впливи), які ініціюються нашим пристроєм через його GPIO-вивід. Нарешті, наш пристрій має можливість передавати журнали подій на ПК через інтерфейс UART.

У випадку використання внутрішньої флеш-пам'яті МК функціонує як «чорна скринька», що ускладнює точне визначення моменту для введення збоїв. Аналіз завантажувача з відкритим кодом та вимірювання енергоспоживання можуть надати певне уявлення, проте обходження перевірки підпису часто потребує кількох днів або навіть тижнів невдалих спроб.

Однак у сценарії із зовнішньою пам'яттю застосування «магічного» пристрою (що виконує роль сніфера) дозволяє майже точно ідентифікувати моменти зчитування підпису та/або вбудованого ПЗ. Це суттєво зменшує часовий проміжок, необхідний для атаки. Дана особливість є першою вразливістю, яку, втім, можна мінімізувати введенням випадкових затримок.

Друга вразливість є критичнішою. Визначивши момент зчитування останнього блоку прошивки перед перевіркою, ми перемикаємось на надсилання модифікованих блоків вбудованого ПЗ, оскільки підпис вже підтверджено. Певною перешкодою для цього вектора атаки може бути кеш XIP. Цю вразливість можна усунути лише апаратними методами.

Нам потрібна додаткова пам'ять SRAM розміром $m \cdot |A|/n$, доступна через периферійний модуль QSPI XIP, де n — розмір кешованого блоку, A — це адресний простір XIP, а m — довжина MAC-коду, причому $m \ll n$. Під час завантаження кожного блоку обчислюється відповідний MAC, і його значення зберігається у цій пам'яті (використання MAC замість CRC є критично важливим). Розумним вибором видається 32-бітний тег UMAC [3] з випадковим значенням nonce, яке генерується при кожному перезапуску.

Після успішної перевірки підпису завантажувач активує механізм контролю цілісності вбудованого ПЗ, який неможливо вимкнути до перезапуску. При зчитуванні будь-якого блоку у кеш XIP його значення перевіряється за MAC, і у разі невідповідності виникає апаратна помилка. Таке рішення повністю усуває другу вразливість.

Скомпрометований механізм перевірки підпису має незначний вплив, якщо вбудоване ПЗ зашифроване і дослідник не може змінювати його довільно. Для периферійних модулів XIP критично важливим є розшифрування «на льоту» за довільними адресами. AES-CTR є обґрунтованим вибором для цієї мети, й МК одного з вищезазначених виробників реалізують саме такий алгоритм.

Якщо досліджуване ПЗ виводить певну постійну інформацію через UART, USB або інший інтерфейс зв'язку, це дає шанс шляхом систематичних спроб модифікації байтів з відповідним кроком відтворити фрагмент(и) гами. Авторами пропонується метод, який (за сприятливих умов) після цього дозволяє модифікувати прошивку таким чином, щоб отримати її вміст.

1. Щербина М.Ю. Покращення стиснення коду для мікроконтролерів ARM Cortex M за допомогою попередньої фільтрації. Вісник Національного університету «Львівська політехніка» «Інформаційні системи та мережі». – 2023. – Вип. 14. – С. 225-234.
2. den Herrewegen J.V., Oswald D., Garcia F.D., Temeiza Q. Fill your Boots: Enhanced Embedded Bootloader Exploits via Fault Injection and Binary Analysis. IACR Transactions on Cryptographic Hardware and Embedded Systems. – 2020. – Vol. 2021, No. 1. – P. 56–81.
3. Krovetz T. UMAC: Message Authentication Code using Universal Hashing. RFC 4418. – 2006. – Режим доступу: https://www.rfc-editor.org/info/rfc4418

Кібербезпека в контексті сучасних конфліктів

УДК 004.056:343
Роман Щипанський[1], Роман Іваницький[2]
[1]*Західноукраїнський національний університет*,
[2]*Тернопільський національний педагогічний університет імені Володимира Гнатюка*,
[1]*dubnokv0709@gmail.com*, [2]*romikiv@ukr.net*

У 2022-2025 роках кіберпростір став ключовим полем протистояння в національних конфліктах, де понад 50% всіх кібератак націлені на малий та середній бізнес, хоча лише 18% компаній мають достатній захист. За прогнозами Cybersecurity Ventures[1], збитки від кіберзлочинності до кінця 2025 року можуть сягнути 12 трильйонів доларів при збереженні поточних темпів зростання (15-20% щорічно). В умовах геополітичної напруженості критично необхідно посилювати заходи кібербезпеки на всіх рівнях, впроваджуючи не лише оперативне реагування, але й випереджувальні стратегії запобігання інцидентам.

Метою даного дослідження є розробка удосконаленої схеми реагування на інциденти кібербезпеки в умовах сучасних конфліктів 2025-2030 років шляхом інтеграції передових технологій штучного інтелекту та автоматизованих систем для ефективного виявлення, аналізу та нейтралізації еволюціонуючих кіберзагроз, що забезпечить захист критичної інфраструктури, мінімізацію часу простою систем та зменшення фінансових втрат організацій різного масштабу.

Створення ефективної системи кіберзахисту потребує впровадження інтегрованого підходу, що об'єднує міжвідомчу координацію, технології штучного інтелекту для виявлення аномалій, системи активного моніторингу та підвищення кваліфікації фахівців. Ключовими компонентами такої системи також є посилений захист критичної інфраструктури та забезпечення обміну

інформацією про загрози в реальному часі, що дозволяє своєчасно реагувати на кіберінциденти та мінімізувати їхні наслідки.

Попередні дослідження зосереджувались на психологічних профілях зловмисників та механізмах виникнення інцидентів, однак сучасні кіберзагрози вимагають розробки адаптивних методів реагування на їх постійну еволюцію. Серед найнебезпечніших атак 2022-2025 років виділяються таргетований фішинг з використанням ШІ, багаторівневі DDoS-атаки, комплексні SQL-ін'єкції, програми-вимагачі з подвійним шифруванням, атаки на ланцюги постачання та експлуатація вразливостей нульового дня[2,3]. Ці загрози потребують спеціалізованих підходів до розслідування та реагування, що враховують особливості кожного типу атак та дозволяють ефективно протидіяти сучасним кіберзагрозам.

Ефективна кіберзахисна стратегія вимагає не лише якісних методів передачі запитів до служби IT-безпеки, але й комплексних систем управління інцидентами. Організації можуть використовувати різноманітні захищені канали комунікації, від телефонних ліній з обов'язковою верифікацією до спеціалізованих порталів самообслуговування з багатофакторною автентифікацією. Ці канали доповнюються централізованими системами управління, такими як Security Operation Center (SOC) та Incident Response Platform (IRP), що забезпечують цілодобовий моніторинг, оперативний аналіз загроз та автоматизацію процесів розслідування інцидентів)[3].

Після впровадження відповідних систем реалізується чітко структурований процес обробки запитів безпеки, що охоплює чотири послідовні етапи: реєстрацію, аналіз, реагування та закриття. На етапі реєстрації черговий спеціаліст або автоматизована система створює заявку та визначає її пріоритет. Потім аналітики безпеки проводять оцінку загрози та визначають напрямок розслідування, після чого команда реагування здійснює нейтралізацію загрози з використанням спеціалізованих інструментів. Завершальний етап передбачає аналіз першопричин інциденту та оновлення бази знань, що забезпечує постійне вдосконалення системи кіберзахисту організації.

У рамках модернізованого підходу до кіберзахисту розроблено удосконалений алгоритм розслідування інцидентів (Рис.1).

