МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
УКРАЇНИ "КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ
ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"

НАВЧАЛЬНО-НАУКОВИЙ
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

# THEORETICAL AND APPLIED CYBERSECURITY

Перша Всеукраїнська
науково-практична конференція,
присвячена 100-річному ювілею
академіка В.М. Глушкова

Матеріали конференції

Київ – 2023

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ "КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"**

**НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**

# THEORETICAL AND APPLIED CYBERSECURITY

**Перша Всеукраїнська науково-практична конференція, присвячена 100-річному ювілею академіка В.М. Глушкова**

## Матеріали конференції

**Київ – 2023**

УДК 004.056(06)
Т44

*Рекомендовано до друку Вченою радою*
*КПІ ім. Ігоря Сікорського*
*(протокол № 8 від 05.06 2023 р.)*



Т44 **Theoretical and Applied Cybersecurity** : Перша Всеукр. наук.-практ. конф., присвячена 100-річному ювілею акад. В. М. Глушкова : матеріали конф. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2023. – 266 с.

**ISBN 978-966-990-083-8**

Подано матеріали доповідей Першої Всеукраїнської науково-практичної конференції «Theoretical and Applied Cybersecurity», присвяченій 100-річному ювілею академіка В. М. Глушкова (TACS-2023, 26 травня 2023 року, м. Київ, Україна).

У збірнику представлені матеріали, присвячені питанням кібернетичної безпеки критичних інфраструктур, моделювання та протидії інформаційним операціям, технологій інформаційно-аналітичних досліджень на основі відкритих джерел інформації. Наведені матеріали з актуальних проблем інформаційної та кібернетичної безпеки, можливості застосування штучного інтелекту, системного аналізу при забезпеченні підтримки прийняття рішень, комп'ютерному моделюванні процесів і систем, актуальні завдання забезпечення інформаційної та кібербезпеки.

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

**УДК 004.056(06)**

ISBN 978-966-990-083-8

# ЛОГІКО-ЙМОВІРНІСНЕ МОДЕЛЮВАННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Л.Б. Алексейчук, О.М. Новіков
Національний технічний університет України
«Київський політехнічний інститут ім. Ігоря Сікорського»,
Навчально-науковий фізико-технічний інститут,
Київ, Україна
alekseichuk.lesia@gmail.com

У роботі розроблено та досліджено логіко-ймовірнісну модель оцінювання ризиків кібербезпеки об'єкту критичної інфраструктури в енергетичній сфері у випадку реалізації множини можливих загроз з кіберпростору.
**Ключові слова:** критична інфраструктура, ризики кібербезпеки.

## Вступ

З розвитком інформаційно-комунікаційних технологій зростає кількість загроз та кібератак на об'єкти критичної інфраструктури з кібернетичного простору.

В роботах [1], [2] запропоновані моделі аналізу кібербезпеки об'єктів критичної інфраструктури енергетичного сектору, в роботі [3] запропоновано та розвинуто логіко-ймовірнісний метод оцінювання безпеки структурно-складних систем. В роботах [4] - [8] розглядались задачі подальшого розвитку та використання логіко-ймовірнісного методу в різних сферах.

**Мета дослідження.** Метою роботи є розробка та дослідження логіко-ймовірнісної моделі оцінювання ризиків кібербезпеки об'єкту критичної інфраструктури в енергетичній сфері у випадку реалізації множини можливих загроз з кіберпростору.

**Логіко-ймовірнісна модель ризику кібербезпеки АСУ ТП.** Оцінимо ризики для АСУ ТП електричної мережі від множини можливих загроз з кіберпростору. Згідно процедури побудови логіко-ймовірнісних моделей

сформуємо структурні, логічні та ймовірнісні моделі безпеки АСУ ТП електричної мережі (рис.1).

На рис.1 розглядаються події, які ведуть до здійснення небажаної події – компрометації системи захисту органів керування автоматичної системи керування рівня PLC ICS $CSS_3$. Подія відбудеться, якщо здійсниться хоча б одна з трьох ініціюючих подій 1-3. На першому рівні зображено 1-6 функціональних вершин, які позначають вихідні елементарні випадкові події $x_1$ – $x_6$. Названі події відбуваються з відомими імовірностями їх здійснення $p_1$ – $p_6$.

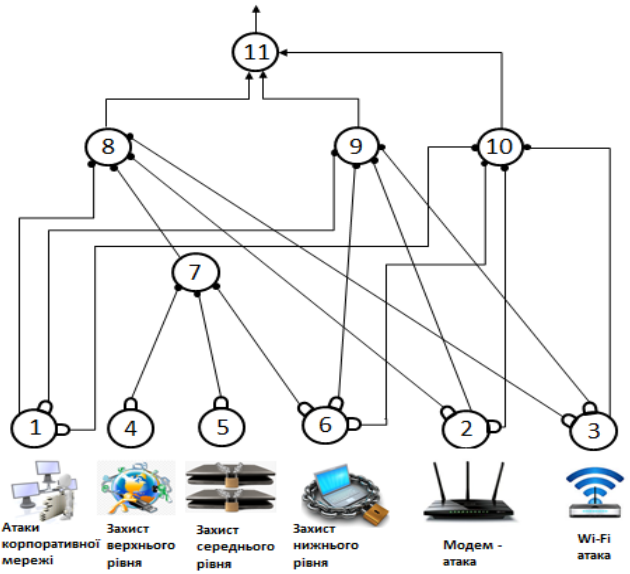


Рис.1. Структурна схема розвитку несприятливої події кібербезпеки

Система логічних рівнянь розвитку несприятливої події від реалізації:

$y_1 = x_1, y_2 = x_2, y_3 = x_3, y_4 = x_4, y_5 = x_5, y_6 = x_6,$
$y_7 = \bar{y}_4\,\bar{y}_5\bar{y}_6, y_8 = y_1\bar{y}_2\bar{y}_3y_7, y_9 = \bar{y}_1y_2\bar{y}_3\bar{y}_6,$
$y_{10} = \bar{y}_1\bar{y}_2y_3\bar{y}_6, y_{11} = y_8 \vee y_9 \vee y_{10}$

Розв'язуючи відповідну систему логічних рівнянь, отримаємо умови здійснення небажаної події – компрометації системи захисту органів керування автоматичної системи керування рівня PLC ICS $CSS_3$:

$$y_{11} = (x_1\bar{x}_2\bar{x}_3(\bar{x}_4\bar{x}_5\bar{x}_6)) \vee (\bar{x}_1x_2\bar{x}_3\bar{x}_6) \vee (\bar{x}_1\bar{x}_2x_3\bar{x}_6) \quad (1)$$

Логічний поліном у диз'юнктивній нормальній формі (ДНФ):

$$y_{11} = (x_2\bar{x}_1\bar{x}_3\bar{x}_6) \vee (x_3\bar{x}_1\bar{x}_2\bar{x}_6) \vee (x_1\bar{x}_2\bar{x}_3\bar{x}_4\,\bar{x}_5\bar{x}_6) \quad (2)$$

В ймовірнісній формі:

$$P = P_2Q_1Q_3Q_6 + P_3Q_1Q_2Q_6 + P_1Q_2Q_3Q_4Q_5Q_6 =$$
$$= (P_2 + P_3 + P_1Q_3Q_4Q_5)Q_1Q_3Q_6 \quad (3)$$

де P - ймовірність реалізації небажаної події,

Q - ймовірність того, що подія не відбудеться.

Логіко-ймовірнісна модель оцінювання ризиків кібербезпеки об'єкту критичної інфраструктури в енергетичній сфері у випадку реалізації множини можливих загроз з кіберпростору з урахуванням, що Q = 1 – P:

$$P = [P_2 + P_3 + P_1(1 - P_3)(1 - P_4)(1 - P_5)](1 - P_1)(1 - P_3)(1 - - P_6) \quad (4)$$

## Висновки

В роботі розроблено логіко-ймовірнісну модель оцінювання ризиків кібербезпеки об'єкту критичної інфраструктури в енергетичній сфері з урахуванням реалізації множини можливих загроз з кіберпростору. Результуюча модель базується на послідовно розроблених структурної, логічної та ймовірнісної моделях можливих загроз. В якості основних можливих загроз розглядалися можливості атак через корпоративну мережу, з'єднання через модем та бездротове з'єднання.

## Перелік використаних джерел

1. Saeed Ahmadian, Xiao Tang, Heidar A. Malki, Zhu Han, Modelling Cyber Attacks on Electricity Market Using Mathematical Programming With Equilibrium Constraints. IEEE Access, vol. 7, 2019

2. Rajaa Vikhram Yohanandhan, Rajvikram Madurai Elavarasan, Premkumar Manoharan, Lucian Mihet-Popa, Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. IEEE Access, vol. 8, 2020.

3. Ryabinin, I.A. Logical-Probabilistic Calculus: A Tool for Studying the Reliability and Safety of Structurally Complex Systems. Automation and Remote Control vol. 64, 2003, P. 1177–1185

4. Alexeev V. Logical and probabilistic analysis of the reliability of the metallurgical complex electric supply. International Journal of Risk Assessment and Management, January 2018, 21(1/2):42

5. V.V. Gorshkov, Logical probabilistic method for calculation of the survivability of complex systems. Cybernetics, vol. 18, 1982, p. 122–126.

6. Zavgorodnii V., Zavgorodnya A., Maiko V., Malikov V., Zhuk D. Methods And Models For Assessment Of Reliability Of Structural-Complex Systems. World Science, No 11(39), 2018

7. Новіков О.М., Тимошенко А.О. Побудова логіко-ймовірнісної моделі захищеної комп'ютерної системи //Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - 2001. - Вип. 3. - С. 101-105

8. Хнигічева О.М., Новіков О.М., Тимошенко А.О. Моделювання безпеки складних інформаційно-комунікаційних систем з використанням логіко-ймовірнісного методу //Наукові вісті НТУУ «КПІ». - 2010. - Вип.6. - С. 70-81

# АДАПТИВНА СТРАТЕГІЯ РОЗПОДІЛУ РЕСУРСУ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Д. Р. Друзь, С. А. Смирнов
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут

У статті розглянуто задачу розподілу ресурсу для захисту інформації від атак зловмисників та різних видів атак змінного профілю. За допомогою аналізу поточної інформації про зміни профілю отримані оцінки для перерахування та оновленні інформації. На основі цих оцінок запропонована та обгрунтована стратегія розподілу ресурсу захисту інформації.
**Ключові слова:** Задача розподілу ресурсу, стратегія, атаки

## Вступ

Захист інформації завжди була однією з найважливіших проблем нашого суспільства. З появою комп'ютерної техніки та впровадження її в усі сфери діяльності проблема загострилася ще більше. З появою Інтернету стовідсоткова захищеність інформації стала неможливою.

Тому важливим нині є питання оптимального розподілу ресурсу захисту інформації для захисту від різних типів атак з урахуванням обмеженості ресурсу.

## 1. Постанова задачі

В даній задачі ми повинні розробити адаптивну стратегію захисту інформації. Це означає, що вона має підлаштовуватися під зміни режиму атак. Якщо перейти до математичних понять, то ми маємо ресурс захисту $x$, і ми повинні розподілити його на $x_j$ для протидії різним типам атак. Тобто $x = \sum_j x_j$ ми повинні знайти розподіл $x$, при якому система буде ефективно протистояти поточному сценарію атак. Принцип оптимальності розподілу ресурсу буде записуватися наступним чином:

$$x_j \sim P_j W_j n_j \quad (1)$$

де $P_j$ – ймовірність успішності атаки, $W_j$ – збитки від успішного завершення атаки j-го типу, $n_j$ – кількість атак j-го типу.

## 2. Моделювання вхідного потоку атак

В даній роботі розглядаються атаки на інформаційний ресурс, що відбуваються протягом фіксованого часового проміжку. Нехай $T_k$ – тривалість атаки, що використовує k-ту вразливість. Оберемо значення $T = max T_k$ – за цей час всі попередні атаки завершуються, та відбуваються лише ті, які розпочались протягом такого інтервалу часу. Будемо використовувати спостереження за такими атаками для встановлення статистичних характеристик вхідного потоку, що складається з атак різного типу.

Обираємо довжину такту як мінімальну відстань між двома атаками що експлуатують різні типи вразливостей. На відповідному проміжку $T$ ми визначаємо кількість атак $n_j$, що використовують конкретний тип j-ї вразливості.

Для j=0 число $n_0$ буде визначати кількість тактів, на яких атак не було. Тоді, $n_j \in [0; l]$, де l – число тактів у вікні, а n – реальна поточна кількість нових атак на часовому проміжку довжиною T.

Для описаної ситуації використаємо пуассонівський процес, як математичну модель вхідного потоку атак.

Характерною особливістю такого процесу є його ординарність, тобто одночасно дві атаки початись не можуть, у відповідності з вказаним вибором довжини такту. Якщо на деякому такті жодна з реальних атак не починається, то будемо вважати, що почалась деяка “фіктивна” атака, яку ми розглядаємо для повноти та замкненості формалізму, та позначаємо індексом j = 0.

Таким чином вхідний потік описується послідовністю $\{t_m\}$ моментів часу початку атак, тоді $L = max_m (t_{m+1} - t_m)$ – природна довжина такту, $n = \frac{T}{L}$ - повне число поточних атак, а також число тактів у вікні (в нашому

випадку 100). Розглянемо $p_j$ – ймовірність того, що атака яка експлуатує вразливість типу j починається протягом такту довжиною $\bigtriangledown$, відповідно $(1 - p_j) = \sum_{h \neq j} p_h$ - ймовірність того, що розпочинається якась інша атака.

Тому в цьому випадку використаємо схему Бернулі, та ймовірність того, що за n тактів розпочнеться $n_j$ атак j-го типу можна визначити біноміальним розподілом:

$$B(n_j, n, p_j) = C_n^{n_j} p_j^{n_j} (1 - p_j)^{n - n_j} \quad (2)$$

Таким чином як результат спостережень виникає вибірка довжиною l, в кожний позиції якої вказується номер (тип) атаки, що розпочинається на відповідному такті. Статистичні методи дозволяють отримати оцінки для ймовірності $p_j$ , які будуть змінюватись при оновленні вибірки з плином часу.

На врахуванні таких зміна значень оцінок $p_j$ буде заснована адаптивна стратегія захисту.

Отже сформульована модель атак на інформаційну систему, яка містить ресурси, які потрібно захистити та ресурси які можна застосувати для захисту — деякі спеціальні ресурси, величина яких завжди обмежена. Тому виникає задача оптимального розподілу ресурсу на відбиття різних типів атак.

## 3. Розв'язок задачі

Як зазначалося раніше, $x$ – об'єм ресурсу захисту та $x_j$ – частина ресурсу, направлена на протидію атаці j-го типу: $x = \sum_{j=1}^{n} x_j$.

В якості принципу оптимізації доцільно використовувати критерій середнього ризику. Оцінка середнього ризику має такий вигляд

$$\sum_{j=1}^{n} P_j W_j n_j. \quad (3)$$

Вважаємо, що для атаки j-го типу ймовірність успішності $P_j$ пропорційна ймовірності того, що атака сталася протягом найдовшого такту $p_j$. Виходячи з того, що не кожна атака досягає цілі, $P_j \leq p_j$, а також, що $P_j$ повинна залежати від використаного для захисту ресурсу, отримуємо монотонно-спадну залежність вигляду:

$$P_j = p_j(1 - \alpha_j x_j)\ , \qquad (4)$$

де $\alpha_j$ – ефективність використання ресурсу, направленого на протидію j-ій загрозі. Підставимо (4) в (3):

$$\sum_{j=1}^{n} P_j W_j n_j = \sum_{j=1}^{n} p_j(1 - \alpha_j x_j) W_j n_j \qquad (5)$$

$$\sum_{j=1}^{n} p_j(1 - \alpha_j p_j) W_j n_j = \sum_{j=1}^{n} (p_j W_j n_j - \alpha_j x_j W_j n_j) \qquad (6)$$

Отримана оцінка залежить від ймовірностей $p_j$ та розподілу $x_j$, а все інше – фіксовані параметри. Мінімізація ризику зводиться до максимізації від'ємника. Залежність лінійна за змінними $x_j$, а значення параметрів $\alpha_j, W_j$ – деякі точкові експертні оцінки, що вважаються відомими.

Ймовірності $p_j$ можуть бути оцінені на основі спостережень за розгортанням атак. Наприклад як точкову оцінку $p_j$ використаємо найбільш несприятливу з множини визначеної інтервальними обмеженнями. Це дозволить реалізувати мінімаксний підхід, та на цій основі отримати більш надійний гарантований результат.

Для розв'язку задачі розглянемо стратегію захисту на основі мінімізації критерію середнього ризику.

За умовою маємо задачу оптимізації з лінійним критерієм $\sum_{j=1}^{n} \alpha_j x_j W_j n_j \rightarrow max$, та обмеження $x = \sum_j x_j$. До задачі доцільно додати інтервальні обмеження $x_j$. Нижніми оцінками $\underline{x}_j$ можна вважати частину ресурсу, яка обов'язково використовується для проведення неперервного моніторингу виникнення атак відповідного типу. Верхні визначатимуться технічними можливостями системи захисту. Задача з вказаними обмеженнями має вигляд:

$$\begin{cases} \sum_{j=1}^{n} \alpha_j x_j W_j n_j \rightarrow max \\ x = \sum_j x_j \\ 0 \le \underline{x}_j \le x_j \le \overline{x}_j \le x \end{cases} \qquad (7)$$

Подібні задачі досліджувались в [1], де встановлено як загальний вигляд розв'язку, так і швидку процедуру його знаходження. Процедура виглядає так:

Для вершин $x^j = \underline{x}_1, \dots, \underline{x}_j, \tilde{x}_j, \overline{x}_1, \dots, \overline{x}_j$ будуємо суму $S^j = \underline{x}_1 + \cdots + \underline{x}_j + \overline{x}_1 + \cdots + \overline{x}_j$. Якщо виконується умова $\underline{x}_j \le 1 - S^j \le \overline{x}_j$, то розподіл $x^j$, являється шуканим. Інакше виконуємо крок $j+1$.

## Висновок

В даній роботі була математично описана задача розподілу ресурсу захисту інформації та представлена стратегія за якою можна будувати адаптивну схему захисту від атак змінного профілю. Надалі передбачається аналіз стратегій з прогнозуванням майбутніх атак та їх застосування до нашої моделі

## Перелік використаних джерел

1. Смирнов С. А., Гонтаренко И. С. Грантированый синтез скалярного критерия для решения задачи многокритериатьной оптимизации – 2006
2. Мушик Э., Мюллер П. Методы принятия технических решений – М. :Мир, 1990

# КІБЕРСТІЙКІСТЬ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ЕНЕРГЕТИЧНОЇ КРИЗИ

Зубок В. Ю.
Науково-навчальний фізико-технічний інститут КПІ ім. Ігоря Сікорського

Невпинне проникнення інфокомунікаційних систем в усі сфери буття і широке використання цифрових технологій отримало назву «цифрова трансформація». Вона розмиває відмінності між інформаційними технологіями та операційними технологіями (відомими нам за скороченням АСУТП) через використання однакових інструментів в інфокомунікаційних системах (ІКС). Будь-які системи демонструють різну здатність до ефективного протистояння ризикам будь-якого походження і характеру,

адаптації до змін середовища, підтримання максимально сталого функціонування завдяки швидкому відновленню. Такі властивості узагальнено отримали назву резильєнтності. Якщо ці властивості демонструє ІКС, або кіберфізична система, або кіберсоціальна система, ми можемо назвати їх кіберрезильєнтністю. Є безпосередній зв'язок між нею та цифровізацією. Для аналізу кіберрезильєнтності пропонується розглянути цифрових суб'єктів, цифрові потреби, цифрові засоби і їхні залежності. Приведено практичні приклади таких залежностей, які формуються під впливом систематичних ракетних атак агресора на енергетичну систему України.
**Ключові слова:** критична інформаційна інфраструктура, цифрова резильєнтність, цифрова стійкість, топологічний простір, цифрові потреби, цифрові засоби, кібербезпека.

**Актуальність.** Законодавство України визначає об'єкти *критичної інформаційної інфраструктури* (ОКІІ) як інформаційні технології (ІТ) та операційні технології (ОТ), які є є невід'ємними частинами сучасної критичної інфраструктури [1]. ІТ протягом 40 років розвивались в напрямку автоматизації бізнес процесів, в той час як ОТ – в керування виробництвом. Однак обидві базуються на інформаційно-комунікаційних системах (ІКС) різноманітного масштабу та складності, з тією різницею, що ОТ працюють у складі кіберфізичних систем, кінцевим продуктом яких є матеріальний об'єкт, в той час як кінцевим продуктом ІТ є інформація. Однак цифрова трансформація призводить до конвергенції цих технологій. Цифрова трансформація (або, як її називають в ЗМІ, «цифровізація» чи «діджиталізація») - характерна риса цифрового суспільства, економіка якого базується на інформаційних технологіях [2]. Семантичне поле цифрової трансформації включає в себе такі поняття, як цифрова економіка, цифрові навички, цифрові права, цифрові інновації, електронні послуги, електронне урядування і багато іншого. Інфраструктура цифрових послуг стає окремим об'єктом як атак, так і захисту.

Масований терор, що вчиняє країна-агресор щодо об'єктів критичної інфраструктури України (перш за все – електроенергетичного сектору), ставить питання не стільки захисту (фізичного чи кібернетичного) ІКС у складі ОКІІ, скільки питання ефективного протистояння ризикам, пов'язаним з атаками на об'єднану енергосистему України, адаптації до змін середовища функціонування, підтримання максимально сталого функціонування завдяки швидкому відновленню. Перелічені властивості узагальнено отримали назву *резильєнтності*. На сьогодні добре відомі поняття кіберстійкості (cyber resilience) [3], цифрової стійкості (digital resilience) [4], але вимоги та метрики для цих характеристик остаточно не сформульовані – дослідження тривають багато років, протягом яких з'являються нові підходи.

С точки зору досліджень резильєнтності надзвичайно цінним є досвід України. Україна протягом десятиріччя була серед лідерів цифрової трансформації до широкомасштабної війни з Росією. Безпрецедентні ракетні атаки на головні об'єкти електроенергетики призводять до масових аварійних відключень електроенергії. Бізнеси, оператори комунікацій, державні інформаційні сервіси, охорона здоров'я та багато інших галузей, в яких наявні ОКІІ, роблять спроби адаптуватися до рівня надання електроенергії, що знижується. При цьому кожна з груп використовує різноманітні доступні засоби та організаційні заходи для більш тривалої підтримки можливості задоволення цифрових потреб. Є актуальною проблема дослідження цифрової резильєнтності та її складових, аби наука зробила свій внесок в розвиток механізмів поглинання негативного впливу, адаптації до нового стану та еволюціонування ІКС, без яких неможлива цифрова резильєнтність. Таке дослідження потребує збору, аналізу, систематизації наявного досвіду (особливо секторального) задля зменшення у майбутньому кількості спроб і помилок при створенні резильєнтних ІКС в умовах обмежень та невизначеностей.

**Метод дослідження.** Для розвитку методів підвищення резильєнтності ІКС до загроз, пов'язаних з

електроенергетикою пропонується визначити деякі множини об'єктів множини цифрових споживачів – $DS$, цифрових потреб – $DN$, та цифрових засобів – $DT$ (рис.1). З цих трьох множин утворюватимуться різноманітні кортежі з трьох елементів:

$$(ds \in DS, dn \in DN, dt \in DT), \quad (1)$$

а також і з двох елементів на основі наявних та доступних сполучень:

цифрового споживача та його цифрових потреб

$$(ds \in DA, (dn_1, dn_2, \dots, dn_{k-1}, dn_k) \in DN); \quad (2)$$

цифрового суб'єкта та доступних йому цифрових засобів

$$(ds \in DA, (dt_1, dt_2, \dots, dt_{k-1}, dt_k) \in DT); \quad (3)$$

цифрових потреб та прийнятних цифрових засобів для їх отримання

$$(dn \in DN, (dt_1, dt_2, \dots, dt_{k-1}, dt_k) \in DT). \quad (4)$$

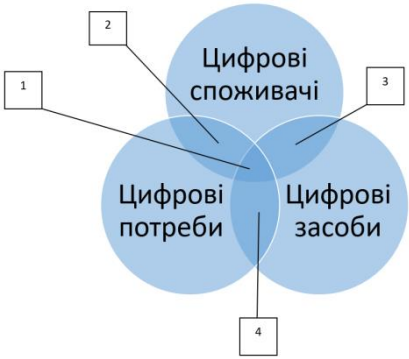


Рисунок 1 – Кортежі, що утворюють взаємозалежності між множиною цифрових споживачів, цифрових засобів та цифрових потреб; позначки 1,2,3 відповідають номеру формули вище.

Нехай існує множина $\mathcal{D}$, така що $\forall da \in \mathcal{D}, \forall dn \in \mathcal{D}, \forall dt \in \mathcal{D}$. Нехай існує система елементів цієї множини $\mathcal{T}$, до якої належать всі можливі комбінації цих елементів, об'єднання та перетини цих множин [5]:

$$\exists \mathcal{T}: \emptyset, \mathcal{D} \in \mathcal{T}; \forall \mathcal{D}', \mathcal{D}'' \in \mathcal{T}: \mathcal{D}' \cup \mathcal{D}'' \in \mathcal{T}; \ \mathcal{D}' \cap \mathcal{D}'' \in \mathcal{T}. \quad (5)$$

Тоді $\mathcal{T}$ відповідає визначенню топології на множині $\mathcal{D}$ , а пара $(\mathcal{D}, \mathcal{T})$ відповідає визначенню *топологічного простору*. Окремі елементи топології – мережеві структури, що можуть бути досліджені з використанням теорії графів, теорії складних мереж, теорії топологічних просторів для розроблення моделей і методів дослідження і підвищення цифрової резильєнтності.

В уявному ланцюгу, що об'єднує цифрового споживача з множиною цифрових потреб за допомогою множини цифрових засобів (рис.2), початковим елементом цифрової резильєнтності є споживач цифрових послуг. Це або фізична особа, або спільнота, або юридична особа, потреби яких дещо відрізняються, і також незначним чином відрізняється для них доступність цифрових засобів. Цифровим споживачем може бути і надавач цифрових послуг.

Цифрові засоби, тобто множина *DT*, є ключовим елементом, що забезпечує доступ до цифрових потреб. Ця множина складається зазвичай з сукупності багатьох ІКС, до яких входять інформаційні технології, засоби електронних комунікацій різних постачальників, інфраструктури центрів обробки даних та іншого, що можна узагальнити терміном «цифрова екосистема». Ризики, пов'язані з нестабільним електропостачанням, впливають на всі без винятку елементи екосистеми. Самі елементи вживають різні заходи для протидії негативному впливу цього фактора (можна назвати їх заходами резильєнтності): накопичення електроенергії, використання альтернативних джерел, альтернативна генерація, зміна графіку роботи, зміна власної архітектури, обрання інших засобів електронних комунікацій тощо.

Однакові заходи можуть мати різну ефективність в різних елементів. Відповідно до запропонованої класифікації (1) – (5), ланцюг від цифрового споживача до цифрової послуги на самому початковому етапі містить велику кількість варіантів забезпечення цифрової резильєнтності самого актора та засобів електронних комунікацій. Кожен захід та засіб може бути

проаналізований та порівняний з іншими, які забезпечують аналогічний результат.

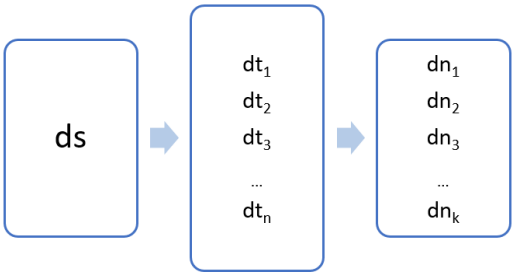


Рисунок 2. Цифрова екосистема – ланцюг від цифрового споживача до цифрових потреб.

**Висновки.** Проблема дослідження цифрової резильєнтності та її складових потребує розробки метрик, які характеризують ефективність засобів резильєнтності на основі їхньої доступності, вартості, швидкості впровадження, надійності та інших критеріїв. Представлення цифрових екосистем у вигляді топологічного простору відкриває шлях до вивчення проблеми цифрової резильєнтності через дослідження групових властивостей, характеристик, спільної динаміки великої кількості мережевих структур.

## Перелік використаних джерел

1. Деякі питання об’єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 943 : станом на 07.09.2022р. URL : https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF (дата звернення: 09.02.2023)

2. Цифрова трансформація: навіщо вона потрібна державі та бізнесу. *Дія Бізнес*. URL : https://business.diia.gov.ua/cases/tehnologii/cifrova-transformacia-naviso-vona-potribna-derzavi-ta-biznesu (дата звернення: 14.01.2023)

3. Linkov, I., Kott, A. (2019). *Fundamental Concepts of Cyber Resilience: Introduction and Overview*. In: Kott, A., Linkov, I. (eds) Cyber Resilience of Systems and Networks. Risk, Systems and Decisions. Springer, Cham. https://doi.org/10.1007/978-3-319-77492-3_1

4. Cuel, R., Ponte, D., & Virili, F. (2022). *Exploring digital resilience: Challenges for people and organizations*. Springer Nature.

5. Зубок, В. *Ефективність використання заходів з підвищення цифрової резильєнтності підчас тривалих відключень електропостачання*. Електронне моделювання (2023). – прийнято до друку.

# АНАЛІЗ ВРАЗЛИВОСТЕЙ ТА ФОРЕНЗІКА МЕРЕЖІ ETHEREUM: ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ЦІЛІСНОСТІ БЛОКЧЕЙНУ

Е.В. Абдуллаєва, Л.Ю.Гальчинський

Навчально-науковий Фізико-технічний інститут, НТУУ «КПІ ім. Ігоря Сікорського», м.Київ, Україна

Дана робота має на меті вивчення блокчейн мережі з метою виявлення незаконних дій. В ній розглядаються поняття та основні уразливості, пов'язані з мережею Ethereum. Об'єктом дослідження є створення алгоритму форензіки для протоколу Ethereum, спрямованого на виявлення злочинності в мережі. Результати проведеного дослідження можуть бути використані для програмної реалізації аналізу та подальшого підвищення рівня безпеки блокчейн мережі.

**Ключові слова:** *блокчейн, аналіз мережі, Ethereum, вразливості, форензіка*

## Вступ

Швидке зростання блокчейну, особливо в криптовалюті, видно на прикладі Ethereum, що прориває в інноваціях та розвитку. Проте, відкритість Ethereum створює проблеми з

незаконною діяльністю, включаючи відмивання грошей та кіберзлочинність. Розуміння цих ризиків критичне для стабільного розвитку технології.

### Вразливості протоколу Ethereum

Ethereum, як відкрита блокчейн-платформа, надає розробникам можливість створювати та розгортати смарт-контракти та децентралізовані програми[1]. Проте, Ethereum має свої вразливості та проблеми. Деякі з основних вразливостей протоколу Ethereum перераховані нижче [2,3]:

1. Атака 51%. Тип , коли більш як 51% мережі контролює один суб'єкт або група, дозволяючи маніпулювати транзакціями і створювати нові блоки.
2. Вразливості смарт-контрактів. Забезпечення виконання угоди відповідно до вбудованої логіки, а кінцевий стан мережі залишається незмінним. До основними вразливостей відносяться помилки кодування, атаки повторного входу, маніпуляції з часовими мітками, відсутність конфіденційності та ризики централізації[4].
3. Вразливості алгоритму консенсусу. Зловмисник, який отримує старі закриті ключі, потенційно може створити альтернативний ланцюжок, починаючи зі старого блоку[2].
4. Фрагментація мережі. Тимчасовий або постійний поділ мережі блокчейну на окремі підмережі, призводить до фрагментація мережі.

## Алгоритм форензіки мережі Ethereum

У ході дослідження був створений алгоритм аналізу блокчейн мережі Ethereum, який буде використовуватися для програмної реалізації з використанням мови програмування Python. Зображення алгоритму наведено на рисунку 1. Він складається з чотирьох основних етапів аналізу мережі[5,6].


Рисунок 1. Алгоритм форензіки мережі Ethereum

1. Збіру даних. За допомогою бібліотеки web3.py можна зібрати точні дані транзакцій. Сервіс infura.io використовується для зручної інтеграції, надаючи доступ до Ethereum через API. Метод отримує основні деталі кожної з них, такі як геш, відправник, отримувач, сума транзакції та комісія.
2. Аналіз зібраних даних. Для цього буде використано різні методи, включаючи підрахунок транзакцій в блоку, перевірку балансу адреси, виявлення підозрілих транзакцій, визначення можливої діяльності ботів, моніторинг великих транзакцій та виявлення транзакцій з високою частотою.
3. Візуалізація графа транзакцій – допомагає в розпізнаванні щільно пов'язаних адрес.
4. Підготовка звіту за результатами аналізу.

## Метрики ідентифікації протиправних дій

Блокчейн форензіка включає аналіз та відстеження транзакцій за допомогою спеціальних методів. Основні криміналістичні показники блокчейна, які допомагають оцінювати безпеку, включають обсяг транзакцій, вартість транзакцій, баланс адрес, коефіцієнт кластеризації та комісію за транзакцію. Детальніші дані можна знайти в таблиці «Метрики».

## Висновки

Дослідження зосереджується на принципах роботи та основних вразливостях блокчейн мережі , а також розробці алгоритму для виявлення незаконної активності в мережі. Воно починається з огляду найбільш поширених вразливостей Ethereum. Далі було розроблено алгоритм для аналізу та дослідження блокчейн мережі з метою виявлення незаконних дій. В цілому, аналіз Ethereum мережі є важливим інструментом для забезпечення безпеки та цілісності блокчейну.

## Перелік використаних джерел


1. What is blockchain technology? — URL: https://www.ibm.com/topics/blockchain.
2. Топчій М., Гальчинський Л. Підвищення рівня безпеки смарт-контрактів у мережі Ethereum від шахрайства за рахунок використання ревесивних токенів. — 2022-11-11. — С. 14—21.
3. Goyal H., B. S. Blockchain Forensics in Policing and It's Global Scenario // Lupine Publishers. — 2022-05-25.
4. Blockchain: A new perspective in cyber technology / T. Venkat Narayana Rao, P. P. Likhar, M. Kurni, S. K. — 2022. — P. 33–66.
5. Salisu S., Filipov V., Penne B. Blockchain Forensics: A Modern Approach to Investigating CyberCrime in the Age of Decentralisation. — 2022-06-30.
6. T. K. Digital forensics of cryptocurrency wallet. — 2022-05-20. — P. 14–21.

# МЕХАНІЗМИ МОНІТОРИНГУ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

Д.О. Шатковська, І.В. Стьопочкіна,
Навчально-науковий Фізико-технічний інститут КПІ ім. Ігоря Сікорського, Київ, Україна

Розглянуто особливості моніторингу кібербезпеки об’єктів критичної інфраструктури, які відносяться до енергетичного сектору. Описані можливі кіберзагрози на об’єкти енергопостачання, в тому числі такі, що притаманні військовому часу. Запропоновано принципи моніторингу показників пристроїв інтернету речей, та відповідні технічні механізми та рішення, які можуть для цього використовуватись.
**Ключові слова:** *Енергетична інфраструктура, моніторинг кібербезпеки, кібератаки, інтернет речей*

## Вступ

У сучасному світі, енергетична інфраструктура (далі – ЕІ) стала ключовим компонентом національної безпеки кожної країни. Під час військового стану почастішали атаки на об’єкти енергопостачання, особливо це стосується порушення функціонування пристроїв інтернету речей, які можуть мати вихід на глобальні мережі, для надсилання певних показників у центри обробки даних. Роботу потенційно вразливих пристроїв слід постійно спостерігати, щоби вловлювати варіації у показниках їхнього функціонування, які можуть свідчити про початок атаки. Відповідні рішення передбачають: 1) вибір протоколу взаємодій; 2) організацію центру моніторингу, який буде приймати поточні значення ключових показників та аналізувати їх стан; 3) способи узагальнення даних по деякій множині об’єктів критичної інфраструктури для швидкого обміну актуальною інформацією про загрозу; а

також зберігання відповідної інформації у розподілених базах даних.

## Загрози об'єктів енергетичної інфраструктури під час війни

Під час війни, питання ІБ об'єктів критичної інфраструктури загострюється, зокрема об'єкти ЕІ є особливо важливими для забезпечення життєдіяльності цивільних, комунікаційних і військових інфраструктур.

Серед загроз, які на практиці зустрічались стосовно об'єктів ЕІ під час воєнного стану в Україні, можна зазначити [1]:

1) Фізичні атаки. Під час війни можливі бомбардування, ракетні атаки або атаки ворожих диверсійних груп з метою знищити або пошкодити енергетичні об'єкти.

2) Кібератаки, які супроводжують чи підсилюють дію фізичних атак. Типовими є впровадження ШПЗ, DDoS, атаки типу replay. Вони призводять до затримок та спотворення показників різних складових об'єкту енергопостачання, що можна відслідкувати за допомогою трекінгу цих показників.

3) Переривання ланцюга постачань, внаслідок економічних та політичних дій.

Моніторинг кібербезпеки може пом'якшити та попередити наслідки кібернетичних атак, забезпечуючи можливості для цілодобового спостереження за ключовими показниками.

## 3. Механізми об'єктів енергетичної інфраструктури

Архітектуру узагальненої моніторингової системи показано на Рис. 1. Пропонується збирати ключові показники від аналогових та цифрових сенсорів, та пристроїв IoT. Частина інформації може оброблятись на місці, у контролерах, або інтелектуальних пристроях (fog computing), і надалі в агрегованому виді передаватись до центру моніторингу та обробки (cloud computing). Центр

моніторингу може візуалізувати інформацію на дашборді (зокрема такі показники як температура, вологість, потужність тощо), однак з точки зору кібербезпеки необхідно забезпечити цілісність інформації, яка передається, за допомогою відповідних протоколів із можливістю контролю цілісності. Так само, сам центр обробки має бути захищеним від атак на відмову в обслуговуванні), а також забезпечувати цілісність оброблюваної інформації. При передачі даних до центру мають бути реалізовані механізми автентифікації об'єкту та пристрою, які є джерелами переданої інформації. Також для об'єкта, який передає дані, повинна бути можливість перевірити автентичність центра (сервера). Збір інформації може здійснюватись для пристроїв IoT засобами протоколу телеметрії MQTT із впровадження криптографічних механізмів [2]. В якості платформи візуалізації та аналітики можна використовувати Grafana - відкриту платформу для аналізу і моніторингу метрик з даними.

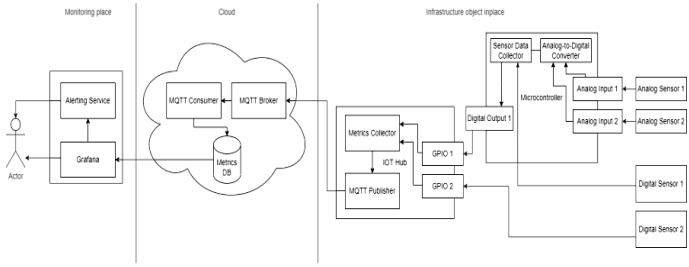


Рисунок 1. Архітектура моніторингової системи.

## Висновки

Застосування підходу моніторингу показників, що збираються від пристроїв IoT є сучасним рішенням, що, при правильній реалізації, сприятиме своєчасному виявленню та реагуванню на зміни в роботі системи. Інвестиції у дослідження та розвиток системи моніторингу об'єктів енергетичної інфраструктури допоможе створити більш стабільну систему, зменшити ризики кібератак та гарантувати надійне енергопостачання для цивільних та військових потреб.

## Перелік використаних джерел

1. Alexander E. Farrell, Hisham Zerriffi, Hadi Dowlatabadi Energy infrastructure and security. Annual Review of Environment and Resources. 2004. Vol. 29 P. 421-469.
2. I. Andrea, C. Chrysostomou and G. Hadjichristofi Internet of Things: Security vulnerabilities and challenges, IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus. 2015, pp. 180-187.


# ІЄРАРХІЧНЕ ФОРМУВАННЯ ПРИЧИННО-НАСЛІДКОВИХ МЕРЕЖ НА ОСНОВІ CHATGPT


Д.В. Ланде[1], Л.Л. Страшной[2]
[1]НН ФТІ КПІ ім. Ігоря Сікорського
[2]The University of California, Los Angeles (UCLA)



Ця робота присвячена опису методики формування причинно-наслідкових (каузальних) мереж шляхом багаторазового звернення до системи ChatGPT, а також візуалізації та аналізу цих мереж за допомогою системи Gephi. Методика базується на використанні системи ChatGPT, попередньо генеративного навченого на великих текстових корпусах перетворювача, який використовує можливості штучного інтелекту для виконання промтів користувачів. Методика охоплює засоби аналізу та візуалізації сформованих мереж за допомогою програми Gephi. У статті показано можливість побудови причинно-наслідкових мереж концептів на основі використання Chat GPT, що дозволяє вирішувати завдання, які раніше вимагали залучення великих ресурсів (людських та тимчасових). У методиці інтегруються засоби інтелектуальної текстової аналітики та аналізу мереж, а також їхня візуалізація.



**Ключові слова:** ChatGPT, Каузальні мережі, Моделі предметної області, Штучний інтелект, Візуалізація графів, Кібербезпека

## Вступ

Останнім часом великі лінгвістичні моделі, такі як ChatGPT набувають все більшого поширення в багатьох областях. Найпоширеніші застосування - це машинний переклад, реферування текстів, узагальнення різного рівня, наприклад, формулювання питань до навчальних матеріалів. Зокрема, ChatGPT від OpenAI – це Генеративний Попередньо навчений Трансформер (GPT), який використовує обробку природної мови для виконання промтів користувачів, використовуючи широкі можливості області штучного інтелекту [1].

Величезні можливості в екстрагуванні основних понять, іменних сутностей дозволяють використовувати ChatGPT у фактографічних системах, зокрема, в медицині, економіці [2]. Інтелектуальні чати інтегруються із зовнішніми системами, такими як геоінформаційні [2], системи аналізу та візуалізації графів, мереж [3]. Зокрема, авторами у роботі [4] показано, як і формувати мережі зв'язків персонажів літературних творів, мережі предметних областей зі зв'язками типу «загальне-приватне».

Ця робота присвячена опису методики формування причинно-наслідкових (каузальних) мереж шляхом багаторазового звернення до системи ChatGPT, а також візуалізації та аналізу цих мереж за допомогою системи Gephi (gephi.org) – найпопулярнішої програми візуалізації графових структур із вільною ліцензією [5]. Для завантаження даних у середу Gephi цілком підходить формат CSV, тому всі запити до ChatGPT будуть супроводжуватись вимогою до формату.

Сформовані причинно-наслідкові мережі забезпечать можливість переходу до сценарного аналізу. Основна проблема, що виникає під час проведення сценарного аналізу на основі каузальних мереж полягає саме у створенні таких систем, що у традиційних випадках потребує великих ресурсних витрат, залучення експертів.

## Формування мережі на базі простого ієрархічного звернення до ChatGPT

Нехай нас, наприклад, цікавить проблематика витоку даних, навіщо попросимо у ChatGPT видати відомі їй причини цього явища. Тобто. центральним вузлом майбутньої мережі має стати поняття "data leakage". Успішне відпрацювання такого запиту визначить другий рівень ієрархії - поняття пов'язані з витоком даних - її причини. Після цього для кожного такого поняття також вимагають безліч причин, що вплинули на нього. Такий процес може тривати нескінченно, але в роботі зупинимося на трьох рівнях. Незважаючи на ієрархічне формування такої каузальної мережі, отримана мережа загалом не буде строго ієрархічною структурою.

Запропонувавши ChatGPT відпрацювати деякий запит, отримаємо множину причин первинного поняття. Система ChatGPT може допомогти отримати зміст CSV-файлу (поля, відповідні іменам понять, розділені точкою з комою). Для цього можна застосувати, наприклад, такий запит до системи ChatGPT:

→List the causes of **data leakageage** in cyber security. The reason is to use no more than three words. The results should be presented in the format "cause;**data leakage**". Each such entry - from a new line

Система видає відповідь приблизно такого вигляду:

human error; data leakage
weak passwords; data leakage
insider threats; data leakage
misconfigured systems; data leakage
phishing attacks; data leakage
unpatched software; data leakage
malware infection; data leakage
social engineering; data leakage
third-party access; data leakage
stolen devices; data leakage

Запити наступного рівня будуть ставитись до наведених у відповіді концептів і мати вигляд, що повністю відповідає первинному запиту, наприклад:

→List the causes of **human error** in cyber security. The reason is to

use no more than three words. The results should be presented in the format "cause; **human error** ". Each such entry - from a new line

Об'єднані в одному CSV-файлі відповіді ChatGPT завантажуються для аналізу та візуалізації програми Gephi.

Завантаживши отримані дані до системи Gephi, вибираємо розмір вузлів, пропорційний ступеня (кількості суміжних зв'язків) і розділивши мережу на кластери за критерієм модулярності отримуємо наочний граф (Рис. 1).