Рис.1. Алгоритм розслідування інцидентів [розроблено автором на основі 3]

План реагування на інциденти забезпечує структурований підхід до кіберзагроз через етапи виявлення, аналізу та відновлення, з чітким розподілом ролей та відповідальності команди, що мінімізує простої та фінансові втрати. Удосконалена схема на 2025-2030 роки впроваджує ML/AI аналіз загроз та автоматизовану відповідь, створюючи інтегрований підхід для сучасного захисту організацій, з перспективою розробки адаптивних механізмів реагування на новітні кіберзагрози.

1. Embroker. (2023). 2023 Must-Know Cyber Attack Statistics and Trends. https://www.embroker.com/blog/cyber-attack-statistics/
2. Globe Newswire. (2022). Cybercrime to Cost the World $10.5 Trillion Annually by 2025. https://www.globenewswire.com/news-release
3. Ceccato, V., & Newton, A. (2025). System thinking for sustainable crime prevention. Routledge. https://doi.org/10.4324/97810032810306.

Методологія криптографічного захисту інформації на основі цілочисельної, модифікованої досконалої та поліноміальної систем залишкових класів

УДК 621.395.7 (043.2)

Ігор Якименко
Західноукраїнський національний університет, jiz@wunu.edu.ua, iyakymenko@ukr.net

Представлена методологія криптографічного захисту інформаційних потоків на основі використання симетричних та асиметричних криптосистем в цілочисельній, модифікованій досконалій та поліноміальній СЗК [1-3] (складається з восьми етапів: 1) процес формування множини блоків відкритого тексту (N, $N(x)$) для цілочисельних і поліноміальних криптографічних систем; 2) Встановлення вимог щодо основних параметрів цілочисельних та поліноміальних симетричних та асиметричних криптографічних систем та захищеності інформації; 3) вибір запропонованих цілочисельних та поліноміальних криптосистем; 4) створення множини базових операцій; 5) формування набору методів виконання операцій; 6) вибір цілочисельної та поліноміальної форм СЗК; 7) програмна реалізація цілочисельних та поліноміальних симетричних та асиметричних криптосистем. Детальний опис запропонованих етапів та взаємозвязок між ними представлено нижче.

Етап 1. Процес формування множини блоків відкритого тексту (N, $N(x)$) для цілочисельних і поліноміальних криптографічних систем в СЗК. На початковому етапі користувач повинен подати у цифровому вигляді набори блоків відкритого тексту для цілочисельного шифрування N=Ui=1M1Ni=N1,N2,...,NM1, і у вигляді поліномів для поліноміального N(x)=Ui=1M2Ni(x)=N1x,N2(x),...,NM1(x) (M1, M2 – кількість блоків відкритого тексту). У основних асиметричних криптографічних системах, таких як RSA, Рабіна та Ель-Гамаль , значення відкритого тексту не повинні перевищувати відповідний параметр відкритого ключа [4].

Величина M_1 визначається шляхом ділення числового значення відкритого тексту на цей параметр. Для цілочисельних та поліноміальних криптографічних систем в СЗК блоки повідомлень повинні задовольняти нерівності відповідно $N<P$ і deg $N(x)<$deg $P(x)$ відповідно, де P=i=1spi, Px=i=1lpix, p_i, $p_i(x)$ - системи попарно взаємно простих модулів та модулів-поліномів, s, l – кількість модулів [5].

При передачі блоків у зашифрованому вигляді по відкритих каналах зв'язку виникають можливі загрози. В результаті формується визначена користувачем множина загроз MЗ=Ui=1z1MЗi=M31,M32,...,M3z2, де z1 – їх кількість.

Етап 2. Вибір модулів та ключів для цілочисельного та поліноміального шифрування в СЗК. На даному етапі відбувається вибір відкритих та таємних ключів для цілочисельних та поліноміальних: симетричних та асиметричних криптоалгоритмів у СЗК (pi, НСДpi,pi-1=1, P=i=1kpi, k – кількість модулів (ключів) для цілочисельної, pi(x), НСДpix,pi-1x=1, P(x)=i=1kpi(x)), двоключового поліноміального симетричного шифрування в СЗК (при генерації поліноміальних ключів абоненти вибирають відомі тільки їм обом системи модулів mix та відповідні їм поліноми six, для яких виконуються такі умови: 1<deg si x<deg mi x та НСД(six,mix)=1), ієрархічних цілочисельних в СЗК, ієрархічних поліноміальних алгоритмів шифрування в ПСЗК (основна система модулів (ключів) першого рівня p1x,p2x,...,pl(x)забезпечує виконання операцій у діапазоні [0, $P_1(x)$), де P1(x)=p1(x)p2(x)...pl(x)=i=1lpi(x). На наступному ієрархічному рівні головна система модулів представляється в новій системі з відповідними основами та діапазонами $q_{11}(x)$, $q_{12}(x)$, …, $q_{1l}(x)$, $q_{21}(x)$, $q_{22}(x)$, …, $q_{2l}(x)$, …, q_{l1}(x), $q_{l2}(x)$, …, $q_{ll}(x)$. Ця процедура триває до останнього (k-го) рівня).

Етап 3. Встановлення вимог щодо основних параметрів цілочисельних та поліноміальних криптографічних систем в СЗК та їх стійкості до криптоаналізу. На основі сформованих множин загроз та блоків відкритого тексту відбувається формування вимог до кількісних показників стійкості криптографічного алгоритму ПЗІ=Ui=1z2Uj=1z3ПЗІij, які записуються у вигляді матриці, та основних параметрів криптографічних систем ПКС=Ui=1z4ПКСi=ПКС1,ПКС2,...,ПКСz4, i1,z4, де z4 – кількість вимог. Для кожного фрагмента відкритого тексту N=Ui=1M1Ni=N1,N2,...,NM1, N(x)=Ui=1M2Ni(x)=N1x,N2(x),...,NM2(x) та кожної ймовірної загрози M3i,i1,z2 встановлюється набір показників захищеності ПЗІ=Ui=1z2Uj=1z3ПЗІij, де z2 – позначає кількість показників для певної загрози та множина вимог до параметрів криптосистеми ПКСi,i1,z3, де z3 – кількість вимог.

Етап 4. Формування множини та вибір цілочисельних та поліноміальних криптосистем в СЗК. На четвертому етапі відбувається вибір розроблених цілочисельних та поліноміальних симетричних та асиметричних криптосистем в залежності від поставлених завзань щодо рівня захисту: симетричний метод шифрування у СЗК, симетрична криптосистема на основі пошуку залишків та КТЗ, методу шифрування в СЗК з допомогою зміни базисних чисел, ієрархічний симетричний криптоалгоритм на основі СЗК, асиметричний алгоритм шифрування у СЗК, трьохмодульної криптосистеми Рабіна на основі операції додавання, асиметричного алгоритму шифрування Ель-Гамаля з використанням системи залишкових класів та векторно-модульного алгоритму

модулярного експоненціювання. Аналогічно до цілочисельних застосувань, поліноми можна успішно використовувати в якості відкритого і зашифрованого тексту, відкритого і таємного ключів при використанні в криптографічних алгоритмах. Серед розроблених поліноміальних криптоалгоритмів на даному етапі можна вибрати: криптосистему Рабіна в поліноміальній системі числення, криптографічні поліноміальні симетричні методи шифрування в поліноміальній системі залишкових класів, двоключовий поліноміальний симетричний криптоалгоритм в СЗК, ієрархічний поліноміальний симетричний криптоалгоритм в поліноміальній СЗК.