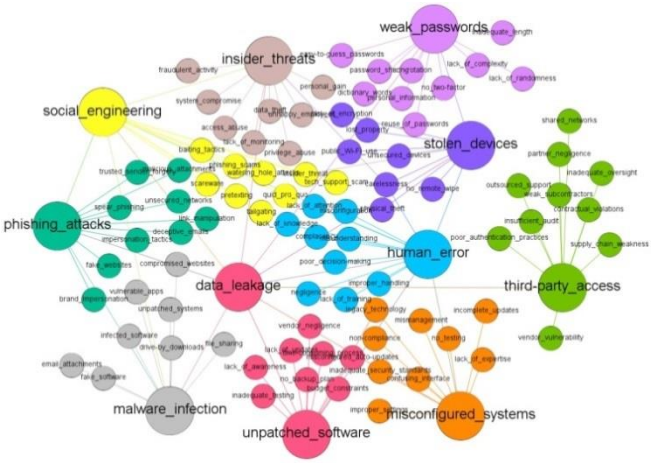


Рисунок 1. Спрямована первинна каузальна мережа, отримана шляхом найпростішого ієрархічного звернення до ChatGPT

Найбільш впливові вузли цієї мережі (найбільший Out-Degree), це:
human error (5), social engineering (4), weak passwords(3), phishing attacks(2).

Очевидно, сформована мережа слабопов'язана, неповна, представлені в ній концепти можуть не точно відображати причини та наслідки. Вважатимемо, що це мережа, отримана в результаті опитування лише одного штучного експерта.

## Формування мережі на основі ієрархічного звернення рою віртуальних експертів до ChatGPT

Система ChatGPT у різні моменти під час обробки тексту може видавати різні варіанти відповідей, причому правильне, і з погляду людської логіки цілком «обґрунтовані». Кожну таку відповідь можна сприймати як відповідь деякого віртуального експерта [3]. Можна припустити, що узагальнюючи відповіді множини (рою) подібних експертів можна отримати більш повну та точну відповідь. Реалізуючи рій віртуальних експертів ми по кілька разів задаємо одні й ті самі запити, що розглядаються в минулому випадку, які стосуються як першого, так і другого рівня ієрархії. Після отримання відповідей від системи, об'єднуємо їх у загальний CSV-файл і передаємо для аналізу та візуалізації програмі Gephi. Завантаживши отримані дані до системи Gephi, отримуємо граф, поданий на Рис. 2. На практиці мережа може поповнюватися доти, доки не стане достатньо повною за оцінкою експерта-людини.

Найбільш впливові вузли цієї мережі (найбільший Out-Degree), це:

Human error (7), social engineering (4), weak passwords(3), phishing attacks(2), unpatched systems(2), insider threats(2).

Як бачимо, кількість важливих концептів збільшилася порівняно з попереднім випадком.

## Формування мережі на основі узагальнення ієрархічного звернення рою віртуальних експертів до ChatGPT

Сформований у попередньому прикладі граф, маючи відносно велику повноту концептів, водночас може містити неточну інформацію, помилково видану ChatGPT при обробці окремих запитів. З припущення, що ймовірність появи тих самих помилок щодо невелика, можна винести з розгляду при побудові мережі концепти, які зустрічаються рідше заданого порогу.

У наведеному нижче випадку (Рис. 3) не розглядалися концепти, які зустрічалися рідше 2 разів.

Найбільш впливові вузли цієї мережі (найбільший Out-Degree), це:

Human error (5), social engineering (3), phishing attacks(2), unpatched systems(2).

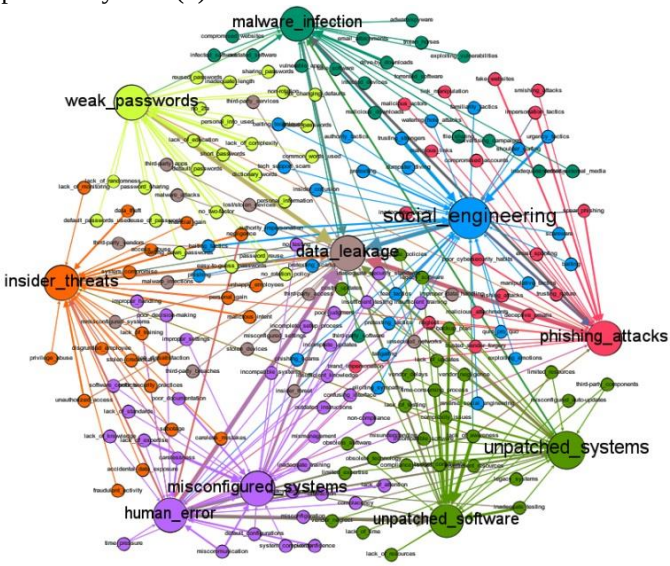


Рисунок 2. Спрямована повна каузальна мережа, отримана шляхом ієрархічного звернення рою віртуальних експертів до ChatGPT

## Висновки

На підставі експертних оцінок можна зробити висновок, що первинна каузальна мережа, отримана шляхом найпростішого ієрархічного звернення до ChatGPT, охоплює найбільшу кількість концептів, які відносно слабко пов'язані (мережа близька до ієрархічної), але завдяки повноті може бути непоганою «сировиною для подальшої аналітичної обробки».

Статистично оброблена друга мережа, каузальна мережа, отримана шляхом ієрархічного звернення роя віртуальних експертів до ChatGPT, є більш точною, ніж первинна мережа і, нарешті, третя мережа, отримана шляхом узагальнення ієрархічного звернення роя віртуальних експертів до ChatGPT, що має найбільший середній свідчить про найбільшу взаємодію окремих концептів, що впливають на ціль у цій причинно-наслідковій мережі. Мабуть, така мережа є найбільш прийнятною для подальшого застосування сценарного аналізу.

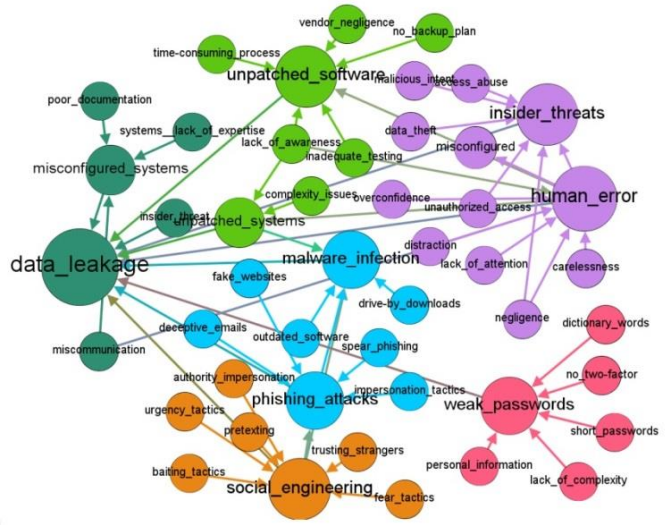


Рисунок 3. Направлена каузальна мережа, отримана шляхом узагальнення ієрархічного звернення рою віртуальних експертів до ChatGPT

Незважаючи на суттєвий виграш у ресурсах (як тимчасових, так і чесловецьких), важливо зазначити, що як сам процес побудови каузальних мереж, так і інтерпретація результатів, вимагають від дата сайнсиста досвіду в предметній галузі, що вивчається, і як і раніше необхідно

спостереження з боку людини для забезпечення достовірності та точності результатів.

## Перелік використаних джерел


1. St. Wolfram. "What Is ChatGPT Doing ... and Why Does it Work?". – Wolfram Media, Inc. March 9, 2023. 112 p.
2. Brady D. Lund, Ting Wang, Nishith Reddy Mannuru, Bing Nie, Somipam Shimray, Ziang Wang. ChatGPT and a new academic reality: Artificial Intelligence-written research papers and the ethics of the large language models in scholarly publishing. JASIST, 2023. / Volume74, Issue5. Pages 570-581. DOI: https://doi.org/10.1002/asi.24750
3. Tamilla Triantoro. Graph Viz: Exploring, Analyzing, and Visualizing Graphs and Networks with Gephi and ChatGPT (March 30, 2023). ODSC Community.
4. Lande, Dmitry and Strashnoy, Leonard, Concept Networking Methods Based on ChatGPT & Gephi (April 17, 2023). SSRN. Available at http://dx.doi.org/10.2139/ssrn.4420452
5. Ken Cherven. “Mastering Gephi Network Visualization”. – Packt Publishing, 2015. 378 p.


# АНАЛІЗ МЕРЕЖЕВОГО ПРОТОКОЛУ ДЛЯ ВИЯВЛЕННЯ ОЗНАК АТАК НА КРИТИЧНУ ІНФРАСТРУКТУРУ


Таран В. Є., Коломицев М. В.
Навчально-науковий Фізико-технічний інститут КПІ ім. Ігоря Сікорського, Київ, Україна
viktoriiatar1@gmail.com, box144.85@gmail.com


Один з найважливіших компонентів для надійної роботи Інтернету - це протокол мережевої інфраструктури Border Gateway Protocol (BGP). Використовуючи BGP, відбувається обмін повідомленнями про маршрутизацію, що дозволяє сигналізувати про наявні активні та несправні маршрути. Проте, під час катастрофічних подій великого масштабу, таких як військові дії або кібервійна,

стабільність Інтернету може постраждати, що призводить до значного збільшення оголошень про несправні маршрути.

**Ключові слова:** аномалії, війна, BGP

## Вступ

Протокол BGP має ключове значення для міждоменної маршрутизації у глобальній мережі Інтернет. BGP забезпечує розширені можливості маршрутизації, враховуючи політичні вимоги, та масштабованість для вирішення складних завдань [1].

## 1. Структура BGP протоколу та повідомлень

Структура протоколу включає атрибути, додаткові полі, сесії, таблиці маршрутизації.

У протоколі BGP існує кілька типів повідомлень, які включають OPEN, UPDATE, NOTIFICATION, KEEPALIVE і ROUTE-REFRESH. Для проведення дослідження використовуються повідомлення BGP UPDATE, які використовуються для оголошення нових маршрутів або видалення існуючих.

Оголошення маршруту містить інформацію: ідентифікатор маршрутизатора моніторингу (AS номер та IP-адреса), мітка часу отримання, префікс мережі та шлях (послідовність ASN). Відкликання містить інформацію: ідентичність моніторингового маршрутизатора, мітка часу отримання та розглядається префікс [2].

## 2. Методи пошуку аномалій

Для виявлення аномалій відстань Кука є переконливим вибором. Формула розрахунку відстані Кука використовується для визначення ступеня аномальності окремих спостережень. Вона включає різницю між передбаченими значеннями та спостережуваними значеннями. Ця відстань Кука може бути обчислена за наступною формулою:

$$D_i = \frac{\sum_{j=1}^{n} (\hat{Y}_j - \hat{Y}_{j(i)})^2}{p \, \mathrm{MSE}},$$

Таким чином, за допомогою формули відстані Кука можна оцінити ступінь аномальності кожного спостереження у наборі даних [3].

## 3. Розробка методики виявлення аномалій

Опис кроків методики виявлення змін у трафіку BGP:

1. Збір та обробка даних BGP.
2. Вибір критерію для виявлення збоїв в мережі.
3. Відбір BGP повідомлень відповідно до обраного критерію з використанням відповідного алгоритму. Цей етап включає фільтрацію повідомлень за певними атрибутами та порівняння поточних значень зі значеннями у минулому.

Перетворення проміжних результатів у датасет та застосування методу пошуку аномалій за допомогою відстані Кука (Рис. 1).

## 4. Результати

У даній роботі була протестована методика виявлення аномалій на даних BGP, які були зібрані з 24 лютого 2022 року по 30 квітня 2022 року [4].

Згідно проведеного аналізу, було встановлено лінію впливу, яка складає 7%. Крім того, було виявлено 4 аномалії, які перевищують цю лінію. Аномалії відповідають таким датам: 8 квітня 2022 року, 13 квітня 2022 року, 19 квітня 2022 року та 25 квітня 2022 року.

## Висновки

Дослідження надають підстави для припущень про взаємозв'язок між військовими діями і їх впливом на мережевий трафік. Розроблена методика була успішно перевірена, і було знайдено зв'язок між аномаліями і значними воєнними подіями.

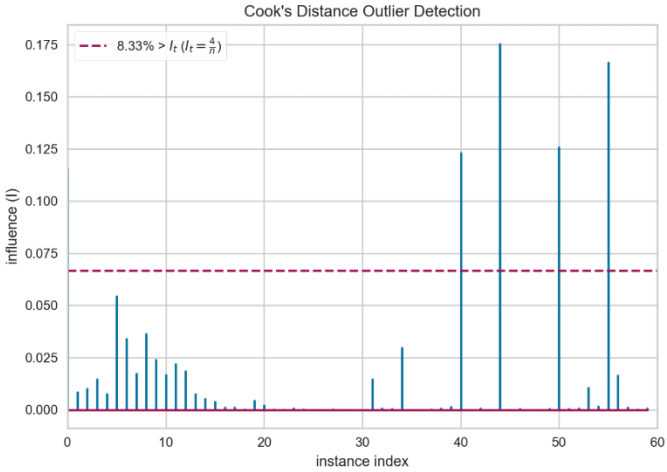


Рисунок 1. Ступінь аномальності спостережень

## Перелік використаних джерел

1. Border Gateway Protocol. — URL: https://en.wikipedia.org/wiki/Border_Gateway_Protocol.
2. BGP messages formats. — URL: https://techhub.hpe.com/eginfolib/networking/docs/switches/3600v2/5998-7619r_l3-ip-rtng_cg/content/442284290.htm.
3. Cook’s Distance. — URL: https://rpubs.com/DragonflyStats/Cooks-Distance.
4. Bgpdata. — URL: http://archive.routeviews.org/bgpdata

# ВИЯВЛЕННЯ І ПРОТИДІЯ ПІДМІНІ БАЗОВОЇ СТАНЦІЇ В МЕРЕЖАХ МОБІЛЬНОГО ЗВ'ЯЗКУ 5G

А. С. Живодьоров, Ю. Г. Даник
Навчально-науковий Фізико-технічний інститут КПІ ім. Ігоря Сікорського, Київ, Україна

Масове впровадження мобільного зв'язку п'ятого покоління несе не лише нові можливості, а й потребу у виявленні та нейтралізації загроз, особливо у сфері кібербезпеки. Ця робота має на меті розглянути архітектуру 5G з цих точок зору, порівняти її з архітекторами попередніх поколінь і класифікувати вразливості, успадковані від 4G LTE, і вразливості, отримані внаслідок впровадження нових технологій. Метою даної роботи є розробка методу виявлення та боротьби з підробленими базовими станціями в мережах мобільного зв'язку 5G.

**Ключові слова:** 5G, Загрози 5G, протидія підміні станції 5G

## Вступ

5G – це нове покоління мобільного зв'язку, яке активно впроваджується в усьому світі та з часом досягне й України. Для прискорення надання послуг нові станції встановлюються на несамостійній основі (Non-standalone). Тобто до існуючої структури мережі LTE додається лише базова станція, яка взаємодіє зі старим ядром мережі. Ця архітектура дає користувачам можливість отримати швидкість, передбачену технологією, але без використання основних функцій нового 5G, а саме хмарної віртуалізації та сервіс-орієнтованої архітектури. Однак завдяки новим можливостям використання базових станцій 5G зв'язок наступного покоління має стати стандартом. Тому питання безпеки є найгострішими. У цій роботі розглядаються основні відмінності між 5G і LTE, а також зібрані та систематизовані вразливості 5G

порівняно з його попередниками. Визначено найбільш небезпечна атака та запропоновано контрзаходи.

## Архітектура 5G

Для аналізу вразливостей 5G в першу чергу потрібно знати її архітектура[1], яка складається з трьох рівні, зображених на рисунку (1):

1. RAN - радіомережа, яка поєднує користувацьке обладнання з базовими станціями;
2. Core Network - ядро мережі, яке відповідає за всі функції та взаємодії в 5G, включаючи автентифікацію, безпеку, управління сеансами та агрегацію трафіку з кінцевих пристроїв;
3. Edge - перетин користувацького й обчислювального рівнів.

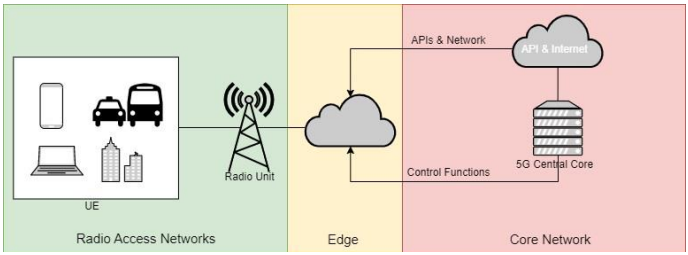


Рисунок 1. Архітектура 5G

## Аналіз вразливостей

Методом виявлення вразливостей стало дослідження існуючих атак на мобільні мережі попередніх поколінь з проекцією їх на 5G. Також була приділена увага й вразливостям пов'язаним з новими технологіями.

Для порівняння загроз було використано метод попарного порівняння. Він є одним з підходів, використовуваних для оцінки та вибору, в нашому випадку, найнебезпечнішої атаки серед знайдених альтернатив. Цей метод дозволяє виконати порівняння на основі різних факторів та зробити ранжування альтернатив на основі їх

значимості. За методом проводиться попарне порівняння між кожними двома альтернативами (атаками), в ході чого між ними розподіляються оцінки, а саме 10 балів. В результаті виходить матриця попарного порівняння. Для обчислення вагів проводиться ділення суми рядка на суму всіх елементів матриці.

За результатами проведеного дослідження було виявлено 16 основних вразливостей 5G та атак на нього. Оцінку вразливостей було представлено у вигляді порівняльної таблиці вразливостей 4G LTE та 5G.

Таблиця заповнена з градацію від зеленого до червоного відповідно до небезпечності кожної з загроз: зелений – незначна, або вирішена, червоний – потребує особливої уваги. За результатами аналізу було виявлено, що найбільшу загрозу становить атака з підміни базової станції.

## Підміна базової станції

Атака з підміни базової[2] станції виконується через встановлення зловмисником станції мобільного зв'язку з налаштуваннями існуючих. Вона працює через відсутність будь-якої перевірки валідності станції перед підключенням.

Ця атака надає зловмиснику можливості виконувати MITM атаку через налаштування нешифрованого з'єднання з обмеженою швидкістю передачі й подальшим перехопленням трафіку. Також стає можливим DOS девайсів, а також мережевих ресурсів за допомогою ботнетів без загрози блокування від станції. Всі ці фактори становлять велику загрозу одному з основних юзкейсів мережі п'ятого покоління, а саме – автоматизованому керуванню дронами, автопілотом в машинах, розумним будинкам, цехам та іншим кіберфізичним системам.

Таблиця 1. Вразливості LTE та 5G

| LTE | 5G |
|---|---|
| IMSI catching | IMSI protection |
| DNS Spoofing | FirstPoint DNS |
| Traffic Hijack | Traffic Hijack |
| Jamming | Jamming |
| Interworking and roaming threats | Interworking and roaming threats |
| - | NFV vulnerabilities |
| - | Network slicing vulnerabilities |
| - | SDN vulnerabilities |
| Sniffing Base station configuration | Sniffing Base station configuration |
| Downgrade | Downgrade |
| Device tracking | RNTI-based tracking |
| Reuse of AS keystream | Getting the keystream through XOR |
| VoLTE (Spamming, Spoofing, Phishing) | VoNR (security setting is the same as VoLTE) |
| Attacks on SMS | Attacks on SMS |
| DoS | Dos |
| Rogue Base Station | Rogue Base Station |

Для них навіть збій в роботі може призвести до катастроф, не зважаючи вже про перехоплення керування. Актуальність цієї загрози саме для 5G підкріплює той факт, що через малий радіус дії й велику кількість потенційних користувачів таких станцій розташовано має бути дуже щільним.

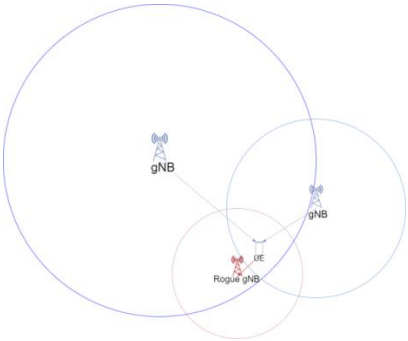


Рисунок 2. Атака з підміни базової станції

## Протидія підміні базової станції

Першим кроком для протидії підміні базової станції є безпосередньо її виявлення. Для цього існують наступні методи:

1. Найпростіший з вбудованих методів виявлення фейкових станцій базується на забороні експлуатації закордонних мереж[3]. Тобто, якщо станція буде транслювати мобільний код іншої країни, то її швидко виявлять. Цей спосіб може мати широке застосування, коли на світовий ринок вийде більше виробників.

2. Також можливим методом виявлення фейкової базової станції є аналіз її поведінки[3]. Наприклад фальшиві станції часто використовують потужніші радіосигнали для заманювання потенційних жертв. Спираючись на цю властивість, при аналізі потужності сигналів близько розміщених станцій можна виявити нелегітимну.

3. Рекомендованим методом виявлення нелегітимних станцій, який пропонується в 3GPP (3rd Generation Partnership Project) [4], є аналіз вимірювальних звітів. Користувацькі девайси в режими RRC_CONNECTED надсилають звіти про встановлені мережею конфігурації. Вони корисні не тільки для виявлення станцій, а й для SUPI/5G-GUTI перехоплювачів. Як і в попередньому методі для виявлення використовується інформація про

силу сигналу, проте також додається й інформація про місцезнаходження.

## Викриття фейкових станцій через аналіз потужності

У роботі запропонована методика виявлення фейкових станій через аналіз просторового розміщення базових станцій та потужності отриманого сигналу [5]. Вона базується на затуханні сигналу. Так як станції мобільного зв'язку розміщуються за принципом ефективного покриття - ще одне джерело потужного сигналу не залишиться непоміченим, особливо якщо воно перевищує норми задля приманювання. Для проведення аналізу в девайс повинно бути внесено координати базових станцій та їх потужність:

$$P_{tx} = 4\pi d^2 \Pi_i(d)$$

Цей показник залежить від типу антени й не змінюється сам по собі. Тому він може бути внесений в девайс як характеристика станції.

За одинцю для порівняння візьмемо потужність отриманого сигналу, що вираховується за формулою:

$$\mathrm{P_{rx}(d)} = \mathrm{P_{tx}} + G_{\mathrm{tx}} - \mathrm{L(d)} + \mathrm{G_{rx}}$$

де $G_{tx}$ коефіцієнт підсилення антени, Grx коефіцієнт підсилення приймача, який також буде відомий; L(d) - затухання.

Принципом роботи застосунку буде визначення відстані до найближчих станцій й обчислення очікуваної потужності сигналів, які будуть порівнюватись з прийнятими. Основною проблемою цього методу є обчислення затухання сигналу:

$$L(d) = -10log10G_{\mathrm{tx}} - 10log10\mathrm{G_{rx}} - 20log10d - 20log10f + 32.44.$$

Зазвичай ці показники табличні. Наприклад в GSM кожне подвоєння відстані від станції збільшує затухання на 6 дБ.

Подальшими діями від мобільного оператора має бути інформування правоохоронних органів та зв'язок з постраждалими абонентами.

## Висновки

У ході роботи було:

- Проведено аналіз деяких особливостей архітектури мережі 5G, важливих з точки зору забезпечення її кібербезпеки.
- Виконано якісне порівняння вразливостей притаманних мережі 4G та 5G.
- Визначено найбільш небезпечні для кожної з мереж. Для мережі 5G згідно з результатами дослідження найбільший ризик має реалізація загрози з підміни базової станції.
- Для зниження ризиків пов'язаних з реалізацією цієї загрози в роботі запропонована методика виявлення фальшивих базових станцій й протидії їх деструктивним діям.

## Перелік використаних джерел


1. Simmons A. 5G Standalone (SA): What is it? And How Does it Work? — URL: https://dgtlinfra.com/5g-standalone-sa/
2. 5The Evolution of Security in 5G. — 2019. — Aug. 16. — URL: https://www.5gamericas.org/the-evolution-of-security-in-5g-2/
3. Nakarmi P. K. Detecting false base stations in mobilenetworks. — 06/15/2016. — URL: https://www.ericsson.com/en/blog/2018/6/detecting-falsebase-stations-in-mobile-networks
4. Cedex S. A. 5G; Security architecture and proceduresfor 5G System. — 2020. — URL:https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.03.00_60/ts_133501v160300p.pdf
5. Кравчук С. О. Поширення радіохвиль взоні покриття безпроводових мереж зв'язку. — 2020. — URL: https://ela.kpi.ua/bitstream/123456789/36935/1/Poshyrennia_radiokhvyl_NP.pdf

# ЛОКАЛІЗАЦІЯ ПОЗИЦІЙ СТЕГОБІТІВ, ВБУДОВАНИХ ДО ЗОБРАЖЕНЬ-КОНТЕЙНЕРІВ З ВИКОРИСТАННЯМ АДАПТИВНИХ СТЕГАНОГРАФІЧНИХ МЕТОДІВ HUGO ТА WOW

Маманчук М. , Прогонов Д.
Національний технічний університет України «КПІ ім. Ігоря Сікорського», Навчально-науковий Фізико-технічний інститут, м. Київ, Україна
progonov.dmytro@lll.kpi.ua

Аннотація: забезпеченню надійного захисту конфіденційних даних при обміну повідомленнями в локальних та глобальних обчислювальних мережах сьогодні приділяється особлива увага. Враховуючи обмежені можливості сучасних методів виявлення (стегоаналізу) несанкціонованого вбудовування повідомлень (стегоданих) до цифрових зображень-контейнерів (ЗК), становить інтерес вдосконалення методів деструкції сформованих стеганограм. В роботі показана принципова можливість виявлення позиції вбудованих стегобітів при використанні сучасної штучної нейронної мережі U-Net. Отримані результати становлять інтерес для розробки методів деструкції стеганограм, що мінімізують зміни статистичних параметрів ЗК.
**Ключові слова:** цифрова стеганографія, метод HUGO, метод WOW, мережа U-Net

## Вступ

Забезпечення надійного захисту інформації з обмеженим доступом, що циркулює в інформаційно-комунікаційних системах державних установ та приватних організацій, є актуальною та важливою задачею. Особлива увага приділяється розробці методів протидії несанкціонованій передачі конфіденційних даних, зокрема з використанням стеганографічних методів (СМ).

Вагомим обмеження практичного застосування сучасних методів деструкції стеганограм є значні зміни статистичних та спектральних параметрів ЗК, що демаскує проведення атаки на стеганографічний канал. Для зниження рівня даних ознак становить інтерес розробка спеціалізованих методів деструкції, що дозволяють визначати позиції приховання стегобітів до ЗК.

## Огляд літератури

Переважна кількість сучасних СМ заснована на представленні процесу формування стеганограм як вирішення однокритеріальної оптимізаційної задачі з обмеженнями – мінімізації емпіричної функції оцінки спотворень зображення-контейнеру **X** при фіксованій довжині бітового представлення приховуваного повідомлення **M** [1]**.** Таке представлення процесу формування стеганограм дозволяє застосовувати потужний математичний апарат методів оптимізації для мінімізації рівня демаскуючих ознак вбудованих повідомлень при формуванні стеганограм

Поширеним підходом до побудови стегодетекторів є використання ансамблю з декількох статистичних моделей ЦЗ. В якості прикладу можливо навести сучасні статистичні моделі SCRMQ1 [2] та CFA-CRM [3]. Проте вагомим обмеженням практичного застосування даних моделей є надзвичайно велика кількістю параметрів моделі (наприклад, 34,671 параметрів для моделі SRM).

Для подолання даного обмеження широко використовуються методи деструкції стеганограм. Проте застосування даних методів призводить до суттєвих змін статистичних параметрі ЗК, що демаскує факт проведення атаки на стеганографічний канал. Для мінімізації даних змін становить інтерес попередня обробка ЦЗ з метою визначення позицій стегобітів.

Робота присвячена дослідженню точності локалізації положень стегобітів, вбудованих до ЗК із застосуванням стеганографічних методів HUGO та WOW, при використанні новітньої штучної нейронної мережі U-Net [4] для проведення сегментації ЦЗ.

## Локалізація позицій стегобітів з використанням штучної нейронної мережі U-NET

Сучасні методи для проведення сегментації ЦЗ засновані на використанні автокодувальних нейронних мереж. Прикладом даних методів є відома мережа U-Net [4]. Обробка досліджуваного зображення з використання мережі U-Net проводиться в декілька етапів. На першому етапі проводиться попередня обробка ЦЗ з використанням послідовності згорткових шарів для виділення статистичних параметрів ЦЗ. На другому етапі, відбувається проекція отриманих векторів до простору меншої розмірності для виділення характерних параметрів для кожного класу (об'єкту сегментації). На останньому етапі проводиться побудова карти сегментації ЦЗ шляхом застосування даних операцій в зворотньому порядку.

## Експериментальні дослідження

Дослідження точності сегментації стеганограм проводилося з використанням стандартного пакету зображень BOSS. Формування стеганограм проводилося використанням адаптивних стеганографічних методів HUGO та WOW, а ступінь заповнення ЗК стегоданими була рівною 10% та 25%.

Налаштування мережі U-Net проводилося на окремій вибірці зі 450 зображень. За результатами тестування налаштованої мережі U-Net отримано залежності точність виявлення позицій стегобітів від ступеня заповнення ЗК стегоданими. Показано, що точність виявлення позицій стегобітів досягає 17.27% для розглянутих СМ.

## Висновки

Показано, що застосування мережі U-Net для сегментації ЦЗ дозволяє суттєво підвищити точність локалізації положення пікселів, використаних для прихування бітів повідомлення при формуванні стеганограм. Забезпечення високої точності локалізації даних пікселів дозволяє суттєво розширити можливості сучасних методів стегоаналізу

ЦЗ, зокрема щодо вилучення та внесення спотворень (підміни) частин вбудованих стегоданих.

### Перелік використаних джерел

1. J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge: Cambridge University Press, 2009.

2. M. Goljan, J. Fridrich та R. Cogranne, «Rich model for Steganalysis of color images,» в International Workshop on Information Forensics and Security (WIFS), Atlanta, 2014

3. M. Goljan та J. Fridrich, «CFA-aware features for steganalysis of color images,» *Media Watermarking, Security, and Forensics*, San Francisco, 2015.

4. O. Ronneberger, P. Fischer та T. Brox, «U-Net: Convolutional Networks for Biomedical Image Segmentation,» Cornell University Repository (ArXiv), Cornell, 2015.

# QUADRATIC MULTIVARIATE TRANSFORMATIONS IN TERMS OF EXTREMAL GRAPH THEORY AS IMPLEMENTED ENCRYPTION TOOLS

Vasyl Ustymenko[1,2], Aneta Wróblewska[3] and Oleksandr Pustovit[2]

[1] Royal Holloway University of London, United Kingdom.

[2] Institute of telecommunications and global information space, Kyiv, Ukraine

[3] University of Maria Curie-Skłodowska, Lublin, Poland

Vasyl.Ustimenko@rhul.ac.uk, wroblevska-aneta@wp.pl, sanyk_set@ukr. net

We introduce a totality of transformations of a vector space over the finite fields defined via symbolic computations with the usage of algebraic constructions of Extremal Graph Theory. Some of them selected in the case of large fields of characteristic two allow to define quadratic bijective

multivariate public keys such that the inverses of public maps has a large polynomial degree.

**Funding:** This research is supported by British Academy Fellowship for Researches at Risk 2022.

## 1. On Post Quantum, Multivariate and Noncommutative Crytography

Post-Quantum Cryptography (PQC) is an answer to a threat coming from a full-scale quantum computer able to execute Shor's algorithm . With this algorithm implemented on a quantum computer, currently used public key schemes, such as RSA and elliptic curve cryptosystems, are no longer secure. PQC is subdivided into Coding based Cryptography, Multivariate Cryptography, Noncommutative Cryptography, Hash based Cryptography, Isogeny based Cryptography and Lattice based Cryptography.

Each of these six areas is based on the complexity of certain NP-hard problem. Noteworthy that fundamental assumption of cryptography that there are no polynomial-time algorithms for solving any NP-hard problem remains valid. So all six directions are well justified theoretically.

The tender of US National Institute of Standardization Technology (NIST, 2017) is dedicated to the standardization process of possible real life Post-Quantum Public keys. Already selected in July of 2022 four cryptosystems are developed via methods of Lattice based Cryptography. This fact motivates researchers from other four core areas of Post Quantum Cryptography to continue design of new cryptographical primitives. Noteworthy that during the NIST project an interesting results on cryptanalysis of Unbalanced Rainbow Oil and Vinegar digital signatures schemes were found (see [1], [2],[3]).This scheme is defined via quadratic multivariate public rule, which refers to Mini Rank problem. Examples of previously known multivariate quadratic public keys reader can find in classical monographs [2], [4], [5].

Graph based multivariate public keys with bijective encryption maps generated via special walks on incidence graph of projective geometry were proposed in [7] this year. It can be

count as attempt to combine methods of Coding Based and Multivariate Cryptographies.

Classical multivariate public rule is a transformation of $n$-dimensional vector space over finite field $F_q$ which move vector $(x_1, x_2, \dots, x_n)$ to the tuple $(g_1(x_1, x_2, \dots, x_n), g_2(x_1, x_2, \dots, x_n), \dots, g_n(x_1, x_2, \dots, x_n))$, where polynomials $g_i$ are given in their standard forms, i.e. lists of monomial terms in the lexicographical order. The degree of this transformation is the maximal value of $deg(g_i)$. Traditionally public rule has degree 2 or 3.

We use the known family of graphs $D(n, q)$ and $A(n, q)$ of increasing girth (see [7], [8] and further references). There is well defined projective limit of these graphs which is a $q$-regular forest. Cubical transformation groups $GA(n, q)$ and $GD(n, q)$ of $n$-dimensional vector spaces over $F_q$ (see [9], [10]), were used for the design of key exchange protocols of Noncommutative Cryptography in terms of Multivariate Cryptography (see [10]), elements of this groups were used for the creation of stream ciphers.

## 2. On graphs and quadratic maps with the inverses of high degree

We define $A(n,q)$ as bipartite graph with the point set $P=F_q^n$ and line set $L=F_q^n$. We will use brackets and parenthesis to distinguish tuples from $P$ and $L$. So $(p)=(p_1, p_2, \dots, p_n) \in P_n$ and $[l]=[l_1, l_2, \dots, l_n] \in L_n$. The incidence relation $I=A(n,q)$ (or corresponding bipartite graph $I$) is given by condition $p\ I\ l$ if and only if the equations of the following kind hold: $p_2 - l_2=l_1p_1$, $p_3 - l_3= p_1 l_2, p_4 - l_4 = l_1p_3$, $p_5 - l_5 = p_1 l_4$, $\dots$, $p_n - l_n = p_1 l_{n-1}$ for odd $n$ and $p_n - l_n = l_1 p_{n-1}$ for even $n$.

We can consider an infinite bipartite graph $A(q)$ with points $(p_1, p_2, \dots, p_n, \dots)$ and lines $[l_1, l_2, \dots, l_n, \dots]$.

Another incidence relation $I= D(n, q)$ is defined via some change in equations.

Let $\Gamma(n, q)$ be one of graphs $D(n, q)$ or $A(n, q)$. The graph $\Gamma(n, K)$ has so called linguistic colouring $\rho$ of the set of vertices. We assume that $\rho(x_1, x_2, \dots, x_n)=x_1$ for the vertex x (point or line) given by the tuple with coordinates $x_1, x_2, \dots, x_n$. We refer

to $x_1$ from $K$ as the colour of vertex $x$. It is easy to see that each vertex has a unique neighbour of the chosen colour. Let $N_a$ and $J_a$ be operators of taking the neighbour with colour $a$ and jump operator changing the original colour of point or line for new colour $a$ from $K$. Let $[y_1, y_2, \ldots, y_n]$ be the line $\boldsymbol{y}$ of $\Pi(n, K[y_1, y_2, \ldots, y_n])$ and $(\alpha(1), \alpha(2), \ldots, \alpha(t))$ and $(\beta(1), \beta(2), \ldots, \beta(t))$ are the sequences of colours of the length at least 2. We form $(\beta^*(1), \beta^*(2), \ldots, \beta^*(t))=(y_1+\beta(1), y_1+\beta(2), \ldots, (y_1)+\beta(t-1), (y_1)^2+\beta(t))$ and consider the sequence ${}^0v=y$, ${}^1v=J_{\alpha(1)}({}^0v)$, ${}^2v=N_{\beta^*(1)}({}^1v)$, ${}^3v=N_{\alpha(2)}({}^2v)$, ${}^4v=N_{\beta^*(2)}({}^3v)$, $\ldots$, ${}^{2t-2}v=N_{\beta^*(t-1)}({}^{2t-3}v)$, ${}^{2t-1}v=N_{\alpha(t)}({}^{2t-2}v)$, ${}^{2t}v=J_{\beta^*(t)}({}^{2t-1}v)$.

Assume that $v={}^{2t}v=[v_1, v_2, \ldots, v_n]$ where $v_i$ are from $K[y_1, y_2, \ldots, y_n]$. We consider bijective quadratic transformation $h(\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t)), t \geq 2$ of affine space $K^n$ of kind $y_1 \rightarrow y_1 + \beta(t)$, $y_2 \rightarrow v_2(y_1, y_2)$, $y_3 \rightarrow v_3(y_1, y_2, y_3)$, $\ldots$, $y_n \rightarrow v_n(y_1, y_{2,\ldots,} y_n)$.

**Theorem 1** [10]. *Let $K$ be the finite field $F_q$, $q=2^r$. Then transformation $h=h(\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t))$ is a quadratic transformation of the vector space $(F_q)^n$. The polynomial degree of its inverse transformation is at least $2^{r-1}$.*

## 3. Quadratic Multivariate Public Key

Alice selects finite field $F_q$, $q=2^r$, dimension $n$ of the vector space over $F_q$, ${}^1T$ and ${}^2T$ from $AGL_n(F_q)$ defined by matrices with most entries distinct from zero. She chooses parameter $t=O(n)$, elements $\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t)$ for which $\alpha(i) \neq \alpha(i)$, $\beta(i) \neq \beta(i+1)$, $i=1, 2, \ldots, n$ and compute the standard form of $F={}^1Th(\alpha(1), \alpha(2), \ldots, \alpha(t), \beta(1), \beta(2), \ldots, \beta(t))^2T$. She presents $F$ of kind $y_i \rightarrow f(y_1, y_2, \ldots, y_n)$, $i=1, 2, \ldots, n$ as public map. Public user Bob use this transformation to encrypt his plaintext $p$ in time $O(n^3)$. Alice knows the decomposition ${}^1T\, h\, {}^2T$ and sequences $\alpha(i)$ and $\beta(i)$, $i=1, 2 \ldots, t$. It allows her to decrypt in time $O(n^2)$.

## References


1. Canteaut, A., Standaert, F.-X. (eds.): 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques Zagreb, Eurocrypt 2021, LNCS 12696 Croatia, October 17–21, 2021, Proceedings, Part I, Springer, 2021, 839 p.

2. Ding, J., Deaton, J., Vishakha, Yang, B.-Y.: The Nested Subset Differential Attack A Practical Direct Attack Against LUOV Which Forges a Signature Within 210 Minutes, In Eurocrypt 2021, Part 1, pp. 329-347.
3. Beullens, W.: Improved Cryptanalysis of UOV and Rainbow, In Eurocrypt 2021, Part 1, pp. 348-373.
4. Goubin, L., Patarin, J., Yang, B.-Y.: Multivariate Cryptography, Encyclopedia of Cryptography and Security (2nd Ed.) 2011, pp. 824-828.
5. Koblitz, N.: Algebraic aspects of cryptography, Springer (1998), 206 p.
6. Ustimenko, V.: Linear codes of Schubert type and quadratic public keys of Multivariate Cryptography, IACR e-print archive, 2023/175
7. Lazebnik, F., Ustimenko, V., Woldar, A.J.: A new series of dense graphs of high girth, Bulletin of the AMS 32 (1) (1995), pp. 73-79.
8. Ustimenko, V.: On the extremal graph theory and symbolic computations, Dopovidi National Academy of Sci, Ukraine, 2013, No. 2, pp. 42-49.
9. Ustimenko, V., Klisowski, M.: On Noncommutative Cryptography with cubical multivariate maps of predictable density, In: Intelligent Computing, Proceedings of the 2019 Computing Conference, Volume 2, Part of Advances in Intelligent Systems and Computing (AISC), volume 99, pp. 654-674.
10. Ustimenko, V.: Graphs in terms of Algebraic Geometry, symbolic computations and secure communications in Post-Quantum world, University of Maria Curie-Sklodowska Editorial House, Lublin, 2022, 198 p.

# МЕТОДИ РАННЬОГО ВИЯВЛЕННЯ АТАК ШИФРУВАЛЬНИКІВ НА РІВНІ МЕРЕЖЕВОГО СХОВИЩА

Войцеховський А.В., Ільїн М.І.
a.voitsekhovskyi@kpi.ua, m.ilin@kpi.ua

В роботі досліджено методи раннього виявлення атак шифрувальників в мережевому сховищі, з метою вдосконалення антивірусного програмного забезпечення та систем виявлення вторгнень. На основі динамічного

аналізу виділено особливості роботи шкідливих зразків у файловому сховищі.
**Ключові слова:** Шкідливе програмне забезпечення, шифрувальники, мережеве сховище

## Вступ

З кожним роком все більше користувачів надають перевагу зберіганню своїх даних в хмарному сховищі. Дані сервіси можуть бути скомпрометовані, що надалі буде використано зловмисниками для виконання шифрувальника, з метою вимоги викупу або нанесенню шкоди [1]. Зазвичай дані вдається відновити з резервного мережевого сховища, але в багатьох випадках користувачі втрачають свої дані, або змушені платити викуп за їх відновлення. Особливо серйозною проблемою є інфікування систем віртуалізації, що призводить до відмови в роботі і втрати багатьох сервісів. Протягом 2022-2023 років, збільшились випадки атак, з використанням сімейства шифрувальників, спрямованих на інфікування гіпервізора Vmware ESXI. В роботі запропоновано методи аналізу роботи шифрувальника в мережевому сховищі, для виявлення його шкідливої активності на ранньому етапі.

## Загальні методи аналізу

Сучасні зразки ШПЗ застосовують багато механізмів захисту від статичного аналізу, такі як виконання зашифрованих функція, під час роботи програми або динамічне завантаження додаткового коду. Виникає потреба удосконалювати засоби динамічного та гібридного аналізу, запускаючи ШПЗ в ізольованому середовищі, вивчаючи поведінку зразка[2]. Ці методи дозволяють підвищити ефективність класифікації та виявлення шкідливого програмного забезпечення.

## Аналіз інфікованих файлів

При попередньому статичному аналізу ефективно обчислювати ентропію інфікованих файлів, результати якої буде відрізнятись від ентропії не пошкодженого файлу[3].

Попередньо потрібно обчислити значення для різних типів файлів аби уникнути помилок.

Для створення системи динамічного аналізу пропонується використовувати власний програмний інтерфейс файлової системи мережевого сховища для логування таких підозрілих операцій як: запис зашифрованих байтів, створення шкідливих файлів, зміна назви файлів, зміна прав, видалення та інших. Оскільки даний програмний інтерфейс працює на Unix подібних операційних системах, для аналізу мережевих сховищ на базі Windows server, надається доступ до змонтованого мережевого диску. Відповідно програмний інтерфейс аналізує зміни над файлами в обох операційних системах. Отримані дані логів далі можна використати для класифікації методами машинного навчання [4], використовуючи особливості послідовності запису та зміни файлів, що відрізняються від роботи легітимних програм, таких як архіватори та системи резервного копіювання. Виявивши шкідливу активність на ранньому етапі, можливо відновити інфіковані файли з попередньо створених резервних копій, використовуючи мінімальну кількість ресурсів[5].

## Висновок

В даній роботі досліджено використання динамічного аналізу з метою виявлення шкідливої діяльності шифрувальника в мережевому сховищі. Для раннього детектування шифрувальника запропоновано аналізувати операції запису та зміни файлів сховища. Створену модель динамічного аналізу можна використовувати для класифікації ШПЗ з використанням методів машинного навчання.