Для генерування ключів цілочисельних симетричних та асиметричних криптосистем, процесу шифрування та розшифровування використовуються такі операції: пошук залишку, найбільшого спільного дільника, використання розширеного алгоритму Евкліда, оберненого елемента за модулем, відновлення десяткового числа за його залишками (алгоритм з додаванням модулів та залишків, алгоритм Гарнера, китайська теорема про залишки), квадратичний лишок, модулярне множення та модулярне експоненціювання. Для забезпечення формування симетричних та асиметричних криптосистем поліноміальній системі числення (ПСЧ) використовуються операції: пошук залишку в ПСЧ, найбільшого спільного дільника двох поліномів, оберненого полінома за модулем іншого полінома на основі методу невизначених коефіцієнтів, відновлення поліному за його залишками (алгоритм з додаванням поліномів модулів та залишків, алгоритм Гарнера та КТЗ в ПСЧ), пошук кореня квадратного полінома в ПСЧ на основі алгоритму додавання модуля.

Етап 5. Створення множини базових операцій. Для забезпечення процесу шифрування та розшифрування в цілочисельній та поліноміальній системах числення на п'ятому етапі формується відповідна множина базових операцій, які використовуються у симетричих та асиметричних криптоалгоритмах БО=Ui=1z5БОi=БО1,БО2,...,БОz5, i1,z5, де z5 – кількість операцій в цілочисельній системі числення, ПБО=Ui=1z6ПБОi=ПБО1,ПБО2,...,ПБОz6, i1,z6, де z6 – кількість операцій в ПСЧ.

Етап 6. Формування набору методів виконання операцій. На шостому етапі здійснюється формування набору методів для реалізації операцій в цілочисельній та поліноміальній системі числення, визначених на попередньому етапі: ЦО=Ui=1z7ЦОi=ЦО1,ЦО2,...,ЦОz7, i1,z7, де z7 – кількість методів для цілочисельної системи числення, ПО=Ui=1z8ПОi=ПО1,ПО2,...,ПОz8, i1,z8, де z8 – кількість методів для поліноміальної системи числення. Зокрема, для операцій в цілочисельній системі числення: визначення залишку, модульного множення та піднесення до степеня можуть бути застосовані векторно-модульний підхід, тоді як інші операції реалізуються через додавання чи множення модулів.

Для поліноміальних операцій: пошук залишку в ПСЧ, найбільшого спільного дільника двох поліномів (здійснюються на основі операції ділення поліномів), оберненого полінома за модулем іншого полінома, відновлення поліному за його залишками (алгоритм з додаванням поліномів модулів та залишків, алгоритм Гарнера в ПСЧ, китайська теорема про залишки в ПСЧ), пошук кореня квадратного полінома в ПСЧ.

Етап 7. Вибір цілочисельної та поліноміальних форм СЗК. Для оптимізації обчислень за рахунок розпаралелення і зменшення розмірності операндів на четвертому етапі більшість операцій можна виконувати в СЗК, множина форм якої формується на сьомому етапі: ЦФС=Ui=1z9ФСi=ЦФС1,ЦФС2,...,ЦФСz9, i1,z9, де z9– кількість цілочисельних форм СЗК, ПФС – поліноміальна форма СЗК . Окрім традиційної цілочисельної форми, особливий інтерес для використання в асиметричних криптографічних системах становлять ДФ та МДФ СЗК, які є фундаментом для створення нових стандартів безпеки.

Етап 8. Програмна реалізація цілочисельних та поліноміальних криптосистем. Восьмий етап передбачає програмну реалізацію запропонованих цілочисельних та поліноміальних симетричних та асиметричних криптосистем з використанням базових модулярних операцій (етап 4) на основі вибору методу їх виконання (етап 6) або з використанням відповідних форм СЗК (етап 7): методу шифрування у СЗК, на основі пошуку залишків та КТЗ, методу шифрування в СЗК з допомогою зміни базисних чисел, ієрархічного симетричного криптоалгоритму на основі СЗК, асиметричний алгоритм шифрування у СЗК, трьохмодульної криптосистеми Рабіна, асиметричного алгоритму шифрування Ель-Гамаля з використанням СЗК та векторно-модульного алгоритму модулярного експоненціювання, та для реалізації розроблених поліноміальних криптоалгоритмів: криптосистеми Рабіна в поліноміальній системі числення, криптографічного поліноміального симетричного методу шифрування в СЗК, двоключового поліноміального симетричного криптоалгоритму в СЗК, ієрархічного поліноміального симетричного криптоалгоритму в СЗК.

Ця методологія забезпечує комплексний підхід до розробки, реалізації та оптимізації запропонованих симетричних та асиметричних цілочисельних, поліноміальних криптосистем на основі використання СЗК, векторно-модульних методів пошуку залишків, модулярного множення та експоненціювання, методу невизначених коефіцієнтів для пошуку оберненого поліному в поліноміальній системі числення, методів відновлення поліному за його залишками на основі додавання добутку модулів, що дає змогу досягти високого рівня захисту інформації при мінімальних витратах на обчислення.

1. Yakymenko, I., Martyniuk, O., Martyniuk, S., Yakymenko, Y., Kasianchuk, M. Hierarchical Encryption in a Residual Number SystemProceedings - International Conference on Advanced Computer Information Technologies, ACIT This link is disabled., 2024, pp. 496–499

2. Yakymenko, I., Karpinski, M., Shevchuk, R., Kasianchuk, M. Symmetric Encryption Algorithms in a Polynomial Residue Number System. Journal of Applied Mathematics., 2024, pp. 1-12.

3. Nykolaychuk, Y.M., Yakymenko, I.Z., Vozna, N.Y., Kasianchuk, M.M. Residue Number System Asymmetric Cryptoalgorithms. Cybernetics and Systems AnalysisThis link is disabled., 2022, 58(4), pp. 611–618.

4. Okeyinka A. Computational Speeds Analysis of RSA and ElGamal Algorithms. Proceedings of the World Congress on Engineering and Computer Science (WCECS 2015), San Francisco (USA), V. I, 2015, pp. 237-242.

5. Барсов В. И., Сорока Л.С., Краснобаев В.А. Методология параллельной обработки информации в модулярной системе счисления. Харьков: УИПА, 2009, 268 с.

Криптозахист аудіострімінгових сервісів з урахуванням кодеків стиснення

УДК 004.056.5

Анна Якимова[1], Лідія Тимошенко[2]
Національний університет «Одеська політехніка,
[1]9560419@stud.op.edu.ua, [2]l.m.timoshenko@op.edu.ua

Сучасний світ активно використовує аудіострімінгові сервіси, що створює нові виклики у сфері захисту переданої інформації. Потоки аудіо часто містять конфіденційні або авторські дані, які потребують надійного захисту від перехоплення, підміни або несанкціонованого доступу. Особливої складності додає використання кодеків стиснення, які змінюють структуру аудіоданих і впливають на сумісність із криптографічними методами [1].

Метою роботи є розробка доступного та ефективного засобу для захисту аудіо-стрімінгових сервісів з урахуванням кодеків стиснення.

Одним з найбільш ефективних способів забезпечення конфіденційності та цілісності є алгоритм AES у режимі GCM[2]. Цей режим дозволяє одночасно шифрувати дані та перевіряти їхню автентичність за допомогою тегу, є придатним для обробки потокових даних у реальному часі. Надійність алгоритму базується на використанні унікального вектора ініціалізації та тегу автентифікації, що унеможливлює атаки повторення або підміни [3].