## Перелік використаних джерел

1. Ransomware review: April 2023 https://www.malwarebytes.com/ blog/threat-intelligence/2023/04/ransomware-review-april-2023

2. A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions – Harun Oz,Ahmet Aris, Albert Levi, A. Selcuk Uluagac

3. Machine Learning Based File Entropy Analysis for Ransomware Detection in Backup Systems – Kyungroul Lee Sun-young Lee Kangbin Yim

4. Detecting Ransomware using Support Vector Machines – Yuki Takeuchi, Kazuya Sakai, Satoshi Fukumoto

5. Ransomware's Early Mitigation Mechanisms – Routa Moussaileb, Benjamin Bouget, Aurélien Palisse, Hélène Le Bouder

# МОДЕЛІ АТАК ВІДМОВИ В ОБСЛУГОВУВАННІ НА КІБЕРФІЗИЧНІ СИСТЕМИ

Овчарук М.В, Сириця В.О, Ільїн М.І.
Навчально-науковий Фізико-технічний інститут
e-mail: m.ovcharuk@kpi.ua

У роботі досліджено математичні моделі атак відмови в обслуговуванні. Розглянуто загрози кінетичного впливу на компоненти кіберфізичних систем. Результати моделювання свідчать про успішний розв’язок поставленої задачі.

**Ключові слова**: кіберпростір, кіберфізична система, DDoS, епідеміологічна модель

## Вступ

Для дослідження динаміки DDoS-атак та адаптивного захисту від них застосовано аналогії з біологічними вірусами [1]. Математична модель ґрунтується на припущеннях, які обмежують її застосовність в різних масштабах: у моделях на базі диференціальних рівнянь можна отримати гарні результати у великих масштабах (щодо глобальної поведінки), але для невеликих локальних мереж чи окремих хостів вони не дуже застосовні [2]. В

даній роботі розглянуто вплив початкових умов на результати атаки та виконано моделювання для аналізу отриманої системи.

## Постановка задачі

Метою роботи є моделювання атак відмови в обслуговуванні на кіберфізичні системи за допомогою мережі ботів (ботнету). Математичну модель, створену на основі епідеміологічного моделювання, застосуємо для аналізу динаміки розповсюдження ботів у комунікаційних системах, яка відрізняється врахуванням кінетичних атак на компоненти мережі, які полягають у фізичному виведенню з ладу вузлів або їх знищенню.

## Опис моделі

Досліджується замкнута мережа з двома підмножинами: атакуючою (attack) та цільовою (target). Динаміку моделі описує система диференціальних рівнянь [3], яка була доповнена шляхом введення до розгляду змінної σ, яка описує реакцію системи на фізичні впливи у кіберфізичному просторі:

$$\frac{dS_a}{dt} = \mu - \beta S_\alpha I_\alpha - \mu S_\alpha + \xi I_\alpha \quad (1)$$

$$\frac{dI_a}{dt} = \beta S_\alpha I_\alpha - (\xi+\mu) I_\alpha \quad (2)$$

$$\frac{dS_{low}}{dt} = -\lambda S_{low} - \sigma S_{low} = -(\lambda+\sigma) S_{low} \quad (3)$$

$$\frac{dI_{low}}{dt} = \lambda S_{low} - \gamma_{low} I_{low} - \sigma I_{low} = \lambda S_{low} - (\gamma_{low}+\sigma) I_{low} \quad (4)$$

$$\frac{dR_{low}}{dt} = \gamma_{low} I_{low} - \xi_{low} R_{low} \quad (5)$$

$$\frac{dS_{high}}{dt} = -\lambda(1-\varepsilon) S_{high} + \xi_{high} R_{high} + \xi_{low} R_{low} - \sigma S_{high} \quad (6)$$

$$\frac{dI_{high}}{dt} = \lambda(1-\varepsilon) S_{high} - (\gamma_{high} + \sigma) I_{high} \quad (7)$$

$$\frac{dR_{high}}{dt} = \gamma_{high} I_{high} - \xi_{high} R_{high} \quad (8)$$

$$\frac{dD}{dt} = \sigma(S_{high} + S_{low} + I_{high} + I_{low}) \quad (9)$$

де S - сприйнятливі хости; I - інфіковані хости; R - відновлені хости; μ - коефіцієнт набору в ботнет (рекрутинг інфікованих хостів); β - швидкість поширення шкідливого ПЗ; γ - коефіцієнт відновлення (вилучення) атакованих хостів; ξ - коефіцієнт відновлення хостів цільової мережі, які переходять у сприйнятливий стан; ε - рівень безпеки цільової мережі; σ - кінетичний фізичний вплив на цільові системи

## Дослідження моделі атак відмови в обслуговуванні

Розглянемо поведінку системи за стандартних умов, зі зміною рівня захисту цільової системи та з під впливом фізичних атак.

За вихідних стандартних умов хости переходять в стан кращого захисту (Рис. 1), тобто поступово впроваджуються захисні механізми та закриваються вразливості, що призводили до атаки.

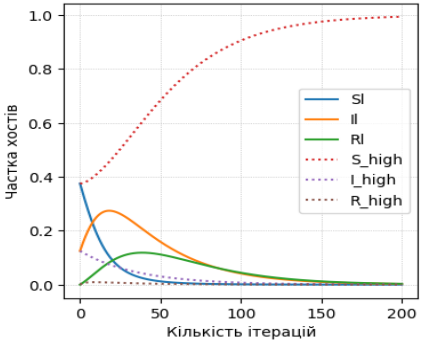


Рисунок 1. Динаміка кількості хостів під час атаки

Рівень захисту цільової мережі **ε** впливає на пікові значення кількості інфікованих хостів і відповідно, на пікову потужність ботнету (Рис. 2).

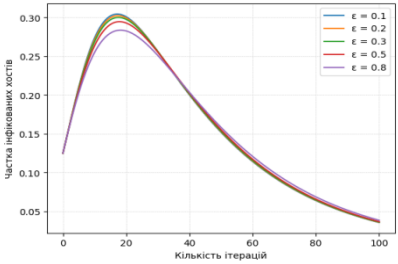


Рисунок 2. Динаміка зміни кількості інфікованих хостів

Додатково, модель враховує фізичні атаки на системи в кіберпросторі, де інтенсивність кінетичного впливу на атаковані хости враховується коефіцієнтом σ. Фізичні атаки можуть призвести до руйнування інфраструктури та тимчасового зниження доступності цільових систем.

Досліджена модель демонструє, що фізичні кінетичні атаки обмежують створення ботнету (Рис. 3), як наслідок. З одного боту фізичні атаки можуть призвести до незворотнього втрати доступу для цільової системи (атака успішна), але з іншого боту це негативно впливає на потужність атаки відмови в обслуговуванні. Загалом досліджена модель забезпечує основу для розуміння процесу розгортання ботнету і вплив захисних механізмів цільових систем на це.

## Висновки

В роботі виконано дослідження моделей атак відмови в обслуговуванні на кіберфізичні системи. В математичній моделі для аналізу розповсюдження ботів в комунікаційних мережах враховано вплив кінетичних атак на компоненти мережі. В подальших дослідженнях, з метою отримання більш деталізованої карти динаміки атак і захисту, модель

може бути розширена для врахування топології мережі та зв'язків між хостами.

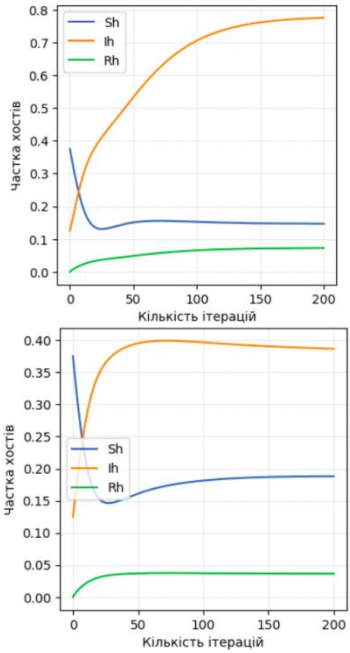


Рисунок 3. Динаміка зміни хостів в звичайних умовах та під впливом фізичних атак

## Перелік використаних джерел

1. І.В. Стьопочкіна, М.В. Грайворонський Моделювання розпосюдження комп'ютерних вірусів на основі імовірнісного клітинкового автомату. //Захист інформації. — 2015. — №4, С.1-9.

2. М.С. Дякуненко, І. В. Стьопочкіна «Моделювання процесів розповсюдження шкідливого ПЗ в мережі інтернет» // Теоретичні і прикладні проблеми фізики, математики та інформатики: матеріали XIX Всеукраїнської науково-практичної конференції студентів, аспірантів та

молодих вчених (13 − 14 травня 2021 р., м. Київ, Україна). с. 212-215

3. Ahmad, Ashraf & Abu Hour, Yousef & Alghanim, Firas. (2021). A Novel Model for Distributed Denial of Service Attack Analysis and Interactivity. Symmetry. 13. 10.3390/sym13122443.

# SSESSING CYBERSECURITY RISK WITH Q-ANALYSIS

Polutsyganova V.I., Smirnov S.A.
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute” Kyiv, Ukraine

This work examines structurally and functionally complex risk assessment approaches where vulnerabilities and resulting damages can be implemented together and interdependent. For such cases, the classic risk assessment formula is modified. With the help of Q-analysis, the structural dependencies between vulnerabilities are described, allowing for a clearer assessment of the damage.
**Keywords:** risk, Q-analysis, connectivity, cyber security

## Introduction

The classic formula for calculating average risk is based on the assumption that the probabilities of occurrence of the risks are uncorrelated, i.e. the circumstances that lead to the loss occur independently of each other. Let's review the classic formula for calculating risk:

$$R = \sum_i p_i V_i; \quad (1)$$

where $p_i$ is – probability of event occurrence (realization of vulnerability), $V_i$ – amount of loss when event occurs, – $i = \overline{1,n}$ vulnerability index. In reality, the situation is much more complicated, so this paper proposes a risk assessment approach that takes into account the fact that system vulnerabilities are interdependent and can be implemented simultaneously. This is

how interdependencies arise when the connections in a system are complex. Q analysis [3] is a good way to describe and analyze them. The weak system can then be described as a simplex complex, and Q-analysis can be used to calculate and evaluate the relationship. This allows for a clearer picture of how security systems are built in real systems and a better understanding of the issues involved. For systems with complex structures, this paper proposes a method for calculating risk, taking into account interdependent vulnerabilities and resulting losses.

## Risk Calculation Method for Complex System

The sweet structure of cybersecurity systems creates a complex system of vulnerabilities. The connections between them often have non-trivial connections. So we have to use simplicial complex for better description and Q-analysis for better understanding. For example, our system has a large number of subsystems. Each of them has its own weaknesses $A_1, A_2, \dots, A_n$[1]. At the same time, each vulnerability indirectly affects the vulnerabilities of other subsystems.

Then there are dependencies similar to dependencies in the simplex complex. A mere dot is shown if the vulnerability does not affect or depend on others. When connecting two holes, an edge appears between the simplex. If 3 holes are related, a face appears, if 4 - tetrahedron and so on [4].

This vulnerability structure may result in damage to one of the subsystems, while also causing damage to other subsystems. Although direct intervention may not take place in the associated subsystem. It turns out that certain vulnerabilities in the system compromise integrity and security. For such cases, the risk should be calculated taking into account the structure of the system, but requires a modification of the classical formula, since it is based on the assumption that all losses and their probability of occurrence are independent of each other. The general risk formula is as follows:

$$R_{general.} = R - R^* \quad (2)$$

where $V^*$ is a note on "gluing" simplexes.

We also wanted to note that if several simplexes are "glued" to one edge, then the correction for gluing has the form

$$R^* = m\sum_i R_i; \quad (3)$$

where is the total penetration at the place of gluing, while "m" should be one less than the number of simplexes that are glued at a certain place. Additionally, Q-analysis can be performed to examine complex relationships among vulnerabilities. Then you can improve the previous formula so that some simplexes in the complex (i.e. holes in a leaky system) are considered no more than once. The report considers examples of complex functional dependencies between damages associated with vehicle breakdowns. It shows how structural dependencies affect the most common vulnerabilities and how Q-analysis can be used to identify them.

## Example

To assess the risk of any information system, a preliminary inventory of software, network, hardware and, if it is possible, the qualifications of employees in the field of cyber security should be conducted.

To generalize, each of the above elements will be considered as an independent simplex or subsystem. The relationship between them is determined according to their structural characteristics. If each subsystem (simplex) is interconnected, then the relationship is taken into account.

To calculate the risk, it is necessary to calculate the risk of individual elements, the risk of binary cases and the risk of triple cases of exploiting vulnerabilities. The option of simultaneous failure of all subsystems is not considered in this model, as this would lead to the collapse of the business.

If we take real events as a basis, then the probability of occurrence of combinations of events in general is not equal to the sum of probabilities. most often it is smaller. Losses in the case of joint implementation can be both greater and smaller than the sum of individual cases of implementation of vulnerabilities.

## Conclusion

Identifying and assessing risk is an important step in building the security of any system. At the same time, the vulnerability of the system is determined by its structure, which in turn leads to interdependence and makes miscalculation more difficult. In the study, with the help of Q-analysis, a vulnerability structure is constructed and risks are calculated using the example of automobile risks. Methods of modifying the risk calculation to take into account the functional structure are shown.

## Literature


1. Kachynskyi A. B. Security of complex systems / under the editorship. Corresponding member of the National Academy of Sciences of Ukraine Dovhoy S.O.—K. : Euston, 2017—498 p.
2. Vyshnyakov Y. D., Radaev N. N. General theory of risks.—2 ed.—M. : Academy, 2008—368 p.
3. Atkin R. H. “Mathematical structure in human affairs”, Heinemann Educational Books, (1973); 143. doi: 10.1137/1018064.
4. Beaumont J.R., Gatrell A.C. “An introduction to Q-analysis” Catmog 34, 1982. URL:https://alexsingleton.files.wordpress.com/2014/09/34-an-introduction-to-q-analysis.pdf.
5. Polutsyganova V. I., Smirnov S. A. The inverse problem of Q-analysis of complex systems structure in cyber security / Scientific journal “Theoretical and Applied Cybersecurity” Vol. 4 No. 1 (2022) p. 61–68.

# КРИМІНАЛЬНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ, ОСОБЛИВОСТІ КВАЛІФІКАЦІЇ КІБЕРЗЛОЧИНІВ В УКРАЇНІ

Хахановський В.Г.[1], Гавловський В.Д.[2]
[1]Національна академія внутрішніх справ,
[2]Міжвідомчий науково-дослідний центр з проблем боротьби
з організованою злочинністю при Раді національної безпеки та оборони України

Розглянуто проблеми тлумачення та класифікації кіберзлочинів, проведено аналіз статистичної звітності Національної поліції України щодо показників про кіберзлочинність. Пропонується перелік «традиційних» кримінальних правопорушень, які можуть відноситися до категорії кіберзлочинів. Надаються рекомендації щодо кваліфікації окремих кіберзлочинів.
***Ключові слова:*** кіберзлочин, класифікація кіберзлочинів, статистичні показники, «традиційні» кримінальні правопорушення як кіберзлочини.

Поняття «кіберзлочинність» і «комп'ютерна злочинність» нерідко використовуються як синоніми. Однак саме термін кіберзлочинність найбільшою мірою відображає сутність цього явища.

У Законі України «Про основні засади забезпечення кібербезпеки України» кіберзлочинність визначається як сукупність кіберзлочинів. А кіберзлочин – як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачено законом України про кримінальну відповідальність та/або визнано злочином міжнародними договорами України [1]. Отже, сьогодні в законодавстві України не існує чіткого визначення поняття «кіберзлочин».

Конвенція Ради Європи про кіберзлочинність містить набір основних засад для будь-якої країни, яка розробляє національне законодавство з протидії кіберзлочинності. Разом з тим, наведена в Конвенції класифікація, на думку низки західних та вітчизняних дослідників, не є всеосяжною.

У звіті Комітету внутрішніх справ Парламенту Великобританії з кіберзлочинності у 2013 році кіберзлочини поділяють на три категорії:

- виключно мережеві злочини, де цифрові системи є основною метою, одночасно виступають і засобами посягання. Ця категорія включає посягання на комп'ютерні системи для знищення інфраструктури інтернет-технологій і незаконне заволодіння даними;

- традиційні злочини, які були переведені в площину кіберзлочинів через використання Інтернету;

- використання Інтернету з метою торгівлі наркотиками та як допоміжний інструмент для вчинення інших видів злочинів [2].

У спільному повідомленні Європейської комісії 2013 р. до Європейського парламенту, Ради Європейського економіко-соціального комітету та комітету регіонів кіберзлочинність також розкривається через три основні категорії: традиційні види злочинів (шахрайство, підробка документів), що вчиняються з використанням електронних комунікаційних мереж та інформаційних систем; розміщення незаконного контенту в електронних медіа; атаки на інформаційні системи, блокування програмного забезпечення сайтів та хакерство [3].

Більшість дослідників пропонують розділяти кіберзлочини на види залежно від об'єкта та предмета посягання. Найпоширеніший поділ – це комп'ютерні злочини та злочини, вчинені за допомогою комп'ютерів, мереж та інших пристроїв для доступу до кіберпростору. Ця позиція була підтримана на Десятому Конгресі ООН, де поняття кіберзлочин розглядалося у двох аспектах: у «вузькому» та «широкому» сенсі.

1. Кіберзлочин у вузькому значенні (комп'ютерний злочин): будь-яке протиправне діяння, вчинене за

допомогою електронних операцій, метою якого є порушення безпека комп'ютерних систем та оброблюваних ними даних.

2. Кіберзлочин у широкому розумінні (як злочин, пов'язаний з комп'ютерами): будь-яке протиправне діяння, вчинене за допомогою комп'ютерів або яке пов'язане з комп'ютерами, комп'ютерними системами або мережами, включаючи незаконне володіння та пропозицію або розповсюдження інформації за допомогою комп'ютерних систем або мереж.

Разом з тим, у доповіді цього ж Конгресу вказується, що термін «комп'ютерні злочини» був розроблений для охоплення як абсолютно нових форм злочинності, орієнтованої на комп'ютери, мережі та їх користувачів, так і традиційних злочинів, які в даний час вчиняються з використанням або за допомогою комп'ютерного устаткування [4].

До того ж у виступі Генерального секретаря ООН на X Конгресі було висловлено: використання нових технологій у злочинних цілях призвело до виникнення абсолютно нових форм злочинності. З іншого боку, більш традиційні злочини нині вчиняються новими методами, які дозволяють збільшити вигоди чи знизити ризики злочинців.

Зарубіжні вчені, зокрема Майк Макгуайр та Саманта Даулінг (Англія) також вважають, що кіберзлочинність є загальним терміном, який використовується для опису двох різних, але тісно пов'язаних між собою злочинних діянь: кіберзалежні та кіберутворюючи (злочини, пов'язані з кіберпростором).

Злочини, вчинені за допомогою комп'ютерів, комп'ютерних мереж чи інших комунікаційних форм ІКТ. Такі, наприклад, як поширення шкідливих програм, DDoS-атаки, зламування серверів для захоплення мережевої інфраструктури або веб-сторінок. Такі злочини спрямовані на пошкодження комп'ютерів та мережевих джерел.

Злочини, пов'язані з кіберпростором – це традиційні злочини, масштаби яких збільшуються чи досягаються за допомогою комп'ютерів, комп'ютерних мереж чи інших ІКТ. Вони досі можуть бути скоєні без використання ІКТ.

Можна стверджувати, що доктринальні підходи до розуміння поняття кіберзлочинів є різними. Проте слід зазначити, що попри наявні альтернативні дефініції саме термін кіберзлочинності найбільше відбиває сутність цього явища.

За класифікацією кіберзлочинів, можна дійти невтішного висновку, що більшість дослідників пропонують розділяти кіберзлочини на види залежно від об'єкта і предмета зазіхання: нові злочини стали можливими завдяки новітнім комп'ютерним технологіям (злочини, передбачені розділом XVI КК України); традиційні злочини, що вчиняються за допомогою комп'ютерних технологій та Інтернету.

В Україні найбільш повно статистичні дані про кіберзлочини відображаються у відомчій статистичній звітності Національної поліції України, зокрема у Звіті про результати роботи підрозділів Національної поліції, де, крім злочинів, передбачених розділом XVI КК, позначені й інші, вчинені з використанням електронно-обчислювальної техніки: «Порушення авторського права та суміжних прав» (ст. 176); «Крадіжка» (ст. 185); «Шахрайство» (чч. 3 та 4 ст. 190). До цієї категорії належать також злочини, передбачені статтями 200, 229, 231, чч. 3, 4 та 5 ст. 301 КК України.

Крім того, окремі показники про кіберзлочини, передбачені іншими статтями КК, відображено в інших статистичних звітах, зокрема злочини, передбачені ст. $376^1$ «Незаконне втручання у роботу автоматизованої системи документообігу суду» – у Єдиному звіті про кримінальні правопорушення (готується Офісом Генерального прокурора України).

У розділі ІІ «Участь служб та підрозділів Національної поліції у розкритті кримінальних правопорушень (за видами), досудове розслідування за якими закінчено» відображено результати розкриття (розслідування) кримінальних правопорушень, передбачених КК: «Привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем»; «Підроблення документів, печаток, штампів та бланків, а також збут або використання підроблених документів,

печаток, штампів»; злочини у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів чи прекурсорів та ін. Таким чином, не всі традиційні злочини, вчинені за допомогою комп'ютерних технологій та Інтернету, відображаються у звітах як кіберзлочин.

Частина українських вчених до кіберзлочинів відносять злочини, передбачені статтями глави XVI КК та злочини, показники про які відображаються у звіті Національної поліції України.

Водночас деякі вчені, зокрема О. В. Савченко, вважають, що крім правопорушень, наведених у звіті, під категорію кіберзлочинів можуть підпадати й інші, передбачені КК України, за умови, що знаряддям їх вчинення були мережеві технології та/або їх наслідки відображатимуться в кіберпросторі.

До кіберзлочинів можуть належати такі: діяння, вчинені задля насильницької зміни чи повалення конституційного ладу чи захоплення структури державної влади (ст. 109); посягання на територіальну цілісність та недоторканність України (ст. 110); державна зрада (ст. 111); диверсія (ст. 113); шпигунство (ст. 114). Сюди можуть бути віднесені дії, передбачені такими статтям КК: 132; 145; ч. 1 ст. 158; 159; 161; 163; 168; 182; 232; 259; 263; 295; 300; 303; 307; 312; 313; 328; 330; 345; $345^1$; ч. 1 ст. 346 та ін.

Варто також зазначити певні проблеми кваліфікації кіберзлочинів. Як зазначають фахівці, основним критерієм відмежування злочинів, передбачених статтями 361–$363^1$ КК від інших, пов'язаних із використанням комп'ютерної техніки як знаряддя чи засоби вчинення злочину, є об'єкт зазіхання. Так, особливістю кримінально-правової кваліфікації злочинів проти власності, які вчиняються з використанням комп'ютерної техніки, визнається необхідність вирішення питання про доцільність додаткової кваліфікації дій винної особи за статтями, які передбачають відповідальність за злочини у сфері використання комп'ютерної техніки. У такому разі слід керуватися тим, що використання комп'ютерної техніки при вчиненні злочинів проти власності утворює самостійний склад злочину лише тоді, коли завдано певної

шкоди відповідному об'єкту – відносин власності на комп'ютерну інформацію, коли певну інформацію було незаконно знищено, блоковано, модифіковано. А у випадках, коли певні інформаційні системи використовуються за призначенням, додаткова кваліфікація не потрібна [5].

Також зараз існує проблема кримінально-правової кваліфікації дій, які користувачі комп'ютерів здійснюють у сфері обігу криптовалют та застосування штучного інтелекту.

*Так, у 2018 р. дослідники з університету RWTH Aachen University (Німеччина) виявили, що блокчейн Bitcoin містить близько 1600 файлів, де є сцени жорстокого поводження з дітьми, при цьому не менше 8 файлів – з порнографічним контентом. Блокчейн містить зовнішні посилання на 274 відеофайли, присвячені жорстокому поводженню з дітьми, і близько 142 посилань на darkweb. За словами вчених, знахідка може поставити блокчейн поза законом, проте сьогодні не існує жодних судових ухвал із цього приводу, очевидно через складність кримінально-правової кваліфікації. Усі, хто бере участь у процедурі Майнінг або має біткоїни, можуть бути причетні до появи порнографічного контенту в мережі [6].*

На практиці у працівників правоохоронних та судових органів виникає багато проблем щодо кваліфікації кіберзлочинів. Особливо це стосується випадків вчинення таких їх видів, які посягають на кілька об'єктів, які охороняються кримінальним законом. Найчастіше помилки зустрічаються при кваліфікації одного діяння, яке, здавалося б, містить ознаки кількох складів. Так, основною проблемою тут є визначення наявності чи відсутності у вчиненому ідеальної сукупності злочинів.

Під час вчинення кіберзлочину шкода може завдаватися: 1) суспільним відносинам, що виникають у ході забезпечення (за допомогою ІТС) життєдіяльності людини, суспільства, держави; 2) традиційним суспільним відносинам (за допомогою ІТС); 3) традиційним суспільним відносинам, які охороняються законом, для

заподіяння шкоди використовуються ІТС, яким не завдано шкоди.

Перша група відносин охороняється розділом XVI Особливої частини КК. Ці відносини є частиною другої та третьої групи відносин, але у другій групі їм завдається шкоди разом із традиційними відносинами кримінально-правової охорони, а у третій – ні.

Ідеальною сукупністю злочинів вважається два чи більше злочини, вчинені однією дією. Згідно із зазначеними групами відносин, яким завдано шкоди при вчиненні такого діяння у разі скоєння кіберзлочину, можна виділити три групи цих злочинів: 1) злочини у сфері використання ЕОМ, їх систем, комп'ютерних мереж, мереж електрозв'язку; 2) злочини, що кваліфікуються за ст. КК відповідно до об'єкта зазіхання з додатковим посиланням на статті глави XVI КК; 3) злочини, що кваліфікуються за статтями КК відповідно до об'єкта посягання без додаткового посилання на статті розділу XVI КК.

Тобто дії з першої та третьої групи є одиничними злочинами, а з іншого – ідеальною сукупністю злочинів. Однак у практиці зас+тосування норм КК протидії кіберзлочинності діяння, які стосуються різних із зазначених груп, нерідко плутаються. Найчастіше злочини другої групи кваліфікуються лише за однією статтею, і навпаки, злочини першої чи третьої групи кваліфікуються за кількома статтями, хоча потребують додаткової кваліфікації. При цьому стаття застосовується при кваліфікації другої групи злочинів або розділу XVI КК, або інша – відповідно до безпосереднього об'єкта посягання. Очевидно, що в обох випадках частина злочину кваліфікації не охоплюється, що порушує принципи повноти і точності кваліфікації, а у разі кваліфікації одного діяння, що містить один склад злочину, за двома статтями, порушується ще й принцип заборони подвійного інкримінування.

Узагальнення судової практики свідчить, що значна частина кіберзлочинів припадає на випадки, коли зазіхання у сфері використання ІТС здійснюється з корисливих спонукань з метою викрадення чи заволодіння чужим

майном із заподіянням матеріальних збитків і є способом скоєння таких злочинів проти власності, як: шахрайство (ст.190 КК) чи присвоєння чи заволодіння майном шляхом зловживання службовим становищем (ст. 191 КК). У більшості випадків суди кваліфікують такі дії щодо сукупності злочинів: за статтею глави XVI КК та тією статтею, в якій передбачено відповідальність за конкретний злочин проти власності, способом здійснення якого було використання ІТС.

*Наприклад, Печерський районний суд м. Києва визнав М. винним у тому, що він, працюючи провідним інженером відділу пластикових карток комерційного банку, як посадова особа, зловживаючи службовим становищем, маючи доступ до бази даних про клієнтів та їх рахунки, що містилася в його робочому комп'ютері, діючи з метою заволодіння грошима, виконав операцію з персоналізації сторонньої картки, скопіювавши на неї інформацію одного з клієнтів банку. З використанням картки-дублікату та банкоматів М. зняв та привласнив готівкою з рахунку клієнта кошти на загальну суму 65 тис. 900 грн. Зазначені дії М. суд кваліфікував за ч. 4 ст.191 КК як заволодіння чужим майном шляхом зловживання службовим становищем, вчинене у великих розмірах. Крім того, суд кваліфікував дії М. ще й за сукупністю ч. 3 ст. 362 КК, оскільки М., будучи особою, яка мала право доступу до інформації, що обробляється на комп'ютерах та зберігалася на носіях, несанкціоновано її скопіював, що призвело до витоку інформації та завдало значної шкоди.*

*Однак у деяких випадках суди кваліфікують зазначені дії лише за статтями глави XVI Особливої частини КК України. Так, Червоногвардійський районний суд м. Дніпра визнав Є. винним за ч. 1 ст. 361 КК України та призначив йому відповідне покарання. З матеріалів справи вбачається, що Є., діючи з корисливих спонукань, за допомогою спеціальних комп'ютерних програм створив дублікат-макет сайту компанії, яка спільно із ЗАТ КБ «ПриватБанк» надавала послуги з прискореного перерахування платежів за комунальні послуги та мобільний зв'язок через Інтернет. В результаті такої*

*діяльності Є. протягом певного часу викрадав кошти з рахунків клієнтів ЗАТ КБ «ПриватБанк».*

В останньому випадку, оскільки Є. шляхом обману неодноразово опановував грошовими коштами за допомогою незаконних операцій з використанням ЕОМ, а втручання у роботу ЕОМ є способом скоєння злочину проти власності, то такі дії потребують додаткової кваліфікації ще й за ст. 190 КК України. Вважаємо, що тут справді є сукупність злочинів, але вона вже врахована до КК у ч. 3 ст. 190, отже, потрібна кваліфікація за цією нормою без додаткових посилань на норми КК [7].

Однією із загальних проблем кримінально-правової кваліфікації є питання кваліфікації ідеальної сукупності злочинів, а саме поглинання одного злочину іншим, яке було його частиною. Ця проблема досі потребує вирішення вченими. Зокрема, Т. І. Созанський формулює правило щодо злочинів, які мають додаткові об'єкти зазіхання: «Якщо ці об'єкти співвідносяться як основний та додатковий, то діяння кваліфікується як одиничний злочин, якщо ж обидва (або більше) об'єкти є основними, то діяння утворює ідеальну сукупність злочинів» [8].

У п. 11 Постанови Пленуму Верховного Суду України. зазначено: «Якщо у складі злочину передбачено діяння, у поєднанні з іншими обставинами завжди утворює склад іншого злочину, то питання щодо його кримінально-правової оцінки необхідно вирішувати з урахуванням того, наскільки охоплюється складом цього злочину таке діяння, а також з урахуванням змісту санкцій відповідних статей КК. У випадках, коли складом певного злочину охоплюється вчинене одночасно з цим злочином відповідне діяння та санкцією статті (частини статті) КК встановлено за цей злочин більш строге максимальне основне покарання, ніж за відповідне діяння, таке діяння не утворює сукупності злочинів та окремої кваліфікації».

**Висновки**

Сьогодні офіційного, закріпленого в міжнародних документах визначення кіберзлочинності поки не існує. У вітчизняному законодавстві нині також не існує

чіткого визначення поняття кіберзлочину. Дискутуються різні точки зору щодо класифікації кіберзлочинів. Отже, є нагальна потреба визначитися з переліком «традиційних» злочинів, які можуть відноситися до категорії кіберзлочинів, внести зміни до відомчої статистичної звітності Національної поліції України.

Таким чином, кримінально-правове забезпечення боротьби з кіберзлочинністю потребує подальшого вдосконалення, імплантації у національні правові норми міжнародних стандартів. Крім того, кваліфікація кіберзлочинів має свої особливості, які потрібно враховувати. Ці та інші проблеми боротьби з кіберзлочинністю далеко не вичерпані, вони можуть розглядатись на наукових міжнародних конференціях, а також виступати предметом подальших наукових досліджень, у тому числі – на дисертаційному рівні.

## Перелік використаних джерел

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

2. Home Affairs Committee E-crime Fifth Report of Session 2013–14.
URL:https://publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf.

3. Joint communication to the European parliament, the Council, the European economic and social committee and the committee of the regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 02.2013 // URL: http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=celex:52013JC0001.

4. Десятый Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями. Вена, 10-17 апреля 2000 года. URL: https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-RU.pdf;
https://digitallibrary.un.org/record/432653/files/A_CONF.187_10-RU.pdf?version=1.

5. Науково-практичний коментар Закону України «Про основні засади забезпечення кібербезпеки України» за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.

6. У блоках Bitcoin виявили сліди дитячої порнографії. URL: https://www.volynnews.com/news/all/u-blokakh-Bitcoin-vyiavyly-slidy-dytiachoyi-pornohrafiyi-/.

7. Узагальнення опрацьовано суддею Верховного Суду України М.І. Грицівим та головним консультантом управління вивчення та узагальнення судової практики Верховного Суду України В.В. Антощуком. - Режим доступу: http://www.viaduk.net/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257B7C00499C02.

8. Созанський, Т. І. Кваліфікація сукупності злочинів: автореф. дис. ... канд. юрид. наук: 12.00.08; Львів. держ. ун-т внутр. справ. Львів, 2009. 18 с.

# АНАЛІЗ ДОВЖИНИ СТІЙКОГО ПАРОЛЮ КОРИСТУВАЧА ІНФОРМАЦІЙНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Кудінов В.А.
Національна академія внутрішніх справ, м. Київ, Україна,
kudinov_va@ukr.net

У роботі проведено аналіз довжини стійкого паролю користувача інформаційних систем спеціального призначення Національної поліції України. Для забезпечення стійкості паролю цих систем запропоновано використовувати не менше 12 знаків.

**Ключові слова:** інформаційні системи, системи спеціального призначення, пароль, злом, стійкість парольного захисту до перебору, Національна поліція України.

## Вступ

Останніми роками в МВС України вживаються заходи щодо створення єдиної інформаційної системи [1]. Однією з її функціональних підсистем є інформаційно-комунікаційна система «Інформаційний портал Національної поліції України» (далі – ІПНП) [2]. Інформаційними ресурсами системи ІПНП є інформація, що використовується для наповнення та підтримки в актуальному стані баз (банків) даних, які входять до єдиної інформаційної системи МВС [3].

Серед призначень системи ІПНП є забезпечення комплексного захисту інформації та розмежування доступу до інформації, що зберігається в її базах даних [2]. Тому виникає важлива проблема щодо уникнення неправомірного використання зловмисниками правами доступу поліцейських до баз даних. Одним з шляхів її вирішення є створення стійких (надійних) паролів користувачів цієї системи.

Враховуючи зазначене, актуальним, на наш погляд, є дослідження впливу довжини паролю користувачів зазначених ресурсів на його стійкість, що і є *ціллю роботи*.

## Результати та їх обговорення

Як відомо, пароль – це набір символів, який користувач повинен ввести через обладнання вводу інформації, перш ніж він почне обробку інформації в інформаційній системі. Пароль призначений для підтвердження особистості або повноважень користувача і в інформаційних системах використовується для захисту інформації від несанкціонованого доступу. Як відомо, злом парольних систем може відбуватися за допомогою таких методів злому: 1) прямий перебір; 2) підбір по словнику; 3) метод соціальної інженерії; 4) перевірка по словнику найпопулярніших паролів; 5) перевірка послідовностей символів тощо.

Департамент кіберполіції МВС України вважає, що конфіденційність даних не надійно захищена, якщо пароль

є нестійким до зламу [4]. Надійний пароль – це пароль, який неможливо вгадати або зламати методом перебору.

Хакери за допомогою сучасних комп'ютерів за лічені секунди зламують короткі паролі, що складаються тільки з літер і цифр [5]. Третина всіх паролів, що використовуються, зламаються шляхом простого перебору варіантів зі словника [6].

Тому користувач, перш за все, повинен переконатися, що його пароль довгий. Відомчі інструкції МВС України щодо правил формування атрибуту «Пароль» окремих інформаційних систем протягом останніх десятиріч регламентували довжину пароля не менше 5 знаків [7; 8]. Станом на сьогодні Департаменти кіберполіції та інформатизації вважають, що пароль повинен містити не менше 8 знаків [4; 5]. Існують також інші думки фахівців: не менше 8-10, 8-12, 10-12, 12 [7]. Зрозуміло, що більш довгі паролі більш безпечні. Кожен додатковий знак в паролі експоненціально збільшує кількість можливих комбінацій. Це робить захист надійніше.

Найпростіші математичні обчислення дозволяють точно дізнатися про максимальну тривалість атаки (час, за який можна перебрати весь простір паролів заданої довжини, який буде залежати від технічних характеристик обладнання). Відповідно до роботи [9], якщо пароль містить 8 знаків, то час перебору для його зламу складає 11 місяців, 9 знаків – 32 роки, 10 знаків – 1 162 роки, 11 знаків – 41 823 роки, 12 знаків – 1 505 615 років.

Таким чином, 12 знаків у паролі цілком достатньо, щоб користувач створив стійкій пароль. Але при цьому необхідно, щоб користувач дотримувався ще додаткових вимог щодо створення паролю [10]. Крім того, бажано користувачу провести перевірку пароля на його відсутність у реєстрах зламаних та найпопулярніших паролів, а також оцінити його програмами за ступенем надійності [5].

## Висновки

Таким чином, у роботі проведено аналіз довжини стійкого паролю користувача інформаційних систем спеціального призначення Національної поліції України. Вважаємо, що в

системах авторизації для забезпечення стійкості пароля необхідно встановити обмеження на довжину пароля не менше 12 знаків.

## Перелік використаних джерел


1. Про затвердження Положення про єдину інформаційну систему МВС та переліку її пріоритетних інформаційних ресурсів : Постанова Кабінету Міністрів України від 14 лист. 2018 р. Урядовий кур'єр від 12 груд. 2018 р. № 235.

2. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» : Наказ МВС України від 03 серп. 2017 р. № 676. Офіційний вісник України від 26 вер. 2017 р. № 75. Стор. 385. Ст. 2306. Код акта 87310/2017.

3. Про Національну поліцію : Закон України від 02 лип. 2015 р. № 580-VIII. Відомості Верховної Ради України. 2015. № 40-41. Ст. 379.

4. Правила створення та використання надійних паролів – рекомендації кіберполіції. Кіберполіція України : [сайт]. URL: https://cyberpolice.gov.ua/article/pravyla-stvorennya-ta-vykorystannya-nadijnyx-paroliv--rekomendacziyi-kiberpolicziyi-3711/ (дата звернення: 07.05.2023).

5. Рекомендації щодо протидії кіберзагрозам на робочих місцях, розроблені Департаментом інформатизації МВС України : Лист Департаменту освіти, науки та спорту МВС України від 25.10.2022 № 32060/48-2022.

6. Buriachok V., Platonenko A., Semko O. Selection of the rational password generation method for the expected multiples. Ukrainian Scientific Journal of Information Security. 2019. Vol. 25. Issue 1. Pp. 59–64.

7. Кудінов В. А. До проблеми щодо створення надійних паролів користувачів Інтегрованої інформаційно-пошукової системи МВС України. Актуальні проблеми управління інформаційною безпекою держави : матеріали VIII наук.-практ. конф. (Київ, 24 трав. 2017 р.). Київ: Нац. акад. СБ України, 2017. С. 54–56.

8. Кудинов В. А., Рыбалко Т.В. Автоматизированное рабочее место дежурного дежурной части МВД–УМВД(Т): метод. рек. Киев: РИО МВД Украины, 1996. 100 с.

9. 10 дивних фактів про паролі. Kharkiv IT Cluster : [сайт]. URL: https://it-kharkiv.com/10-dyvnyh-faktiv-pro-paroli/ (дата звернення: 07.05.2023).

10. Кудінов В. А. Загальний підхід щодо створення та використання надійних паролів користувачів інформаційних систем. Interdisciplinary research: scientific horizons and perspectives: I International Scientific and Theoretical Conference (Vol. 2), March 12, 2021. Vilnius, Republic of Lithuania: European Scientific Platform, 2021. P. 47–48.

# АНАЛІЗ ІНСТРУМЕНТІВ DAST ТА SAST ДЛЯ ПОКРАЩЕННЯ БЕЗПЕКИ КОДУ В DEVSECOPS

Коломицев М.В., Сендецький К.В.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», НН Фізико-технічний інститут, Київ, Україна

У роботі розглянуті питання покращення безпеки в процесі розроби програмного забезпечення з використанням методології DevSecOps. Було розглянуто основні інструменти статичного аналізу (SAST) та динамічного аналізу (DAST), їх місце та роль, порівняння їх переваг та недоліків.
Ключові слова: DevOps, DevSecOps, SAST, DAST.

## Вступ

У сучасному світі розробки програмного забезпечення концепція DevOps грає ключову роль в прискоренні та покращенні процесів розробки, тестування та доставки програм. DevOps став популярним завдяки своїй можливості скоротити час між створенням коду та його випуску на production-сервери.

Але не слід забувати про безпеку, кожен день з'являються нові загрози та вразливості. Безпека являється ключовою задачею при розробці програмного забезпечення. Тому в останні роки стає актуальним концепція DevSecOps [1]. Головним аспектом DevSecOps являється інтеграція безпеки в процес розробки та використання інструментів та методів забезпечення безпеки на всіх етапах життєвого циклу програми, починаючи з розробки та тестування програми, закінчуючи розгортанням та моніторингом. Однією з важливих складових цього процесу є аналіз коду на наявність уразливостей та помилок безпеки. Основними інструментами аналізу програми є Static Application Security Testing (SAST) [4] та Dynamic Application Security Testing (DAST) [3], які дозволяють автоматично знаходити потенційно небезпечні місця в коді та тестувати програми на наявність уразливостей у реальному часі. SAST використовують на етапі проєктування та розробки програми, а DAST зазвичай на етапі тестування. Далі ми детальніше розглянемо ці інструменти та як їх використання зможе покращити безпеку коду в DevSecOps.

## 1. Інструменти SAST. Основні програми Статичного тестування безпеки програм

Static Application Security Testing (SAST) або "White-box testing" – формат тестування програми, який сканує вихідний код та всі його компоненти для виявлення потенційних вразливостей. Він може виявляти такі вразливості та недоліки як SQL-Injection, XSS, переповнення буфера, зберігання конфіденційної інформації в коді та інші [2].

Переваги використання SAST:

- Тестування на ранніх етапах розробки.
- Може застосовуватися до широкого спектра програм.
- Видає повну інформацію щодо вразливості, де вона виникла, з яких причин, та запропонує варіанти вирішення проблеми.

- Аналізую тільки код, без запуску програми.

Недоліки використання SAST:

- Не завжди точно визначає вразливість.
- Може видавати хибні спрацьовування.

Деякі з популярних інструментів: Checkmarx, Veracode [7].

## 2. Інструменти DAST. Основні програми Динамічного тестування безпеки програм

Dynamic Application Security Testing (DAST) – або "Black-box testing" – формат тестування, який шукає вразливості шляхом впровадження типових сценаріїв атаки на додаток. Інструмент відстежує вектори атак, поведінку вразливостей та видає детальну інформацію щодо доступних загроз [2].

Переваги:

- Може виявити вразливості втрачені під час використання SAST
- Більш широкий спектр тестів у порівнянні з SAST
- Може сканувати в реальному часі

Недоліки:

- Тестування тільки після завершення розробки.
- Може видавати хибні спрацьовування.
- Займає багато часу та потребую багато ресурсів.

Деякі популярні інструменти: OWASP ZAP, Burp Suite [6].

## 3. Інтеграція SAST і DAST у процес розробки програмного забезпечення та як їх використання може підвищити безпеку коду в DevSecOps

Інструменти статичного та динамічного аналізу коду, такі як SAST та DAST, можуть суттєво підвищити безпеку додатків у DevSecOps. Інтеграція інструментів у процес розробки програмного забезпечення дозволяє виявляти та виправляти вразливості в коді ще на ранній стадії розробки та тестування.

SAST аналізує код щодо потенційних вразливостей на основі статичного аналізу. Його використання на ранньому

етапі розробки дозволяє вчасно знаходити та запобігти появі вразливостей на наступних етапах DevSecOps.

DAST тестує роботу програми в режимі реального часу, що дозволяє виявляти вразливості, пов'язані з конкретними вхідними даними та конфігурацією програми. Це дозволяє виявити загрози які не були виявлені інструментами SAST.

Без застосування інструментів SAST та DAST, команда розробників та тестувальників може допустити наявність вразливостей в програмі, що може призвести до таких наслідків як витік даних, порушення конфіденційності та доступності серверів.
Використання SAST та DAST в парі дозволить зменшити ризики випуску незахищеного додатка. Їх інтегрують в CI/CD пайплайн для автоматичного сканування коду на наявність уразливостей при кожному коміті в репозиторій та регулярного сканування в процесі тестування.

Крім того, необхідно враховувати, що інструменти SAST та DAST мають свої особливості та можуть надавати різний набір результатів. Для того, щоб отримати максимальну віддачу від використання цих інструментів, потрібно провести аналіз їх можливостей і вибрати інструменти, які найкраще підходять для конкретного проєкту та завдань.

## Висновок

Використання інструментів SAST та DAST може значно підвищити безпеку розробки програмного забезпечення в методології DevSecOps. Інтеграція цих інструментів у процес розробки дозволяє виявляти вразливість та помилки безпеки на ранніх етапах життєвого циклу ПЗ і навіть у процесі його експлуатації. Як було визначено, кожен сканер має свої переваги та недоліки, щоб мінімізувати проблеми, кращим рішенням буде використовування їх в парі, враховуючи вимоги цільового проєкту.

## Перелік використаних джерел

1. DevSecOps [Електронний ресурс] – Режим доступу: https://aws.amazon.com/what-is/devsecops/?nc1=h_ls

2. DevSecOps tools [Електронний ресурс] – Режим доступу: https://www.gitguardian.com/glossary/devsecops-tools
3. DAST [Електронний ресурс] – Режим доступу: https://www.microfocus.com/en-us/what-is/dast
4. SAST [Електронний ресурс] – Режим доступу: https://www.synopsys.com/glossary/what-is-sast.html
5. Порівняння DAST та SAST [Електронний ресурс] – Режим доступу: https://snyk.io/learn/application-security/sast-vs-dast/
6. Інструменти DAST [Електронний ресурс] – Режим доступу: https://www.getastra.com/blog/security-audit/top-dast-tools/#zap
7. Інструменти SAST [Електронний ресурс] – Режим доступу: https://owasp.org/www-community/Source_Code_Analysis_Tools

# ВИЗНАЧЕННЯ ЦІЛЕЙ ПРИ РОЗРОБЦІ КІБЕРРЕЗИЛЬЄНТНИХ СИСТЕМ ЗГІДНО NIST

Бакалинський О.О., Коробейніков Ф.О.
ІПМЕ ім. Г.Є. Пухова НАН України, Київ, Україна

Представлено підхід до визначення цілей при розробці кіберрезильєнтних систем, відповідно до рекомендацій, викладених у стандартах Національного інституту стандартів і технологій США (NIST). Робота покликана стати частиною дорожньої карти для дослідників і практиків кіберрезильєнтності у створенні інформаційних систем, які можуть витримувати й адаптуватися до несприятливих умов, збоїв та атак і забезпечувати гарантоване виконання всіх основних функцій кіберсистем.

**Ключові слова:** resilience, NIST, framework, goals, цілі, передбачення, протистояння, відновлення, адаптація, кіберсистема.

## Вступ

В наш час потреба у створенні резильентних систем стає дедалі актуальнішою. У зв'язку з постійно змінним ландшафтом загроз, посиленням політичної, соціальної та кліматичної нестабільності, тотальною глобалізацією цифрових мереж і зростаючою залежністю більшої частини жителів нашої планети від технологій при отриманні основних послуг, стандартні стратегії кібербезпеки вже не можуть забезпечити гарантоздатність систем.

Приймаючи той факт, що *сучасний рівень технологій передбачає принципову неможливість гарантувати повну безпеку інформаційних активів*, NIST розробив стандарт SP 800-160, Volume 2 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, який обумовлює новий підхід до забезпечення безпеки систем, шляхом створення адаптивних механізмів, що поглинають наслідки руйнівних інцидентів, атак, або внутрішніх збоїв і підтримують роботоспроможність критичних процесів місій або організацій.

Предметом цього дослідження є процес визначення, узгодження та розробки пропозицій щодо імплементації цілей при побудові резильєнтних систем згідно NIST.

Метою роботи є визначення практичних аспектів високорівневої конструкції «ЦІЛІ» (Goals) фреймворку побудови кіберрезильєнтності, розробленого NIST, які містять у собі: обґрунтування необхідності впровадження резильєнтності в організації; висвітлення її ключових відмінностей від кібербезпеки; узгодження цілей резильєнтності на всіх рівнях організації; визначення відповідальних за впровадження та створення високорівневих механізмів контролю ефективності досягнення цих цілей.

## Поняття резильєнтності

Другий том стандарту 800-160 сконцентрований навколо поняття кіберрезильєнтності. Дається його дефініція: «Кіберрезильєнтність – це здатність передбачати, витримувати, відновлюватися та адаптуватися до

несприятливих умов, навантажень, атак чи компрометацій систем, які використовують чи забезпечуються кіберресурсами» [1] (Cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources).

Також зазначається, що «всі дискусії про кіберрезильєнтність зосереджені на гарантуванні виконання місії або бізнес-функцій та ґрунтуються на припущенні, що супротивник все ж таки подолає захист і встановить довготривалу присутність в системах організації» [1].

Тобто, відразу чітко підкреслюється відмінність від стандартних стратегій кібербезпеки, які містять вказівки щодо систем, спроектованих з акцентом на *забезпечення конфіденційності, цілісності та доступності інформаційних активів (цілі кібербезпеки)*. В другому томі стандарту на чільне місце стає гарантування життєздатності критичних систем, що включають кіберресурси - вбудовуючи в них елементи резильентності, пропонується забезпечити здатність *передбачати атаки, витримувати їх, відновлюватись і адаптуватися до загроз* (цілі кіберрезильєнтності) гарантовано виконуючи покладені на них місії, незважаючи на збої, несприятливі умови, стреси, атаки, компрометації тощо.

**Фреймворк побудови кіберрезильєнтності**

Стандарт NIST Special Publication 800-160, Volume 2 розглядає: фреймворк побудови кіберрезильєнтності; конструкції кіберрезильності, які є частиною цього фреймворку; концепцію використання фреймворку, а також міркування щодо впровадження кіберрезильєнтності в життєвий цикл систем, компаній чи організацій. Конструкції є базовими елементами (тобто будівельними блоками) фреймворку і включають цілі, задачі, методи, підходи до реалізації, заходи зі зниження ризиків і наслідків, та принципи проектування.

Фреймворк фокусується на кіберрезильєнтності, яка хоча і має зв'язок з безпекою та відмовостійкістю, але має

відмітну структуру для ідентифікації своєї проблемної галузі та галузі вирішення.

Хоча SP 800-160, v. 2 зосереджен на інженерії кіберрезильєнтності, але концепції вищого рівня (тобто цілі, задачі та методи забезпечення кіберрезильєнтності) визначені таким чином, щоб їх можна було застосовувати в широкому контексті. Їх визначення написані в нейтральній до технологій манері та не містять згадок про кіберресурси.

Цілі та задачі кіберрезильєнтності визначають "що" є кіберрезильєнтністю - тобто, які властивості та поведінка є невід'ємними для кіберрезильєнтних систем (Рис. 1).


Рисунок 1: взаємозв'язок між конструкціями кіберрезильєнтності (NIST SP 800-160, 2.1.5)

## Цілі кіберрезильєнтності

Цілі - це *високорівневі* формулювання бажаних результатів, які є спільними для багатьох визначень резильєнтності. Вони включені у фреймворк побудови кіберрезильєнтності, щоб забезпечити зв'язок між рішеннями з управління

ризиками на системному рівні, рівні місії та бізнес-процесів, а також на рівні організації [1]. Стратегії управління організаційними ризиками можуть використовувати цілі кіберрезильєнтності та пов'язані з ними стратегії для інтеграції кіберрезильєнтності.

Цілі кіберрезильєнтності - це не стільки кінцеві орієнтири, скільки поточні стратегічні завдання, які формують операційний ландшафт організації. Вони є наріжним каменем системи побудови кіберрезильєнтності NIST і мають життєво важливе значення для розробки комплексної стратегії кіберрезильєнтності. Ці цілі спрямовують рішення з управління ризиками на різних рівнях - системи, місії, бізнес-процесів та організації. Вони забезпечують більш уніфікований підхід до управління ризиками, усуваючи прогалини між різними організаційними рівнями та сприяючи формуванню культури проактивної кіберрезильєнтності.

Відповідно до визначення кіберрезильєнтності, дуже важливо розуміти, що бажані результати виходять за рамки простої підготовки до кіберзагроз і реагування на них. Вони також включають здатність розвиватися і адаптуватися під впливом цих загроз, покращуючи таким чином загальні кіберпотужності відповідної організації. Кіберрезильєнтність – це не статична якість, а динамічна, яка потребує постійного розвитку та вдосконалення.

Для того, щоб зрозуміти суть кіберрезильентності та її відмінність від кібербезпеки, необхідно розглянути кожну з цілей, які описані у фреймворку:

ПЕРЕДБАЧИТИ (ANTICIPATE): Ця ціль зосереджена на проактивних заходах для прогнозування і з'ясування того, які елементи системи є найбільш важливими для діяльності організації та вразливими для професійних атак підвищеної складності, непередбачуваних збоїв або інцидентів. *Усі ризики з критичним рівнем шкоди, незважаючи на ймовірність їхньої реалізації, мають бути враховані та опрацьовані із застосуванням до них рішень резильєнтності, виходячи з припущення, що загроза, наскільки б неймовірною і складною в реалізації вона не була, все ж таки буде реалізована.*

Розвідка загроз, оцінка ризиків і прогностична аналітика відіграють ключову роль у досягненні цієї цілі. Недостатньо просто реагувати на загрози; організації повинні випереджати їх, впроваджуючи елементи резильєнтності в найбільш критичні і слабкі елементи системи функціонування організації.

NIST виступає за проактивну, випереджувальну позицію щодо загроз. Це передбачає проведення комплексних операцій з розвідки нових типів загроз для визначення потенційних векторів атак і прогнозування нових загроз. Це також включає регулярний аудит і стрес-тестування систем для виявлення вразливостей до того, як вони можуть бути використані. Таке випереджувальне мислення має пронизувати всі рівні організації, заохочуючи пильність і безперервне навчання.

Ця ціль також передбачає розвиток культури обізнаності, освіти та постійної пильності.

ПРОТИСТОЯТИ (WITHSTAND): Фреймворк кіберрезильєнтності допомагає створити додатковий захисний контур організації, що спрацьовує тоді, коли елементи кібербезпеки не можуть впоратися з атакою, збоєм або несприятливою подією.

Практична реалізація цієї цілі означає, що резильєнтні системи мають бути спроможні протистояти негараздам, гарантуючи мінімальну необхідну функціональність (наприклад, функціональність задоволення критичних потреб місії). Нові кіберзагрози при дослідженні можуть тестуватись на полігоні або в ізольованому середовищі з метою встановлення спроможності системи протистояти їм. Розуміння обмежень окремих сутностей, організацій та систем має основне значення.

Резильєнтність також повинна досягатися завдяки захисним заходам по запобіганню втілення кіберзагроз у реальні атаки. Це можуть бути такі заходи, як впровадження багаторівневих стратегій захисту, розробка безпечного програмного забезпечення та систем, використання надійного шифрування та дотримання належної кібергігієни. Однак це також поширюється і на людські елементи кібербезпеки: працівники повинні бути

навчені розпізнавати і протистояти атакам соціальної інженерії, наприклад. Метою тут є зміцнення захисту організації за допомогою методів які не входять до фреймворку інформаційної безпеки.

ВІДНОВИТИ (RECOVER): Здатність швидко відновити нормальну роботу після кіберінциденту має вирішальне значення для кіберрезильєнтності. Швидке та ефективне відновлення може значно пом'якшити вплив інциденту на діяльність, роботоспроможність та репутацію організації.

Відновлення - це багатогранний процес. Він включає не лише технічні аспекти відновлення систем і даних після інциденту, але й управління ширшими наслідками кібератаки. Це може включати комунікаційні стратегії для управління репутаційною шкодою або юридичні міркування у разі витоку даних. Фреймворк кібербезпеки NIST [2] включає функцію "Відновлення", яка надає вказівки щодо розробки та впровадження надійних планів відновлення.

Дотримуючись цілей, викладених NIST, системи повинні не тільки протистояти ударам і відновлюватися після них, а й виконувати ітерації, внаслідок чого вони стануть ще надійнішими.

АДАПТУВАТИСЯ (ADAPT): Мабуть, найбільш важливим аспектом кіберрезильєнтності є здатність безперервно накопичувати інформацію про інциденти, вразливості, нові технології та супротивників і відповідно адаптувати стратегії. Це може включати перегляд політик безпеки, вдосконалення розвідки загроз і переоцінку стратегій управління ризиками, які мають відбуватись із заданою періодичністю.

Під час атаки резильєнтна система має бути здатною швидко адаптуватися, знаходити нові ресурси, пристосовуватися (навіть зі скороченням своїх функцій), щоб виконувати основні завдання і мінімізувати збитки від можливих загроз і атак.

Безперервне навчання і еволюція систем є ключем до збереження резильєнтності в постійно мінливому ландшафті кіберзагроз. Саме така адаптивність у поєднанні з надійним підходом до передбачення, протистояння та

відновлення після кіберзагроз визначає справді стійку організацію.

Цілі не є лінійними етапами, які потрібно виконати один за іншим, а скоріше перетинаються і є взаємозалежними аспектами кіберрезильєнтності.

Ключовою особливістю цієї частини концепції фреймворку є припущення, що всі чотири цілі повинні вирішуватися одночасно. Наприклад, навіть витримуючи кібератаку або відновлюючись після неї, керівні структури місії або організації повинні передбачати інші атаки. Навіть передбачаючи, витримуючи атаки або відновлюючись після них, сегменти місії/бізнесу, а також місія або бізнес-процеси, які на них покладаються, постійно розвиваються, щоб відповідати мінливому оперативному і технічному середовищу [3].

На всіх рівнях фреймворку підхід до кіберрезильєнтності має циклічний і безперервний характер. Незалежно від того, на якому етапі перебуває організація - передбачення майбутніх загроз, протистояння атакам, відновлення після інцидентів та адаптація стратегій повинні бути постійними процесами.

Згідно зі стандартом NIST SP 800-160, v 2, визначення та узгодження цілей кіберрезильєнтності є спільною роботою за участю різних зацікавлених сторін в організації. Цей процес повинен керуватися Стратегією управління ризиками організації (RMS) і бути інтегрований до фреймворку управління ризиками (RMF).

У NIST вказується, що відповідальним за цей процес є Керівник з управління ризиками (функція) [4], який забезпечує, щоб питання, пов'язані з ризиками для безпеки окремих інформаційних систем розглядалися з загальноорганізаційної точки зору з огляду на загальні стратегічні цілі та завдання організації у виконанні її місій та бізнес-функцій. Також він відповідає за те, щоб управління ризиками, пов'язане з окремими інформаційними системами, було узгодженим в рамках всієї організації, і відображало організаційну толерантність до ризиків, та розглядалося разом з іншими

організаційними ризиками, що впливають на успіх місії/бізнесу.

Функція управління ризиками може бути поставлена в обов'язки групі, яка, як правило, включає керівників вищого рівня. Вони, по-перше, потрібні мати повну інформацію про пріоритетні цілі самої організації, та про ті критичні процеси, без яких організація не може функціонувати на рівні, достатньому для досягнення цих цілей. І, по-друге, мати повноваження приймати рішення, засновані на оцінці ризиків, що впливають на організацію в цілому. Усі керівні ролі в організації повинні співпрацювати для виконання завдань, пов'язаних з управлінням ризиками. Це включає встановлення та узгодження цілей кіберрезильєнтності. Цілі повинні відображати результатах оцінки ризиків і мають бути доповнені задачами таким чином, щоб забезпечити резильєнтність, в першу чергу, найбільш критичних систем, операцій і даних організації.

У зв’язку з тим, що цілі є високорівневими конструкціями фреймворку побудови кіберрезильєнтноті, метрики, що оцінюють рівень їх досягнення, мають бути конструктивно значущими для прийняття стратегічних рішень на вищому рівні організаційної ієрархії. Водночас, для забезпечення всеосяжного розуміння і прийняття цих метрик, результати мають бути подані таким чином, щоб вони були доступними і зрозумілими для осіб, які не володіють спеціалізованими знаннями на всіх рівнях організації. Беручи до уваги ці фактори та враховуючи відсутність у стандартах NIST чітко визначених метрик для оцінки цілей резильєнтності високого рівня, пропонується регулярно використовувати наведені нижче метрики, і застосувати лонгітюдний метод для відстеження динаміки змін.

Для цілі ПЕРЕДБАЧИТИ (ANTICIPATE) доречною буде метрика, яка вимірює час безвідмовної роботи критичних систем (Uptime Metric).

Час безвідмовної роботи - це відсоток часу, протягом якого критичні системи організації або місії працюють і

доступні для використання. Він розраховується як ((Загальний час - Час простою) × Загальний час) × 100%)

Це показник ефективної резильєнтності, і, чим краща буде свідома готовність, чим краще планування на випадок непередбачуваних ситуацій, тим більший показник буде при розрахунку цієї метрики.

Для розуміння успішності досягнення цілі ПРОТИСТОЯТИ (WITHSTAND) керівництву організації необхідно знати, який відсоток з усіх інцидентів, пов'язаних з критичними процесами і системами, не спричинив простою в роботі організації. Для цього треба від загальної кількості інцидентів, які були спрямовані на критичні системи треба відняти кількість інцидентів, що призвели до простою (критичних інцидентів), отримане значення поділити на загальну кількість інцидентів, які були спрямовані на критичні системи, і помножити на сто відсотків. Більший відсоток буде означати більш високий рівень резильєнтності організації, і виражати її вміння протистояти атакам і несприятливим умовам.

Широковживана метрика MTTR - це виразний показник цілі ВІДНОВИТИ (RECOVER). Інциденти неминучі, але резильєнтні системи повинні швидко відновлюватися.

Середній час вирішення проблеми - це середній час, необхідний для усунення збою, чи наслідків атаки, і відновлення роботи критичних систем.

Він розраховується так: загальний час простою критичних систем треба поділити на кількість критичних інцидентів, які призвели до цих простоїв.

Ефективність високорівневої адаптації систем організації або місії (ADAPT) можна виміряти за допомогою метрики MTBF, яка розраховує середній час від одного критичного інциденту до наступного (за умови внесення адаптаційних змін в системи після інцидентів).

MTBF розраховується як: (Загальний час - Часу простою) / кількість критичних інцидентів". Збільшення показника MTBF показує більш високу резильєнтність організації.

**Висновки**

У роботі визначено та проаналізовано високорівневі цілі резильєнтності, згідно фреймворку NIST. Представлено визначення та призначення кожної з цілей кіберрезильєнтності з точки зору організації в цілому, а також основні елементи взаємодії всіх рівнів організації при впровадженні резильєнтності.

Запропоновано метод і метрики для високорівневої оцінки і контролю досягнення цілей резильєнтності.

Пояснені ключові відмінності між цілями кіберрезильєнтності та кібербезпеки.

## Перелік використаних джерел


1. NIST Special Publication 800-160, Volume 2. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach [Електронний ресурс] // NIST. – 2021. – Режим доступу до ресурсу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf.
2. NIST Cybersecurity Framework [Електронний ресурс] // NIST. – 2018. – Режим доступу до ресурсу: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf .
3. Cyber Resiliency Engineering Framework [Електронний ресурс] / D.Bodeau, R. Graubart, J. Picciotto, R. Mcquaid // MITRE. – 2011. – Режим доступу до ресурсу: https://www.mitre.org/sites/default/files/media/publication/11_4436_2.pdf.
4. Definition of term “risk executive (function)”. Glossary of Computer Security Resource Center (CSRC) [Електронний ресурс] // NIST – Режим доступу до ресурсу: https://csrc.nist.gov/glossary/term/risk_executive.

# МАТЕМАТИЧНА МОДЕЛЬ СУСПІЛЬНОЇ ПОВЕДІНКИ В УМОВАХ ІНФОРМАЦІЙНОГО ВПЛИВУ

Д.О.Горбачов, І.М.Терещенко,
КПІ ім. Ігоря Сікорського, НН ФТІ, Київ, Україна

В даній роботі розглянута математична модель взаємодії різних груп агентів. Досліджено поведінку певної множини активних агентів, які намагаються подіяти на дві групи суспільства з різною реакцією на інформаційний вплив, з урахуванням того, що під впливом пасивні агенти перетворюються в активних. За основний фактор при аналізі інформаційного впливу активних агентів на пасивних було взято внутрішню валюту.
**Ключові слова:** інформаційний вплив, рефлексивна гра, внутрішня валюта, агенти впливу.

## Вступ

Останнім часом відчувається серйозний вплив на поведінку та думки різних груп суспільства внаслідок різних несприятливих обставин, спричинених війною. Люди, керуючись своїми внутрішніми уявленнями, намагаються знайти відповіді на важливі для них життєві питання. Крім того, думка оточення може впливати на вибір підсвідомо, а іноді ми навіть відмовляємося вибирати саме через вплив оточення. В даній ситуації ми можемо говорити про інформаційний вплив [1]. Моделі прихованого та інформаційного керування, описані у [2], дозволяють описати поведінку під дією інформаційного впливу. У наступній роботі будуть розглянуті різні види агентів, зокрема активні агенти, які управляють суб'єктом у процесі інформаційного керування та пасивні агенти, які є об'єктом керування. Також буде проаналізований перехід від пасивного до активного агента як реакція на інформаційний вплив.

## Постановка задачі

Нехай маємо три групи агентів $\theta_1, \theta_2, \theta_3$. $\theta_1$ – активні агенти, $\theta_2, \theta_3$ - дві групи пасивних, які мають певні обмеження в виді порогів, щодо впливу. Загальна кількість агентів $N = N_1 + N_2 + N_3$, де $N_i$ – кількість агентів з $\theta_i$. Крім того активні агенти мають можливість тричі завдавати вплив, тож формально вважатимемо їхню кількість збільшеною в три рази від фактичної.

## Внутрішня валюта

В якості регулятора діяльності активних агентів буде виступати числова характеристика цінностей агента, яку називають внутрішня валюта. Це поняття вперше введено Лефевром в роботі [3].

Пропонується наступне обчислення внутрішньої валюти, яке відповідає змінам цінностей агентів під інформаційним впливом:

$$H^{\theta_i} = a_i + b_i \beta_i(x_t), i = 2,3$$

$$\beta_i(x_t) = \begin{cases} \sin \frac{\pi x_t}{N_i}, & x_t < N_i \\ 0, & x_t \geqslant N_i \end{cases}$$

$a_i$ – зацікавленість інформацією і-тої групи агентів;

$b_i$ – максимально можлива зацікавленість, яку можуть нав'язати агентам і-тої групи;

$\beta_i$ – кількість агентів, які піддалися впливу за час $t$

Тоді $H_{min}{}^{\theta_i} = a_i$, $H_{max}{}^{\theta_i} = a_i + b_i$

## Обчислення змін кількостей агентів

Введемо $x_t{}^i$, i $= \overline{1,3}$– функції кількості тих, хто піддався впливу на момент часу $t$.

$$x_t^1(t_0, n_1, n_2) = \begin{cases} n_1, t \leqslant t_0 \\ n_2, t \geqslant t_0 \end{cases}$$

$t_0$ – прогнозований час початку піку впливу;

$n_1$– кількість членів групи впливу до початку піку впливу;

$n_2$– кількість членів групи впливу під час піку впливу.

$$x_t^2(n) = \begin{cases} \left[\frac{n}{5}\right], & H^{\theta_2} < 0.3H_{max}^{\theta_2} \\ 2\left[\frac{n}{3}\right], & 0.3H_{max}^{\theta_2} \leqslant H^{\theta_2} < 0.55H_{max}^{\theta_2} \\ 3n, & 0.55H_{max}^{\theta_2} \leqslant H^{\theta_2} \end{cases}$$

$$x_t^3(n) = \begin{cases} \left[\frac{n}{5}\right], & H^{\theta_3} < 0.3H_{max}^{\theta_3} \\ 2\left[\frac{n}{3}\right], & 0.3H_{max}^{\theta_3} \leqslant H^{\theta_3} < 0.4H_{max}^{\theta_3} \\ 0, & 0.4H_{max}^{\theta_3} \leqslant H^{\theta_3} \end{cases}$$

## Параметри чисельного експерименту

Розглянемо застосування розробленої моделі на реальних числах. $N = 10000, N_1 = 0.05N,\ N_2 = 0.85N, N_3 = 0.1N.$ Агенти $\theta_1$ діють фіксованими групами з наступними параметрами $t_0 = 40, n_1 = 15, n_2 = 50.$

За різних параметрах у внутрішній валюті отримуємо 2 наступні ситуації: велика $(a_2 = 12, b_2 = 60, a_3 = 1, b_3 = 70)$ і мала $(a_2 = 2, b_2 = 50, a_3 = 1, b_3 = 70)$ початкова зацікавленість. Ефективність заданого впливу будемо обраховувати, як частку кількості агентів, які піддалися впливу й їх початкову загальну кількість.

## Результати у вигляді графіків

Розглянемо розвиток впливу на групу агентів $\theta_3$:

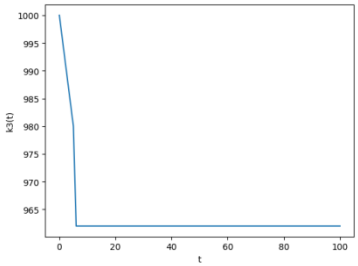


Рис.1. Зміна кількості агентів $\theta_3$ у часі

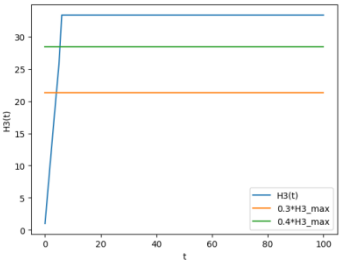


Рис.2. Внутрішня валюта агентів $\theta_3$

На Рис.1 бачимо, що агенти цієї групи були під впливом 7 ітерацій, на Рис.2 бачимо причину такої поведінки: їх внутрішня валюта пройшла другий поріг.

Розглянемо, як ітераційно задавався вплив:

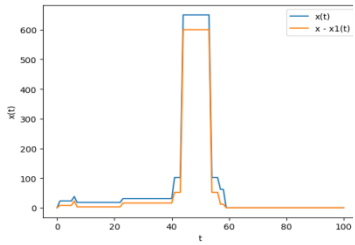


Рисунок 3. Кількість агентів, які піддалися впливу в часі (ситуація 1: ефективність 70,8%)

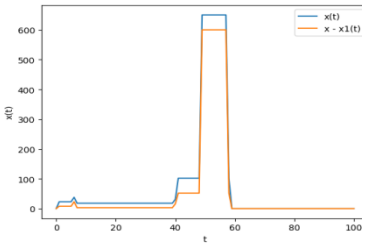


Рисунок 4. Кількість агентів, які піддалися впливу в часі (ситуація 2: ефективність 63,6%)

На Рис. 3 і Рис. 4 помаранчева лінія - кількість агентів, які піддалися впливу, синя - кількість агентів, які піддалися впливу плюс агенти впливу. Роботу агентів впливу можна побачити як різницю між значеннями ліній.
На Рис. 5 і Рис. 6 помаранчева лінія - сумарна за всі ітерації кількість агентів, які піддалися впливу. Звідси легко бачити процес збільшення кількості агентів, що піддалися впливу, а також й пік впливу.

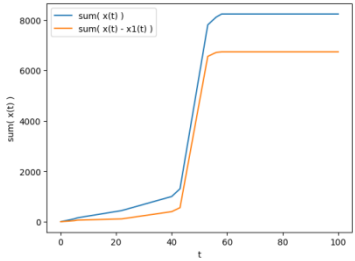


Рисунок 5. Кількість агентів, які піддалися впливу за час $t$ (ситуація 1: ефективність 70,8%)

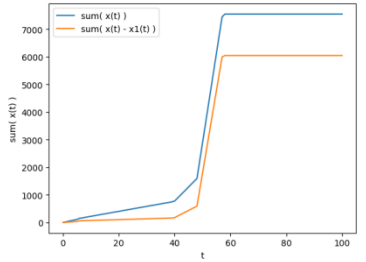


Рисунок 6. Кількість агентів, які піддалися впливу за час $t$ (ситуація 2: ефективність 63,6%)

## Висновок

Розроблено математичну модель інформаційного впливу активних агентів на пасивних за рахунок їх внутрішньої валюти. Дослідження вказаної моделі показало можливість її практичного застосування. Отримано та проаналізовано завданий вплив на групу агентів $\theta_3$. Окремо розглянуто

розвиток у групі $\theta_2$ у різних ситуаціях. Така модель може бути використана для прогнозування інформаційного впливу та способів його завдання на певних верствах населення.

## Перелік використаних джерел


1. Fudenberg D., Tirole J. Game theory. — MIT Press, 1991.
2. Hörner J., Skrzypacz A. The Economics of Informational Decentralization: Complexity, Efficiency, and Stability // American Economic Journal: Microeconomics. — 2009. — Т. 1, № 2. — С. 225—247.
3. Lefebvre V. Conflicting Structures. — Los Angeles, CA : Leaf & Oak Publishers, 2015.


# ПЕРСПЕКТИВИ ВИКОРИСТАННЯ DID ДЛЯ АВТЕНТИФІКАЦІЇ ВИБОРЦІВ ПІД ЧАС ІНТЕРНЕТ-ГОЛОСУВАННЯ


П.І. Щур, Ю.Г. Даник
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут



**Анотація**
У статті розглянуто проблему автентифікації виборців під час проведення інтернет-голосування, використання децентралізованих ідентифікаторів для покращення та забезпечення захищеності автентифікації від кібератак.



**Ключові слова:** автентифікація, інтернет-голосування, децентралізований ідентифікатор, DID, кібератака.


**Вступ:**
Інтернет забезпечує доступ до необхідної інформації, роботу і навчання в режимі онлайн, різноманітні розваги, доступ до нього став основоположним елементом правової демократичної держави. Все більше і більше набуває популярності послуга інтернет-голосування, коли виборець

здійснює волевиявлення не з виборчої дільниці, а з будь-якого комфортного для себе місця за допомогою пристроїв підключених до всесвітньої мережі.

Зважаючи на ці процеси, особливо актуальною стала проблема забезпечення надійної процедури автентифікації виборців під час інтернет-голосування, яка б забезпечувала високий рівень захисту від можливих кібератак, одним з таких способів є автентифікація з допомогою децентралізованих ідентифікаторів DID.

## Автентифікація в контексті інтернет-голосування

Інтернет-голосування - це такий тип волевиявлення, який дозволяє громадянам здійснювати волевиявлення за допомогою пристроїв з доступом до мережі. Зазвичай системи інтернет-голосування використовуються для виборів на рівні місцевих органів влади, компаній, громадських організацій, а також для проведення референдумів і петицій. Однією з переваг цих систем є зручність та доступність, дана процедура суттєво заощаджує час, активізує пасивну частину виборчого електорату, дозволяє забезпечити активну участь у «житті держави» для кожного громадянина [1].

Автентифікація – це процес встановлення приналежності когось до чогось, перевірка автентичності. Автентифікація в контексті електронного голосування – це процес перевірки і підтвердження особистості виборців, що беруть участь в голосуванні через інтернет. Відсутність фізичної присутності учасника робить цей процес вразливим до різноманітних підробок, підмін ідентифікаторів, бюлетенів тощо. Також варто врахувати небезпеку хакерських атак які ставлять за мету заволодіння конфіденційною інформацією виборця, змінити його вибір або навіть унеможливити здійснення процесу голосування для певних груп виборців. Всі ці деструктивні дії обов’язково спричинять різноманітні репутаційні збитки, матеріальну шкоду [2].

## Використання децентралізованих ідентифікаторів

Децентралізований ідентифікатор (Decentralized Identifier – DID ) – це унікальний цифровий ідентифікатор, який був створений для представлення сутностей в децентралізованій інформаційній структурі. DID забезпечує можливість ідентифікації будь-яких суб'єктів: фізичної особи, організації, предмета, моделі даних, абстрактної сутності тощо. На відміну від загальноприйнятих ідентифікаторів, DIDs розроблено таким чином, що їх можна відокремити від централізованих реєстрів, постачальників ідентифікаційних даних і центрів сертифікації, саме тому DID-ідентифікацію називають самосуверенною ідентифікацією або децентралізованою ідентифікацією. В основі DID лежить технологія blockchain – вибудуваного за певними правилами ланцюжка блоків, копії яких зберігаються в різних місцях незалежно один від одного. Рядок DID-су, як і блокчейну являє собою буквено-циферний рядок, та складається з декількох частин (URI- схема, метод DID, ідентифікатор DID). Децентралізований ідентифікатор також вказує на документ DID , що являє собою набір даних, описуючих суб'єкт DID та його механізми. [3]

DID може використовуватись для автентифікації виборців під час проведення інтернет-голосування: користувач повинен зареєструватися в системі, створити власне електронне сховище (гаманець). Наступним етапом буде завантаження спеціальної програми-середовища голосування. Для безпосереднього отримання DID, виборцю необхідно зробити запит до системи голосування, підтвердити свою особистість (eID, біометрія, паролі) та підписати дані за допомогою приватного ключа. Після всіх цих маніпуляцій виборець отримує свій персональний DID який він може використовувати для автентифікації в різноманітних сервісах, зокрема і для голосування через інтернет.

Зважаючи на специфіку використання DID, у цього методу автентифікації є певні вразливості як на етапі зберігання ідентифікатора, так і на етапі його перевірки на

сервері. До вразливостей на стороні клієнта можна віднести соціальну інженерію та фішинг, наявність шкідливого програмного забезпечення на пристрої з якого здійснюється голосування, за допомогою цих вразливостей можна заволодіти ідентифікатором , приватним ключем виборця. Слабкою ланкою у процедурі автентифікації є також процес «спілкування» між сервером та користувачем, існує ймовірність здійснення MITM-атак, які передбачають перехоплення ключів, DID-ідентифікаторів, їх підміну тощо. Варто також зазначити, що існують загрози на серверній стороні, вплив людського чиннику.

Варто зазначити, що DID-автентифікація ніде практично не використовується, а існує тільки в якості тест-проектів та концепцій, це пояснюється недостатньою довірою державних інституцій до блокчейн-технологій, слабкого розвитку децентралізованих систем, високою вартістю впровадження таких систем та низьким рівнем дослідженості DID-ідентифікаторів.

## Висновок

В даній роботі було розглянуто процес автентифікації виборців в системах інтернет-голосування, його особливості та наявні кіберзагрози. Було представлено концепцію використання децентралізованих ідентифікаторів для автентифікації, проблеми і недоліки цього способу перевірки особистості виборця.

## Перелік використаних джерел


1. Електронний Уряд: сутність, особливості та перспективи розвитку. [Електронний ресурс] — Режим доступу: https://politics.chdu.edu.ua/article/view/76115
2. Introducing Electronic Voting: Essential Considerations. [Електронний ресурс] — Режим доступу: https://www.corteidh.or.cr/tablas/28047.pdf
3. Decentralized Identifiers (DIDs). Core architecture, data model, and representations. [Електронний ресурс] — Режим доступу: https://www.w3.org/TR/did-core/.

# ВИЯВЛЕННЯ GOLDEN TICKET АТАКИ У СЕРЕДОВИЩІ ACTIVE DIRECTORY

Мельник А.М., Гальчинський Л.Ю.
Навчально-науковий Фізико-технічний інститут, КПІ ім. Ігоря Сікорського, Київ, Україна

**Анотація**
Active Directory – це одна з найпопулярніших і найбільш широко використовуваних систем керування ідентифікацією та доступом у корпоративних мережах, що робить її критично важливим компонентом IT-інфраструктури для багатьох організацій і водночас надзвичайно привабливою мішенню для хакерів. Особливо небезпечною є атака Golden Ticket, що спрямована на підробку квитків системи автентифікації Kerberos і дозволяє зловмисникам підвищувати свої привілеї і отримувати неавторизований доступ до служб і ресурсів у мережі. Точне та швидке виявлення атак підробки квитків Kerberos є критично важливим для захисту мережі на основі Active Directory та вчасного реагування на потенційні загрози.
**Ключові слова:** Kerberos, Active Directory, підробка квитків, контролер домену, авторизація

## Вступ

Active Directory (AD) – це служба каталогів від Microsoft, що використовується для контролю доступом і керуванням ресурсами у мережі. Сьогодні Microsoft AD використовують в своїй інфраструктурі понад 90% компаній зі списку Global Fortune 1000 [1]. Незважаючи на свою популярність, мережі на основі Active Directory є досить вразливими. Атака підробки квитків Golden Ticket дозволяє злочинцю підвищити привілеї і отримати доступ до захищених конфіденційних ресурсів в обхід механізмів авторизації. Тому мережі на основі AD потребують постійного моніторингу і вчасного виявлення зловмисної активності для запобігання потенційні шкоді.

## Kerberos автентифікація

Головні компоненти у системі Kerberos [2]: служба автентифікації (Authentication Service, AS), що відповідальна за автентифікацію клієнта у мережі; Служба видачі квитків (Ticket-Granting Service, TGS), що відповідальна за видачу квитків доступу до сервісів у мережі Active Directory (Service Ticket, ST) і видачу так званих квитків на квитки (Ticket-Granting Ticket, TGT); Центр видачі ключів (Key Distribution Center, KDC) – це служба, яку запущено від імені акаунта krbtgt на контролері домену і яка включає в себе AS і TGS.
Процес автентифікації складається з наступних кроків [3]:

- *KRB_AS_REQ*
  Клієнт надсилає до AS свої дані для автентифікації
- *KRB_AS_REP*
  Клієнт отримує від AS квиток TGT
- *KRB_TGS_REQ*
  Клієнт надсилає до TGS запит на ST до певного сервісу у мережі і вкладає у запит TGT
- *KRB_TGS_REP*
  Клієнт отримує ST із правами відповідно до наданого TGT
- *KRB_AP_REQ*
  Клієнт надсилає ST на сервер застосунку і отримує права, вказані у ST

## Атака Golden Ticket

Атака Golden Ticket [4] спрямована на підробку Kerberos TGT квитка в процесі автентифікації. TGT квитки зашифровані і підписані з використанням паролю krbtgt акаунта, який при нормальному процесії автентифікації відповідальний за видачу TGT. Отже для підробки такого квитка, зловмиснику необхідно скомпрометувати хеш паролю krbtgt. Маючи підроблений TGT, зловмисник отримує змогу створювати квитки до будь-яких сервісів у мережі імперсоніфікуючи будь-якого користувача домену і вказуючи будь-які привілеї, що в свою чергу означає повну компрометацію домена. На основі підробленого TGT

квитка, зловмисник може створювати і ST які вважатимуться валідними, оскільки вся інформація, що вказана в TGT також вважатиметься достовірною. Ці квитки можуть мати довільний час валідності, який не залежить від політик домену. Небезпека цієї атаки обумовлена ще й тим, що пароль krbtgt за замовчуванням майже ніколи не змінюється, за випадком ситуацій, коли оновлюється контролер домена, що робить цю атаку особливо ефективною для закріплення в домені

## Механізм ідентифікації підроблених TGT квитків

Реалізація механізму ідентифікації підроблених TGT квитків базується на співставленні TGT квитків у KRB_AS_REP із квитками у KRB_TGS_REQ. Для цього формується таблиця із усіма квитками TGT, що були знайдені у KRB_AS_REP повідомленнях, тобто видані контролером домена легітимно. Після цього, кожен TGT квиток у запиті KRB_TGS_REP порівнюється із значеннями у створеній раніше таблиці. Якщо відповідностей не знайдено, це означає що контролер домену ніколи не видавав квиток, який пред'являє користувач, і він є підробленим.

## Висновки

В ході дослідження було виявлено сигнатури, які можна використовувати для ідентифікації атаки підробки квитків Kerberos Golden Ticket. Вчасне виявлення атак є критично важливим у мережах, що містять чутливі дані та інформацію з обмеженим доступом.

## Перелік використаних джерел

1. Krishnamoorthi S., Carleton J. Active Directory Holds the Keys to Your Kingdom, But Is It Secure? — 03/20/2020. — URL: https://insights.frost.com/hubfs/Content%5C%20Uploads/DGT/2020/Research%5C%20Preview/ICT/%5C%7B6198df00-ed17-4d0d-bae8-e47a74339398%5C%7D_FS_WP_Alsid-AD_14Feb20-v2_jw.pdf.

2. Garman J. Kerberos: The Definitive Guide. — O'Reilly Media, 16.09.2003. — 274 с. — ISBN 9780596004033.
3. Kerberos Subprotocols. —. — URL: https://learn.microsoft.com/en-us/windows/win32/secauthn/kerberos-subprotocols.
4. MITRE ATT&CK: Steal or Forge Kerberos Tickets: Golden Ticket. —. — URL: https://attack.mitre.org/techniques/T1558/001/

# ПІДХОДИ ДО ФОРМУВАННЯ МОДЕЛІ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

Івко С.О., Смоляр В.Г., Дубик А.М.
Військовий коледж сержантського складу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Полтава, Україна, ck4vkss@ukr.net

Проаналізовано сучасні підходи до мілітаризації кіберпростору. Запропоновані напрями вдосконалення моделі національної системи кібербезпеки. Наведені пропозиції до цілей та завдань воєнної політики України у кіберпросторі.
**Ключові слова:** інформаційна безпека, інформаційно-психологічний вплив, інформаційна операція, кібербезпека, кібероборона, кібервійна.

## Вступ

Кібербезпека стає все більш актуальною темою на національному та міжнародному рівнях. Згідно з дослідженнями, опублікованими у публікаціях[1-3], більшість сильних країн світу, включаючи держави блоку НАТО, США, Росію, Китай, Індію та інші, перетворюють свої військові потенціали з огляду на можливості використання мережі Інтернет. Це означає, що кіберпростір стає все більш важливою сферою для ведення бойових дій, поряд із традиційними "Земля", "Повітря", "Море" та

“Космос”. Спеціалізовані кібер-підрозділи збройних сил багатьох країн світу все активніше діють у цій сфері.

Експерти з кібербезпеки країн НАТО вже пропонують трактувати масштабні кібератаки як такі, що підпадають під 5 статтю Північноатлантичного договору і вважаються атаками на всіх членів Альянсу. Така позиція НАТО відображена і у новій “Стратегічній концепції НАТО” [2].

Наразі, в умовах збройної агресії Російської Федерації, в Україні склалася критична ситуація, коли першочерговим пріоритетом забезпечення національної безпеки є забезпечення воєнної безпеки та оборони держави.

## 1. Сучасні підходи до мілітарізації кіберпростору

Особливість кіберпростору полягає в тому, що на ньому зосереджена тотальна цифровізація озброєнь. Ця реалія має як технологічну, так і людську складові. Серед основних технічних аспектів можна відзначити персональні комп’ютери військовослужбовців, обладнання для операторів безпілотних апаратів, використання технологій SCADA та застосування інформаційних технологій у всіх видів озброєння – артилерійських системах, бронетехніці, літаках, кораблях, ракетах та ручній зброї. Щорічно залежність військової техніки від інформаційно-комунікаційних технологій зростає, що зумовлює необхідність взаємного обміну даними між військовими інфокомунікаційними пристроями, які є неодмінним елементом загального кіберпростору. Така складна ситуація вимагає від військових структур різних країн спеціальної уваги до проблеми кібербезпеки, що стає предметом широкої дискусії як на національному, так і на міжнародному рівнях.

Про рівень занепокоєності провідних держав світу у сфері кібербезпеки свідчить і бажання врегулювати на міжнародному рівні можливість визнання кібератаки “актом війни”. Відома позиція США щодо трактування кібератак на свої комп’ютерні мережі як початку потенційної кібервійни набуває свого продовження і в межах НАТО, що відображено в “Стратегічній концепції НАТО”[4].

## 2. Напрями вдосконалення моделі національної системи кібербезпеки

Для забезпечення кібербезпеки в Україні важливо розглядати державу як партнера суспільства та бізнес-структур. Ефективне державне управління в цій сфері, впорядкування нормативно-правового поля та розвиток інфраструктури кібербезпеки є ключовими компонентами для забезпечення безпеки в кіберпросторі.

Однією з ключових складових забезпечення кібербезпеки країни є національна система кібербезпеки. Вона передбачає об'єднання у форматі співпраці різних суб'єктів, зокрема центральних органів виконавчої влади, військових формувань, правоохоронних органів, органів державного регулювання у сфері інформатизації, електронних комунікацій та захисту інформації, органів місцевого самоврядування, наукових установ і організацій.

Метою створення національної системи кібербезпеки є своєчасне запобігання кіберзагрозам, забезпечення належного рівня обороноздатності та безпеки держави в кіберпросторі, а також оперативне виявлення, запобігання, протидія та розслідування злочинних проявів, які базуються на використанні інформаційних та інформаційно-комунікаційних технологій. Така система має стати ефективним механізмом державного управління у сфері кібербезпеки, який забезпечить впорядкування нормативно-правового поля та розвиток необхідної інфраструктури [4].

В рамках системи пропонується передбачити такі функціональні елементи:

- спеціалізований центр керування та координації діяльності з кібербезпеки, що має на меті забезпечення оперативної реакції на кіберзагрози та організацію співпраці між усіма зацікавленими сторонами;
- відповідальні органи з кібербезпеки, які забезпечують реалізацію стратегії та політики в галузі кібербезпеки на рівні центральних та місцевих органів влади;

- комплекс заходів щодо підвищення кваліфікації кадрів, що забезпечують функціонування та захист інформаційних технологій;
- систему моніторингу та аналізу кіберзагроз, яка дозволяє оперативно виявляти, аналізувати та реагувати на кіберзагрози;
- інформаційно-аналітичний центр з кібербезпеки, який забезпечує аналіз та прогнозування кіберзагроз та розроблення рекомендацій з їх запобігання.