Значну роль відіграє поєднання криптографії з особливостями кодеків стиснення. Шифрування аудіо до або після стиснення вимагає розуміння змін структури потоку для уникнення втрат якості та забезпечення сумісності. Важливо забезпечити таку обробку, яка не вплине на час передачі, не знизить продуктивність та не порушить якість відтворення [4].

Особливу увагу приділено синхронізації між відправником і приймачем. Кожен зашифрований пакет містить вектор ініціалізації, послідовний номер та тег автентифікації. Така структура гарантує правильне дешифрування, виявляє втрати пакетів і забезпечує захист від атак типу replay.

Результатом роботи є розроблений застосунок для криптозахисту аудіо-стрімінгових сервісів, який успішно шифрує та дешифрує аудіо за 0.2 сек. Застосунок тестувався на різних аудіофайлах і показав стійкість до атак, та може застосовуватись в медіа-програмах і комунікаційних системах.

Отже, ефективне впровадження AES-GCM в аудіо-стрімінгові сервіси дозволяє забезпечити баланс між безпекою, продуктивністю та якістю обслуговування користувачів.

1. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. Boston: Pearson, 2020. 752 p.

2. Корченко О. Г., Сіденко В. П., Дрейс Ю.О. Прикладна криптологія : системи шифрування. Житомир : ДУТ, 2014. 448 с.

3. Dworkin M.J. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST Special Publication 800-38D. Gaithersburg, MD: NIST, 2007. 56 p.
4. Baccour L., Atri M. Security Challenges in Multimedia Streaming Services: A Survey. Multimedia Tools and Applications. 2022. 27973 p.

Криптосистема McEliece на основі коригуючих кодів системи залишкових класів

УДК 004.056.5

Василь Яцків[1], Степан Івасьєв[2], Наталія Яцків[3]
Західноукраїнський національний університет,
[1]vy@wunu.edu.ua, [2]isv@wunu.edu.ua, [3]n.yatskiv@wunu.edu.ua

З розвитком квантових обчислень традиційні криптографічні алгоритми, такі як RSA, DSA та алгоритми на основі еліптичних кривих, опинилися під загрозою через ефективність атак з використанням квантових комп'ютерів. У даному контексті актуальною проблемою є розробка нових криптографічних алгоритмів для забезпечення необхідної стійкості в майбутньому. Одним із перспективних напрямів побудови постквантових криптосистем є криптосистеми на основі кодів, серед яких важливе місце займає криптосистема McEliece, яка тривалий час залишається стійкою до різних типів атак [1].

Криптосистема McEliece базується на складності задачі декодування випадкових лінійних кодів з шумом, що є NP-важкою проблемою. Вона характеризується високою швидкістю шифрування та розшифрування, але при цьому має значний недолік – великі розміри ключів. Незважаючи на це, McEliece пройшла до фінального етапу конкурсу NIST з відбору постквантових криптографічних стандартів, що підтверджує її практичну релевантність і високий рівень безпеки (табл.1) [2, 3].

Таблиця 1

Основні параметри криптосистеми Classic McEliece

Рівень стійкості (NIST)	**Тип коду**	**Довжина коду, n**	**Кількість помилок, t**	**Розмір відкри-того ключа, байт**	**Розмір приват-ного ключа, байт**	**Зашифро-ваний текст, байт**
Рівень 1	Бінарний код Гоппа	3488	64	~ 261 120	~ 6 492	96
Рівень 3		4608	96	~ 524 160	~ 13 608	156
Рівень 5		6688	128	~ 1 044 992	~ 13 932	208

З метою зменшення обсягу ключів у цій роботі пропонується модифікація криптосистеми McEliece шляхом використання коригуючих кодів, побудованих

на основі системи залишкових класів (СЗК). Такі коди мають високу здатність до корекції помилок, модулярну структуру та можливість ефективного паралельного обчислення, що робить їх перспективними для використання в поствквантових алгоритмах шифрування.

Алгоритм шифрування McEliece – СЗК складається з наступних кроків:

1. Побудова матриці G. Кожен рядок матриці G відповідає одному біта інформації, а стовпці розподілені по модулях mi. Розмір матриці дорівнює (kn), де n – кількість модулів. Для кожного i-го інформаційного біту в повідомленні, його вплив на залишки всіх модулів можна представити як:

якщо i - й біт дорівнює 1, використовуються залишки числа 2i для кожного модуля;

якщо i - й біт дорівнює 0, використовуються залишки числа 0 для кожного модуля.

Таким чином, стовпці матриці G будуть заповнені залишками від ділення чисел 20, 21, 22,⋯2k-1 на кожен з модулів mi.

Приклад обчислення генераторної матриці G:

якщо k=4, n=4, модулі m1=3, m2=5, m3=7, m4=11:

– для 0-го біту: [20 mod 3, 20 mod 5, 20 mod 7, 20 mod 11]=[1, 1, 1, 1];

– для 1 -го біту: [21 mod 3, 21 mod 5, 21 mod 7, 21 mod 11]=[2, 2, 2, 2];

– для 2-го біту: [22 mod 3, 22 mod 5, 22 mod 7, 22 mod 11]=[1, 4, 4, 4];

– для 3-го біту: [23 mod 3, 23 mod 5, 23 mod 7, 23 mod 11]=[2, 3, 1, 8].

2. Створення відкритого ключа:

$$G'=G\cdot S\cdot P,$$

де G – генераторна матриця в системі залишкових класів з розширеною системою модулів розміром k×n, S – маскувальна матриця розміром n×n, P – матриця перестановки розміром n×n.

3. Шифрування даних:

$$c=x\cdot G'+e,$$

де x – повідомлення в двійковій системі числення довжиною k біт, e – вектор помилки.

Розшифрування даних здійснюється за формулою:

$$x'=(c\cdot P-1)\cdot S-1,$$

де S-1 – обернена матриця до S в полі цілих чисел.

Для отримання x використовуємо китайську теорему про залишки та алгоритм виправлення помилок [3].

Проведене дослідження складності ISD-атаки від вага помилки, показало, що при меншій довжині коду, порівняно з класичною McEliece, можна досягти необхідну стійкість за рахунок збільшення ваги помилки (таблиця 2).

Таблиця 2

Оцінка складності ISD-атаки від вага вектору помилки

Довжина коду, n	**Вага вектору помилок,** t	**Безпека (біт)**
376	22	65,6
376	53	128,8
376	79	194,4
376	99	258,7

Представлено нову модифікацію класичної криптосистеми McEliece на основі коригуючих кодів системи залишкових класів. Використання СЗК з розширеною системою модулів забезпечує ефективну корекцію помилок і тим самим підвищує складність до атак.

1. Classic McEliece. URL: https://classic.mceliece.org/impl.html (дата звернення: 30.04.2025).
2. Singh, Harshdeep. Code based cryptography: Classic mceliece. arXiv preprint arXiv:1907.12754, 2019.
3. Xiao, H., Garg, H. K., Hu, J., & Xiao, G. New error control algorithms for residue number system codes. *Etri Journal*, 2016, *38*(2), pp. 326-336.

Транспортна інформаційно-комунікаційна мережа як об'єкт кіберзагроз

УДК 004.056.5:004.08

Родіон Хворостяний

Державний університет інформаційно-комунікаційних технологій,
rodionhvorostyanoy@gmail.com

У сучасних умовах гібридної війни та відкритих військових дій кіберзагроз та пов'язані з ними кібератаки стають невід'ємною складовою збройного протистояння. Зі зростанням напруження в інформаційному та кіберпросторі фіксується значне зростання кількості кібератак, які спрямовані як на критичну інфраструктуру, так і на інформаційні системи державного та приватного секторів. Одним з елементів таких інформаційних систем є транспортні інформаційно-комунікаційні мережі регіонального та глобального рівня передачі даних.