## Висновки

Зазначене дозволить здійснити обґрунтування сучасної моделі національної системи кібербезпеки, в якій визначається склад та порядок взаємодії органів державного управління в національній системі кібербезпеки України.

## Перелік використаних джерел


1. Dubov D.D. Cyberspace as a new dimension of geopolitical rivalry: [Monograph]. Kyiv: The National Institute for Strategic Studies, p.328. 2014.
2. О.Г. Пузиренко, С.О. Івко, О.О. Лаврут Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційно-телекомунікаційних систем, Системи обробки інформації, Вип.8 (124) С. 128-134. 2014.
3. О.Г. Пузиренко, С.О. Івко, О.О. Лаврут, О.К. Климович Застосування моделей оцінювання ризиків інформаційної безпеки в інформаційно-телекомунікаційних системах, Системи обробки інформації, Вип.3 (128) С. 75-79. 2015.
4. Chernonoh O., Ivko S., Moskalenko A. Analysis of the cyber security policy of Ukraine/ Markina I., Aranchiy V., Safonov Y., Zhylinska O. and other. Security management of the XXI century: national and geopolitical aspects. Issue 2: [collective monograph] / in edition I. Markina. - Prague. - Nemoros s.r.o. - Czech Republic. - 138-142 p. 2020.

# ВПЛИВ ПОГОДНИХ УМОВ НА ВИЯВЛЕННЯ БПЛА ПОБЛИЗУ ПІДПРИЄМСТВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА ДОПОМОГОЮ ОЕС

Мятка І.І., Василенко О.Д.
Навчально-науковий Фізико-технічний інститут КПІ ім. Ігоря Сікорського, Київ, Україна

В роботі розглянуто можливість виявлення БПЛА за допомогою тепловізійних пристроїв при різних погодних умовах.
**Ключові слова:** оптико-електронна система, БПЛА, інфрачервоний діапазон, тепловізор, метеоумови.

## Вступ

Виявлення безпілотного повітряного літального апарату (БПЛА) є першою умовою для його протидії. Без виявлення факту польоту в межах контрольованої зони протидія йому за допомогою окремих засобів нейтралізації є неможливою.

В сучасних системах дедалі частіше починає з'являтись оптико-електронна станція (ОЕС) виявлення, основна мета якої – ідентифікація, визначення точних координат цілі та передача їх засобу нейтралізації. Однак основним недоліком системи є сильна залежність від погодних умов, від яких виявлення безпілотника стає менш ефективним.

## Вибір оптимального спектрального діапазону

Сучасні тепловізори працюють в «вікнах» прозорості атмосфери 3 – 5 мкм та 8 – 12 мкм, де поглинання водяною парою є значно меншим ніж в інших спектральних діапазонах.

Експерементальні дослідження оптичного випромінення БПЛА в спектральних діапазонах 3 – 5 мкм та 8 – 12 мкм, які були проведені за допомогою спеціального вимірювального комплексу, дозволили встановити, що потужність випромінення дрону в спектральному діапазоні

3 – 5 мкм є суттєво меншою ніж в діапазоні 8 – 12 мкм. Це пояснюється тим, що в конструкції БПЛА використовується відносно малопотужні двигуни внутрішнього згорання, які інтенсивно охолоджуються повітряним потоком від руху гвинту. Виходячи з вищезазначених факторів можна вважати, що найбільш прийнятним діапазоном в тепловому каналі є «вікно» прозорості 8 – 12 мкм.

## Розрахунок дальності виявлення

Максимальну дальність виявлення малих безпілотних апаратів з температурою Т пасивничи інфрачервоними системами можна визначити за формулою:

$$R_{\text{іч}} = \sqrt{\frac{S_{\text{ц}} * S_{\text{пр}} * \tau_{\text{пр}}}{P_{\text{пор}}} * \int_{\lambda_1}^{\lambda_2} \tau_{\text{ср}}(\lambda) * J_{\text{с.т}}(\lambda) d(\lambda)}$$

Для розрахунку була вибрана камера серії Titanium, робочий діапазон якої 3 – 5 мкм, 8 – 12 мкм та додатково 1,5 – 5 мкм. В якості БПЛА було обрано модель «DJI Mini 2 Fly More Combo».

Спектральний коефіцієнт пропускання середовища розраховується по формулі:

$$\tau(\lambda) = \tau_{\text{п}}(\lambda) * \tau_{\text{о}}(\lambda)$$

В результаті обрахунків отримана наступна діаграма залежності дальності виявлення від аерозольних частинок (Рис. 1).

## Висновки

В результаті роботи було обрано оптимальний спектральний діапазон роботи тепловізора для виявлення дронів. Найбільший вплив вносить злива, легкий та густий туман, що пояснюється високим вмістом частинок крапель на 1 км атмосферної траси. Використання ОЕС для цілодобового, автономного контролю за повітряним простором є неефективним через високе падіння прозорості атмосфери на великих відстанях та сильну залежність від погоди.

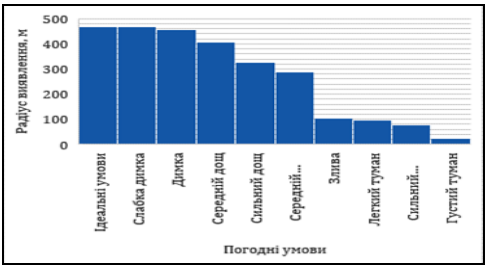


Рисунок 1. Діаграма залежності дальності виявлення від аерозольних частинок

Використання тепловізійного каналу виявлення буде оптимальним при застосуванні його в парі з радіолокаційною станцією (РЛС) для ідентифікації та отримання відповідних параметрів БПЛА та передача їх для засобів нейтралізації. Ефективність системи зростає зі зменшенням відстані від цілі до тепловізора, збільшенням розмірів БПЛА або діаметра лінзи тепловізора, збільшенням абсолютної температури дрону та з покращенням погодних умов.

## Перелік використаних джерел

1. Даник Ю. Г., Бугайов М. В. Аналіз ефективності виявлення тактичних безпілотних літальних апаратів пасивними та активними засобами спостереження // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. — 2015. — С. 5—18.

2. Якушенков Ю. Г. Теория и расчет оптико-электронных приборов. — 4-е,переработанное и дополненное. — М.: Логос, 1999. — 500 с.

3. Смолин В. А., Якименко И. В., Рассказа Д. С. Оптико-информационный метод обнаружения беспилотных воздушных судов роботизированной оптико-электронной системой. — 2022.

# ОБРОБКА ПРИРОДНОЇ МОВИ ІЗ ВИКОРИСТАННЯМ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ З МЕТОЮ ЗАПОБІГАННЯ ШАХРАЙСТВУ

Дрозд С.Ю.
Навчально-науковий Фізико-технічний інститут, НТУУ «КПІ ім. Ігоря Сікорського», м. Київ, Україна

У роботі розглянуто розпізнавання шахрайських оголошень за допомогою обробки природної мови та методів машинного навчання. Для розширенні класу шахрайських оголошень було створено синтетичні зразки даних, застосовували алгоритми балансування. Досліджували та порівнювали точності різних алгоритмів класифікації на датасетах, збалансованих різними способами без та з синтетичними зразками. Виявлено, що використання синтетичних даних покращує якість класифікації. Найефективнішим методом балансування був SMOTE-NC, а найкращим алгоритмом класифікації - MLPClassifier. Розроблена модель ефективно виявляє шахрайські оголошення, зменшуючи ризик шахрайської діяльності.
**Ключові слова:** фішинг, обробка природної мови, машинне навчання, синтетичні дані

## Вступ

Україна та Європа неспроможні забезпечити соціальним житлом багатомільйонний потік мігрантів [1], що виник після початку війни з Росією 24 лютого 2022 року. Тому у пошуках житла біженці звертаються до Інтернету, що створює сприятливі умови для поширення онлайн-шахрайства. Зараз зловмисники успішно проникають на відомі онлайн-платформи, такі як Booking, Craigslist чи OLX [2]. Тому проблема шахрайства в сфері оренди житла є дуже актуальною.

Багато звичайних методів боротьби з фішингом, таких як методи білих і чорних списків, пошук аномалій, тощо, не є достатньо ефективними, бо шахраї обманюють жертву до

того, як їх оголошення будуть розпізнані та видалені. Тому потрібно залучати нові методи для протидії фішингу.

Метод, пропонований у даній роботі, оснований та обробці природної мови за допомогою штучного інтелекту. Головна мета роботи полягає у визначенні ефективності застосування такого підходу для виявлення шахрайства і розробці ефективно класифікатора для виявлення фіктивних оголошень.

## Дані

Для дослідження було використано відкритий набір даних з платформи GitHub, який містить записи про оренду житла з міжнародного сайту оголошень Craigslist.
Набір даних складається з 2487 оголошень (2469 правдивих та 18 шахрайських), тобто співвідношенням фальшивих та реальних зразків 1:152 відповідно, що свідчить про значний дисбаланс вибірки. Для вирішення цієї проблеми було згенеровано додаткові синтетичні зразки даних за допомогою розширеної нейронної мережі LSTM (11 нових шахрайських оголошень) та мовної моделі чат-боту ChatGPT (75 шахрайських оголошень). Крім того, вихідні датасети (з та без синтетичних даних окремо) були оброблені за допомогою кількох алгоритмів балансування окремо, з подальшим аналізом для вибору найкращого.

Для навчання і тестування класифікаторів вибірки були поділені у пропорції 60% до 40% відповідно із стратифікацією за класом і походженням (справжні, синтетичні).

## Методи

Архітектура моделі LSTM для генерації синтетичних даних зображена на Рис. 1.

Для отримання синтетичних оголошень з ChatGPT, чат-боту було надано реальні оголошення як приклад та послано запит на генерацію подібних зразків.

Для балансування датасету використовували випадкову надмірну та недостатню вибірку, SMOTENC та класове зважування.

Для розпізнавання фішингових оголошень аналізували 7 алгоритмів класифікації – метод k-найближчих сусідів (KNN), наївний Байєсівський класифікатор (MNB), дерево рішень (DTC), випадковий ліс (RFC), метод опорних векторів (SVM), логістична регресія (LR), багатошаровий перцептрон (MLP). Таким чином всього було отримано 70 моделей. Для визначення найкращої моделі в задачі розпізнавання шахрайських оголошень використовували наступні метрики для вимірювання точності: precision (1), recall (2), f1-score (3), roc-auc (4).

$$precision = \frac{(TP+FP)}{TP}, \quad (1)$$

$$recall = \frac{TP+FN}{TP}, \quad (2)$$

$$f1-score = 2 * \frac{Precision+Recall}{(Precision*Recall)} \quad (3)$$

$$ROC-AUC = \int \left(\frac{TP}{TP+FN}\right)\left(\frac{FP}{FP+TN}\right) d\left(\frac{FP}{FP+TN}\right) \quad (4)$$

## Результати

Результати класифікаторів, навчених на збалансованих даних з синтетичними та без синтетичних зразків, наведені на тепловій карта на рис. 2.

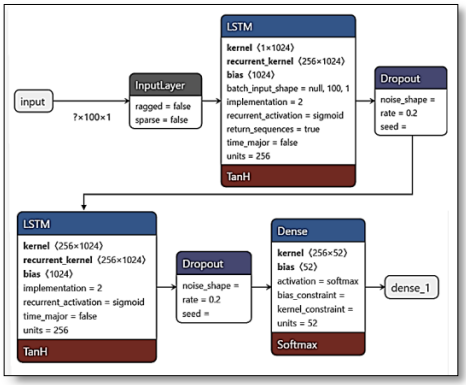


Рисунок 1. Архітектура нейронної мережі LSTM для генерації синтетичних оголошень

Було встановлено, що додавання синтетичних зразків суттєво впливає на покращення точності класифікації. З Рис. 2, найкращою комбінацією для розпізнавання шахрайських оголошень про оренду є алгоритм балансування SMOTE-NC, застосований на датасеті з синтетичними зразками, та модель MLPClassifier( MLP), навчена на даному датасеті (roc-auc 0.997, recall 0.9, precision 0.99 та f1-score 0.94)

## Висновки

В цій роботі досліджували метод для виявлення шахрайських оголошень про оренду за допомогою обробки природної мови з використання штучного інтелекту. Для навчання моделей використовувалися дані з синтетичними та без синтетичних зразків, застосовувалися різні методи балансування.

| Balance method | Model | Real data | | | | Real+synthetic data | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | roc-auc | precision | recall | f1-score | roc-auc | precision | recall | f1-score |
| random oversampling | DTC | 0,72 | 0,96 | 0,45 | 0,59 | 0,83 | 0,97 | 0,67 | 0,79 |
| | KNC | 0,64 | 0,96 | 0,20 | 0,33 | 0,86 | 0,97 | 0,65 | 0,78 |
| | LR | 0,95 | 0,97 | 0,57 | 0,71 | 0,97 | 0,98 | 0,83 | 0,90 |
| | MLP | 0,94 | 0,80 | 0,16 | 0,25 | 0,99 | 1,00 | 0,79 | 0,88 |
| | MNB | 0,95 | 0,80 | 0,18 | 0,29 | 0,98 | 1,00 | 0,60 | 0,74 |
| | RFC | 0,92 | 0,20 | 0,03 | 0,05 | 0,99 | 1,00 | 0,71 | 0,83 |
| | SVC | 0,90 | 0,81 | 0,77 | 0,77 | 0,91 | 0,92 | 0,65 | 0,76 |
| SMOTE-NC | DTC | 0,76 | 0,96 | 0,54 | 0,66 | 0,90 | 0,98 | 0,82 | 0,89 |
| | KNC | 0,85 | 0,94 | 0,65 | 0,76 | 0,92 | 0,96 | 0,80 | 0,87 |
| | LR | 0,97 | 0,98 | 0,48 | 0,63 | 0,99 | 0,98 | 0,89 | 0,93 |
| | MLP | 0,97 | 0,96 | 0,16 | 0,27 | 1,00 | 1,00 | 0,88 | 0,94 |
| | MNB | 0,96 | 1,00 | 0,21 | 0,33 | 0,99 | 1,00 | 0,65 | 0,78 |
| | RFC | 0,95 | 0,20 | 0,04 | 0,06 | 1,00 | 1,00 | 0,82 | 0,90 |
| | SVC | 0,93 | 0,81 | 0,86 | 0,82 | 0,92 | 0,92 | 0,65 | 0,76 |
| random downsampling | DTC | 0,69 | 0,67 | 0,80 | 0,72 | 0,82 | 0,82 | 0,82 | 0,82 |
| | KNC | 0,83 | 0,87 | 0,80 | 0,82 | 0,86 | 0,92 | 0,75 | 0,82 |
| | LR | 0,87 | 0,80 | 0,86 | 0,82 | 0,94 | 0,94 | 0,81 | 0,86 |
| | MLP | 0,78 | 0,85 | 0,66 | 0,66 | 0,99 | 0,80 | 0,73 | 0,76 |
| | MNB | 0,86 | 0,00 | 0,00 | 0,00 | 0,92 | 0,60 | 0,02 | 0,03 |
| | RFC | 0,88 | 0,71 | 1,00 | 0,82 | 0,99 | 0,93 | 0,97 | 0,95 |
| | SVC | 0,86 | 0,86 | 0,83 | 0,83 | 0,91 | 0,95 | 0,65 | 0,77 |
| class weighting | DTC | 0,68 | 0,22 | 0,37 | 0,27 | 0,82 | 0,66 | 0,66 | 0,66 |
| | KNC | 0,64 | 0,21 | 0,20 | 0,20 | 0,85 | 0,61 | 0,65 | 0,63 |
| | LR | 0,95 | 0,60 | 0,09 | 0,15 | 0,96 | 0,88 | 0,45 | 0,60 |
| | MNB | 0,89 | 0,00 | 0,00 | 0,00 | 0,90 | 0,50 | 0,02 | 0,03 |
| | RFC | 0,97 | 0,00 | 0,00 | 0,00 | 0,99 | 0,98 | 0,67 | 0,80 |
| | SVC | 0,93 | 0,05 | 0,80 | 0,09 | 0,91 | 0,38 | 0,66 | 0,48 |

Рисунок 2. Теплова карта точностей побудованих класифікаційних моделей

Аналіз показав, що використання синтетичних зразків покращує точність класифікації. Методи балансування, що змінюють розмір датасету, були ефективнішими. Найточнішою моделлю була MLPClassifier з високими показниками roc-auc, recall, precision та f1-score. Розроблена

модель може допомогти виявляти шахрайські оголошення про оренду та зменшити ризик шахрайства.

## Перелік використаних джерел


1. Вплив повномасштабної війни на міграцію українців: як масштаби переміщення оцінюють держава Україна та міжнародні організації [Електронний ресурс] // Опора. – 2022. – Режим доступу до ресурсу: https://www.oporaua.org/report/viyna/24523-vpliv-povnomasshtabnoyi-viini-na-migratsiiu-ukrayintsiv-iak-masshtabi-peremishchennia-otsiniuiut-derzhava-ukrayina-ta-mizhnarodni-organizatsiyi .
2. Шахраям – ні: що варто знати про пошук та оренду житла під час війни [Електронний ресурс] // OLX. – 2022. – Режим доступу до ресурсу: https://blog.olx.ua/28224/shho-varto-znati-pro-poshuk-ta-orendu-zhitla-u-period-vijni/.


# ВИЯВЛЕННЯ КІБЕРАТАК ПРИ ЗАСТОСУВАННІ АНОМАЛЬНОГО ДЕТЕКТУВАННЯ ЧАСТКОВО РОЗМІЧЕНИХ ДАНИХ


Палагін Д.В.[1], Палагіна О.А.[2], Івченко О.В.[3], Палагін В.В.[4]
[1]Universite Sorbonne Paris Nord, France
[2, 3, 4]Черкаський державний технологічний університет, Черкаси, Україна



Запропоновано новий метод реалізації напівавтоматичного навчання, який дозволяє використовувати не весь набір розмічених даних для розв’язання задачі аномального детектування, а лише тієї частини, яка задовольняє заданій точності. Такий підхід суттєво скорочує як час, так і фінансові ресурси при підготовці даних при побудові моделей машинного навчання для виявлення кібератак та загроз при передачі даних.



**Ключові слова**: кібератака, машинне навчання, напівавтоматичне виявлення аномалій.

## Вступ

Захист інформації, яка зберігається, обробляється та передається в комп'ютерних системах і мережах, є одним з ключових завдань в контексті інформаційної безпеки. Виявлення кібератак у великих комп'ютерних мережах має вирішальне значення для багатьох організацій [1]. З цією метою різні типи детекторів аналізують дані, що може надати відомості про наявність атак і створення небезпек на окремі комп'ютерні системи. Такий результат аналізу доводиться до відома аналітика безпеки, який приймає відповідні необхідні рішення. Автоматизація цього процесу відіграє ключову роль у якості і оперативності прийнятих рішень.

Виявлення кібератак за допомогою методів машинного навчання є новим і перспективним напрямком обробки даних. Основою виявлення кібератак є аналіз даних, які відносяться до аномальних [2]. Аномалії, які часто називають рідкісними подіями або девіантами, - це дані або шаблони даних, які не відповідають поняттю нормальної поведінки. Виявлення аномалій даних забезпечує виявлення кібератак у реальному часі, відстежує аномальну поведінку користувачів, що захищає підприємства від загроз.

Кожному алгоритму машинного навчання потрібні дані, на яких навчаються і будуються моделі. Але при величезній кількості даних насправді маркується лише невелика їх частка алгоритмічно чи вручну. Отримання маркованих даних часто вимагає кваліфікованої людини (експерта) або фізичного експерименту. Тому повна реалізація маркування даних може зробити процес навчання нездійсненним.

При класифікації даних моделі можна надати «підказку», як будувати певні категорії даних. В цьому випадку модель буде працювати точніше на основі інших даних, які вже марковані. Для цих цілей використовуються напівавтоматичні методи навчання – Semi-supervised learning, коли маркується тільки частина даних. Такий підхід активно розвивається і може мати велике практичне

значення, але і він теж може виявитися достатньо ресурсозатратним.

Метою роботи є підвищення ефективності алгоритмів машинного навчання шляхом виявлення аномалій в даних для задач кібербезпеки при застосуванні нового методу частково розмічених даних.

## Метод напівавтоматичного виявлення аномалій при позитивних і нерозмічених даних

Вхідні дані для алгоритмів бінарної класифікації, зазвичай характеризуються двома різними наборами. Один набір - це «позитивні» вхідні дані x, для яких мітка y=1 (аномальні дані), а інший набір «негативний» – характеризується протилежними властивостями даних x, для яких y=0 (нормальні дані). Нехай доступні вхідні дані містять лише неповний набір позитивних даних та набір немаркованих даних, які можуть бути як позитивними (y=1), так і з протилежними властивостями (y =0). Таке маркування може виникнути тоді, коли частково маркуються тільки позитивні набори (аномалії), але не на всьому наборі.

Необхідно отримати традиційний двійковий класифікатор з врахуванням нетрадиційного навчального набору даних. Адаптуємо дану задачу для виявлення аномальних даних та побудови програмних засобів його реалізації для *позитивних та немаркованих даних* (ПНД).

Нехай набір даних x розподілений на два класи і має бінарне маркування $y \in \{0,1\}$. Позначимо умову маркованих даних x, як $m = 1$, і не маркованих даних, як $m = 0$. Для сформульованої умови задачі тільки позитивні набори є марковані, для яких $y = 1$ при $m = 1$. При $m = 0$ немарковані дані x можуть бути позначені як $y = 0$, або $y = 1$. З урахуванням набору даних, в якому ми маємо позитивні та немарковані дані, ймовірність того, що певна вибірка є позитивною $P(y = 1)$, дорівнює ймовірності того, що вибірка позначена як маркована $P(m = 1)$, розділена на ймовірність того, що позитивна вибірка є маркованою в наборі даних $P(m = 1|y = 1)$.

Хоча немає достатньо позначених даних для навчання класифікатора, щоб визначитися, чи є вибірка позитивною чи негативною, у сценарії ПНД достатньо маркованих даних для визначення позитивної вибірки, як маркованої. Цього припущення достатньо, щоб оцінити ймовірність того, що вибірка є позитивною.

Проведені чисельні експерименти на тестових наборах даних, зокрема при використанні методу XGBClassifier, показали наступне. Часткове маркування позитивних даних на рівні 50% дає показник ефективності порядку f1=0.75 для тестової вибірки, яка складає 30% від 10000 даних (в модельному прикладі всього 1% аномалій, тобто 100 даних). Приблизно така сама ефективність досягається і при частковому наборі даних (20%), але при повному маркуванні, що потребує 1400 маркувань для тренувального набору (весь тренувальний набір складає 7000 даних). В той же час застосування запропонованого методу (ПНД) дало змогу промаркувати тільки 50% аномальних даних в тренувальному наборі, що склало всього 35 даних. Таким чином, до *40 разів* потрібно менше ресурсів для підготовки даних у порівнянні з традиційним підходом при досягненні однакової ефективності.

## Висновки

Запропонований новий метод напівавтоматичного виявлення аномалій на основі часткового маркування позитивних даних показав свою високу ефективність у порівнянні з традиційним підходом, що суттєво заощаджує ресурси на підготовку даних для алгоритмів машинного навчання при виявленні кіберзагроз.

## Перелік використаних джерел

1. Marina Evangelou, Niall M. Adams, “An anomaly detection framework for cyber-security data”. Computers & Security, 97(10):101941, 2020.
2. Anna L Buczak and Erhan Guven, “A survey of data mining and machine learning methods for cyber security

intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016

# AN APPROACH TO ANOMALY DETECTION METHODS CLASSIFICATION

Shovak M.I., Tkach V.M.

National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Educational and Scientific Institute of Physics and Technology, Kyiv, Ukraine

The article is devoted to the classification of anomalies in the context of cyber protection and information protection. The article describes various types of anomalies that can be identified during various attacker attacks. Also described is a list of detection methods that are best used to detect certain types of anomalies. The taxonomy can be useful for building a comprehensive protection system and quickly identifying anomalies over time.

**Keywords:** taxonomy, anomaly, attack, classification, detection methods.

## Introduction

One of the vital aspects of maintaining cyber security there is detection of anomalies[1]. The classification method allows displaying various types of anomalies, organizing them into separate categories and simplifying the process of detecting vulnerabilities in the system[3]. Different types of anomalies can be seen in different phases of attacks, so it is important to have an understanding of what anomalies can be observed in each phase and how they can be detected. The research was conducted on the example of real attack scenarios and the use of various tools to detect anomalies. The results of this work will help improve approaches to cyber protection and ensure more effective protection of information in the modern digital world.

## Types of anomalies

In this work, a classification is based on anomalies that can be encountered during various types of attacks and the data in which they are observed. After conducting an overview of modern attack techniques, it was possible to identify the following categories:

1. Anomalies in user behavior: these anomalies occur when users behave unusually for their usual way of doing things, or when they perform actions that have no logical explanation.
2. Network traffic anomalies: these anomalies are associated with abnormal network activity, such as excessive traffic or unusual addressing.
3. Anomalies in syslogs: these anomalies are related to changes in syslogs, such as an unusual number of entries or changes in critical entries.
4. Data Anomalies: these type of anomalies occurs when the data stored in the system contains errors or unexpected values.
5. Resource anomalies: this type of anomalies occurs when the system consumes too many resources (such as CPU, RAM, disk, etc.) or when some resources are misused.
6. Software Anomalies: these are unusual events or system conditions that indicate software problems. These can be errors in the code, vulnerabilities that can be used to hack the system or lose data.
7. Anomalies in the system architecture: this is a deviation from the normal architectural design of the system, which may be the result of errors in the design, development and implementation of the system, or as a result of its modifications.
8. Anomalies in identification and authentication: these anomalies are related to security and ensuring access to the system or resources. Anomalies in identification occur when the user cannot be identified or identified incorrectly. Also, authentication anomalies occur when a user is identified correctly but cannot access a resource.

9. Anomalies in protection against vulnerabilities: this type of anomalies occurs when the system cannot effectively protect itself against potential attacks using known vulnerabilities. For example, these may be deviations from best practices defenses in various systems; human errors in the configuration systems.
10. Cloud anomalies: these are anomalies that occur in cloud computing environments due to unauthorized access to cloud resources or unusual cloud activity.
11. Time-related anomalies: these are anomalies that arise as a result of unusual activity that occurs at a certain time.

## Classification of anomaly detection methods

Methods are usually divided into three classes: behavioral methods, computational intelligence methods, and machine learning methods. [2] Systems that are built on behavioral methods use the method of comparing current indicators with a pattern of normal behavior to detect anomalies and signal a possible attack. Behavioral methods include: **Statistical analysis**, **Wavelet analysis**, **Fractal analysis**, **Models based on finite state machines**.

Computational intelligence methods use computer algorithms to detect anomalies. These methods are usually used to solve problems for which traditional mathematical methods are not effective or suitable[4]. Computational intelligence methods include: **Models based on neural networks**, **Genetic algorithms**, **Method of support vectors**, **Models based on nonlinear dynamics**, **Role algorithms**.

Machine learning methods are an approach to solving artificial intelligence problems, which is using algorithms and statistical models to make predictions, identify patterns, classify objects and perform other actions on the basis of data. The result of such an analysis can be the detection of unknown anomalous events that can be potentially harmful to the system. Machine learning methods include: **Decision trees**, **Bayesian networks**, **Cluster analysis**, **Regression algorithms**.

## Mapping types of anomalies to methods of their detection

The most versatile methods for detecting anomalies are statistical methods and clustering algorithms. You can read more about the mapping of anomalies to detection methods at the link: “Mapping of anomalies to detection methods”

## Conclusions

Based on the received information, 11 types of anomalies were identified, which differ in their characteristics and source of occurrence. To ensure the security of information systems, the classification of methods for detecting abnormal behavior was considered. A list of methods that would be appropriate to use for each type of anomaly was analyzed and selected. In the field of cybersecurity, the most common methods are statistical methods, machine learning-based models, and neural network-based methods. In general, the most effective anomaly detection models depend on the type of data being used and the context in which it is being used. In practice, a combination of different models and methods can give better results in detecting anomalies.

## References


1. "Anomaly" ScienceDirect [Electronic resource] – Resource access mode: https://www.sciencedirect.com/topics/computer-science/anomaly
2. Lykhosherst, V. R. Algorithm of DenStream classification and cluster analysis for solving information security problems. — 2021
3. "Anomaly detection" [Electronic resource] – Resource access mode: https://www.ibm.com/topics/anomaly-detection
4. A review of unsupervised anomaly detection methods for time series by Chandola, Varun, Arindam Banerjee, and Vipin Kumar. ACM computing surveys (CSUR) 45.1 (2013): 1-41. https://dl.acm.org/doi/10.1145/2523813

# БЕЗПЕКА ВІРТУАЛЬНОЇ ІНФРАСТРУКТУРИ В ПРОЦЕСАХ DEVOPS

Є. О. Носова, В. В. Демчінський
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», НН Фізико-технічний інститут. Київ, Україна
**Ключові слова:** DevOps, LAMP, модель загроз, DevSecOps фреймворк, автоматизація.

## Вступ

Стек LAMP — це популярна платформа веб-розробки, яка складається з Linux, Apache, MySQL і PHP. Разом із зростанням популярності LAMP стеку збільшується ймовірність атак на системи, які його використовують.

Суб'єктом загроз є зовнішній зловмисник, який може діяти від лиця як користувача так і адміністратора, та внутрішній зловмисний користувач, який може діяти від особи адміністратора. Точкою входу в систему є веб-застосунок вордпресу, Google Cloud консоль, API або сервіс. Базовими контролями безпеки є шифрування даних по протоколу HTTPS та шифрування даних на збереженні у сховищі та базі даних.

## DevSecOps фреймворк для реалізації автоматизованого захисту LAMP-стеку

Незважаючи на те, що безпека важлива при розробці системи, часто вона отримує нижчий пріоритет, ніж бізнес-пріоритети. Часто безпека застосовується наприкінці розробки як вимушене вбудовування у вже розроблений дизайн. Для забезпечення безпеки системи, усунення вразливостей і захисту від різних загроз, більш ефективним способом є створення засобів контролю безпеки на кожному етапі розробки, розгортання та експлуатації системи.

Наведений фреймворк забезпечує безпеку протягом усього робочого процесу. Так, під час стадій планування, кодування та коммітування,необхідні такі контролі, як

створення метрик безпеки, рецензування коду, реєстрації його в безпечному репозиторії коду та тестування під час розробки та виправлення несправних збірок. В фазах збірки, інтеграції та пакування необхідно провести перевірку залежностей, забезпечити безпеку контейнерів та проаналізувати склад ПЗ. Протягом стадій пакування, випуску та конфігурації необхідно провести тестування на проникнення, навантажувальне, продуктивне та регресійне тестування.Під час конфігурації, затвердження та розгортання необхідно зміцнити та протестувати інфраструктуру, провести тестування безпеки та застосувати патчі безпеки.Та протягом стадій розгортання, моніторінгу і адаптації необхідно зробити сповіщення безпеки для обробки інцидентів, запровадити безперервне сканування вразливостей, провести пентести та посилити безпеку. Протягом всіх цих стадій отримується безперервнний зворотній зв'язок та тестування, завдяки яким формуються нові вимоги та пріорітети, що запускає цикл розробки повторно.

## Реалізація автоматизованого захисту LAMP-стеку у хмарному середовищі

Для реалізації LAMP стеку в даній роботі використовується операційна система Ubuntu 20.04, MySQL 8.0 та PHP додаток - Wordpress, в якості хмарного середовища використаємо Google Cloud Platform.

Для забезпечення безпечного зовнішнього доступу до внутрішньої мережі ми будемо використовувати бастіонний хост (JumpHost). Через айпі адресу бастіону ми будемо виконувати ssh підключення до серверів, що знаходяться у хмарі. З метою безпеки ми також будемо використовувати інший порт замість стандартного 22 порту. Ми можемо бачити хост бастіону поряд з серверами WordPress.

На серверах Wordpress ми встановлюємо ModSecurity в якості брандмауеру безпеки веб-додатків, Fail2Ban для протидій брутфорс атакам, та ClamAV для захисту від вірусів. Також ми налаштуємо OAuth2, двохфакторну автентифікацію, для захисту від підбору/витоку паролів.

Окрім цього, всередині самого Wordpress ми скористаємося плагінами Wordfence для захисту від атак спрямованих на Wordpress. В якості інструмента для проведення аудіту ми скористаємося інструментом з відкритим кодом Lynis.

В якості SIEM системи був реалізований ELK - (Elasticsearch, Logstash, Kibana). Окрім цього, на серверах Wordpress ми встановили Filebeat - легкий інструмент для пересилання даних журналу подій.

В якості системи виявлення вторгень ми використаємо Cloud IDS та розмістимо її перед брандмауером. Для автоматизації були використані такі інструменти як Ansible і Terraform.

## Висновки

Проведене дослідження та запропоновані міри безпеки доводять, що використання DevSecOps у реалізації автоматизованого захисту LAMP-стеку у хмарному середовищі дозволяє забезпечити високий рівень безпеки, надійність та ефективність роботи програмного забезпечення. Це реалізується за допомогою включення безпеки з самого початку розробки, що сприяє ранньому виявленню та виправленню потенційних вразливостей. Це досягається завдяки постійній інтеграції безпекових інструментів та процесів у розробку, швидкому виявленню та реагуванню на потенційні загрози, а також забезпеченню безперебійної роботи LAMP-стеку в хмарі.

## Перелік використаних джерел

1. Dharmaratna, N. S., & Disanayake, C. (2021). A Mini Security Framework for LAMP Stack Deployments on the Cloud-Research Proposal. Methodology, 1, 8.

2. Tonello, J. S. (2022). Extend Your DevOps Capabilities with Git. In Practical Linux DevOps: Building a Linux Lab for Modern Software Development (pp. 279-310). Berkeley, CA: Apress.

3. Kumar, R., & Goyal, R. (2020). Modeling continuous security: A conceptual model for automated DevSecOps using

open-source software over cloud (ADOC). Computers & Security, 97, 101967.

# USE OF BLOCKCHAIN TECHNOLOGY TO PROTECT WEB-BASED ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

Piroh O.V.
Zhytomyr Polytechnic State University,
Zhytomyr, Ukraine, e-mail: pirogov@ztu.edu.ua

The article discusses the main modern trends in the use of blockchain and its use by government. The main document management web services have been analyzed, including those that have an expert opinion on compliance with technical information protection requirements in Ukraine.
**Keyword:** electronic document management systems, EDMS, blockchain.

Forbes talked about the main trends in the use of blockchain, which will cover numerous activity areas (Marr, 2021), namely:

- Tracking and distribution of vaccines.
- Enterprise blockchain (banking and financial services).
- Tokens (NFT, non-fungible token) for digital assets (images, music, code).
- Blockchain as a service.

Gartner analysts have published a list of recommendations on the areas in which government agencies should implement blockchain (Goasduff, 2021). According to researchers forecasts, by 2025 blockchain technologies will become the basis for a global decentralized identification system. Government officials considering the possibility of using blockchain already have a number of practical options for using this technology:

1. Elections.
2. Social services.
3. Digital assets markets.
4. Increasing efficiency.

5. Document management.

Let's consider the main web services currently used for document management.

The most famous and used services are Google Drive, Dropbox and OneDrive.

Google Drive integrates with third-party applications, including DocuSign for electronic signatures, CloudLock for additional layers of security, and LucidCharts for layouts.

Dropbox (Microsoft). Advanced sharing allows only selected users to see important files, and files can be remotely erased if sensitive data is compromised.

OneDrive ensures cross-platform synchronization and prevents data loss.

Next, we will provide a list of applications that have an expert opinion on compliance with the requirements of technical information protection in Ukraine (State service of special communication and information protection of Ukraine, n.d.).

MODX has data backup and attribute-based access control, the ability to create HTML templates. Additionally, there are snapshot that allow you to clone sites. MODX has API.

Tresorit is a cloud-based file synchronization and sharing solution with encryption. Offers remote device cleaning, file recovery, file history and two-factor authentication. The service has role-based access rights. The solution is GDPR and HIPAA compliant, ISO 27001 certified and a member of the Trusted Cloud and Cloud Security Alliance.

FileCloud is a secure platform for enterprises, educational institutions and government organizations. The service provides sharing control, management, data leakage protection and digital rights management are fully integrated into public, private or hybrid cloud models.

SmartVault is document management software. The service offers two-factor authentication, file version control, payment processing, collaboration management, electronic signature fixation and more. CCPA, GDPR, SEC, GLBA, FINRA compliance. SmartVault makes it easy to integrate with various third-party applications (Salesforce, Hubdoc, TaxCalc, Xero, FreshBooks, Method CRM, Microsoft Outlook).

iDOC is a document management tool, a control system and an adaptive mobile version. The system allows you to sign documents and online contracts with clients using EDS.

CleverForms ensures the creation, registration, saving of electronic documents and scanned originals of documents, signing of electronic documents in accordance with DSTU 4145-2002. It meets the requirements of the current DSTU, meets the requirements of the Law of Ukraine "On Electronic Documents and Electronic Document Circulation", the Law of Ukraine "On Electronic Trust Services".

Megapolis.DocNet is a business tool covering all stages of the documents life cycle to archival storage with an electronic signature. The system is built on the UnityBase platform, which allows various types of authentication: Basic, Digest, based on the client's IP address, Negotiate (Kerberos, NTLM), based on RSA public / private keys, OpenIDConnect. To prevent man-in-the-middle attacks, CSRF attacks, each request is accompanied by a unique signature. The service provides role-based access control. It has an audit journal.

Various private platforms (for example, IBM Hyperledger Fabric, Corda, Waves Enterprise) allow for confidential data exchange within the blockchain network in various ways, mainly due to the interaction of private databases outside the blockchain network with data hash storage in the blockchain.

Corda is an open source blockchain platform. There is also its commercial edition - Corda Enterprise. Corda Enterprise extends the Corda edition and supports additional features, including support for commercial databases (Oracle, MSSql), HSM, increasing productivity (parallel thread execution), high availability node setup and tools for Corda network deployment.

Hyperledger Fabric is an open source blockchain framework that enables the development of blockchain-based products, solutions and applications. It has a modular architecture.

Waves Enterprise is a hybrid enterprise blockchain platform that integrates public and private network approaches.

Thus, there are many offers of online document management systems in the enterprise price segment, even with the use of blockchain technologies. In the low price segment

document protection offers are possible either for an additional price or with the use of third-party tools, connected or developed.

The author developed, modeled and tested the web application for registering electronic documents using blockchain technology.

## Reference


1. Marr, B. (2021). The 5 Biggest Blockchain Trends In 2022. *Forbes.* https://www.forbes.com/sites/bernardmarr/2021/11/19/the-5-biggest-blockchain-trends-in-2022/
2. Goasduff, L. (2021). Leaders must determine the suitability of blockchain and set the right expectations. *Gartner.* https://www.gartner.com/en/articles/how-governments-can-successfully-embark-on-any-blockchain-project
3. Software Advice. (n.d.) https://www.softwareadvice.com/
4. State service of special communication and information protection of Ukraine. (n.d.) Technical information protection tools list that have an expert opinion on compliance with the requirements of technical information protection. https://cip.gov.ua/ua/news/zasobi-tzi-yaki-mayut-ekspertnii-visnovok-pro-vidpovidnist-do-vimog-tekhnichnogo-zakhistu-informaciyi


# ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ПРОТОКОЛУ MQTT


Бурячок А.А., Носок С.О.
Навчально-науковий Фізико-технічний інститут, КПІ ім. Ігоря Сікорського, м. Київ, Україна



Робота присвячена ознайомленню з технологією Інтернету речей та його особливостями, аналізу протоколів обміну повідомленнями та дослідженню вразливостей протоколу

MQTT. Розглянуто основні небезпечні місця в системах та пристроях, які можуть призвести до витоку конфіденційних даних або реалізації масованих атак.
**Ключові слова:** Інтернет речей, вразливості, протокол обміну повідомленнями, MQTT.

## Вступ

Зі стрімким розвитком Інтернету речей забезпечення безпеки в таких системах стало першочерговою проблемою. Оскільки мільярди взаємопов'язаних пристроїв спілкуються та обмінюються даними між собою, вразливості та загрози, які пов'язані з конфіденційністю, цілісністю та доступністю, привертають все більше уваги.

Протокол MQTT став популярним вибором для ефективного та легкого обміну повідомленнями між пристроями. Однак, не зважаючи на його широке застосування, він може становити серйозні виклики безпеці систем, в яких використовується.

## Інтернет речей

Інтернет речей – це концепція, що описує мережу фізичних об'єктів або «речей», які мають вбудовані датчики, програмне забезпечення, електроніку та інші технології для забезпечення підключення та обміну даними з іншими пристроями та системами через Інтернет.

Основна ідея полягає в тому, щоб замість обмеженої кількістю потужних обчислювальних пристроїв, таких як ноутбук, планшет або телефон, мати велику кількість менш потужних пристроїв, таких як парасолька, дзеркало або холодильник [1].

## Протоколи обміну повідомленнями

Протоколи обміну повідомленнями відіграють вирішальну роль у полегшенні зв'язку між пристроями в екосистемі Інтернету речей. Вони визначають правила та формати для передачі та отримання повідомлень, що забезпечує безперебійну взаємодію та обмін даними.

Згідно з публікацією [2], можна виділити найпопулярніші протоколи обміну повідомленнями, серед яких HTTP, MQTT, CoAP. Кожен з них має свої сильні та слабкі сторони та використовується в тих чи інших системах, в залежності від її вимог.

## Вразливості протоколу MQTT

MQTT (Message Queuing Telemetry Transport) – це легкий протокол обміну повідомленнями, який зазвичай використовується мережах з низькою пропускною здатністю та високою затримкою. Протокол працює за моделлю публікації/підписки, коли одні пристрої публікують дані брокеру, а інші – можуть підписуватися на отримання цих даних. Візуальна схема наведена на Рис. 1.

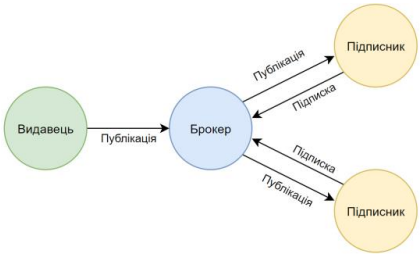


Рисунок 1. Принцип роботи протоколу MQTT

MQTT має наступні вразливості:

- Недостатня автентифікація та авторизація: якщо брокери та клієнти не налаштовані належним чином, неавторизовані особи або пристрої можуть отримати доступ до системи, що потенційно може призвести до витоку даних, контролю пристроїв або несанкціонованих операцій.
- Відсутність шифрування даних: протокол не має вбудованого шифрування. Це дозволяє зловмисникам переглядати або навіть модифікувати дані, якими обмінюються пристрої.
- Слабка безпека тем: протокол покладається на зв’язок на основі тем. Зловмисник може підписатися на

конфіденційні теми та отримати несанкціонований доступ до даних або навіть команд керування.

- Відмову в обслуговуванні: брокери можуть бути вразливими до атак, коли зловмисник надсилає велику кількістю повідомлень, перевантажуючи його та спричиняючи перебої в роботі.
- Уразливості програмного забезпечення: клієнти та брокери можуть мати вразливості, пов'язані з переповненням буфера, ін'єкційними атаками або слабкими алгоритмами шифрування.
- Використання незахищеного транспортного протоколу: MQTT зазвичай використовує TCP як транспортний протокол, який сам по собі не забезпечує шифрування чи автентифікації.

**Висновки**

Протоколи обміну повідомленнями відіграють важливу роль у забезпеченні зв'язку між пристроями, збиранням та обробкою даних. У цій сфері використовується кілька таких протоколів, і вибір конкретного залежить від вимог програми, стану мережі та інших факторів. До найпоширеніших протоколів обміну повідомленнями відносять MQTT, CoAP та HTTP.

Для забезпечення безпеки MQTT потрібно реалізувати такі механізми як: автентифікація клієнтів за допомогою облікових даних, контроль та розмежування доступу до публікації, підписки, тем та рівнів якості обслуговування, шифрування трафіку на транспортному або прикладному рівнях, забезпечити валідацію даних, а також впровадити найкращі практики щодо покращення відмовостійності.

## Перелік використаних джерел

1. Adrian McEwen, Hakim Cassimally, Designing the Internet of Things, 2014
2. Khalid Aloufi, Omar Alhazmi, Secure IoT with Access Control over RESTful Web Services, 2020

3. Omprakash Kaiwartya, Keshav Kaushik, Sachin Kumar Gupta, Ashutosh Mishra, Manoj Kumar, Security and Privacy in Cyberspace, 2022

# СИМЕТРИЧНА АВТЕНТИФІКАЦІЯ ІНТЕРНЕТ РЕЧЕЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПОЛІЦЕЙСЬКИХ ОХОРОННИХ СИСТЕМ

Клімушин П.С., Бондаренко Є.С.
Харківській національний університет внутрішніх справ
e-mail: klimushyn@ukr.net

В тезах доповіді розглянуто: ключова технологія безпечного керування комп'ютерними ресурсами та мережами; особливості мікросхем CryptoAuthentication компанії Atmel що допомагають протистояти різним зовнішнім атакам; сучасні криптографічні протоколи, зокрема ECDSA для цифрового підпису та ECDH для генерації спільних сеансових ключів симетричного шифрування. Показано особливості процедур симетричної автентифікації.
**Ключові слова:** комп'ютерний ресурс, мережа, криптографічний ключ, автентифікація.

Автентифікація є ключовою технологією для безпечного керування комп'ютерними ресурсами та мережами. Технологія автентифікації потрібно враховувати недолік обмежених ресурсів IoT. Як відомо, автентифікація пристрів IoT в мережі виконується з допомогою криптографічних перетворень – симетричним і асиметричним методами. Відмінності цих методів полягають в кількості та використанні криптографічних ключів. Автентифікація – симетрична, якщо використовується один криптографічний (сеансовий) ключ на хоста і клієнта для шифрування і дешифрування. При асиметричної автентифікації використовується два

математично пов’язані ключа публічний та приватний, один служить для шифрування, а другий для дешифрування ідентифікаційних даних. о.

На практиці застосовуються комбінації симетричного та асиметричного підходів із їх плюсами – швидкістю роботи симетричного та безпекою асиметричного. Компанія Atmel випускає мікросхеми для обох типів автентифікації [1].

Ключовими особливостями мікросхем CryptoAuthentication компанії Atmel є безпечне зберігання ключів та апаратні блоки, що допомагають протистояти різним зовнішнім атакам, у тому числі агресивним. Ці пристрої, що мало споживають електроенергії, підтримують сучасні криптографічні протоколи, зокрема ECDSA для цифрового підпису та ECDH для генерації спільних сеансових ключів симетричного шифрування. Вони можуть працювати з будь-яким зовнішнім мікроконтролером, вимагають лише одну лінію вводу/виводу, діють у широкому діапазоні напруги живлення. Все це допомагає розробникам без особливих проблем додавати до своїх виробів сучасний, надійний рівень інформаційної безпеки за мінімальну вартість [2].

Особливістю процедури симетричної автентифікації відповідно до схеми "Запит - відповідь" із зберіганням таємного (сеансового) ключа в захищених пристроях хоста та клієнта є швидкодіюча процедура автентифікації, захищені криптографічні мікрочипи з обох сторін забезпечують безпечне зберігання таємних ключів. Однак, недоліком такої схеми є необхідність мати на стороні хоста захищену криптографічну мікросхему для зберігання таємних ключів.

Більш економічною є процедура симетричної автентифікації IoT, яка не припускає використання захищених криптографічних мікросхем на стороні хоста для зберігання таємних ключів. Такий підхід має назву «фіксований запит».

Особливістю автентифікації в схемі «фіксований запит» є також швидкодіюча процедура автентифікації та економія апаратного обладнання за рахунок відмови від випадкової складової в процедурі автентифікації і заміні цієї складової

певною парою заздалегідь обчислених чисел (значення запитів і відповідні відповіді, що записуються в енергонезалежну пам'ять мікроконтролера на стороні хоста). Ця заміна, з одного боку, наводить к спрощенню схеми автентифікації, а з другого боку, веде до зниження її криптостійкості через заміну випадкових чисел на певні пари заздалегідь обчислених чисел, так як криптоаналітик може розгадати певну пару заздалегідь обчислених чисел з допомогою логічного аналізатора на інформаційної шині [3].

## Висновки

Таким чином, багато розробників в даний час покладаються на спеціалізовані апаратні криптографічні засоби, включаючи закінчені пристрої та захищені інтегральні мікросхеми різного класу. В загальному разі такі засобі пропонують наступні рішення: сильний захист криптографічних ключів; належне використання режимів та протоколів для криптографічних операцій; високоякісні генератори випадкових чисел, які ґрунтуються на випадкових фізичних подіях та які досконально протестовані.

Апаратно захищені мікросхеми сімейства CryptoAuthentication компанії Atmel належать до таких спеціалізованих криптографічних засобів. Вони можуть застосовуватись у широкому діапазоні кінцевих додатків поліцейських охоронних систем.

## Перелік використаних джерел

1. Клімушин П.С., Спасібов Д.В. Симетрична автентифікація: потенційне застосування апаратно захищених мікросхем для забезпечення безпеки інтернет речей. Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів міжнарод. наук.-практ. конф. (м. Харків, 27 травня 2022 р.). Харків : ХНУВС, 2022. С. 75-78.

2. Krivchenko I. Hardware-protected chips of the CryptoAuthentication family: potential applications of

ATSHA204A. Components and technologies. 2015, no. 10, pp. 60–65.

3. Klimushin P., Solianyk T., Kolisnyk T., Mozhaev O. Potential application of hardware protected symmetric authentication microcircuitsto ensure the securityof internet of things. Advanced Information Systems. 2021. Vol.5, Харків : 2021, No.3, p. 103-111.

# ІДЕНТИФІКАЦІЯ I/O COMPLETION PORT ЯК МЕХАНІЗМ ПІДВИЩЕННЯ ЗАХИСТУ ВІД АТАК НУЛЬОВОГО ДНЯ ОС WINDOWS

Тислицький Д.В., Гальчинський Л.Ю.
Навчально-науковий Фізико-технічний інститут,
КПІ ім. Ігоря Сікорського, Київ, Україна

AIO (асинхронний ввід/вивід) – потужний механізм у багатопотокових програмах для швидкого оброблення файлів. Проте він може використовуватися не тільки в корисних цілях. Так зловмисники використовують AIO для обходу наявних механізмів захисту. Наприклад, Ransomware може використовувати AIO для шифрування файлів та отримання конфіденційної інформації. Саме тому важливо усвідомлювати ризики AIO, вміти їх ідентифікувати, а також знати найпріоритетніші реалізації для зловмисників.

**Ключові слова:** асинхронний ввід/вивід, атака нульового дня, RaaS, I/O Completion Port.

## Вступ

Windows - найпоширеніша десктопна операційна система, яку використовують 74% [5] користувачів у всьому світі. Це призводить до поширення зловмисного програмного забезпечення, що призначене саме для цієї ОС. Але з підвищенням захисту ОС, використовуються й більш креативні методи атак, зокрема з використанням AIO.

## Використання I/O Completion Port при реалізації атак нульового дня

Одним з найвідоміших прикладів використання AIO при виконанні корисного навантаження ШПЗ безумовно є Sodinokibi/REvil. З'явившись у 2019 році він швидко здобув популярність у атакуючих, через своє використання у якості RaaS (Ransomware as a Service) [6].

При аналізі отриманого зразку експертами було виявлено, що при реалізації механізму шифрування файлів використовується досить не популярний засіб AIO: I/O Completion Port (IOCP). Принцип його роботи полягав у наступному:

1. Створення I/O Completion Port.
2. Створення пулу потоків.
3. Усі потоки очікують події *GetQueuedCompletionStatus()*.
4. Коли файл знайдений за допомогою *mw_enum_path_files()* він додається до I/O Completion Port.
5. Пакет завершення публікується, щоб функція *PostQueuedCompletionStatus()* повідомила потік про те, що файл потрібно зашифрувати. [7, 8]

Доцільність використання IOCP тут пояснюється швидкістю його роботи, в порівнянні з альтернативними механізмами. Так, порівняльна характеристика по часу для однакового вхідного набору файлів показала, що IOCP більш ніж у 1.5 рази ефективніший у використанні в порівнянні з APC (Asynchronous Procedure Calls).

## Механізм ідентифікації використання I/O Completion Port

При реалізації механізму ідентифікації I/O Completion Port використовувалися засоби статичного та динамічного аналізу програмного забезпечення. При цьому статичний аналіз базується на пошуку рядків, що відповідають назвам Windows API функцій роботи з IOCP [9] у виконуваному

файлі *.exe*. Натомість динамічний аналіз відстежує виклики заданих функцій у реальному часі з фіксацією безпечного інтервалу часу.

Додатковим методом захисту є перевірка виконуваного файлу за допомогою найбільшого сервісу ідентифікації ШПЗ VirusTotal, що впроваджено через відповідні API виклики.

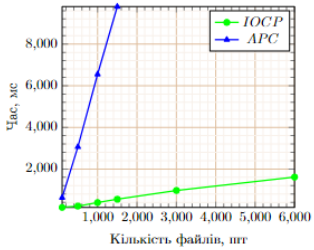


Рисунок 1. Порівняння по часу використання IOCP та APC

## Висновки

В ході дослідження було розглянуто використання IOCP при реалізації атак нульового дня на прикладі Ransomware Sodinokibi/REvil. Наглядно продемонстровано переваги використання IOCP в порівнянні з альтернативними механізмами, а також запропоновано концепт механізму ідентифікації зловмисного використання IOCP для подальшого покращення виявлення атак нульового дня ОС Windows.


Рисунок 2. Приклад роботи механізму ідентифікації IOCP

**Перелік використаних джерел**

5. "StatCounter Global Stats - Browser, OS, Search Engine including Mobile Usage Share" [Електронний ресурс] – Режим доступу: https://gs.statcounter.com/
6. Secureworks. (2019, August 6). REVIL/Sodinokibi Ransomware. [Електронний ресурс] – Режим доступу: https://www.secureworks.com/research/revil-sodinokibi-ransomware
7. Amossys. (2021, June 16). Sodinokibi malware analysis. [Електронний ресурс] – Режим доступу: https://www.amossys.fr/fr/ressources/blog-technique/sodinokibi-malware-analysis/
8. Mark Russinovich Windows Internals, 7th Edition. [Текст] / Mark Russinovich, David A. Solomon, Alex Ionescu. - Microsoft Press, 2012. – 1120 с.
9. Russinovich M. Inside I/O Completion Port. — 07/30/1998. [Електронний ресурс] — Режим доступу: https://web.archive.org/web/20101031075704/http://doc.sch130.nsc.ru/www.sysinternals.com/ntw2k/info/comport.shtml

# PROPOSING OF FUZZY LOGIC DRIVEN FEATURE BASED METHOD FOR SUGGESTIVE INFLUENCE DETECTION

Наконечна Ю.В.
КПІ ім. І. Сікорського, Навчально-науковий Фізико технічний інститут, Київ, Україна

This study proposes a way of suggestive influence identification and classifying tools used in information operations. The method is based on combining fuzzy sets theory and fuzzy inference methods with feature based analysis approach for tools like propaganda, fake, disinformation, manipulation, and artificial narrative

**Keywords:** Suggestive influence, warfare, propaganda, disinformation, manipulation, fuzzy logic, Mamdani.

## Introduction

As the information space has become a significant platform for conducting hybrid warfare, utilizing various techniques, it can directly impact the public, national security, defense, public administration, establish spheres of influence and ideological and psychological foundations through propaganda. It becomes crucial for researchers to prioritize the development of comprehensive measures to safeguard the information environment, detect information operations, and deploy effective countermeasures.

## Problem

Given the intricate and multifaceted nature of detecting the aforementioned techniques of suggestive influence, it is an urgent challenge to devise methods that can differentiate information operations from regular informational activities.

## Feature-based analysis methodology

Numerous techniques have been suggested for identifying propaganda, disinformation, fake news, and other forms of information distortion. These techniques encompass data mining and text mining through ensemble methods, detection based on linguistic analysis and social network analysis, the application of natural language inference, sentence-level analysis, and the utilization of sentiment analysis techniques [1]. Mentioned approaches and methods are based on feature analysis, focusing on the detection and classification of suggestive techniques at the level of specific information features. The feature sets utilized in these investigations are typically derived from existing datasets used for detecting fake, lying, or propaganda content. While features can be categorized and grouped based on the objectives of the analysis, the variations in the essence of the features themselves are minimal.

## Feature-to-instrument classification markers

In [1] was investigated the typical characteristics of suggestive influence instruments based on various sources. The unique 20 markers list has been provided like:

1. emotionally charged rhetoric; 2. appeal to authority; 3. lack of credible and/or verifiable sources; … 19. informality, poor grammar or spelling; 20.hoaxes or scams.
2. Hypothesis was developed that each mentioned marker can be characterized by some set of features (full features list has been given in [2] as well): 1. feature-based analysis makes it possible to draw a conclusion regarding the belonging of some piece of information to the tools of information influence; 2. the presence of suggestive influence can be determined by indicating methods described as markers that allow specifying the type of information influence tools.

By establishing correlations between features and indicators of suggestive influence, it becomes feasible to distinguish between different types of suggestive tools during the identification or detection process and possible to associate specific markers with forms of suggestive influence.

As a result of establishing correlation between a features set and markers corresponding to them, an adjacency matrice was compiled for sets of suggestive influence instruments, their corresponding markers and features, where:

1. Suggestive influence instruments set $I$ consists of concepts: propaganda $I_1$, fake $I_2$, disinformation $I_3$, manipulation $I_4$, narrative $I_5$.
2. Markers set $M$ contains markers enumerated above as emotionally charged rhetoric $M_1$, appeal to authority $M_2$, ..., hoaxes or scams $M_{20}$.
3. Feature set is built based [2] descriptions and consists of extracted data features as relative frequency of words $F_1$; characters $F_2$; ... replies $F_{32}$ [1].

To test the hypothesis, a cognitive mapping approach has been adopted, enabling us to establish a network of connections among features, markers, and types of suggestive influence tools using a cognitive map. After assigning weights to the strength of connections between concepts of a cognitive map using correspondence between linguistic and numeric terms, which brings us to the fuzzy suggestive influence model.

**Fuzzy models**

Relying on the set of rules for instrument-marker-feature connection, rule-based fuzzy model can be applied. In these models, the relationships between variables are represented by means of if-then rules with imprecise predicates, like: If the fridge cooling is low then the temperature will lower slow. Qualitive predicate as «high» or «low» is defined by linguistic variable compared to a numerical range. E.g. an usual predicate scale is given in range [0,1] and divided into intervals according to linguistic variables used.

Due to specifics of features analysis use, mentioned in [1,2], the result of the analysis presented in the form of numerical coefficients of the intensity of the presentation of one or another characteristic (or features, as we refer to them). This gives us the opportunity to establish an appropriate scale of the intensity of the appearance of this or that feature and to put a linguistic variable in accordance with the intervals. Then, for our instrument-marker-feature case we can create a set of fuzzy rules which in general would be as following [3]:

$$R_i: if\ x\ is\ A_i\ then\ y\ is\ B_i, \quad i = 1,2,\dots,K,$$

where R is a rule, A and i B are linguistic terms (such as «small», «large», etc.), represented by fuzzy sets, and K is the number of rules in the model. The linguistic fuzzy model is useful for representing qualitative knowledge such as in the following illustrative example.

Due to adjacency matrice obtained in [7], let us present concepts $I, M, F$ as variables, then fuzzy rule for suggestive instrument classification via markers and feature would be as follows:

$$R_i: if\ \big((F\ is\ A_{i1}\ then\ M\ is\ B_{i1})\ and\ (F\ is\ A_{i2}\ then\ M\ is\ B_{i2})\ and\ \dots\big)\ \dots\ then\ , \quad i = 1,2,\dots,K,$$

In this model, the antecedent (if-part of the rule) and the consequent (then-part of the rule) are fuzzy propositions, so we are getting the Mamdani-similar model. That means we can use fuzzy logic methods to process feature-based analysis results for suggestive influence instruments classification/detection.

**Summary**

We propose a way of suggestive influence identification and classifying tools used in information operations based on combining fuzzy sets theory and fuzzy inference methods with feature based analysis, allowing to process feature-based text analysis results and use fuzzy inference systems for suggestive influence instruments detection and classification.

**References**

1. Nakonechna *Y*., Feature based analysis for suggestive influence detection// Materials from all-Ukrainian science conference for students and young scientists «Theoretical and Applied Problems of Math, Physics and Computer Science». - 2020. - С. 216-219.
2. Rastogi S., Bansal D. Disinformation detection on social media: An integrated approach // Multimedia Tools and Applications. - 2022. - Vol. 81. P. 40675-40707.
3. Robert Babuška. Identification Using Fuzzy Models // Control systems, robotics, and automation. -2004. - Vol. VI

# МЕТОДИКА АНАЛІЗУ ТА ОЦІНКИ ПОТЕНЦІЙНИХ ВРАЗЛИВОСТЕЙ В СИСТЕМАХ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

Товстенко А.Є., Даник Ю.Г.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», НН Фізико-технічний інститут, Київ, Україна

У роботі пропонується комплексний підхід до аналізу та оцінки потенційних вразливостей в системах електронного голосування з метою забезпечення їх надійності та стійкості до кібератак. У контексті зростаючої актуальності кібербезпеки та її впливу на демократичні процеси, ця робота включає дослідження існуючих методик, аналіз типових атак та загроз, а також розробку рекомендацій для

підвищення рівня кібербезпеки систем електронного голосування.

**Ключові слова:** кібервразливість, електронне голосування, методика, стандарти, аналіз, аутентифікація та авторизація

## Вступ

У сучасному світі системи електронного голосування набувають все більшої актуальності, оскільки вони можуть сприяти підвищенню ефективності та прозорості виборчого процесу. Проте й зростає необхідність вдосконалення методів оцінки кібервразливостей таких систем, з метою забезпечення їх надійності та стійкості до різних видів кібератак.

Одним з ключових аспектів у розробці методик оцінки кібервразливостей є врахування специфіки систем електронного голосування, таких як анонімність голосів, відкритість результатів та прозорість процесу.

## 1. Типи загроз на системи електронного голосування

### 1.1 Типи загроз

Основні типи загроз які можуть бути використані для атак на систему електронного голосування, а саме: Віруси та шкідливе ПЗ, DDoS-атаки, атаки на аутентифікацію та авторизацію,внутрішній зловмисник(так званий інсайдер). За останні 10 років, відбулося близько десятка атак при проведенні електронного голосування, одним з прикладів є атака на сайт Центральної виборчої комісії у день президентських виборів 25 травня 2014 року, також були випадки коли країни відмовлялися від електронного голосування на користь звичайного бюлетеневого.

## 2. Дослідження вразливостей на системи електронного голосування

### 2.1 Методи дослідження вразливостей

Для виявлення вразливостей системи електронного голосування можна використовувати ряд методів, таких як:

аналіз коду, коли при детальному перегляді можливо виявити потенційні проблеми та шляхи доступу до системи, пенетраційне тестування, для симуляції кібератаки на систему, ревізія безпеки, експерти з кібербезпеки проводять комплексний аналіз системи електронного голосування, щоб виявити вразливості та рекомендувати заходи щодо їх усунення.

### 2.2 Методи дослідження потенційних загроз

Для дослідження потенційних загроз за допомогою аналізу ризиків, визначити пріорітетні напрямки та цілі для посилення безпеки системи, можливість моніторингу загроз на підготовчому рівні, для цього на об'єкти моніторингу такі, як сервери, бази даних та компоненти авторизації і аутентифікації, встановити системи відслідковування загроз. Порядок такого моніторингу визначається певною методикою.

Для контролю та аналізу, тобто сповіщення та агрегація даних, відслідковування кореляції подій та створення звіту для оцінки ефективності використаних методів,методами моніторингу можуть бути застосовані різноманітні способи аналізу коду, наприклад, динамічні та статичні, перехоплення пакетів мережі та підготовка персоналу, використання систем управління інцидентами. Також це розробка певної стратегії захисту для мінімізації ризиків та стійкості системи.

### 2.3 Запобігання та уникнення потенційних загроз

Постійний аудит та контроль — один з головних методів запобігання загроз, це стосується як процесів систем електронного голосування, так і контроль доступу та розмежування людей по ролям, використання багаторівневої системи автентифікації зменшує ризик фальсифікації голосування та несанкціонованого доступу, розробка протоколів реагування на інциденти, важливий крок для усунення наслідку кібератаки, мінімізуючи їх вплив на виборчий процес. Корисними функціями для забезпечення захисту та конфіденційності голосувань може бути використання технології блокчейн, основною

функцією якого є призначити під одного користувача – один голос, який неможливо скомпрометувати.

## Висновки

Отже в роботі, було розглянуто актуальність дослідження шляхів забезпечення кібербезпеки в контексті систем електронного голосування. Застосування електронного голосування має забезпечити зручність, доступність та прозорість виборів. Однак, впровадження таких систем супроводжується виникненням нових вразливостей та ризиків, пов'язаних з кібератаками. У роботі були досліджені різні типи загроз та атак, які можуть бути використані проти систем електронного голосування, а також розглянуті реальні випадки кібератак на виборчу інфраструктуру в минулому.

З урахуванням отриманих результатів, можна визначити перспективи подальшого дослідження та розробки в галузі кібербезпеки систем електронного голосування, це покращення методів аналізу ризиків, тестування на проникнення для систем електронного голосування, з метою виявлення нових видів вразливостей та атак, нові протоколи та стандарти для систем електронного голосування, які враховують вимоги кібербезпеки та захисту даних, можливість впровадження нових технологій, таких як блокчейн, для додаткової стійкості, розробка програм навчання персоналу для роботи з системами електронного голосування та одним з основних є впровадження електронного голосування для підвищення довіри до них з боку держави та громадян.

## Перелік використаних джерел

1. Adrià Rodríguez-Pérez - Five Common Attacks Against Online Voting - EDGE Elections – 2021.
2. Peter Stone - Cyber attacks and electronic voting errors threaten 2020 outcome, experts warn - US elections 2020 – 2020.
3. Feng Hao and Peter Y A Ryan - Real-World Electronic Voting: Design, Analysis and Deployment – 2016 – C.161-163

# OSINT TIME SERIES FORECASTING METHODS ANALYSIS

Feher A., Lande D.
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" Kyiv, Ukraine

Time series forecasting is an important niche in the modern decision-making and tactics selection process, and in the context of OSINT technology, this approach can help predict events and allow for an effective response to them.
For this purpose, LSTM, ARIMA, LPPL~(JLS), N-gram were selected as time series forecasting methods, and their simple forms were implemented based on the time series of quantitative mentions of starlink systems obtained and generated using OSINT technology. Based on this, their overall effectiveness and the possibility of using them in combination with OSINT technology to form a forecast of the future were investigated.
**Keywords:** time-series, prediction, forecasting, OSINT

## Introduction

Business, finance, logistics, medicine, biology, and chemistry, use forecasting as one of the most applied methods of science that help to effectively solve typical problems and contribute to overall developments. At the same time, in the modern world, the latest neural network developments find their fits in various cybersecurity fields, such as threat intelligence, malware detection, and endpoint protection, which use probabilistic forecasting concepts for training, as well as show overall needs in the chosen topic.

Time-series forecasting methods as a scientific attitude use historical and current data to predict future values over a period of time or at a certain point in the future. By analysing the available data stored in the past, forecasting helps to understand future trends and allows you to respond to them in the most effective way.

In today's world, a well-designed forecasting system frees up hands and gives freedom in the field of the targeted application, even within the framework of national and cyber security. From the point of view of military and civilian security, such a system allows for the correct construction and adjustment of tactics and strategy at different time intervals in accordance with the forecasted events.

The task of the study is, first of all, to create a basis of the most effective forecasting methods for effective further research, and make qualitative comparisons between methods of its different nature. The methods themselves are analysed and used in conjunction with Open Source Intelligence (OSINT) technology to prove the application probability concept. The time series considered for the forecasting study represent quantitative collected information obtained using OSINT technologies.

## Methodology

The selected time series for the study represents a complex dependence of the number of selected events obtained using OSINT technology on the time interval of one year. The selected event for analysis was presented as a dependence on the quantitative characteristics of mentions of Starlink systems in news, blogs, and articles over the Internet on the corresponding time period of the 2022 year.

To create a comparative base, only 333 days out of 364 were used to train the selected models, where the last month in a count of 31 days of the selected year was used as the predicted outcome values for further analysis. The main modern approaches to forecasting are considered to be the following: neural network, statistical, econometric, and linguistic. Each of them is actively used in their respective industries, and in some cases, a combination of several approaches or tuning modifications is used to obtain the most relevant values of needs.

As typical modern representatives of the described approaches, the following methods have been chosen to study time series and build forecasts series corresponding to them:

- Long Short-Term Memory (LSTM) as the most common neural network method;
- Autoregressive Integrated Moving Average (ARIMA) as the most widely used statistical method;
- Log Periodic Power Law (LPPL) or Johansen-Ledoit-Sornette (JLS) as an econometric method, which is subject to criticism and is not popular, but is used in some cases;
- N-gram as a linguistic one, which is already quite strongly implemented in modern technologies and life aspects.

Depending on the selected dataset, chosen forecasting models can predict the quantitative characteristics of selected events based on corresponding values there is possible to calculate the average error between the real and predicted data.

To determine the accuracy of the forecasting models, we used the mean square error (MSE) using the formula \eqref{eq:mse} and the root mean square error (RMSE) using the formula \eqref{eq:rmse} as the most accurate methods for determining such kind of errors.

$$MSE = \frac{1}{n}\Sigma_{i=1}^{n}\left(x_i - \overline{x_i}\right)^2$$

$$RMSE = \sqrt{\frac{1}{n}\Sigma_{i=1}^{n}\left(x_i - \overline{x_i}\right)^2}$$

## LSTM

LSTM is a kind of recurrent neural network model, with the difference that LSTM can handle long time series of data. In addition, the conventional recurrent model has a vanishing gradient problem for long data sequences, while LSTM can prevent this problem during training and perform qualitative results.

The model can recall previous long-time series of data [1] and has automatic controls to keep relevant features or discard irrelevant features. It is because of these factors that LSTM was

chosen among other recurrent methods as a method for the study.

For LSTM, we used its single-layer configuration with 32 units, and the Adam optimizer as an extension to stochastic gradient descent which gave more relevant results, with batch size and epoch values of 512 which defines a number of predictions at the time, the output data was (inverse) transformed by normalization to obtain the predicted series.

## ARIMA

ARIMA is an autoregressive integrated moving average model, where the AR part shows that the time series is regressed on its own past data. The MA part shows that the forecast error is a linear combination of past corresponding errors. The I part shows that the data values have been replaced by different values of order $d$ to obtain stationary data, which is a requirement of the ARIMA approach.

It is because of this complexity that the ARIMA model is effective in re-examining past data using this combined learning approach and helps to effectively predict future points in the time series [2]. This attitude creates a base of popularity for the method and its practical value.

For ARIMA, we used its one-layer configuration with $p$ = 33 which defines the number of lag observations included in the model, $d$ = 2 which defines the number of times that the raw observations are differenced as a degree of differencing, $q$ = 0 which defines the size of the moving average window, the values of which were determined empirically according to the more relevant output forecast values.

## LPPL

The LPPL – or Johansen-Ledoyt-Sornett (JLS) model -- attempts to diagnose, time, and predict the end of financial bubbles, a common term in the financial industry for crisis points when the majority of participants lose confidence during speculative growth.

Despite the widespread criticism [3], the creators of the model provide a motivation based on some natural assumptions,

including risk-neutral assets, rational expectations, local self-reinforcing imitation, and probabilistic critical moments for the algorithm to calculate the stages of bubble development directly [4] with a simple equation.

This way, we can see how the chosen forecasting algorithm work with an atypical for it time series.

For the LPPL (JLS), were used its modification using the Covariance Matrix Adaptation Evolution Strategy (CMA-ES), which gives a more varied and relevant forecasted series.

## N-gram

N-grams represent a continuous sequence of *N* elements from a given set of texts. The N-grams technique has found its main application in the field of probabilistic language models. They estimate the probability of the next element in a sequence of words, and this is the basis of the theoretical approach to assume study time series forecasting.

This approach to language modeling estimates a close relationship between the position of each element in the string, calculating the occurrence of the next word in relation to the previous one and the frequency of their occurrence.

In a broad sense, these elements do not necessarily mean strings of words, they can also be phonemes, syllables, or letters [5], depending on what exactly is required, and it is thanks to this flexibility that the work was able to be based on numeric time series as well.

There is an additional variation in modeling by creating semantically connected elements in turn, in this paper, the unigram was studied as N-gram with one connection inside, to provide a complete forecast of 31 days, with other values of *N* the model could not produce a chain of values with a length of 31 values, and a simple general type of tokenization of all elements was used.

## Result and Discussion

The software was developed for each method, and the time series was adjusted to obtain the predicted results. The graphs shown in Figure 1 of actual (real) and predicted values were

modeled according to the dataset of chosen time series, and the processes were repeated to obtain the most relevant predicted series.

Neural network and statistical approaches proved to be the most effective for forecasts, while econometric and linguistic methods proved to be rather limited in their use in forecasting such time series.

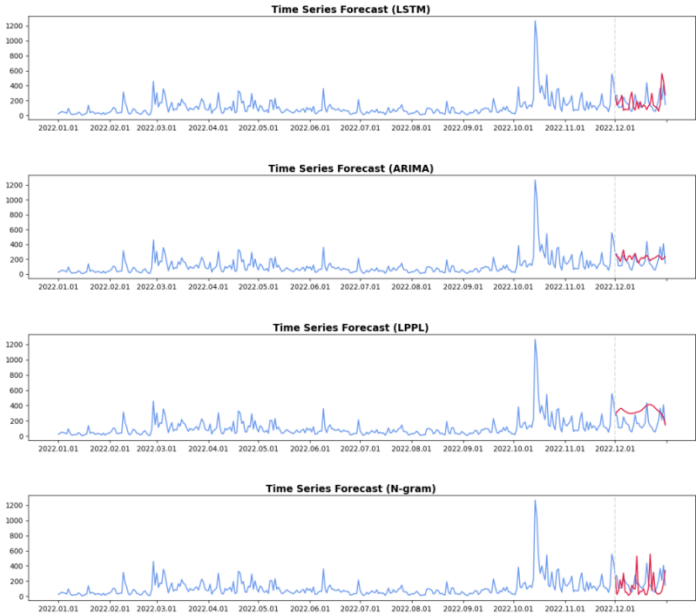


Figure 1. Time series and predictions

## LSTM

The LSTM method is quite flexible and can be easily adjusted to the specifics of the time series, due to its complexity, the method works stably, without fail, and the predicted results are quite close to the real ones. It is also possible to adjust additional parameters [6], so it is possible to create a multilayer model with stronger rejection, which can give more accurate predicted results.

## ARIMA

ARIMA was a good choice, it is less flexible in use, but with the correct selection of parameters *p, d, q* it makes its forecasts quite accurately according to different kinds of time series, among the selected options it showed itself to be the best.

## LPPL

In another way, LPPL performs rather poorly as a method for forecasting time series, which is not surprising due to its narrow focus on solving other mentioned problems. The model is still evolving over time, partly in response to valid criticism, and in the course of the study was found that the strategy of evolutionary adaptation of the covariance matrix CMA-ES is a good improvement that allows for more accurate results, but despite this, when using generative algorithms such as CMA-ES to improve the forecast, the complexity of the calculation itself increases proportionally. It turned out that the calculation of individual large numerical values is also problematic, which requires taking their logarithmic representation, which can also affect the distortion of the forecast.

## N-gram

The N-gram model presented a rather limited version of time series forecasting due to the limited number of previous possible values according to which the forecast can take them. That is, considering this method within the framework of non-stationary series, the forecast is limited by the threshold values of the time series and cannot go beyond it, which reduces its accuracy. Therefore, in studying time series, there is wide room for improvement when using the model with the N-1 algorithm, in which the forecast distortion at short intervals will be much smaller and gradually graduated with respect to time, and the addition of a recurrent component that can increase the accuracy at longer time intervals.

It is also worth noting the creation of joint or separate dictionaries for different series, which will increase the accuracy of joint series if there is an appropriate semantic

correlation, but vice versa in the absence of such correlations. To determine the accuracy of the models were calculated their mean square error (MSE) and root mean square error (RMSE). The results can be found in Table. where a lower number reflects a higher accuracy of the forecast.

| | LSTM | ARIMA | LPPL | N-gram |
|---|---|---|---|---|
| MSE | 21009.85 | 10242.77 | 36911.94 | 33618.03 |
| RMSE | 144.9477 | 101.2065 | 192.1248 | 183.3522 |

## Conclusion

Based on the practical part, it can be noted that each of the considered methods satisfies the task, despite the low accuracy of effective time series forecasting of such models as LPPL and N-gram, they provide much more creative space for further study and optimisation. In turn, LSTM and ARIMA models have proved to be quite effective, so it is not surprising that these models and their approaches are dominant in terms of time series forecasting.

Thanks to the study carried out, there is a basis for further study of the topic, forecasting various types of events obtained from open sources, and in particular the models themselves. In the context of this study, having the means of automated OSINT data collection, it is possible to confirm the effectiveness of their use for building predictive options for the future.

## References

1. *Sudriani Y., Ridwansyah I., Rustini H. A.* Long short term memory (LSTM) recurrent neural network (RNN) for discharge level prediction and forecast in Cimandiri river, Indonesia. — 2019. — DOI: 10.10 88/1755-1315/299/1/012037.

2. *Brownlee J.* Introduction to Time Series Forecasting with Python. — 1st ed. — 2020. — 365 p.

3. *Fantazzini D., Geraskin P.* Everything You Always Wanted to Know about Log Periodic Power Laws for Bubble Modelling but Were Afraid to Ask // European Journal of Finance. — 2011. — Jan. — Vol. 19. — P. 11–13. — DOI: 10.1080/1351847X.2 011.601657.

4. *Shu M., Zhu W.* Diagnosis and Prediction of the 2015 Chinese Stock Market Bubble. — 2019. — arXiv: 1905.09633 [q-fin.ST].

5. *Jurafsky D., Martin J. H.* Speech and Language Processing. — 3rd ed. — 2023. — 636 p.

6. *Staudemeyer R. C., Morris E. R.* Understanding LSTM – a tutorial into Long Short-Term Memory Recurrent Neural Networks. — 2019. — arXiv: 190 9.09586 [cs.NE].

# РОЛЬОВА МОДЕЛЬ: ВПЛИВ НА БЕЗПЕКУ ТА ДЕЦЕНТРАЛІЗАЦІЮ БЛОКЧЕЙНУ RONIN

Гузенко Г. С., Гальчинський Л. Ю.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», НН Фізико-технічний інститут, Київ, Україна

Наводиться аналіз структури протоколу Ronin, пояснюється сутність моделі консенсусу Proof of Authority (PoA). Фокусується на рольовій політиці доступу до функцій смартконтрактів у протоколі Ronin та вивчається вплив такого доступу на децентралізацію та загальну безпеку блокчейн системи.

**Ключові слова:** Ronin, PoA, безпека, рольова політика

## Вступ

Протокол Ronin – це інноваційна сайд-блокчейнплатформа, призначена для гри Axie Infinity, яка здійснюється на базі неперервної блокчейн технології. Завдяки своїм унікальним функціям та особливостям, Ronin забезпечує широкий спектр можливостей для гравців, а також стабільну та ефективну криптовалютну економіку, що допомагає забезпечити безпеку, швидкість та масштабованість гри. [1]

Ronin походить від Ethereum і спочатку використовував консенсусний алгоритм Proof-of-Authority з низькими комісіями та високою швидкістю транзакцій. Зараз протокол вдосконалили, використовуючи гібридний

механізм Proof-of-Authority та Proof-ofStake. Головною метою цієї платформи було зниження вартості транзакцій та покращення швидкості обробки операцій для забезпечення більш ефективного та економічного функціонування Axie Infinity. [2]

## 1. Складові протоколу Ronin

Основні елементи сайдчейну включають:

1. Основний блокчейн - це блокчейн, що використовується для зберігання ключової інформації та забезпечення досягнення консенсусу між учасниками.
2. Смарт-контракти - це програми, що забезпечують виконання складних операцій у блокчейні, включаючи передачу активів та зберігання даних. Ці контракти можуть бути розгорнуті як у основному блокчейні, так і у сайдчейнах.
3. Сайдчейн - це блокчейн, який функціонує паралельно з основним блокчейном і забезпечує спільну безпеку та консенсус з ним. Сайдчейни можуть мати власні правила консенсусу та механізми безпеки, відмінні від основного блокчейна.
4. Мости - це компоненти, що дозволяють передавати активи між бічними ланцюгами і основним блокчейном. Вони забезпечують безпеку та досягнення консенсусу між різними блокчейнами.
5. Протоколи обміну повідомленнями - це протоколи, що дозволяють взаємодіяти та обмінюватися повідомленнями між бічними ланцюгами і основним блокчейном. Ці протоколи забезпечують передачу даних та сприяють взаємодії між різними блокчейнами. [3]

У сайдчейнах технології смарт-контрактів та транзакцій мають свої особливості та різницю використання. Транзакції використовуються для передачі активів між користувачами, здійснення платежів у межах мережі та взаємодії зі сторонніми сервісами, такими як мережеві експлорери або біржі.

З іншого боку, смарт-контракти використовуються для визначення умов виконання транзакцій. Код смарт-контракту автоматично виконується при досягненні певних умов, описаних у контракті. Це дозволяє створювати автоматизовані та програмовані умови для виконання операцій, без необхідності додаткових втручань.

Отже, транзакції використовуються для обміну активами та взаємодії з зовнішніми сервісами, тоді як смарт-контракти визначають умови та автоматично виконують код при досягненні цих умов. Ці дві технології часто співпрацюють разом для забезпечення повноцінного функціонування сайдчейнів та їх взаємодії з основним блокчейном. [4]

## 2. Алгоритми консенсусу Ronin

Раніше протокол Ronin використовував механізм Proof of Authority (PoA) - доказ на основі авторитету, для перевірки мережі. В цьому механізмі авторитетні вузли, визначені компанією Sky Mavis, були відповідальні за підтвердження транзакцій та створення нових блоків у мережі Ronin. Кожен авторитет мав свій публічний ключ, за допомогою якого він підписував блоки та транзакції.

Однією з переваг механізму PoA є відсутність необхідності великої обчислювальної потужності та енерговитрат, які вимагаються в механізмі Proof of Work (PoW). Крім того, PoA забезпечує швидкість та масштабованість транзакцій, що дозволяє мережі Ronin обробляти великі обсяги даних. Однак, PoA має свої недоліки. Наприклад, він може бути менш децентралізованим порівняно з PoW, оскільки контроль над мережею знаходиться в руках обраних авторитетів. Крім того, PoA не дозволяє користувачам майнити та отримувати винагороди за підтримку мережі, як це відбувається в механізмах PoW або Proof of Stake (PoS). Це призводить до більшої централізації мережі та можливості атак.

Зараз протокол Ronin використовує гібридний механізм, який поєднує елементи Proof of Authority (PoA) та Proof of

Stake (PoS), з метою поліпшення децентралізації та безпеки мережі. [6]

## Використовуваний наразі алгоритм

Так, розробники працюють над поєднанням технологій Proof of Authority (PoA) та Delegated Proof of Stake (DPoS) для створення швидкого, масштабованого та безпечного алгоритму консенсусу.

Proof of Stake (PoS) є консенсусним механізмом, в якому вибір творця наступного блоку визначається через процес випадкового вибору на основі власності токенів. Однак розробники вирішили використати вдосконалену версію - Delegated Proof of Stake (DPoS). У DPoS, учасники можуть ставити свої токени в заставу, і чим більше токенів вони ставлять, тим більше їх шанси стати валідатором. В кожному слоті один валідатор випадковим чином обирається як пропонент блоку і відповідає за створення нового блоку та його розповсюдження по мережі. Також, в кожному слоті випадковим чином обирається комітет валідаторів.

DPoS є модифікованою версією Proof of Stake, яка використовує делегацію та вибір обмеженого числа валідаторів для поліпшення швидкості транзакцій та масштабованості мережі. Однак, в порівнянні зі звичайним PoS, DPoS може бути менш децентралізованим, оскільки вибір валідаторів обмежений. Втім, це рішення дозволяє досягти більшої швидкості та ефективності мережі, забезпечуючи одночасно достатню децентралізацію та безпеку. [7] Різницю між цими двома механізмами видно на Рис. 1.

## 2.1. Гібрид

Механізм, використовуваний у Ronin, може бути охарактеризований як гібридний, оскільки розробники використали дві раніше згадані технології - Proof of Authority (PoA) та Delegated Proof of Stake (DPoS) - паралельно.

Узагальнюючи, концепція такого механізму може бути представлена наступним чином:

• Набір валідаторів складається з 22 слотів, з яких 12 зарезервовано для керуючих валідаторів, які вибираються у спосіб PoA. Решта 10 слотів відкриті для всіх, хто бажає стати валідатором і відповідає мінімальним вимогам до ставок. Вони називаються стандартними валідаторами.

• Користувачі, які зареєструвалися, щоб стати валідатором, мають роль кандидата в валідатор, доки їх не буде обрано як стандартний валідатор.

• Делеганти делегують свою власну частку будьякому валідатору на свій вибір, збільшуючи шанс валідатора бути обраним стандартним валідатором і отримати доступ до виробництва блоків .

• Вибрані валідатори отримують винагороду за блок після перевірки транзакцій у блоці, і ці винагороди потім діляться з їхніми делегаторами.

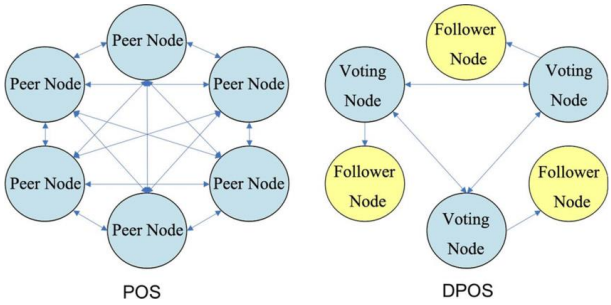


Рисунок 1. Різниця між механізмами консенсусу

## 3. Смарт контракти протоколу Ronin

Ронін, як незалежний протокол, має власний набір смарт-контрактів. Смарт-контракт - це програмний код, що містить умови та правила, які автоматично виконуються при заданих умовах. Цей код зберігається в блокчейні та поширюється по всій мережі. Смарт-контракти є надійним та безпечним засобом забезпечення виконання умов угод,

оскільки вони автоматично виконуються без посередництва.

У попередній версії протоколу Ronin був доступний набір смарт-контрактів, які використовувалися лише в контексті Proof of Authority (PoA) консенсусу. Проте розробники оновили протокол та впровадили новий пакет смарт-контрактів, які підтримують виконання умов у контексті Delegated Proof of Stake (DPoS) консенсусу. Це означає, що тепер у протоколі Ronin доступні смарт-контракти, які можуть виконуватися згідно з умовами, визначеними в рамках DPoS консенсусу.

## Насправді смарт-контракти мають багатий функціонал...

Наприклад:

1. Обробка транзакцій: Смарт-контракти в Ронін можуть використовуватися для автоматичної обробки транзакцій між користувачами. Наприклад, контракт може автоматично виконати переказ коштів від одного користувача до іншого при виконанні певних умов.

2. Створення токенів: Смарт-контракти можуть бути використані для створення та управління токенами на Ронін. Це може бути корисно для випуску власних токенів, стабільних монет або для організації ICO.

3. Розподіл доходів: Смарт-контракти можуть бути використані для автоматичного розподілу доходів між різними учасниками. Наприклад, контракт може автоматично розподілити прибуток від децентралізованої фінансової платформи між інвесторами та розробниками.

4. Організація голосування: Смарт-контракти можуть бути використані для організації голосування за прийняття різних рішень. Контракт може збирати голоси від різних учасників та автоматично підраховувати результати.

5. Управління активами: Смарт-контракти можуть бути використані для управління активами на Ронін. Наприклад, контракт може автоматично розподілити прибуток. [8] А так за версією «Journal of Computing Science and Engineering» взаємодія смарт-контрактів та сайдчейнів із

результатом запису головної інформації схематично виглядає як на Рис. 2.

## 4. В чому проблема порушення децентралізації та ролей

За обидвами аудитами від Verichains, видно, що розробники протоколу Ronin вибудували рольову політику доступу до функціоналу смарт-контрактів. Що означає що певний смарт-контракт може бути виконаний користувачем з певною роллю. Це вже порушує раніше розглянуту концепцію смарт-контракту з автоматичним виконанням умов контракту. Це може вказувати на те що механізм роботи блокчейну має бути ще в розробці, або ж розробники не вбачають проблеми у наданні доволі обширного доступу.

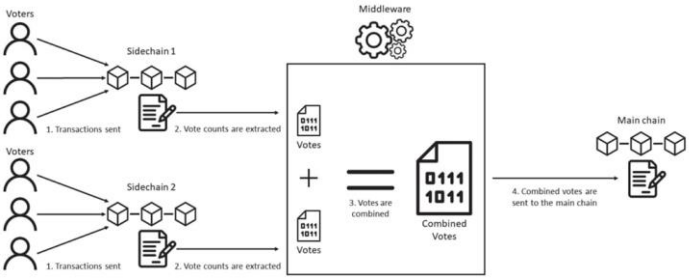


Рисунок 2. Механізм роботи смарт-контрактів

Прикладом є такі функції з роллю OnlyAdmin:

1. setValidatorContract() : Встановити валідатора.
2. setThreshold() : Встановіть порогове значення для кворуму
3. pause() / unpause() : призупинити/відмінити контракт
4. setThreshold() : Встановіть порогове значення ваги голосування високого рівня.