Транспортна інформаційно-комунікаційна мережа - це мережа, що забезпечує передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду між підключеними до неї телекомунікаційними мережами доступу. Під терміном транспортної інформаційно-комунікаційної мережі (ТрІКМ) приймемо сукупність інформаційних систем, корпоративний мереж та каналів передачі інформації, а також способів комунікації та управління інформаційними потоками, призначеними для передачі інформації між великими регіонами в межах однієї держави, чи в межах міждержавного обміну даними на рівні глобальних світових регіонів [1].

Типова побудова регіональної ТрІКМ подана на Рис 1. Її складовими є верхній рівень магістральної транспортної мережі глобальної передачі даних, місцева транспортна мережа забезпечення даними окремих корпоративних мереж та рівень транспортної мережі доступу [1].

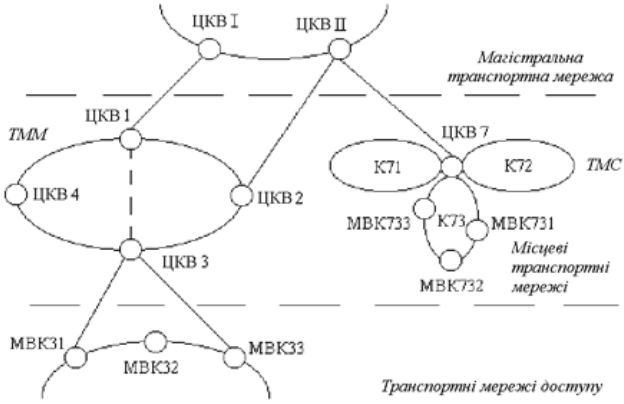


Рис.1 Структура регіональної (місцевої) транспортної мережі.

Її складовими є цифрові комутаційні вузли (ЦКВ), мультиплексори виділення каналів передачі даних (МВК), концентратори потоків передачі даних (К) та окремі корпоративні мережі передачі даних (ТММ, ТМС).

Класично в ТрІКМ виділяють чотири рівні [1]:

1. Рівень мережі – відповідає за взаємодію вузлів ІКС.

2. Рівень операційних систем – відповідає за обслуговування програмного забезпечення, яке реалізує вищі рівні, та його взаємодію з обладнанням мережі.

3. Рівень систем управління базами даних (СУБД) - відповідає за збереження ня та обробку даних.

4. Рівень прикладного програмного забезпечення – включає прикладні компоненти та інтерфейс взаємодії з користувачем.

Необхідно відмітити, що ТрІКМ обробляють різноманітні види трафіку. До яких можна віднести: трафік реального часу, потоковий трафік, еластичний трафік, сигнальний трафік. Тобто виникає потреба в захисті кожного з вказаних видів трафіку від цільових кібератак [1,2].

Відповідно до НД ТЗІ 2.5-005-99 [9] ТрІКС являє собою організаційно - технічну систему, яка поєднує операційну систему (ОС), фізичне середовище, персонал та оброблювану інформацію [3]. Кожна з цих складових безпосередньо впливатиме на загальний рівень захищеності, мати набір характеристик, вимог щодо налаштування та організації функціонування системи її кіберзахисту.

Аналіз та оцінка сучасного стану кібербезпеки України, дослідження механізмів захисту національної безпеки від кібератак та аналіз сучасного її стану показує, що як глобальні так і регіональні ТрІКМ можуть стати об’єктом кіберзагроз різного характеру [4,5]. Виходячи з призначення, типової топології побудови та складових елементів в якості кіберзагроз для ТрІКМ визначимо наступні, що подані в Табл. 1 [4,5].

Таблиця 1.

Типи кіберзагроз транспортної інформаційно-комунікаційної мережі

Тип кіберзагрози	Мета атаки, тип	Об'єкт атаки	Тип трафіку
Порушення доступності	Оприманння доступу до ТрІКМ. DDoS - атака	Сервери, локальні мережі	Трафік реального часу
Порушення конфіденційності	Перехопленння конфіденційних даних. Скіфінг, фішинг	Бази даних, інформаційні сховища, файли	Потоковий трафік
Блокування систем захисту	Виведення з ладу або знищення обладнання захисту. Поширення шкідливого ПЗ	Засоби управління кіберзахистом, міжмережеві екрани, маршрутизатори	Мережевий трафік (ICMP). Прикладний трафік (SMPT, SIP, H323)
Використанння вразливостей	Застосування експойлерів. SQL-ін'єкції, кібершпигунство	Веб-додатки, хмарні сервіси	Прикладний трафік (HTTP, SQL) Мережевий трафік (IP) Транспортний трафік (TCR)

Вирішення задання забезпечення кібернетичної безпеки ТрІКМ не можливо без наявності та використання відповідних моделей кіберзахисту. В свою чергу процес розробки такої моделі повинен врахувати види кіберзагроз, типи кібератак та об'єкти, що під них можуть потрапити. Базовим матеріалом, який може бути використаний для розробки такої моделі є інформація, що подана в Табл.1.

Таким чином, в роботі визначено термін транспортної інформаційно-комунікаційної мережі, як об'єкти впливу кіберзагроз, подані їх основні види, типи кібератак, що використовуються для їх реалізації, об'єкти впливу кібератак та види трафіку потоків даних через які реалізуються подані кіберзагрози.

1. http://vnstele.com/system-komut/lecz-ok/102-44-lecz-ok.html
2. https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf

3. НД ТЗІ 2.5-005 -99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу

4. Mynenko, S., Kochnieva, V., & Babych, Y. (2024). Оцінка рівня кібербезпеки України в умовах війни. *Європейський науковий журнал Економічних та Фінансових інновацій*, *2*(14), 487-500. https://doi.org/10.32750/2024-0243

5. Толкачов М. Ю Механізми захисту трафіку в кіберпросторі. Сучасний захист інформації, №4 (2024), С. 85-99. DOI: 10.31673/2409-7292.2024.040009

Аналіз механізму впливу імпульсної нефлуктаційної завади на цілісність дискретного сигналу, що передається інформаційно-комунікаційною мережею

УДК 004.056.5:004.08

Євген Бондаренко
Державний університет інформаційно-комунікаційних технологій,
bondarenko.alfa.inet@gmail.com

У сучасних умовах гібридних війни та відкритого військового протистояння надзвичайно важливим є збереження цілісності корисної інформації в умовах впливу різноманітних завад та збурень по всьому спектру каналів інформації.

Особливо важливе це відносно радіоканалів передачі корисних даних в умовах впливу різноманітних завада різного характеру [1].

Відомо, що в сучасних радіоканалах поряд із шумовими завадами (релєєвське завмирання, адитивний білий гауссівський шум) часто присутні й нефлуктуаційні завади від різних джерел. Це можуть бути як природні причини формування різних радіо шумів, так і похибки радіоапаратури та порушенням технології радіозв'язку. Необхідно прийняти до уваги, що поява нефлуктаційних завад в радіопросторі передачі дискретних сигналів може обумовлюватися не тільки природніми причинами але і через навмисні дії протиборчої сторони, яка прагнуть створити певні перешкоди для роботи радіоканалу передачі цифрових даних [2].

Встановлено, що основними та найбільш небезпечними для порушення цілісності дискретних сигналів нефлуктаційними завадами є гармонічна завада, фазоманіпульована завада, ретрансльована завада, скануюча завада, хаотична імпульсна завада, мультиплікативна завада. Але, тільки при навмисно створеному прицільному впливі, саме імпульсна завада може нанести найбільшого порушення цілісності дискретному сигналу [2,4].

Вплив імпульсної завади проявляється в зростанні імовірності символьної помилки. Інтесивність впливу імпульсної завади загалом визначається спектром та енергією шуму, який оцінюється в загальних залежностях розрахунку символьної помилки співвідношенням сигнал/загальний шум в каналі передачі інформації.

Відповідно встановленим результатам проведених досліджень, мінімальна ймовірність помилки на символ дискретного сигналу з деяким типом модуляції *M* визначається залежністю [1,2]:

$$P_S(M) \approx 2\Phi\left(\sqrt{2\pi\gamma_b}\sin\frac{\pi}{M}\right) \quad \Phi(x) = \frac{1}{2\pi\int_x^{\infty} e^{-t^2/2}\,dt} \quad \gamma_b = E_b/N_0$$

,

де $P_b(M)$ – відношення сигнал/шум, що перераховане на один біт інформації.

Символьна помилка пов'язана з бітовою помилкою дискретного сигналу співвідношенням:

$$P_b(M) = ((M/2)/M - 1)\,P_s$$

Показано, що вплив імпульсної завади на дискретний сигнал буде проявлятися в появі та зростанні символьної та бітової помилки, як складових параметру цілісності дискретного сигналу.

Розрахунки впливу повного спектру нефлуктаційних завад на цілістність дискретного сигналу, розраховані відносно бітової помилки подано на Рис.1.

Аналіз одержаних залежностей показує, що вплив таких завад на цілісність дискретних сигналів по критерію бітової помилки визначається співвідношенням сигнал/шум та зростає з підвищенням ступені модуляції дискретного сигналу. Особливо це проявляється при зростанні ступені модуляції сигналу до значень $M > 4$ [2].

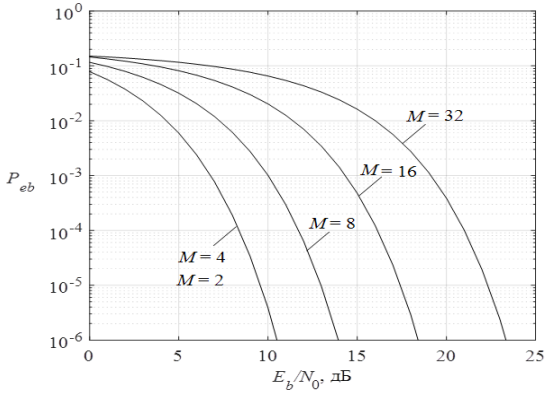


Рис. 1. Залежності імовірності бітової помилки від відношення сигнал/шум при умові когерентного прийому цифрових сигналів в умовах впливу нефлуктаційних завад для різних значень ступені модуляції $M = 2^k$

Таким чином, встановлено, що механізм впливу імпульсної нефлуктаційної завади на цілісність дискретного сигналу, що передається інформаційно-

комунікаційною мережею, проявляється в появі символьної та бітової помилки і зростає з збільшенням ступені модуляції дискретного сигналу.

1. Балашов В. О., Воробієнко П. П., Ляховецький Л. М., Педяш В. В. Системи передавання широкосмуговими сигналами. Одеса: Вид. центр ОНАЗ ім. О.С. Попова, 2012. 336 с.

2. Туровський О. Л., Мелешко Т. В.,Дробик В. О. Методологія оцінки впливу нефлуктуаційних завад на завадостійкість прийому дискретних сигналів з багатопозиційною фазовою маніпуляцією. Звя'зок. №5 (159), С. 29-34, 2022. https://doi.org/10.31673/2412-9070.2022.053439.

Моделювання часових показників протидії витоку інформації матеріально-речовим каналом

УДК 004.056.5:004.08

Богдан Чабан
Державний університет інформаційно-комунікаційних технологій,
Bohdan.chaban96@gmail.com

На сьогоднішній день кількість загроз інформаційній безпеці підприємств постійно зростає. При цьому, особливої актуальності набуває проблема витоку інформації матеріально-речовим каналом. Сучасні зловмисники вже не задовольняються лише відомостями про нові технології, вони прагнуть отримати матеріальне підтвердження запроваджених технологій у виробництво для подальшого копіювання та продажу. Відтак, дослідження методів протидії витоку даних через матеріальні (фізичні) носії інформації є актуальним завданням для науковців.

В публікації [1] було запропоновано модель системи захисту інформації від витоку матеріально-речовим каналом на базі ланцюгів Маркова (рис. 1).

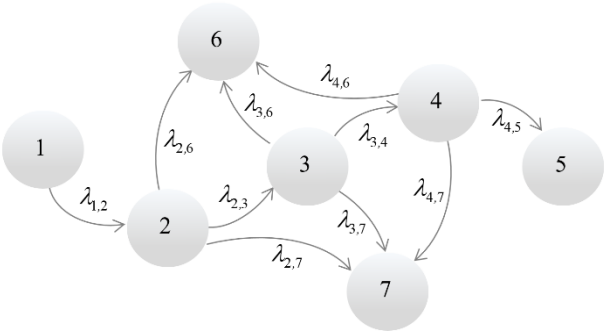


Рис. 1. Модель системи захисту інформації від витоку матеріально-речовим каналом

Ключовим параметром такої моделі є інтенсивності $\lambda_{i,j}$, які є оберненими функціями часу і виражають часові параметри взаємодії у системі "організація–зловмисник". Разом з тим, існують певні складнощі з визначенням $\lambda_{i,j}$, оскільки організації вкрай неохоче діляться відомостями про компрометацію власних ресурсів. Відтак, основним джерелом відомостей про часові показники можуть бути лише емпіричні дані або моделювання.

В публікації [2] виділено 7 основних часових індикаторів, які використовуються при побудові ефективних систем кіберзахисту: Time to Triage (TTT); Time to Qualify (TTQ); Time to Invest (TTI); Time to Mitigate (TTM); Time to Recover (TTRv); Time to Detect (TTD); Time to Response (TTR).

Як показано в публікації [3] більш доцільно розглядати інші часові показники:

1. Середній час виявлення (MTTD) – час, потрібний для виявлення загрози безпеці або інциденту.

2. Середній час відповіді (MTTR) – час, необхідний для контролю та усунення загрози.

Для побудови ефективної моделі протидії витоку інформації матеріально-речовим каналом відповідно до Марківського підходу, наведеного у [1], пропонується наступна схема часових показників (Табл. 1).