За аудитом двох компаній, надані функції є надважливими, вони можуть змінювати властивості цілої системи, що не мало б відбуватись просто так, відповідно до політики безпеки блокчейну та смартконтрактів. [4]. Таке застосування дозволяється для тестової або приватної

мережі, однак у реальній мережі інтернет це несе велику загрозу [9]. Хакеру достатньо скомпрометувати лише один обліковий запис з такою роллю, або ж стати користувачем з такими привілеями, і він отримає доступ до усього функціоналу. Хакеру при цьому доступні безліч векторів атак, наприклад компрометація валідатора з даною роллю та підвищення привілеїв. При цьому використання інших функцій дозволить хакеру залишатись довго непоміченим [8]

Варто зазначити, що роозробники не надають ніякої інформації про системи моніторингу. При цьому в аудиті від CertiC зга- дується що розробникам негайно необхідно ввести таку. З чого можна зробити припущення що моніторингова система в або відсутня або в стадії розробки. Що дозволить хакеру залишатись непоміченим більшу кількість часу.

За дослідженням китайського Інституту Технологій та Науки, валідатори обрані консенсусом PoA мають певні привілеї. Такі "довірені особи"можуть влаштувати приховане відмивання активів на основі невидимості транзакцій в певні моменти затримки. [9]

## Висновки

З огляду на нехтування безпекою та впливом механізмів консенсусу та рольової моделі, дане питання має бути розглянуте детальніше. Тематика є актуальною насьогодні, розробки все ще тривають, та на жаль деякі протоколи піддаються масштабним атакам.

## Перелік використаних джерел

1. Mavis S. Official Axie Infinity Whitepaper. — 01/01/2023.

2. Mavis S. Official Ronin Whitepaper Consensus. — 04/28/2023.

3. Lee M. Ronin: The engine powering Axie Infinity’s growth. — 10/01/2022.

4. Hanna H., Natalia L., Semi M. Understanding Smart Contracts as a New Option in Transaction Cost Economics //

Electronic Library (AISeL). — 2019. — URL: https://core.ac.uk/download/pdf/30138 4316.pdf.

5. Alam O. Understanding the economies of blockchain games: an empirical analysis of Axie Infinity // Distributed Computing Group Computer Engineering and Networks Laboratory ETH Zürich. — 2022. — URL: https://pub.tik.ee.ethz.ch/students/2 022-FS/BA-2022-08.pdf.

6. BEHNKE R. EXPLAINED: THE RONIN HACK (MARCH 2022). — 03/30/2022.

7. Vishal B., Aniruddha B. Preferential Delegated Proof of Stake (PDPoS)—Modified DPoS with Two Layers towards Scalability and Higher TPS // MDPI. — 2023. — URL: https://www.mdpi.com /2073-8994/15/1/4/pdf.

8. CertiK. Security Assessment Ronin DPoS Contracts. — 03/30/2023.

9. Exploring Unfairness on Proof of Authority: Order Manipulation Attacks and Remedies / W. Qin, L. Rujia, W. Qi, C. Shiping, X. Yang. — 05/01/2022.

# ЗАХИСТ ПРОМИСЛОВИХ СИСТЕМ ТА СИСТЕМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД НИЗЬКОЛІТАЮЧИХ БПЛА

Кирилюк Д.В., Василенко О.Д.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», НН Фізико-технічний інститут, Київ, Україна

Робота присвячена розгляду особливостей виявлення низьколітаючих БПЛА при захисті промислових систем та систем критичної інфраструктури.

**Ключові слова:** БПЛА, низьколітаючі об’єкти, радіолокаційне виявлення

## Вступ

Під час війни супротивник нерідко використовує БПЛА, як небезпечну зброю, що може на дальніх відстанях уражати не тільки військову техніку, але й підприємства критичної

інфраструктури. Тому є необхідність їх виявлення безпосередньо на підльотах до цих об‘єктів.

## Найбільш ефективний метод виявлення

Напади в більшості випадків здійснюються в нічний час, коли видимість обмежена, виявлення та фіксація оптичними системи БПЛА стає складним завданням. Отже, єдиним на сьогодні найбільш ефективним методом є радіолокаційне виявлення.[2]

- РЛС може працювати в будь-яких погодних умовах і в будь-який час доби.
- РЛС мають високу точність визначення положення та швидкості об'єктів, зокрема БПЛА.
- РЛС можуть виявляти БПЛА на значній відстані, що дозволяє попереджати про можливу небезпеку та вживати запобіжних заходів на ранній стадії.
- Крім того, радіолокаційне виявлення може використовуватися, як складова частина комплексної системи безпеки, що може включати різні датчики та системи, такі як відеокамери, теплові датчики та інші.

## Труднощі виявлення БПЛА на низьких висотах

Виявлення низькошвидкісних цілей ускладнюється через накладання спектру їх луна-сигналів на спектр перешкод у доплерівській області. При придушенні спектру перешкод, одночасно відбувається і придушення луна-сигналу від низькошвидкісної цілі, що суттєво утруднює її виявлення.

Крім того,через низьку висоту і швидкість польоту спектр луна-сигналу близький до нульової частоти в доплерівській області частот і, одночасно перекривається з сильними завадами від землі та повільними перешкодами. Традиційними методами фільтрації в частотній області важко виявити ціль.

Оскільки RCS невелика, енергія відбиття низька та може бути менша за суму перешкод та шумів. Тому виявлення такого БПЛА стає дуже важким.

## Вплив інтерференції на виявлення

При виявленні цілі у вільному просторі узагальнене рівняння дальності має вигляд [1]:

$$R = \sqrt[4]{\frac{P_{пер} G_{пер} G_{пр} \lambda^2 \sigma_ц}{(4\pi)^3 P_{пор_{РЛС}}}},$$

Однак ця формула не враховує інтерференційні явища, коли ціль знаходиться поблизу землі. У цьому випадку, за рахунок відбиття від поверхні землі з'являється сильна інтерференція, що іноді призводить до повного пропадання луна – сигналу від цілі на деяких висотах - така ситуація зображена на Рис. 1

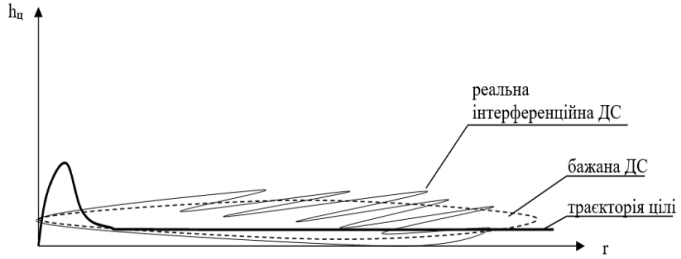


Рисунок 1.

При виявленні низьколітаючих об'єктів (r >> H) кут місця невеликий і ціль зазвичай знаходиться в нижній частині першої пелюстки діаграми спрямованості антени (ДС). Тоді максимальна відстань [3] виявлення цілі має вигляд:

$$r = \sqrt[8]{\frac{8\pi\, P\, \tau\, G^2\, h^4\, \sigma\, H^4}{\lambda^2\, q^2\, k\, L\, T}}$$

P - потужність антени: $10^4$ Вт, $\tau$-тривалість імпульсу: $10^{-9}$с, h - висота антени: 2 м, $\lambda$ - довжина хвилі: 3 см = 0.03 м, q - відношення сигнал/шум: 4, $G$ – коефіцієнт спрямованості антени (прийом-передача): 430, $\sigma$ – ефективна площа розсіювання: 0.02 м$^2$, k – стала Больцмана:$1.38*10^{-23}$ Дж/К, T - шумова температура: 300 К,

L - коефіцієнт відхилення характеристик від оптимальних (від 1 до 8): 4,

Нижче (рис.2)наведений графік інтегральної оцінки дальності виявлення для висоти цілі від 0 до 100 м.

Оцінка наведеної залежності, показує, що зі збільшенням висоти польоту БПЛА, ( коли зменшується вплив інтерференції) збільшується максимальна відстань виявлення. Так, при висоті польоту цілі 8 м, теоретично максимальна відстань виявлення буде 2000 м, а при висоті у 100 м то 7071 м.

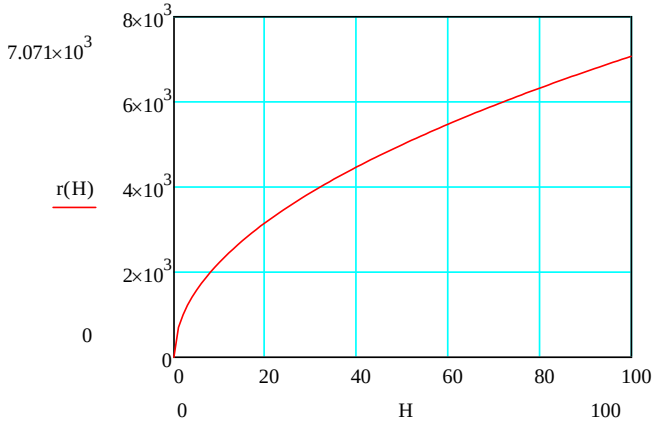


Рисунок 2.

## Висновки

Наведені особливості виявлення низьколітаючих БПЛА при захисту промислових систем та систем критичної інфраструктури.Показано, що коли відстань між радаром та БПЛА перевищує висоту останнього у багато разів (r>>H) потрібно враховувати інтерференційні впливи на луна-сигнали та використовувати відповідну формулу. Отримана за розрахунками інтегральна залежність максимальної відстані виявлення від висоти польоту для дрона DJI Mavic 3 для середніх показників параметрів виявлення.

## Перелік використаних джерел

1. Ю.Г. Даник, М.В. Бугайов. Аналіз ефективності виявлення тактичних безпілотних літальних апаратів пасивними та активними засобами спостереження. — Вип. 10 / Житомирський військовий інститут імені С. П. Корольова Державного університету телекомунікацій. – Житомир. — ЖВІ ДУТ, 2015. — 5 с.
2. Конспекти лекцій по дисципліні “Радіонавігаційні прибори і системи” Демиденко П.П. — Одеса. — 2010.
3. Казаринова Ю. Радиотехнические системы. — 1990. — 221 с


# ПОБУДОВА ТАКСОНОМІЇ ТЕХНІК АНТИВІРТУАЛІЗАЦІЇ ІЗ ВИКОРИСТАННЯМ АПАРАТУ Q-АНАЛІЗУ


Д.І. Флекевчук
Навчально-науковий Фізико-технічний інститут,
КПІ ім. Ігоря Сікорського, Київ, Україна



Ця стаття містить інформацію про техніки для протидії віртуалізації, які покладаються на аналіз діяльності користувача, щоб визначити природу середовища. У статті також запропоновано метод побудови класифікації технік, та результат роботи цього методу. Розглянуто варіанти протидії різним класам технік ухилення від віртуалізації, які можуть використовувати зловмисники при розробці ШПЗ.


**Ключові слова:** віртуалізація, ШПЗ, класифікація, Q-аналіз.


## Вступ

У міру того, як методи дослідження шкідливого програмного забезпечення, що використовують віртуалізацію, стають все популярнішими, зловмисники

почали використовувати способи для уникнення виявлення. Якщо шкідливий софт здатний визначити віртуальне середовище, воно може приховати свій повний функціонал, ускладнюючи цим своє виявлення.

Основна мета цієї роботи – протистояти технікам обходу віртуалізації, які основані на аналізі дій користувача, оскільки не існує єдиного підходу або фреймворку, який би допоміг дослідникам створити надійне маскування своїх лабораторій для боротьби з шкідливим ПЗ, яке використовує ці техніки.

## Інформація про існуючі техніки

Перевірка наявності активності користувача в середовищі є часто використовуваною методикою для виявлення віртуалізації. Дії, які характерні для активного використання комп'ютера, такі як натискання клавіш або миші, прокрутка веб-сторінок та документів, рухи мишею, а також артефакти, що виникають під час використання комп'ютера, як записи в реєстрі, вкладки та історія браузера, відкриті документи та інше, можуть свідчити про активність користувача. Відсутність таких ознак може бути використана зловмисниками, щоб уникнути виявлення віртуалізації. В літературі мною було знайдено реалізацію таких технік.

- Перевірка на наявність файлів в ключових директоріях.
- Перевірка кількості недавно редагованих документів та процесів
- Перевірка встановленості базових пакетів та утиліти
- Перевірка кількості записів в історії браузеру
- Перевірка атрибутів цільового користувача
- Перевірка руху курсору
- Прокручування документів та застосунків, кліки.
- Перевірка з допомогою взаємодії з користувачем.

## Методи досліджень

Для початку потрібно визначити формат в, якому ми зберігатимемо дані про техніки. Потрібен зручний підхід,

що враховуватиме нові техніки. Найпростіший варіант це зв'язок техніка тег. Техніка буде представлена текстовим описом, іменем, та набором тегів, що виділяють її основні властивості. В свою чергу запис про тег буде представляти собою ідентифікатор ID, назву, та опис.

Для побудови класифікації цей спосіб представлення дуже допоможе, адже легко знаходити зв’язки, що є між техніками. Чим більше спільних зв’язків-тегів тим більше споріднені техніки, якщо таких споріднених технік відносно багато то ми можемо говорити про те, що вони утворюють клас.

Q-аналіз застосовують для дослідження зав’язків, отже ми можемо дослідити, зв’язки в середині комплексу, який утвориться якщо обрати теги за вершини а техніки за симплекси, з допомогою нього. За результатами Q-аналізу ми отримаємо набір симплексів. Де кожен сиплекс є класом еквівалентності відносно q де q – розмірність зв’язку 1. На основі утворених класів можна побудувати класифікацію.

В класифікації потрібно визначити імена класів. Імена можна дати на основі q найпопулярніших тегів серед технік у симплексі-класі, де q розмірність зв’язку на рівні. Застосуймо алгоритм на даних, що було зібрано. Рис 1.

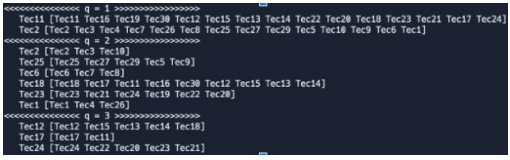


Рисунок 1. Результати Q-аналізу

Пройдемось алгоритмом по зібраним даним і отримаємо.

Варто додати, що мною були відібрані теги, які пов’язані з підсистемами ОС, подіями які генерує користувач. Таким чином ми отримаємо класи, що об’єднують техніки на основі того, відсутність чого використовують техніки в своїй роботі, для детекції віртуального середовища.

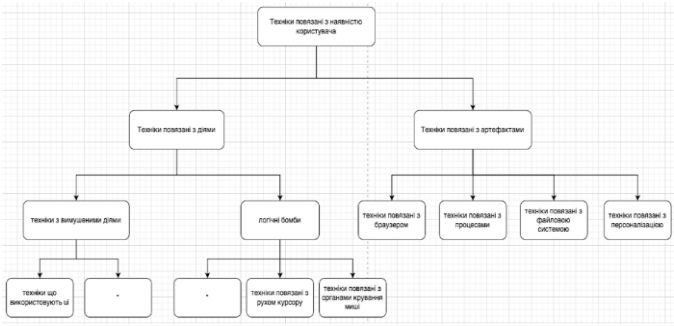


Рисунок 2. Класифікація

## Висновки

В ході роботи ми отримали класифікацію, метод за якім вона побудована та структура даних, в якій вони подані дозволяє розширювати її просто додаючи нові теги та техніки за потреби. З допомогою цієї класифікації можна побудувати застосунок, що маскуватиме наше віртуальне середовище.

## Перелік використаних джерел

1. Casti J. Connectivity, Complexity, and Catastrophe in Large-Scale Systems. — John Wiley & Sons, 01.01.1979. — 203 с. — ISBN 0471276618X.

# ПРОТИДІЇ ЗАГРОЗАМ, НАЦІЛЕНИМ НА DATA PLANE І CONTROL PLANE

Дорош А.О., Демчинський В.В.
Навчально-науковий Фізико-технічний інститут,
КПІ ім. Ігоря Сікорського, Київ, Україна

Стаття має на меті розглянути методи для їх протидії основних векторів атак, що націлені на Data Plane і Control Plane програмно-визначених мереж.

**Ключові слова:** Програмно-визначені мережі; площина управління; площина керування; безпека SDN; SDN; площина керування; площина пересилання.

## Вступ

Програмно-визначені мережі (SDN) - це парадигма мережевої архітектури, яка дозволяє створювати гнучку, централізовано керовану мережеву інфраструктуру. Цей процес досягається за рахунок розділення площини управління і площини даних на окремі сутності.

Площина управління (Control Plane) бере на себе відповідальність за прийняття рішень щодо напрямку потоку трафіку. Southbound інтерфейси використовується площиною керування для передачі інструкцій до площини даних.

Площина пересилання (Data Plane), яку зазвичай називають площиною даних, відповідає за передачу пакетів між двома різними точками. Система включає в себе різні пристрої, такі як комутатори і маршрутизатори, які виконують фізичну передачу і прийом пакетів даних відповідно до правил, встановлених площиною управління.

## Визначення потенційних загроз

На визначення і класифікацію потенційних загроз напряму впливає визначена топологія мережі. Проте у той самий час можливо визначити потенційні атаки, що притаманні саме площині керування, площині управління і інтерфейсами між ними.

До атак, що націлені саме на площину керування можна віднести Sybil attack, підміну ідентифікаторів каналів передачі даних, Packet-In flooding, Controller hijacking, тощо.

Площина пересилання вразлива переважно до маніпуляції таблицею потоків або ж її переповнення, що може призвести зокрема до DoS.

Атаки на Southbound інтерфейси і внутрішні інтерфейси у раніше згаданій площині пересилання включають в себе MiTM, або ж її варіацію - Eavesdrop.

## Методи протидії загрозам

Аналіз потенційних загроз дозволив винести наступні заходи для їх протидії: архітектурні рішення, шифрування каналів зв’язку, автентифікація пристроїв, сегментація мережі, якісне логування і моніторинг.

Оскільки безпека будь-якої системи починається ще на етапі проектування, важливо використати всі можливості, які надають SDN, і одразу визначити необхідний функціонал. Сюди входить реалізація специфічних рішень, таких як алгоритми запобігання DoS-атакам, оперативне виявлення ARP спуфінгу, а також утилізація правил потоку, які зберігають комутатори.

Наступний етап - захист каналів зв'язку між вузлами мережі. Потенційними варіантами є використання TLS, або ж еліптичні криві (ECC), проте дослідження щодо визначення найкращого методу шифрування саме для SDN ще тривають.

Автентифікація пристроїв за допомогою цифрових сертифікатів або PKI необхідно для гарантії, що лише авторизовані пристрої беруть участь у мережевому спілкуванні.

Сегментація мережі дозволяє розділити мережу на ізольовані сегменти, підвищуючи безпеку та продуктивність. У той час як класичні мережі зазвичай використовують статичні віртуальні локальні мережі (“port-based”), SDN дозволяє адаптувати правила потоків для реалізації всіх доступних типів VLAN: port-based, MAC-based, protocol-based, тощо. До того ж тегування пакетів можна і зовсім оминути, визначивши критерії для розподілу пакетів ще на етапі визначення правил потоку.

Якісне реагування на інциденти починається з моніторингу і отримання оперативної інформації про систему. Використання різні інструменти, включаючи SIEM + SOAR для аналізу журналів, (N)IDS/IPS для виявлення вторгнень, NBA для аналізу аномалій трафіку, а також системи класу “deception” для збільшення поверхні атаки є варіантами.

## Висновки

Потенційні загрози для цих площин залежать від топології мережі, і можуть включаючи Sybil атаки, підміну ідентифікаторів каналів передачі даних, перехоплення контролерів на площині управління, маніпуляції з таблицями потоків або і зовсім їх переповнення, а також MiTM-атаки або їх різновид - Eavesdrop.

Контрзаходи включають архітектурні рішення, шифрування каналів зв'язку, автентифікацію пристроїв, сегментацію мережі, а також комплексне ведення журналів і моніторинг.

## Перелік використаних джерел


1. ONF. SDN Architecture 1.0 Overview. — 12.2016.
2. Flow wars: Systemizing the attack surface and defenses in software-defined networks / C. Yoon, S. Lee, H. Kang, T. Park, S. Shin, V. Yegneswaran, P. Porras, G. Gu // IEEE/ACM Transactions on Networking. — 2017. — Т. 25, No 6. — С. 3514—3530.
3. ONF. OpenFlow Switch Specification. — 04.2013.


# КОМПЛЕКСНИЙ МЕТОД ВИЯВЛЕННЯ GPS SPOOF АТАК НА БЕЗПІЛОТНІ ЛІТАЛЬНІ АПАРАТИ


Нетаврована А.В., Степаненко В.М.
Навчально-науковий Фізико-технічний інститут
КПІ ім. Ігоря Сікорського, Київ, Україна



В роботі досліджено метод комплексного захисту безпілотних літальних апаратів, на основі перевірки сигналів на нереалістично високі рівні потужності та класифікації підробок з використанням взаємної кореляції отриманих сигналів.



**Ключові слова:** GPS, GNSS, БПЛА, супутник, система

навігації, спуфер, детектування.

## Вступ

Розробка методів захисту від GPS Spoof атак є критично важливою для забезпечення безпеки та ефективності безпілотних літальних апаратів у різних сферах їх застосування. Такого роду атаки можуть стати причиною як відхилення від маршруту, так і повної втрати контролю над апаратом.

## GPS навігація

Система GPS навігації на найвищому рівні складається з супутників, що обертаються навколо землі двічі на день і знаходяться на середній навколоземній орбіті.

У найпростішому випадку, GPS-приймач L-діапазону приймає сигнали від супутників і за допомогою коду визначає свою відстань до нього. Якщо відстань до чотирьох супутників можна виміряти одночасно, то приймач може обчислити власну позицію в режимі реального часу.

## GPS Spoof атаки

Для реалізації GPS Spoof атаки, зловмисник може використати пристрій для підміни, що знаходиться на відстані від БПЛА. В такому випадку спуфер отримує реальні сигнали від супутників на одну з антен, на основі них генерує фальшиві, вирівняні за фазою коду з реальними сигнали і передає через іншу антену на БПЛА.

Щоб змусити літальний апарат прийняти підроблені сигнали за реальні, сигнали спуфера повинні перевищувати потужність сигналів супутників та з високою точністю прогнозувати для кожного отриманого сигналу величини:

1) Значення модульованих навігаційних даних;
2) Допплерівський зсув частот;
3) Зміщення фази;

Захист від GPS Spoof атак полягає в виявленні атаки та відновленні реальної позиції БПЛА. Стратегії виявлення підробки в основному базуються на двох підходах:

виявлення відмінностей між підробленими та справжніми сигналами та виявлення взаємозв'язку між ними. Найефективнішими з них є комплексні методи, які поєднують декілька підходів для забезпечення високої ймовірності виявлення атаки та реконструкції спотворених сигналів.

## Комплексний захист БПЛА від GPS Spoof атак

Для захисту безпілотного літального апарату на основі аналізу частот і потужностей отриманих сигналів, на першому кроці отримання, відбувається пошук всіх можливих допплерівських зсувів фаз коду і опорних частот. Тоді в випадку появи в пакеті сигналів більше одного незвичайного сигналу, тобто того, який перевищує встановлений поріг, можна сигналізувати про атаку.

Після цього весь набір сигналів від запідозреного в підміні супутника проходить процес класифікації, де на основі кореляційної функції та коефіцієнтів кореляції, сигнали сортуються на підроблені та справжні, за логікою, що підроблений набір сигналів має високий пік кореляції. Після такого визначення підроблених сигналів, реалізується відсіювання.

На основі таких перевірок кожного окремого каналу, підроблені сигнали видаляються з оригінальних оцифрованих зразків. Після видалення підроблених сигналів, приймач повторює цей процес ще раз, щоб виявити потенційно підроблені сигнали, що не були виявлені за першої ітерації

## Висновки

Окремі методи захисту GPS приймачів від Spoof атак мають свої власні недоліки, тому реалізація комплексного підходу, де методи доповнюють один одного – є сильним безпековим рішенням для захисту навігаційних сигналів.

Запропонований комплексний метод захисту навігаційних сигналів БПЛА, здатен виявляти спотворення, класифікувати їх та зменшувати шкідливий вплив підроблених сигналів. Такий підхід може підвищити

чутливість виявлення спотворень, а робота антиспуфінг застосувань всередині GPS приймача є взаємодоповнюючою.

## Перелік використаних джерел

1. Unmanned Aircraft Capture and Control Via GPS Spoofing / A. Kerns, D. Shepard, J. Bhatti, T. Humphreys // Journal of Field Robotics. — 2014. — July. — Vol. 31.

2. Psiaki M., Humphreys T. GNSS spoofing and detection // Proceedings of the IEEE. — 2016. — Квіт. — Т. 104. — С. 1—13.

3. Development of Anti-Spoofing Equipment Architecture and Performance Evaluation Test System / [J. Jung, S. Park, J. Hyun та ін.]. // Journal of Positioning, Navigation, and Timing. – 2018. – С. pp. 127–138

4. Pre-Despreading Authenticity Verification for GPS L1 C/A Signals / [A. JAFARNIA-JAHROMI, A. BROUMANDAN, J. NIELSEN та ін.]. // Journal of The Institute of Navigation. – 2014. – С. 1–11.

# ОЦІНКА ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Жембровська О., Ткач В.
Навчально-науковий Фізико-технічний інститут
КПІ ім. Ігоря Сікорського, Київ, Україна

Робота присвячена аналізу та аналітичному огляду існуючих методів оцінки захищеності інформаційної системи. Пошуку універсального методу, або алгоритму, за допомогою якого, спеціаліст з кібербезпеки може оцінити наскільки система захищена.

**Ключові слова**: інформаційна система, захищеність, критерії, оцінка

## Вступ

Інформаційні системи використовуються в різних сферах діяльності, таких як бізнес, урядові установи, освіта, наука,

медицина та багато інших. Вони можуть бути розроблені для специфічних завдань або включати у себе комплексні рішення.

Оцінка захищеності інформаційної системи є надзвичайно важливою задачею, оскільки забезпечення безпеки інформації є критичним аспектом для будь-якої організації чи підприємства.

## Основна частина

Для аналізу і аналітичного огляду різних методів і моделей необхідно було визначити критерії за якими варто оцінювати інформаційну систему. Найбільш важливими і вагомими для побудови захищеної інформаційної системи є: конфіденційність, цілісність, доступність, аутентифікація, авторизація, надійність, відновлюваність, спостережуваність.

В роботі порівнюється Security Maturity Model, Threat and Risk Assessment, а також інші.

## Security maturity model

Security maturity model - це модель, яка допомагає компаніям оцінити та покращити рівень зрілості їхньої інформаційної безпеки, включає 5 рівнів зрілості: неформальний рівень безпеки, рівень реакції, рівень запобігання, рівень управління ризиками, рівень оптимізації.

Модель зрілості безпеки використовують як інструмент для визначення областей, які потребують пріоритетності для вдосконалення, і порівняння прогресу під час створення середовища контролю безпеки.

## Threat and Risk Assessment (TRA)

Threat and Risk Assessment (TRA) - це процес оцінки потенційних загроз та ризиків для системи, її інфраструктури та даних. Процес TRA складається з таких етапів: ідентифікація активів, визначення потенційних загроз, оцінка вразливостей, оцінка наслідків, оцінка ризиків, розробка плану захисту.

SMM допомагає зосередитися на розвитку та підвищенні рівня безпеки системи, тоді як TRA зосереджується на ідентифікації та зменшенні ризиків, пов'язаних з безпекою системи.

## Рівні захищеності системи

На основі проведеного аналізу, було створено новий універсальний метод оцінювання захищеності інформаційної системи, оснований на принципі ієрархічності піраміди Маслоу. Перш ніж перейти на інший рівень захищеності необхідно задовольнити попередній.

Завдяки ієрархічній структурі даної моделі, з'являється можливість чітко визначити на якому рівні інформаційна система в даний момент.

**Рівень доступу**: Система має базові заходи безпеки, такі як встановлення паролів і обмеження доступу до конфіденційної інформації.

**Рівень контролю**: Система має розширені заходи безпеки, які включають в себе регулярне оновлення програмного забезпечення, встановлення антивірусного програмного забезпечення, аутентифікацію користувачів і контроль доступу до конфіденційної інформації.

**Рівень оборони**: Система має високий рівень захисту, що включає в себе захист від відомих та невідомих загроз, в тому числі захист від атак з використанням соціальної інженерії, а також захист від внутрішніх загроз, таких як зловживання даними або крадіжки інформації. Крім того, така система може мати складну інфраструктуру з високим рівнем автоматизації процесів забезпечення безпеки.

**Рівень випередження**: Система має найвищий рівень захисту, що включає в себе захист від невідомих загроз, захист від атак з використанням передових технологій та захист від внутрішніх загроз з боку найбільш привілейованих користувачів. Вона може мати складну інфраструктуру з високим рівнем автоматизації процесів забезпечення безпеки.

## Висновок

В ході роботи було розроблено метод оцінювання захищеності інформаційної системи за допомогою якого спеціалісти кібербезпеки з легкістю зможуть передавати роботу один одному, адже зазначивши на якому рівні зараз знаходиться система, інший спеціаліст одразу зрозуміє обсяг роботи який йому необхідно впровадити задля забезпечення найвищого рівня захищеності системи.

## Перелік використаних джерел


1. [Ел. ресурс] – https://www.geeksforgeeks.org/the-cia-triad-in-cryptography/
2. НД ТЗІ 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”


# ЗАХИСТ ЦИФРОВИХ ПІДСТАНЦІЙ ВІД ЗОВНІШНІХ АТАК


Гільгурт С.Я.

Інститут проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України, Київ, Україна,
hilgurt@ukr.net



Розглянуто проблему захисту від зовнішніх атак цифрових електричних підстанції, побудованих на основі стандарту МЕК 61850. Досліджено питання створення систем виявлення атак на такі об’єкти.



**Ключові слова:** МЕК-61850, цифрова підстанція, СВВ, специфікаційні правила.


## Вступ

На жаль, застосування сучасних цифрових технологій автоматизації промислових систем підвищує загрози кібербезпеки. У випадку об’єктів критичної інфраструктури, зокрема, енергетичної галузі, наслідки від

кібератак можуть бути набагато більш важкими в порівнянні з традиційними галузями застосування інформаційних технологій [1, 2]. У даній роботі розглянуто проблему захисту від зовнішніх атак об’єктів електроенергетики, а саме – цифрових підстанції (ЦПС).

## 1. Стандарт МЕК 61850

Електричні підстанції є одними з найчисленніших об'єктів енергетики та відіграють вирішальну роль у всій енергосистемі, виконуючі важливі функції з розподілу та перетворення енергії [3]. Для вирішення проблеми взаємодії пристроїв декількох поколінь, не сумісних між собою було створено стандарт МЕК 61850 «Мережі та системи зв'язку на підстанціях» [4].

Відповідно до стандарту МЕК 61850 система автоматизації інформаційного обміну на енергооб'єкті за схемою ЦПС складається з трьох рівнів [3]: станційний (Station Level) – найвищій рівень, рівень приєднання (Bay Level) та рівень процесу (Process Level) або "польовий" (Field Level) – найнижчий рівень. Кожен рівень виконує притаманні йому функції, за які відповідають певні типи пристроїв. Комунікації можливі як всередині рівнів (горизонтальні), так і між рівнями (вертикальні).

## 2. Протоколи стандарту МЕК 61850

На додаток до традиційних протоколів, таких як FTP або HTTP, стандарт МЕК 61850 вводить нові протоколи, а саме: MMS (Manufacturing Message Specification) – для зв'язку інтелектуальних пристроїв (IED) зі станційним рівнем, GOOSE (Generic Object Oriented Substation Events) – для зв'язку IED між собою, SV (Sampled Values) – для зв'язку між IED та MU. Строго кажучи, MMS є не протоколом, а специфікацією, що описує інформаційну модель пристроїв та даних рівня приєднання. Але, оскільки сервіс, що використовує MMS, застосовує рівень додатків стандартного стеку мережевих протоколів OSI, його також можна умовно вважати протоколом обміну. Принаймні, в технічній літературі з питань використання стандарту МЕК 61850 та вирішення проблем захисту інформації в ЦПС на

його основі, скорочення MMS в переважної більшості публікацій згадується саме як протокол.

Достатньо змістовний опис згаданих протоколів, включаючи часові діаграми, можна знайти в літературі, наприклад, в [3]. Зауважимо, що в кіберфізичних системах, побудованих на базі стандарту МЕК 61850, також можуть використовуватися інші мережеві протоколи, наприклад, поширена польова шина MODBUS, або її пропріетарна модифікація MODBUS Plus, протокол часової синхронізації PTP (Precision Time Protocol), протокол виявлення мережевих пристроїв LLDP (Link Layer Discovery Protocol) та ін.

## 3. Системи виявлення вторгнень для цифрових електричних підстанцій

Особливості ЦПС, зокрема, застосування спеціалізованих протоколів, накладають певну специфіку при створенні систем виявлення вторгнень (СВВ) для цифрових підстанцій на базі стандарту МЕК 61850 [5]. Технічно робота таких СВВ зазвичай ґрунтується на використанні званих специфікаційних правил (specification rules) для всіх можливих атак на кожний з протоколів.

В якості прикладів можна навести наступні подібні правила [4]:

(#R1) Повідомлення GOOSE повинні мати MAC-адресу, що починається з 01-0c-cd-01.

(#R2) Повідомлення GOOSE повинні мати поле *TPID* зі значенням0x8100.

(#R3) Повідомлення GOOSE повинні мати поле *ethertype* рівним 0x88B8.

(#R5) Повідомлення GOOSE повинні мати поле *APPID*, відформатоване як шістнадцяткове 4-байтове (наприклад, 0000-3FFF).

(#R12) Кількість повідомлень, виявлених протягом певного періоду часу, не має дорівнювати нулю.

(#R13) Мітка часу передавача не повинна бути більше мітки часу приймача.

(#R14) Мітка часу передавача з повідомлень GOOSE не повинна знаходитись на відстані більше 4 мс від мітки часу

приймача.

(#R15) Метрика *Recency*, що представлена останнім повідомленням GOOSE, повинна відповідати мінімальному та максимальному пороговому значенню.

(#R16) Показник частоти, представлений середньою кількістю отриманих повідомлень GOOSE, повинен відповідати мінімальному та максимальному заздалегідь визначеному порогу.

(#R21) Кількість байтів, які проходять за секунду, не повинна перевищувати заздалегідь визначеного порогу.

(#R22) Кількість пакетів, які рухаються в секунду, не повинна перевищувати заздалегідь визначеного порогу.

(#R23) Довжина пакета (вказана в заголовку пакета) не повинна перевищувати заздалегідь визначеного порогу.

(#R24) Загальний розмір пакету не повинен перевищувати заздалегідь визначеного порогу.

## Висновки

В роботі досліджені питання створення системи виявлення вторгнень для цифрових електричних підстанцій на основі стандарту МЕК 61850. Наведені відомості щодо побудови таких систем з використанням підходу на базі специфікацій.

## Перелік використаних джерел

1. Sanger D.E. Cyberattack Forces a Shutdown of a Top U.S. Pipeline / D.E. Sanger, C. Krauss, N. Perlroth // The New York Times (May 8, 2021). – Режим доступу: https://www.nytimes.com/2021/05/08/us/ politics/cyberattack-colonial-pipeline.html.

2. Radichel T. Colonial Pipeline Hack / T. Radichel // 2nd Sight Lab (May 15, 2021). – Режим доступу: https://medium.com/cloud-security/colonial-pipeline-hack-4486d16f2957.

3. Communication Networks and Systems in Substations. IEC Std. 61850.

4. Quincozes S.E., Albuquerque C., Passos D., Mossé D. A survey on intrusion detection and prevention systems in

digital substations // Computer Networks. – 2021. – Vol. 184. – Article 107683.

5. Yang Y., Xu H.-Q., Gao L., Yuan Y.-B., Sezer S. Multidimensional intrusion detection system for IEC 61850-based SCADA networks // IEEE Trans. Power Deliv, 2017. – Vol. 32, № 2. – P. 1068-1078.

# АНАЛІЗ ВРАЗЛИВОСТЕЙ WI-FI МЕРЕЖ

Колісник Т.П., Маслов Б.С.
Харківській національний університет внутрішніх справ

Розглянуто особливості масового зростання кількості кібератак через загальнодоступні мережі Wi-Fi. Показано найпоширеніші вразливості бездротової мережі: використання SSID і паролів за замовчуванням; розміщення точки доступу, де може статися втручання; використання вразливого протоколу WEP; вразливість до злому WPA2
**Ключові слова:** WiFi, кібератака, SSID, DNS-сервер, WEP, WPA2, NetSpectre

Багато підприємств перейшли від дротових до бездротових технологій, що негативно вплинуло на їх стан безпеки. Дротові мережі, як правило, набагато легше захистити, ніж бездротові, і погана реалізація часто створює вразлості в мережах WiFi. Багато компаній також не виконують ретельний аналіз ризиків, що означає, що ці вразливості не визначаються та не усуваються. Через ці недоліки безпеки та легкість їх використання атаки на бездротові мережі є поширеними.

Раніше за доступ до Wi-Fi доводилося платити, але зараз безкоштовний Wi-Fi став для багатьох людей само собою зрозумілим. Відвідувачі готелю, кав'ярні, бару, торгової точки чи ресторану тепер очікують, що Wi-Fi буде надаватися безкоштовно. На рішення про використання певного закладу часто впливає наявність безкоштовного Wi-Fi, але все частіше якість з’єднання є фактором у процесі прийняття рішення.

Масове зростання кількості кібератак через

загальнодоступні мережі Wi-Fi у поєднанні з попередженнями про ризики Wi-Fi у основних ЗМІ свідчать про те, що багато споживачів віддають перевагу закладам, які пропонують безпечний доступ до Wi-Fi.

Наведемо деякі з найпоширеніших вразливостей бездротової мережі. Ці вразливості можна легко використати в реальних атаках на бездротові мережі, щоб викрасти конфіденційні дані, отримати контроль над маршрутизатором або підключеним пристроєм або встановити зловмисне програмне забезпечення чи програми-вимагачі.

*Використання SSID і паролів за замовчуванням.* Точки доступу Wi-Fi постачаються з SSID і паролем за замовчуванням, які потрібно змінити, але надто часто ці паролі за замовчуванням залишаються на місці. Це спрощує зловмисникам вхід в систему та отримання контролю над маршрутизатором, зміну параметрів чи пришивки, завантаження шкідливих сценаріїв або навіть зміну DNS-сервера, щоб весь трафік спрямовувався на IP-адресу, якою володіє зловмисник. Необхідно змінити паролі за замовчуванням, щоб будь-хто в зоні дії сигналу не міг під'єднуватися та перехоплювати чи прослуховувати трафік.

Якщо бездротові контролери використовуються для керування точками доступу WiFi через веб-інтерфейси, переконайтеся, що стандартні паролі також змінено. Ці паролі за замовчуванням можна легко знайти в Інтернеті та використовувати для атаки на бездротові мережі [1].

*Розміщення точки доступу, де може статися втручання.* Якщо точку доступу розміщено в місці, де до неї можна отримати фізичний доступ, може статися втручання. Повернення точки доступу до заводських налаштувань за замовчуванням займає кілька секунд. Переконайтеся, що точка доступу розташована в безпечному місці.

*Використання вразливого протоколу WEP.* Протокол Wired Equivalent Privacy (WEP) був першим протоколом, використаним для шифрування бездротового трафіку. WEP, як випливає з назви, мав на меті зробити бездротові мережі

такими ж безпечними, як і дротові аналоги, але це не робить бездротові мережі WEP безпечними.

WEP базується на шифрі RC4, який є безпечним. Проблема полягає в тому, як RC4 реалізовано в WEP. WEP дозволяє повторно використовувати вектор ініціалізації, а повторне використання ключів ніколи не є гарною ідеєю. Це дозволяє зловмиснику легко зламати шифрування. У WEP було виявлено кілька інших вразливостей, які роблять його далеко не безпечним.

Незважаючи на те, що WEP знецінився, і існують набагато безпечніші протоколи бездротового шифрування, багато компаній продовжують використовувати WEP, помилково вважаючи його безпечним. WEP надійніший, ніж повне відсутність шифрування – погана безпека краще, ніж відсутність – але є набагато безпечніші варіанти шифрування трафіку WiFi. Якщо ви хочете покращити безпеку та запобігти атакам WLAN, оновіть до WPA2 або WPA3, які використовують набагато безпечніший розширений стандарт шифрування (AES) і не мають вразливості WEP [2].

*Вразливість до злому WPA2*. WPA може бути більш безпечним, ніж WEP, але він не позбавлений власних бездротових вразливостей. Двоє бельгійських дослідників – Меті Ванхоф і Франк Піссенс з Левенського університету виявили серйозний недолік у протоколі безпеки WPA. Недолік отримав назву KRACK, скорочення від Key Reinstallation Attack. Порушення можна використати в атаці "людина посередині", щоб викрасти конфіденційні дані, надіслані через зашифроване WPA-з'єднання WiFi. У разі використання недоліку WPA зловмисник може підслухати трафік і отримати банківські облікові дані, паролі та інформацію про кредитну картку.

Вразливість існує в чотиристоронньому рукостисканні (хендшейку). Зашифроване з'єднання WPA2 починається з чотирьохстороннього рукостискання, але не всі частини цього рукостискання є обов'язковими. Для прискорення повторних з'єднань третя частина передається повторно. Ця третя частина рукостискання може повторюватися кілька разів, і саме цей крок може бути використаний для

атаки на бездротову мережу.

Зловмисник може створити клон точки доступу Wi-Fi, до якої раніше підключався користувач – злий близнюк. Користувачеві нічого не здається підозрілим, оскільки доступ до Інтернету надаватиметься через цього злого близнюка. Зловмисник може змусити користувача підключитися до клонованої мережі WiFi, і вся інформація, надіслана через цю злу подвійну мережу WiFi, може бути перехоплена. Хоча атака не працюватиме на сайтах із шифруванням SSL/TLS, можна використовувати інструменти, які роблять це можливим, змушуючи користувача відвідувати HTTP-версію веб-сайту.

Щоб здійснити атаку KRACK WiFi, мережа WiFi має використовувати WPA2-PSK або WPA-Enterprise, а зловмисник має бути в зоні дії сигналу WiFi. Практично всі маршрутизатори, які зараз використовуються, вразливі до атак KRACK WiFi. Найкращий захист — підтримувати маршрутизатори в актуальному стані та дозволяти користувачам підключатися до бездротових мереж лише за допомогою платного та найновішого VPN. Проблему вирішено в WPA3, який підтримується останніми бездротовими точками доступу. Однак, навіть з огляду на цю винятково поширену вразливість бездротової мережі, WPA2 все ще набагато безпечніший, ніж WEP.

*NetSpectre – віддалений експлойт Spectre.* Spectre — це вразливість, яка впливає на мікропроцесори, які виконують передбачення розгалужень. Цю вразливість можна використати, щоб дозволити зловмиснику отримати доступ до вибраних місць віртуальної пам’яті та таким чином отримати конфіденційні дані. Щоб використати недолік, зловмиснику спочатку потрібно буде переконати користувача завантажити та запустити зловмисний код або відвідати веб-сайт, де в браузері запускається JavaScript. Дослідники з Технологічного університету Граца розробили новий тип атаки, який можна здійснити через мережеві з’єднання, включаючи мережі WiFi. Атака під назвою NetSpectre, на щастя, є складною, тому існують набагато простіші способи атакувати організацію. Тому ризик експлуатації низький.

**Висновки**. Для забезпечення безпеки бездротових мереж розроблено відносно багато методів. Так, наприклад, можна використовувати віртуальні приватні мережі VPN (Virtual Private Network) чи протокол SSL (Secure Sockets Layer).

## Перелік використаних джерел

1. Top 10 vulnerabilities in Today`s WI-FI Networks // Computerworld URL: https://www.computerworld.com/article/2577244/top-10-vulnerabilities-in-today-s-wi-fi-networks.html. (дата звернення: 02.05.2023).
2. Уязвимости Wi-Fi сетей. // WIFI-AC | Все о Wi-Fi системах. URL: https://wifi-ax.com/64-uyazvimosti-wi-fi-setey.html. (дата звернення: 02.05.2023).