Таблиця 1

Часові показники моделі захисту інформації від витоку матеріально-речовим каналом

Інтенсивність	Компоненти часу	Час
$\lambda_{1,2} = 1/\overline{t}_{1,2}$	$\overline{t}_{1,2}$ – асиміляція зловмисника в організації	декілька тижнів
$\lambda_{2,3} = 1/\overline{t}_{2,3}$	$\overline{t}_{2,3}$ – підготовка до атаки	3–5 днів
$\lambda_{3,4} = 1/\overline{t}_{3,4}$	$\overline{t}_{3,4}$ – здійснення атаки	1–3 години
$\lambda_{4,5} = 1/\overline{t}_{4,5}$	$\overline{t}_{4,5}$ – знищення слідів	1–2 години
$\lambda_{2,6} = 1/\overline{t}_{2,6}$	$\overline{t}_{2,6}$ – перехоплення на етапі підготовки	4–7 днів
$\lambda_{3,6} = 1/\overline{t}_{3,6}$	$\overline{t}_{3,6}$ – перехоплення під час атаки	1–2 години
$\lambda_{4,6} = 1/\overline{t}_{4,6}$	$\overline{t}_{4,6}$ – перехоплення під час знищення слідів	30–60 хв
$\lambda_{2,7} = 1/\overline{t}_{2,7}$	$\overline{t}_{2,7}$ – відмова від атаки на етапі підготовки	1–2 дні
$\lambda_{3,7} = 1/\overline{t}_{3,7}$	$\overline{t}_{3,7}$ – відмова від атаки під час її здійснення	20–40 хв
$\lambda_{4,7} = 1/\overline{t}_{4,7}$	$\overline{t}_{4,7}$ – відмова від атаки при знищенні слідів	10–20 хв

На практиці, для протидії спробам витоку (крадіжки) інформації матеріально-речовим каналом через зловмисні дії інсайдерів, часові показники для Табл. 1 можуть визначатися як на етапі прийняття працівника на роботу, так і в процесі його професійної діяльності. Більш надійним є етап прийому на роботу, адже для того, щоб отримати бажане місце, працівник має продемонструвати свої реальні здібності.

Таким чином, застосовуючи тестування працівника при прийомі на роботу, можна виявити потенційного зловмисника ще на етапі його інфільтрації в організацію. Протидія зловмисникам, які не є працівниками організації, залишається сферою відповідальності органів та служб фізичного захисту організації.

1. Чабан Б. В., Котенко А. М. (2024). Модель системи захисту інформації від витоку матеріально-речовим каналом на базі ланцюгів Маркова. Сучасний захист інформації, 4(60), 46–52. https://doi.org/10.31673/2409-7292.2024.040005

2. Cheng, Y., Deng J., Li J., Deloach S., Singhal A., Ou X. Metrics of Security. Cyber Defense and Situational Awareness, 2014, 62, pp. 263–295. https://doi.org/10.1007/978-3-319-11391-3_13

3. Tevet I. Speed Matters: The Crucial Role of MTTD and MTTR in Cybersecurity [online], 2024 [viewed 2025-04-25]. Available from: https://intezer.com/blog/speed-matters-mttd-and-mttr-in-cybersecurity/

Інтелектуальна модель самопідтримки мережевих функцій у середовищі SDN/NFV з елементами захисту від DDoS-атак

УДК 004.8:004.7:621.39

Микола Рижаков[1], Даніїл Сольский[2]
Державний університет інформаційно-комунікаційних технологій,
[1]nykolay.ryjakov@gmail.com

У сучасних телекомунікаційних системах інтеграція штучного інтелекту (AI) із технологіями Network Functions Virtualization (NFV) та Software-Defined Networking (SDN) виступає основою для побудови гнучких, адаптивних та безпечних мереж нового покоління. Такі технології забезпечують можливість централізованого управління мережевими функціями, динамічного розгортання сервісів, а також забезпечення високого рівня надійності та продуктивності в умовах інтенсивного зростання трафіку. З огляду на стрімке зростання складності мережевих архітектур, підвищену кількість користувачів і підключених пристроїв, класичні підходи до управління мережею втрачають свою ефективність, не відповідаючи вимогам сучасної кібербезпеки.

У статті [1] обґрунтовано концепцію інтелектуальної моделі управління, що базується на застосуванні штучних нейронних мереж для вирішення задач прогнозування навантаження, виявлення аномалій та оперативного реагування на кіберінциденти. Зокрема, описується підхід до аналізу часових рядів мережевого трафіку, що дозволяє передбачити пікові навантаження та

потенційні загрози, зокрема DDoS-атаки. Алгоритми глибокого навчання забезпечують можливість постійної адаптації до змін у мережі та прийняття рішень у режимі реального часу, що значно підвищує ефективність управління ресурсами та захисту інфраструктури.

Одним із прикладів функціональної реалізації моделі є оптимізація пропускної спроможності на основі формули середньоквадратичної помилки (MSE):

$$L=1ni=1nyi-yi2 \quad (1)$$

де yi – фактичне навантаження на мережу, yi – прогнозоване, n – кількість спостережень. Навчання моделі здійснюється за допомогою оптимізатора Adam, а ефективність оцінюється за метриками точності, recall і precision.

Дослідження показало, що AI-модель здатна не лише передбачати аномальні сплески навантаження на мережу, але й миттєво реагувати на них, динамічно адаптуючи конфігурацію мережевих ресурсів. Це включає автоматичне переналаштування маршрутів, балансування трафіку між вузлами, а також ізоляцію підозрілих сегментів, що піддаються DDoS-атаці. Такий підхід дозволяє не лише уникнути перевантаження та збоїв у роботі, але й забезпечити безперервність критичних сервісів.

Система здатна самостійно навчатися на основі нових сценаріїв атак, використовуючи механізми постійного донавчання на нових вибірках трафіку та подій. Це дозволяє не лише підвищити точність виявлення загроз, а й забезпечити адаптивність до нових, раніше невідомих типів DDoS-атак. Моделі можуть оновлювати свої параметри безпосередньо під час роботи, аналізуючи зміни в структурі мережевого трафіку, поведінку користувачів, ідентифікуючи відхилення від звичайних шаблонів. Завдяки цьому забезпечується безперервне вдосконалення системи без потреби в ручному втручанні.

Застосування таких моделей значно знижує час реагування на інциденти безпеки (Time to Respond), підвищує рівень якості обслуговування (QoS), зменшує обсяг ручної роботи з боку адміністраторів, знижує ймовірність помилкових спрацювань та дозволяє забезпечити проактивний захист інфраструктури. Система також може накопичувати історичні дані, що використовуються для довгострокового аналізу, трендів і виявлення повільних атак, які важко виявити звичайними засобами.

Повноцінна інтеграція штучного інтелекту в архітектуру SDN/NFV дозволяє створити мережі нового покоління — автономні, гнучкі, стійкі до атак і здатні до самовідновлення. Такі мережі не лише адаптуються до динамічних умов, а й самостійно виявляють загрози, перебудовують структуру взаємодії вузлів, перерозподіляють ресурси для оптимального функціонування, що повністю відповідає вимогам сучасного цифрового середовища, яке характеризується високою складністю, мінливістю та загрозами нового типу.

1. Рижаков М.М., Поночовний П.М. (2025). Модель трансформації на основі ШІ з елементами захисту від DDoS-атак. Прикладні проблеми комп'ютерних наук, безпеки та математики, 4, 14–32.
2. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016.

3. Bhushan B. et al. (2021). Use of AI in SDN for detecting DDoS attacks. IEEE Access, 9, 123456–123471.

Метод виявлення динамічних вразливостей в мобільних додатках

УДК 004.8:004.7:621.39

Ярослав Шавловський

Державний університет інформаційно-комунікаційних технологій, shavlovskyyaroslav@gmail.com

Процес виявлення динамічних вразливостей полягає в періодичному порівнянні поточного стану програмного забезпечення (ПЗ) мобільного додатку в зазначений момент часу з його станом на момент часу початкового застосування його користувачем. Стан мобільного додатку в момент придбання користувачеві вважається еталонним, а саме справним з відсутністю вразливостей.

Нехай $C_E(X(t))$ - еталонний стан, де $X(t) = \{x_1(t), x_2(t), ..., x_n(t)\}$ являє собою набір характеристик ПЗ. Такими характеристиками мобільного додатку є надійність, відмовостійкість, масштабованість, тощо. Позначимо через t_0 - початковий момент часу, коли стан програмного забезпечення є еталонним, тобто виконується рівність

$$C_E(X(t)) = C(X(t_0)) \tag{1}$$

При наявності динамічної вразливості в процесі роботи мобільного додатку відбувається перехід від еталонного стану до поточного. Такий перехід представимо наступним чином

$$C_E(X(t_0)) \to C(X_{n-k}(t_0), X_k(t,\tau)) \tag{2}$$

де $X_{n-k}(t_0)$– набір характеристик ПЗ, які співпадають з еталонними, $X_k(t,\tau)$ - набір характеристик, які відмінні від еталонних за рахунок впливу динамічних вразливостей в момент часу t і кількість яких k, а τ – час, протягом якого діють вразливості в мобільному додатку.

Після виявлення динамічної вразливості і її усунення, відбувається зворотний перехід, який представлено наступним чином

$$C(X_{n-k}(t_0), X_k(t+\tau)) \to C_E(X(t_0)) \tag{3}$$

тобто, мобільний додаток повертається в еталонний стан. На основі проведених досліджень було встановлено, що $k = 1$, тобто при роботі ПЗ присутня тільки одна динамічна вразливість, а ймовірність наявності двох і більше таких вразливостей нескінченно мала і можна прийняти рівної 0. Будемо вважати, що нормальне функціонування ПЗ в мобільному додатку відповідає умові

$$p_{C_E}(X(t_0)) > p_C(X_{n-1}(t_0), X_1(t,\tau)) \tag{4}$$

де $p_{C_E}(X(t_0))$ - ймовірність відсутності динамічної вразливості, $p_C(X_{n-1}(t_0), X_1(t,\tau))$ - ймовірність появи однієї динамічної вразливості.

Виявлення динамічних вразливостей здійснюється на основі аналізу в різні моменти часу станів мобільного застосунку, характеристики яких визначаються протягом скінченної кількості виконання коду, модулів, сервісів, вкладених ресурсів та інших складових, які характеризують поточні властивості ПЗ. Аналізу підлягають зв'язки та алгоритми взаємодії між вказаними елементами. Динамічний стан об'єкта є функцією часу, водночас момент появи і ліквідації динамічних вразливостей носить випадковий характер. Відповідний аналіз здійснюється в певні інтервали часу Δt, які не обов'язково є рівними. Необхідною умовою виявлення є наявність уразливості в момент аналізу Якщо позначити через t_m - момент часу, в який з'явилась динамічна вразливість через m разів експлуатації коду, то отримаємо наступне співвідношення

$$t_m = t_0 + m\Delta t \quad m = 0,1,... \tag{5}$$

. Припущення про можливу наявність динамічної вразливості вразливості визначається фактом відмінності поточного стану об'єкта від еталонного $C_E(X(t_0))$.

Після виявлення та ідентифікації, усунення динамічних вразливостей здійснюється існуючими способами, найпоширенішими з яких є:

А. Статичний аналіз коду, проведення ретельного аналізу вихідного коду програми для виявлення потенційних вразливостей на етапі компіляції. Цей метод передбачає сканування коду на предмет відомих вразливостей і шаблонів без його фактичного виконання.

Б. Динамічний аналіз, запуск програми в середовищі, що контролюється, з метою виявлення вразливостей у реальному часі. Цей метод охоплює моніторинг взаємодії застосунку із зовнішніми ресурсами та аналіз виконання коду на предмет аномалій.

В. Аналіз потоків даних, дослідження потоків даних усередині застосунку для виявлення вразливостей, пов'язаних з обробкою введення-виведення і роботи з даними.

Г. Тестування на проникнення, валідація атак з метою перевірки стійкості програми до різних видів впливів. Цей метод включає в себе спроби злому, зміни даних в процесі їх передачі, та інші атаки на систему.

Д. Моніторинг подій безпеки, встановлення систем моніторингу для реєстрації та аналізу подій безпеки в реальному часі. Це дає змогу виявляти аномалії та нештатні ситуації, пов'язані з можливими загрозами.

Програма виявлення вбудовується в застосунок і після налаштування періодичності тестування (оцінювання) поточного стану реалізується в автоматичному режимі.

Алгоритм виявлення плаваючих вразливостей представлено на рисунку 1.

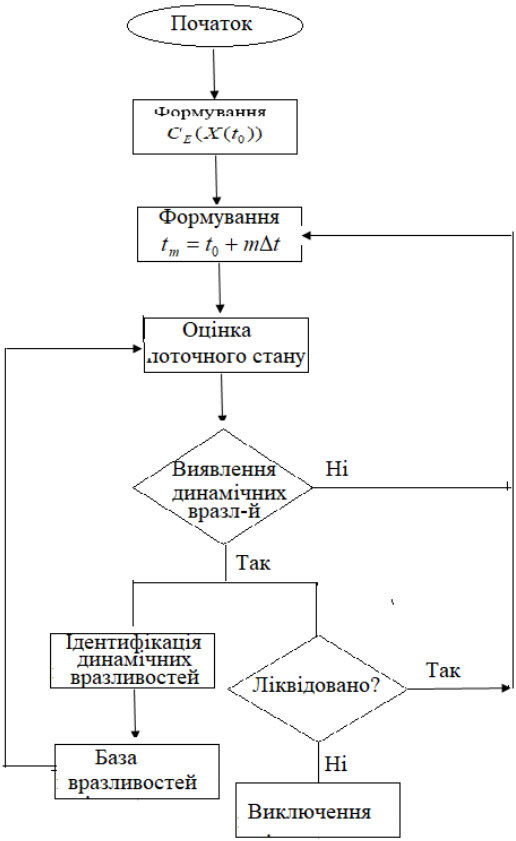


Рисунок 1. Алгоритм виявлення динамічних вразливостей

Алгоритм дає змогу синтезувати програму, що являє собою бібліотеку, спеціально розроблену для впровадження в мобільні додатки під управлінням Android. Ця бібліотека здійснює виявлення та автоматичне усунення плаваючих вразливостей, надаючи розробникам ефективний інструментарій безпеки для підвищення надійності та захищеності додатків.

1. Павликевич А.М. Керований подіями метод вимірювання ефективності контролю інформаційної безпеки в середовищах розробки програмного забезпечення / А.М. Павликевич, М.В. Дзюбан // Сучасний захист інформації, № 3 (2024), с. 42-54.
2. Брезіцький С.М. Методи оцінки якості передавання даних у мережах зв'язку з передачею пакетів / С.М. Брезіцький // Зв'язок, №6 (2024), с. 35-43.

НАУКОВЕ ВИДАННЯ

МАТЕРІАЛИ
XIV Міжнародної науково-технічної конференції
«ITSec: Безпека інформаційних технологій»

22-24 травня 2025 року

м. Тернопіль (Україна)

Організаційний комітет конференції та редакція можуть не поділяти думки авторів і не несуть відповідальність за достовірність викладеної інформації.

За науковий зміст і викладення матеріалу, достовірність та коректність фактичних даних (у тому числі класифікаційного індексу УДК) уся відповідальність покладається на авторів та їх наукових керівників.

Неінформативний текст матеріалів доповіді міг бути скорочений або вилучений на розсуд Оргкомітету конференції.

Оригінал-макет підготовлено на кафедрі кібербезпеки
Західноукраїнського національного університету