# ОЦІНКА ЕФЕКТИВНОСТІ ДЕЯКИХ ЗАСОБІВ МАСКУВАННЯ СИГНАТУРИ ШКІДЛИВОГО КОДУ

Носов В.В., Івахненко О.С.
Харківській національний університет внутрішніх справ

Розглянуто один із способів маскування шкідливих програм є створення зловмисниками - троянів. Проведено дослідження оцінки ефективності деяких відомих програмних засобів маскування вірусів.
**Ключові слова:** комп'ютерний вірус, Remote Access Trojan, RAT Kali Linux, обфускатор, VirusTotal

Одним із способів маскування шкідливих програм є створення зловмисниками так званих троянів (Trojan), які виглядають як звичайні користувацькі файли і навіть зберігають свою функціональність, але додатково містять зловмисний код, що починає приховано виконуватися при запуску/відкриті такого файлу. Зокрема трояни із кодом для отримання віддаленого доступу до системи користувача (Remote Access Trojan, RAT) [1] зазвичай мають вигляд і

функціональність файлів електронних документів (docx, xlsx, pdf, тощо). Відкриття користувачем такого електронного документу приховано запускає в системі жертви сервер віддаленого доступу, який повідомляє клієнтській частині RAT зловмисника про готовність виконувати віддалені команди.

Зловмисник з клієнтської частин RAT має можливість віддалено:

- слідкувати за діями користувача;
- запускати довільні файли;
- відключати та зупиняти сервіси операційної системи;
- робити та зберігати знімки екрану;
- включати веб-камеру;
- сканувати локальну мережу користувача;
- завантажувати свої та модифікувати існуючі файли;
- відкривати та закривати логічні порти системи.

Сучасні антивірусні системи здатні виявляти шкідливий код відомих RAT через пошук відповідних сигнатур у файлах, що перевіряються. Для ускладнення виявлення RAT антивірусом зловмисники додатково модифікують код за допомогою засобів маскування, які застосовують: криптографічні перетворення, стиснення і/або штучну зміну сигнатури коду RAT без втрати функціональності (обфускація або затемнення). Загальна назва таких програм - обфускатори.

В рамках дослідження для оцінки ефективності деяких відомих програмних засобів маскування коду спочатку за допомогою фреймворка Msfvenom в ОС Kali Linux у вигляді документу Microsoft Word був створений RAT файл, який потім окремо був модифікований різними обфускаторами. Далі RAT файл без модифікації і всі модифіковані його версії було завантажено на вебсайт сервісу VirusTotal (https://www.virustotal.com), де здійснювалась сканування файлу різними антивірусними програмами на наявність шкідливого коду. Для дослідження було взято такі обфускатори:

- Shellter (https://github.com/ParrotSec/shellter);
- FuckThatPacker (https://github.com/Unknow101/FuckThatPacker);
- Chimera (https://github.com/tokyoneon/Chimera);
- HanzoInjection (https://github.com/P0cL4bs/hanzoInjection);
- Invoke-Obfuscation (https://github.com/danielbohannon/Invoke-Obfuscation).

У вихідному RAT файлі 51 антивірус сервісу VirusTotal з 71 виявив шкідливий код, результати сканування модифікованих різними обфускаторами файлу RAT наведений у Табл. 1.

Таблиця 1 – Результати виявлення антивірусами сервісу VirusTotal шкідливого обфускованого коду

| **Обфускатор коду** | **Кількість антивірусів, що сканували обфускований код** | **Кількість антивірусів, що виявили шкідливий обфускований код** |
|---|---|---|
| Shellter | 67 | 22 (33%) |
| FuckThatPacker | 69 | 11 (16%) |
| Chimera | 61 | 4 (7%) |
| HanzoInjection | 60 | 0 |
| Invoke-Obfuscation | 71 | 9 (13%) |

Загалом, усі обфускатори показали деяку ефективність у маскуванні сигнатури коду, але модифікований HanzoInjection шкідливий код не був виявлений жодним антивірусом сервісу VirusTotal, що підтверджує необхідність використання комплексних систем захисту, які враховують не тільки відомі сигнатури коду, а і інші чинники.

**Перелік використаних джерел**

1. What is Remote Access Trojan (RAT)? URL: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-remote-access-trojan/ (дата звернення 21.04.2023).

# АНАЛІЗ ФУНКЦІОНАЛЬНОСТІ ДЕЯКИХ ЗАСОБІВ ЗАХИСТУ ВІД BADUSB АТАК

Носов В.В., Мокроусов Д.І.
Харківський національний університет внутрішніх справ

Розглянуто нова форма зловмисного програмного забезпечення, яке працює з мікроконтролерами USB-пристроїв, саморозмножується та не виявляється поточними засобами захисту**.** Показана дія BADUSB атак. Вказані особливості захисту від BADUSB атак в комп'ютерах з ОС Windows. Проведено порівняння функціональності деяких засобів контролю USB-пристроїв.
**Ключові слова:** комп'ютерний вірус, USB-пристрій, BADUSB атака.

Вперше BADUSB атака була продемонстрована на конференції BlackHat USA 2014 [1] дослідниками організації Security Research Labs Карстеном Нолом (Karsten Nohl) та Джейкобом Леллом (Jakob Lell). Вони представили нову форму зловмисного програмного забезпечення, яке працює з мікроконтролерами USB-пристроїв, саморозмножується та не виявляється поточними засобами захисту. В цій атаці мікроконтролери USB-накопичувачів можуть бути перепрограмовані і імітувати інші типи USB-пристроїв, які за умовчанням не несуть небезпеки для операційної системи, що дозволяє запускати шкідливий код з USB-накопичувача в обхід механізмів антивірусного захисту.

В загальному випадку мікроконтролер USB-пристрою при підключенні через порт USB повідомляє системі поряд з

іншою службовою інформацією, класи, до яких належить пристрій. Система завантажує необхідний драйвер і працює з пристроєм виходячи з його класу та цих даних. Один фізичний пристрій може реалізовувати декілька класів і для системи бути декількома окремими пристроями, наприклад, веб-камери реалізують одночасно клас відео та клас аудіо пристроїв [4].

BADUSB атака користується тим, що у більшості випадків виробники USB пристроїв не захищають мікроконтролери від перепрограмування, а операційні системи не перевіряють USB пристрої на справжність. Завдяки цьому зловмисник може змінити програму мікроконтролера і видати один пристрій за інший. Приклади реалізації BADUSB атак наведені в [2, 3], де телефон з ОС Android при підключенні до комп'ютеру через USB порт починає контролювати мережний трафік системи.

Захист від BADUSB атак в комп'ютерах з ОС Windows може бути реалізований шляхом:

- або повного відключення USB портів комп'ютеру в налаштуваннях:
- BIOS/UEFI;
- реєстру;
- диспетчері пристроїв;
- або формуванням через відповідні програмні засоби списку довірених USB-пристроїв та блокування роботи недовірених.

Контроль USB-пристроїв, що підключаються до системи, серед інших реалізують такі програмні засоби:

- Device Control Plus [5];
- GiliSoft USB Lock [6];
- SysTools USB Blocker [7];
- NewSoftwares USB Block [8];
- USB Disk Manager [9].

В Табл. 1 наведено порівняння функціональності і безкоштовності використання цих засобів.

Таблиця 1 – Порівняння функціональності деяких засобів контролю USB-пристроїв

| **Назва** | **Журнал підключень та подій дій** | **Захист паролем** | **Прихований режим роботи** | **Платні функції** |
|---|---|---|---|---|
| Device Control Plus | Так | Ні | Ні | Ні |
| GiliSoft USB Lock | Так | Так | Так | Частково |
| SysTools USB Blocker | Ні | Так | Ні | Так |
| NewSoftwares USB Block | Так | Так | Так | Так |
| USB Disk Manager | Ні | Ні | Так | Ні |

## Висновки

З огляду на результати порівняння (Табл. 1) можна виділити програмний засіб контролю USB-пристроїв GiliSoft USB Lock як максимально функціональний із базовим безкоштовним використанням.

## Перелік використаних джерел


1. Karsten Nohl, Jakob Lell. BadUSB – On Accessories that Turn Evil. URL: https://www.blackhat.com/us-14/briefings.html#badusb-on-accessories-that-turn-evil (дата звернення: 29.04.2023).
2. Jakob Lell. BadAndroid. URL: https://github.com/tstzdouglas/BadAndroid (дата звернення: 29.04.2023).
3. Adam Caudill, Brandon Whitson. Psychson. URL: https://github.com/brandonlw/Psychson (дата звернення: 29.04.2023).

4. Специфікація USB 2.0 / USB Implementers Forum. URL: https://www.usb.org/document-library/usb-20-specification (дата звернення: 29.04.2023).
5. Device Control Software. URL: https://www.manageengine.com/device-control/ (дата звернення: 29.04.2023).
6. Lock USB Port to Prevent Data from Leakage. URL: https://www.gilisoft.com/product-usb-lock.htm (дата звернення: 29.04.2023).
7. SysTools USB Blocker. URL: https://www.systoolsgroup.com/usb-blocker.html (дата звернення: 29.04.2023).
8. Restrict Access of Portable Drives. URL: https://www.newsoftwares.net/usb-block (дата звернення: 29.04.2023).
9. Total control over your USB Disks. URL: https://www.syedgakbar.com/projects/usb (дата звернення: 29.04.2023).

# КІБЕРТЕРОРИЗМ ТА КІБЕРРОЗВІДКА. ЯК ВБЕРЕГТИ ПЕРСОНАЛЬНІ ДАНІ ВІД НЕБАЖАНОГО ВТРУЧАННЯ В УМОВАХ ВІЙНИ

Світличний В.А., Головня А.І.
Харківській національний університет внутрішніх справ

В тезах доповіді розглянуто: фішинг атакі, що спрямовані на збір персональних даних громадян України. Вказано особливості відповідальності згідно зі ст. 182 Кримінального кодексу України.
**Ключові слова:** фішинг, кіберполіція, соціальна інженерія, персональні данні.

В період воєнного стану в Україна значним чином збільшилась кількість фішинг атак, що спрямовані на збір персональних даних громадян України. Фі́шинг або Фішинґ (англ. phishing МФА: ['fiʃiŋ] від fishing — риболовля) —

вид шахрайства, метою якого є виманювання в довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів із переказу або обміну валюти, інтернет-магазинів [1].

З боку росії, за даними працівників кіберполіції, подібні атаки здійснюються регулярно. За припущеннями, збір персональних даних відбувається для подальшого залякування та переслідування громадян. Особливо вразливі групи населення: сім'ї військовослужбовців, військовослужбовці, працівники правоохоронних органів, структури МВС, їх сім'ї. З якою метою робить це супротивник достовірно не відомо, але очевидно, що нічого доброго від цього чекати не слід. Отож, слід бути максимально обачними [2] .

Соціальна інженерія — це наука, що вивчає людську поведінку та фактори, які на неї впливають. Найстрашнішим у цьому виді атаки є те, що вона відноситься до різновиду соціальної інженерії [4]. Це означає, що персональні дані Ви надаєте зловмисникам добровільно, самі того не розуміючи. Це означає, що відповідальності за фішинг не передбачено Законодавством України, а от подальше несанкціоноване використання персональних даних, карається за ст.182

Кримінального кодексу України.

За порушення недоторканості приватного життя, а саме за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації винна особа притягується до кримінальної відповідальності [3].

Як же зловмисник заволодіє Вашими даними, якщо Ви самі того не бажаєте? Є безліч простих та невибагливих способів. Уявіть: на Вашу електронну адресу надіслано лист з подібним змістом: «Ви стали переможником акції від ROZETKA. Сума бонусу складає 20 000 грн. Заповніть форму за посиланням: ……» На місці крапок Ви побачите посилання для наче підтвердження особистості. Але таким нехитрим способом зловмисник отримає будь-яку, цікавлячу його інформацію. Є цілі фішингові сайти, посилання на які також можна

отримати в повідомленнях месенджера або тієї ж електронної пошти.

## Висновки

Щоб не потрапити в тенети кіберрозвідки, використовуйте прості дії та елементарний «етикет» під час роботи в Інтернет-мережі:

- Перевіряйте справжність сайтів, які пропонують залишити на них особисті дані
- Не переходьте за посиланнями від невідомих відправників
- Перевірте справжність електронної адреси, з якої надійшов лист, якщо відправник представляється відомим брендом
- Не залишайте свої дані сумнівним інтернет-магазинам
-

## Перелік посилань


1. Фішинг // Вікіпедія URL:https://uk.wikipedia.org/wiki/%D0%A4%D1%96%D1%88%D0%B8%D0%BD%D0%B3 (дата звернення: 29.04.2023).
2. Рекомендації щодо захисту персональних даних в умовах воєнного стану. Уповноважений Верховної Ради України з прав людини - Головна. URL: https://ombudsman.gov.ua/news_details/rekomendaciyi-shchodo-zahistu-personalnih-danih-v-umovah-voyennogo-stanu (дата звернення: 29.04.2023).
3. Кримінальний кодекс України URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 29.04.2023).
4. Що таке фішинг і як від нього захиститися? URL: https://www.fg.gov.ua/articles/50140-shcho-take-fishing-i-yak-vid-nogo-zahistitis.html (дата звернення: 29.04.2023).

# АНАЛІЗ КАНАЛІВ ВИТОКУ АКУСТИЧНОЇ ІНФОРМАЦІЇ ІЗ ЗАСТОСУВАННЯМ ОПТИЧНИХ ЗАСОБІВ

Логвін Є.О., Степаненко В.М.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», НН Фізико-технічний інститут, Київ, Україна

Робота присвячена огляду загрози витоку мовної інформації з застосуванням оптичних засобів акустичної розвідки: Лазерний мікрофон (ЛСАР), Lamphone та Visual Microphone.
**Ключові слова:** Акустичний канал витоку, ЛСАР, Lamphone, Visual Microphone

## Вступ

Захист акустичної інформації є важливою частиною комплексу технічного захисту інформації. Необхідність перехоплення акустичної інформації, знаходячись поза контрольованою зоною, призвела до створення оптичних засобів акустичної розвідки, що використовують вібруючі об'єкти інтер'єру в якості зовнішніх мембран.

Проблема захисту акустичної інформації стала особливо критичною зі збільшенням можливостей дистанційної роботи, що призводить до можливого озвучення конфіденційної інформації в незахищених умовах.

## Лазерна система акустичної розвідки

Лазерна система акустичної розвідки (ЛСАР) або лазерні мікрофони – це засіб технічної розвідки, що використовує невидимий інфрачервоний лазерний промінь для зняття звукових вібрацій на дальніх об'єктах.

Дані системи поділяються за будовою на розділені та суміщені.

До розділених ЛСАР відносять ті, що складаються з двох окремих пристроїв – передавача (лазера) та приймача (фотодетектора). Лазерний промінь фокусується на

вібруючій поверхні під певним кутом й модульоване небезпечним сигналом випромінювання збирається окремим оптичним приймачем під кутом відбиття променя від об'єкта.

До суміщених ЛСАР відносять пристрої, що містять в собі одночасно лазер та фотодетектор. Найпростішим є лазерний мікрофон на основі інтерферометра Майкельсона. Використання дільника лазерного пучка з напівпрозорим дзеркалом дозволяє сумістити прицілитись на об'єкт під прямим кутом та, в разі когерентного коливання, підсилити відбитий промінь інтерференцією з опорним променем.

## Lamphone (Лампфон)

Lamphone (Лампфон) – це метод перехоплення акустичної інформації з модульованого світлового потоку лампочки, що знаходиться під впливом небезпечного сигналу.

У загальному випадку система складається з оптичної системи (телескопа), фотоелектричного датчика, на який збирається оптичний сигнал лампочки та засобу обробки інформації (ноутбук). Модель перехоплення акустичної інформації засобом Lamphone можна описати як:

1) Озвучення певної інформації у кімнаті жертви створює звуковий сигнал snd(t), що призводить до коливань повітря на поверхні лампочки.

2) Інтенсивність світла лампочки змінюється за вібраційним законом й утворює модульований оптичний сигнал opt(t)

3) Порушник збирає телескопом оптичний сигнал opt(t) на фотоелектричний датчик, перетворюючи світловий потік на звуковий сигнал.

## Visual Microphone (Візуальний мікрофон)

Visual Microphone – це метод виділення звуку на відеозаписах без аудіодоріжки за вібраціями об'єктів, що знаходяться під впливом звукового поля.

Даний метод виявляє невеликі вібрації об'єктів інтер'єру, що реагують на звук, методом порівняння кадрів з деяким обраним «базовим» кадром, після чого зчитана

вібрація проходить обробку для покращення розбірливості й зберігається/відтворюється відповідними пристроями.

Камера має знімати об'єкт за великої частоти кадрів (2-20 кГц), після чого запис можна буде використати для відновлення у будь-який момент. Але й важкість алгоритмів робить неможливим відновлення у реальному часі.

## Рекомендації щодо заходів захисту акустичної інформації

На основі переваг та недоліків розглянутих засобів можна встановити їх стійкість до деяких заходів захисту акустичної інформації. Якщо спостереження буде вестись поза приміщенням, використання ролетів або захисної плівки, для приховування інтер'єру та погіршення відбивання лазера, є кращими методами пасивного захисту, як активний захист – акустичне зашумлення приміщення та застосування вібровипромінювачів.

## Висновки

Найбільш небезпечним, з точки зору використання на великій відстані, є лазерний мікрофон (ЛСАР) через низький рівень затухання та випромінювання на фіксованих діапазонах частот. При використанні засобів Lamphone та Visual Microphone як закладних пристроїв, єдиним ефективним заходом буде фізичний огляд приміщення через їх пасивні методи збору інформації.

## Перелік використаних джерел

1. Горбенко І., Ковальчук Ю. Оцінка характеристик лазерного каналу витоку мовної інформації з урахуванням багатомодового випромінювання лазера.

2. Lamphone: Real-Time Passive Sound Recovery from Light Bulb Vibrations / B. Nassi, Y. Pirutin, A.Shamir, Y. Elovici, B. Zadov.

3. The Visual Microphone: Passive Recovery of Sound from Video / A. Davis, M. Rubinstein, N. Wadhwa,G. Mysore, F. Durand, W. T. Freeman

# АНАЛІЗ ЗАСТОСОВНОСТІ МАШИННОГО НАВЧАННЯ В СИСТЕМАХ АНАЛІЗУ МЕРЕЖЕВИХ АТАК

Полотай О.І., Павлишин А.Ю.
Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

Розглянуто поняття мережевих атак,особливостей машинного навчання для їх виявлення. Розглянуто способи машинного навчання.
**Ключові слова:** мережеві атаки, машинне навчання

## Вступ

В даний час засоби та системи комунікації розвиваються стрімкими темпами, різко збільшилися обсяг та швидкість передачі даних. Інформація безпосередньо впливає на життя людей, функціонування та регулювання організацій та держав у цілому, саме тому інформацію прийнято вважати одним із ключових ресурсів.

У зв'язку з цим гостро постає проблема забезпечення безпеки інформації, яка безпосередньо залежить від зростання обсягу та значущості інформації. Таким чином, існує потреба у дослідженні системи аналізу атак на основі машинного навчання.

## Визначення та класифікація мережевих атак

Мережевою атакою називають навмисні дії третіх осіб (зловмисників), спрямовані на отримання контролю над локальним або віддаленим комп'ютером для подальшого порушення роботи мережі, зміни прав користувачів, отримання персональних даних або реалізації будь-яких деструктивних дій над інформацію.

Прикладами мережевих атак можуть бути [2]:

1. Mailbombing.
2. Застосування спеціалізованих додатків.
3. Переповнення буфера.
4. Мережна розвідка.

5. IP-спуфінг.
6. Man-in-the-Middle.
7. Фішинг.
8. DDOS-атака.
9. XSS-атака.
10. Brute Force.
11. Sql Injection.

## Методи виявлення мережевих атак

Виявленням мережевих атак називається процес розпізнавання аномальної чи підозрілої діяльності. . Даними для аналізу є мережевий трафік у вигляді мережевих пакетів. Ці дані збираються без обробки, після чого можуть бути нормалізовані для завдання ознакових атрибутів загального виду. Такі дані використовуються для створення активного профілю. Далі профіль порівнюється з нормальною діяльністю об'єкта, і при виявленні розбіжностей параметрів профілю фіксується аномалія. Даний алгоритм має кілька варіантів подальшої реалізації: процедура порівняння з граничною величиною (при перевищенні граничної величини фіксується аномалія), ідентифікація несанкціонованих дій шляхом порівняння мережевого трафіку з шаблоном атак, методи інтелектуального аналізу даних (методи обчислювального інтелекту, машинного навчання).

Метод інтелектуального аналізу успішно застосовується при розробці сучасних систем виявлення атак і є перспективним напрямом розвитку даної галузі.

## Способи машинного навчання

Одним із класів методу інтелектуального аналізу є машинне навчання. Машинне навчання (англ. machine learning, ML) - галузь штучного інтелекту, характерною рисою яких є не пряме розв'язання задачі, а навчання, що ґрунтується на використанні даних та алгоритмів для імітації навчання людини. Вирішуючи схожі завдання, поступово підвищується і точність рішень. Для побудови таких методів використовують засоби математичної

статистики, чисельних методів, математичного аналізу, методів оптимізації, теорії ймовірностей, теорії графів, різні техніки роботи з даними в цифровій формі. Способи навчання поділяють на:

1. навчання з учителем (supervised learning).
2. навчання без учителя (unsupervised learning).
3. навчання з підкріпленням (reinforcement learning).

Так, навчання з учителем має на увазі, що дані, підготовлені для аналізу, вже містять правильну відповідь, тому метою алгоритму є не отримати відповідь, а з'ясувати закономірність шляхом виявлення взаємозв'язків. У результаті алгоритм отримує здатність вибудовувати коректні прогнози та моделі з мінімальною похибкою.

Для навчання без вчителя ключовим є якийсь шаблон, отриманий алгоритмом у процесі виявлення закономірностей в оброблюваному масиві даних. На основі виявлених закономірностей і систематизуються дані. Навчання з підкріпленням є окремим випадком навчання з учителем. За такого навчання алгоритм навчається, взаємодіючи з певним середовищем, відгуком якого на дії алгоритму є сигнали підкріплення. У ролі вчителя тут виступає саме середовище [1].

## Моделі, що застосовуються під час машинного навчання

Виконання машинного навчання включає в себе створення якоїсь моделі, яка навчається на вхідних навчальних даних, а потім може обробляти інші дані, для прогнозування [3]. Для систем машинного навчання використовують різні типи моделей, наприклад:

1. Дерево прийняття рішень.
2. Випадковий ліс.
3. Лінійна регресія.
4. Наївний Байєс.

## Висновки

Отже, машинне навчання зачіпає практично всі сфери діяльності людства: від харчової промисловості та

сільського господарства до економіки та науки. Так, основними практичними сферами застосування є: розпізнавання мови, технічна діагностика, медична діагностика, прогнозування часових рядів, виявлення шахрайства, виявлення спаму, кредитний скоринг, та багато інших.

## Перелік використаних джерел


1. Kelleher J.D.. Fundamentals of Machine Learning for Predictive Data Analytics: Algorithms, Worked Examples, and Case Studies / Kelleher J.D., Namee B.M, D'Arcy A. – The MIT Press, 2015. – 624 p. 2.
2. Види мережевих атак. Способи їх виявлення. [Електронний ресурс]. – Режим доступу: https://holodoks.blogspot.com/ 2017/12/blog-post.html
3. Штучний інтелект, машинне навчання та нейронні мережі: в чому різниця і для чого їх використовують – [Електронний ресурс]. – Режим доступу: https://evergreens.com.ua/ua/ articles/machine-learning-overview.html


# КОНЦЕПЦІЯ ШИФРУ НА ОСНОВІ CIP-КВАЗІГРУП


Крайнічук Г., Радченко Є., Пилявець І.
Вінницький національний технічний університет
Вінниця, Україна



Запропоновано концепцію шифру на основі квазігруп з властивістю схрещеної оборотності (CIP-квазігруп). Особливістю такого шифру є послідовність бінарних квазігрупових операцій 4-го порядку, що збільшує його криптостійкість.



**Ключові слова.** Криптографія, шифр, алгоритм, секретний ключ, CIP-квазігрупа, таблиця Келі, парастроф, ізотоп, група Кляйна.

## Вступ

Останні кілька років технологічного розвитку показали справжню цінність інформації. Очевидно, що це стає причиною багатьох випадків викрадення конфіденційної інформації. Як результат, зростає необхідність в засобах захисту інформації, зокрема, в нових алгоритмах шифрування.

Метою дослідження є описання концепції методу шифрування на основі CIP-квазігруп 4-го порядку з функцією оборотності $x^2$.

Подібні криптографічні властивості для квазігрупових парастрофних перетворень 4-го порядку вивчали в [1].

## Квазігрупа: означення та властивості

Особливістю шифрування є послідовність бінарних квазігрупових операцій знайдених за парастрофною симетрією [2]. Шифр базується на основі квазігруп, що мають властивість схрещеної оборотності (так звані CIP-квазігрупи, CIP - cross inverse property) [3]. Квазігрупою є групоїд $(Q;\cdot)$ такий, що для довільних $a,b \in Q$ система рівнянь $a \cdot x = b$, $y \cdot a = b$ має єдиний розв'язок. Квазігрупа $(Q;\cdot)$ називається: середньою, лівою та правою CIP-квазігрупою, якщо відповідно існують відображення такі, що для всіх x, y виконуються рівності $\psi(x) \cdot yx = y;$ $yx \cdot y = \upsilon(x);$ $y \cdot xy = \gamma(x)$, де відображення $\psi$, $\upsilon$, $\gamma$ називаються лівою, правою та середньою функцією оборотності [4]. Многовид середніх CIP-квазігруп з функцією оборотності $x^2$ визначається однією із таких тотожностей:

$$x \cdot yx^2 = y,$$
$$xy \cdot x^2 = y,$$
$$x^2 y \cdot x = y,$$
$$x^2 \cdot yx = y.$$

## Опис шифру на основі квазігруп

Суть потокового шифру полягає у використанні трьох CIP-квазігруп 4-го порядку, описаних серед ізотопів групи Кляйна з функцією оборотності $x^2$ [5] Всього таких квазігруп 4-го порядку над групою Кляйна 8 [6]. Спочатку потік інформації повідомлення кодується у двійковій системі, після чого фіксується послідовність квазігрупових операцій для секретного ключа, здійснюється накладання випадково згенерованої гами і власне саме шифрування. Ступінь спотворення повідомлення збільшується за рахунок використання випадкової квазігрупи з послідовності бінарних квазігрупових операцій для зашифрування кожного окремого фрагменту повідомлення. Додаткову секретність в процес шифрування вносить фіксований набір операцій, який залежить від секретного ключа. Результатом зашифрування є послідовність елементів, кожен з яких це результат перехрестя рядка вхідного повідомлення та стовпчика елементів гами з таблиці Келі відповідної квазігрупи. Для розшифрування обирається відповідний парастроф квазігрупи.

Апаратна реалізація шифру відповідає граничним вимогам складності засобів LW-криптографії, оскільки загальна складність засобу для шифрування складає від 600 до 700 умовних одиниць.

## Висновки

Запропонований метод шифрування на основі бінарних квазігруп 4-го порядку з властивістю схрещеної оборотності з функцією оборотності $x^2$ дасть можливість збільшити швидкість процесу шифрування потоку даних і зменшить апаратні витрати на реалізацію пристроїв.

Подібний шифр можна використовувати у випадку, якщо необхідно мати шифрувальний пристрій невеликого розміру. Для прикладу, мобільні телефони, що мають апаратні модулі шифрування, конструкція яких накладає обмеження на розміри апаратних засобів, або нейронні імпланти, що з’являться на ринку найближчим часом.

## Перелік використаних джерел

1. Dimitrova V., Bakeva V., Popovska-Mitrovik A., Krapez A. Cryptographic Properties of Parastrophic Quasigroup Transformation // 2012. – P. 9.
2. Sokhatsky F. M. Parastrophic symmetry in quasigroup theory // Visnyk Donetsk national university, Ser. A: natural sciences. — 2016. — No. 1–2. — P. 70–83
3. Ilojide E., Jaiyeo T.G., Owojori O.O. Varieties of groupoids and quasigroups generated by linear-bivariate polynomials over the ring $Z_n$ // arXiv:1408.0991v1 [math.GR] 1 Aug 2014.
4. Сохацький Ф.М., Луценко А.В., Фриз І.В. Побудова квазігруп з властивістю оборотності // Мат. методи та фіз.-мех. поля. 64, 2021/
5. Сохацький Ф.М. Оборотні бінарні функції і квазігрупи четвертого порядку // XIII Міжн. алгебр. конф. в Україні / Київ – КНУ ім. Т. Шевченка, 2021, 77-78 с.
6. Крайнічук Г., Пилявець І., Радченко Є. CIP-квазігрупи 4-го порядку з оборотним елементом $x^2$ серед ізотопів групи Клейна // Міжн. наук. конф. «Сучасні пробл. мех. та матем. - 2023», присвяч. 95-річчю від дня народж. академ. Я.С. Підстригача, 2023.


# ПОРІВНЯННЯ ТА АНАЛІЗ СУЧАСНИХ ЗАСОБІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ДАНИХ (АЛГОРИТМИ ШИФРУВАННЯ)


Шафрай І.Ю.

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорьського», НН Фізико-технічний інститут, Київ, Україна



У роботі проводиться дослідження сучасних алгоритмів криптографічного захисту даних. В ході виконання досліду проведено порівняльний аналіз алгоритмів з метою визначення їх переваг та недоліків. Досліджено технічні параметри кожного алгоритму, їх забезпечення безпеки,

швидкість обробки даних та інші фактори, що впливають на їх використання. Результати дослідження можуть бути корисні для визначення найбільш слушного алгоритму криптографічного захисту даних для конкретної ситуації.

**Вступ**

Мета роботи полягатиме в аналізі та порівнянні криптографічних алгоритмів шифрування. Я вважаю, що ця тема є актуальною в нашому часі, оскільки зростає кількість кібератак та інцидентів зі зламом даних. Захист конфіденційної інформації стає все важливішим, і саме криптографічні алгоритми шифрування відіграють ключову роль у забезпеченні цього захисту.

Дослідження та порівняння різних алгоритмів дозволить зрозуміти, які з них є більш надійними, які мають кращі показники ефективності та підходять для захисту різних типів даних. Результати цієї роботи будуть корисними для визначення найкращого алгоритму для конкретних вимог захисту даних, забезпечуючи максимальний рівень безпеки та захисту від кібератак.

**1) Відомості про алгоритми шифрування:**

Основні принципи та функцій для декількох алгоритмів шифрування:

AES - симетричний блочний алгоритм шифрування, AES працює з блоками даних фіксованої довжини (128 бітів), які шифруються з використанням ключа. Ключ може бути розміру 128, 192 або 256 бітів. Шифрування відбувається у декілька етапів (10, 12 або 14 раундів, залежно від розміру ключа), кожен з яких містить в собі змішування байтів, заміну байтів за певними таблицями, перемішування байтів і додавання раундового ключа.

DES - симетричний блочний алгоритм шифрування, шифрування DES базується на заміні і перестановці бітів вхідного блоку з використанням ключа. У процесі шифрування DES використовується 16 раундів з різними ключами.

Blowfish - блочний симетричний алгоритм шифрування. Основна ідея алгоритму полягає в тому, щоб розділити ключ на декілька підключів та застосовувати їх послідовно до блоків даних. Blowfish використовує ітеративний процес, що складається з 16 раундів, у кожному з яких застосовуються різні перетворення до блоку даних.

RSA - асиметричним алгоритмом шифрування. RSA використовує два ключі: публічний та приватний. Публічний ключ використовується для шифрування повідомлень, тоді як приватний ключ використовується для дешифрування повідомлень. Ключі в RSA генеруються шляхом вибору двох великих простих чисел та їх множення. Чим більші ці числа, тим більша безпека у RSA.

**2) Вибір основних критеріїв для аналізу**

Для здійснення порівняльного аналізу алгоритмів шифрування дуже важливо обрати основні критерії, що впливають на їх ефективність та безпеку. Для реалізації методики порівняння алгоритмів були обрані такі критерії як: довжина ключа, кількість раундів, розмір блока, швидкість шифрування та розшифрування, пропускну спроможність алгоритму шифрування, безпеку та інші.

Довжина ключа є одним з основних критеріїв безпеки алгоритмів шифрування, оскільки довгі ключі забезпечують вищий рівень захисту даних від несанкціонованого доступу. Кількість раундів та розмір блока також мають важливе значення для безпеки алгоритму, оскільки вони впливають на кількість можливих комбінацій шифрування та унеможливлюють дешифрування даних з використанням простих методів.

Швидкість шифрування та розшифрування, а також пропускна спроможність кожного алгоритму шифрування, мають важливе значення для практичного застосування алгоритму в різних ситуаціях. Оскільки шифрування та розшифрування можуть займати значну кількість часу, важливо обирати алгоритми з високою швидкістю обробки даних та достатньою пропускною спроможністю.

Всі тестування та заміри швидкості та пропускну спроможність будуть проводитись за допомого python, а саме, модуля Crypto.Cipher.

3)Методика порівняння алгоритмів шифрування

Метод полягає в порівнянні кандидатів (алгоритмів) за визначеними критеріями, з вагою для кожного критерію, яка вказує на його важливість. Далі проводиться оцінка кожної альтернативи відносно кожного критерію за результатами або іншими показниками. Для отримання результатів буде створена програма за допомогою якої ми зможемо отримати: швидкість шифрування та розшифрування, використання ресурсів комп'ютера, пропускну спроможність, інші показники є загально відомими, такі як: кількість раундів, довжина ключа та розмір блока. Програма створюється для замірів в однакових умовах. Загальна оцінка для кожної альтернативи обчислюється як скалярний добуток ваг критеріїв і оцінок альтернатив за кожним критерієм. Таким чином, визначається оптимальний алгоритм шифрування за вибраними критеріями.

## Висновки

З проведеної роботи, можна стверджувати, що порівняння та аналіз криптографічних алгоритмів шифрування є важливим завданням у сфері кібербезпеки. Це дозволяє забезпечити максимальний рівень захисту даних від кібератак та інших загроз, а також вибрати найбільш ефективний та надійний алгоритм для конкретних потреб захисту даних. Крім того, порівняння та аналіз алгоритмів допомагають виявити переваги та недоліки кожного з них, що дає можливість уникнути помилок при виборі алгоритму та забезпечити максимальну безпеку даних. У цілому, проведення порівняння та аналізу криптографічних алгоритмів шифрування є необхідним етапом для забезпечення кібербезпеки та захисту даних у сучасному світі. Враховуючи отримане, можна покращити безпеку інформаційних систем, обираючи алгоритми шифрування за індивідуальними потребами.

**Перелік використаних джерел**

1. A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish[Електронний ресурс] – Режим доступу: https://symbiosisonlinepublishing.com/computer-science-technology/computerscience-information-technology32.php
2. Comparative Study of Different Cryptographic Algorithms [Електронний ресурс] – Режим доступу: https://www.scirp.org/journal/paperinformation.aspx?paperid=100754
3. Secure Your Organization's Data With These Encryption Algorithms [Електронний ресурс] – Режим доступу: https://www.encryptionconsulting.com/comparison-of-various-encryption-algorithms-and-techniques-for-securing-data/

# ВИЯВЛЕННЯ ЗАГРОЗ ПОРУШЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В МЕРЕЖАХ З ДИНАМІЧНОЮ ТОПОЛОГІЄЮ З ВИКОРИСТАННЯМ ІНТЕЛЕКТУАЛЬНИХ МЕТОДІВ

Ю.В. Костюк
Державний торговельно-економічний університет,
kostyuk.yu@knute.edu.ua

Робота присвячена виявленню загроз та вразливостей в мережах з динамічною топологією з використанням інтелектуальних методів. Дослідження показують, що застосування машинного навчання, генетичних алгоритмів та штучних нейронних мереж дозволяє виявляти аномальну активність, передбачати поведінку користувачів мережі та виявляти складні взаємозв'язки між параметрами мережі та загрозами.

**Ключові слова:** загроза, динамічна топрологія, інтелектуальні методи, інформаційна безпека

## Вступ

Виявлення загроз порушення інформаційної безпеки є однією з найбільш важливих задач в галузі комп'ютерної безпеки. За останні роки зростання кількості кібератак та інших загроз постійно зростає, і це ставить питання про те, як ефективно захистити інформацію в мережах з динамічною топологією, оскільки такі мережі швидко змінюють свою структуру, тому їх слід постійно моніторити, щоб уникнути можливих загроз. Це можуть бути такі мережі, як бездротові, хмарні, деякі типи мереж IoT (Internet of Things) та інші.

## 1. Методи

Інформаційна безпека − це комплекс заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації. Для забезпечення цих характеристик інформаційних систем необхідно виявляти загрози та вразливості, які можуть призвести до порушення цих характеристик.

Динамічна топологія мережі може бути причиною зміни умов зв'язку між пристроями, що може спричинити виникнення нових вразливостей або загроз [1]. Тому важливо мати засоби для виявлення цих загроз та вразливостей. Динамічна топологія мережі відноситься до топології, в якій змінюється кількість, конфігурація та розташування вузлів мережі. Це може бути викликано різними факторами, такими як збільшення об'єму даних, збільшення кількості користувачів, зміни бізнес-процесів та багато іншого. Для захисту мереж з динамічною топологією (МДТ) використовуються інтелектуальні методи, що дозволяють ефективно виявляти загрози порушення інформаційної безпеки. Одним з таких методів є аналіз поведінки користувачів. Цей метод заснований на вивченні типової поведінки користувачів в мережі та виявленні аномальних дій [1].

Для виявлення загроз та вразливостей можуть бути використані інші інтелектуальні методи, такі як генетичні алгоритми та штучні нейронні мережі. Інтелектуальні

методи є одним з найбільш ефективних способів виявлення загроз безпеці мережі. Зокрема, машинне навчання може бути використане для виявлення аномальної поведінки, яка може вказувати на можливу загрозу безпеці мережі. Інший інтелектуальний метод − це використання машинного навчання. Він дозволяє розробляти моделі, які навчаються виявляти аномальні дії в мережі. Для цього моделі використовують дані про поведінку користувачів та створюють алгоритми, які дозволяють виявляти аномальні дії.

Один зі способів виявлення аномалій полягає у створенні профілю поведінки користувача. Це може бути зроблено за допомогою аналізу даних, таких як історія входів, звернень до різних ресурсів тощо. Якщо з'являється якась незвичайна діяльність, то це може бути індикатором потенційної загрози [2].

Важливим етапом при виявленні загроз є моніторинг мережі. Моніторинг мережі дозволяє отримувати інформацію про активність пристроїв у мережі, стан з'єднань та інші параметри, які можуть бути використані для виявлення загроз. Іншим способом є аналіз мережевого трафіку. Якщо з'являється незвичайний трафік, який не відповідає звичному зразку, то це може свідчити про потенційну загрозу. Машинне навчання може використовуватись для розпізнавання аномалій у мережевому трафіку.

Для виявлення загроз порушення інформаційної безпеки використовуються спеціальні програмні засоби. Наприклад, брандмауери та системи виявлення вторгнень.

## 2. Результати

Дослідження показують, що використання інтелектуальних методів для виявлення загроз та вразливостей в мережах з динамічною топологією дозволяє покращити ефективність заходів забезпечення інформаційної безпеки. Зокрема, застосування машинного навчання дозволяє створювати моделі, які можуть передбачати поведінку користувачів мережі та виявляти аномальну активність, що може свідчити про наявність загроз або вразливостей [1, 2].

Також, застосування генетичних алгоритмів та штучних нейронних мереж дозволяє виявляти складні взаємозв'язки між параметрами мережі та загрозами, що може бути складно зробити за допомогою традиційних методів аналізу мережі.

Застосування інтелектуальних методів для виявлення загроз та вразливостей в мережах з динамічною топологією дозволяє забезпечити більш ефективний моніторинг мережі та швидше виявляти загрози, що може зменшити ризик їх виникнення та вплив на інформаційну безпеку.

## Висновок

Отже, виявлення загроз та вразливостей в мережах з динамічною топологією є критично важливим для забезпечення інформаційної безпеки. Використання інтелектуальних методів, таких як машинне навчання, генетичні алгоритми та штучні нейронні мережі, дозволяє покращити ефективність процесу виявлення загроз та вразливостей. Такі методи дозволяють виявляти аномальну активність, передбачати поведінку користувачів мережі та виявляти складні взаємозв'язки між параметрами мережі та загрозами. Застосування цих методів може значно зменшити ризик виникнення загроз та вразливостей, забезпечуючи більш ефективний моніторинг мережі та швидше виявлення проблем.

## Перелік використаних джерел

1. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

2. Лахно В. А. Моделі, методи та інформаційні технології захисту корпоративних систем транспорту на основі інтелектуального розпізнавання загроз / В. А. Лахно // Системні технології. - 2014. - Вип. 5. - С. 73-83.

# ПОСОБИ РЕЗЕРВНОГО КОПІЮВАННЯ ДАНИХ В ОС WINDOWS

Б.Ю. Овдієвич, Н.А. Христинець
Луцький національний технічний університет, м. Луцьк, Україна

Розглянуті механізми забезпечення безпеки операційних систем родини Windows – резервного копіювання –для можливостей відновлення оригіналів інформації або важливих компонент системи у разі несанкціонованого доступу чи пошкодження цілісності інформації.
**Ключові слова:** резервне копіювання, Windows 10, відновлення даних, копіювання даних, системні образи

Резервне копіювання даних є важливим елементом забезпечення безпеки в ОС Windows. Це дозволяє відновити важливу інформацію в разі випадкового видалення, пошкодження файлів або виходу з ладу жорсткого диска. Давайте розглянемо декілька способів резервного копіювання даних.[1]

ОС Windows пропонує різноманітні способи резервного копіювання даних. Один з них - використання вбудованих інструментів, таких як "Резервне копіювання і відновлення" (Backup and Restore) або "Історія файлів" (File History), доступних в різних версіях ОС Windows.

"Резервне копіювання і відновлення" є вбудованим інструментом в ОС Windows, який дозволяє створювати повні системні резервні копії. Цей інструмент дозволяє зберігати копії файлів та налаштувань системи на зовнішньому пристрої, такому як зовнішній жорсткий диск або мережевий пристрій зберігання.

"Історія файлів" - це інша опція резервного копіювання, доступна в ОС Windows 10. Вона автоматично створює резервні копії ваших особистих файлів на зовнішньому пристрої або в мережі. Це дозволяє легко відновити попередні версії файлів або відновити весь папку у разі потреби.

Крім вбудованих інструментів, існують також сторонні програми для резервного копіювання даних в ОС Windows. Деякі популярні програми включають Acronis True Image, EaseUS Todo Backup, Macrium Reflect тощо.

Резервне копіювання на зовнішній жорсткий диск є одним з найпоширеніших способів забезпечення безпеки даних в ОС Windows. Це може бути портативний пристрій, підключений до комп'ютера через USB, який забезпечує зручний спосіб зберігання резервних копій.

Хмарні сховища є іншим популярним варіантом резервного копіювання в ОС Windows. Сервіси, такі як Google Drive, Dropbox або Microsoft OneDrive, надають можливість зберігати ваші файли у хмарі, що забезпечує додатковий рівень безпеки та доступу до них з будь-якого пристрою з Інтернетом.

Системні образи є ще одним ефективним способом резервного копіювання в ОС Windows. Вони створюють повний образ вашої операційної системи, включаючи всі файли, програми та налаштування. Це дозволяє відновити систему до працездатного стану у разі великих проблем або відмови жорсткого диска.

Автоматизація процесу резервного копіювання є важливим аспектом. В ОС Windows можна налаштувати регулярне резервне копіювання за заданим графіком або в залежності від змін у файлах. Це допомагає запобігти втраті даних, оновлюючи резервні копії автоматично.

Отже, незалежно від вибраного способу резервного копіювання, важливо періодично перевіряти та тестувати резервні копії, щоб забезпечити їх цілісність. Також рекомендується зберігати резервні копії в безпечному місці, окрім комп'ютера, для захисту від фізичного знищення або крадіжки.

## Перелік використаних джерел

1. https://uk.wikipedia.org/wiki/Резервне_копіювання (дата звернення: 07.05.2023).

# ОБ'ЄКТИВНІСТЬ ДЕФІНІЦІЙ СФЕРИ КІБЕРБЕЗПЕКИ ВІДПОВІДНО ДО МІЖНАРОДНИХ СТАНДАРТІВ

Живило Є.О., Кузь В. С.
Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна

На підставі завдань, які визначені у Стратегії кібербезпеки України [1] щодо гармонізації нормативних документів (Далі – НПБ)у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки (Далі – КБ), відповідно до міжнародних стандартів і стандартів ЄС та НАТО, зокрема [2, 3, 4, 5, 6, 7], необхідно здійснити гармонізації термінів/визначень та нормативних документів України у сфері кібербезпеки та кібероборони відповідно до міжнародних стандартів і стандартів ЄС та НАТО.
**Ключові слова:** нормативний документ, стандарт, дефініція, кібербезпека, захист інформації.

## Вступ

В термінології, як розділі лексикології, аксіомою є те, що визначення будь-якого терміну (дефінієндуму) та зміст і значення визначаючого поняття (дефінієнса) мають бути тотожними та вичерпувати один одного, мати змістовно схоже навантаження (денотат). Проаналізувавши визначення та терміни існуючої НПБ України, необхідно зауважити, що із 21 розглянутих дефініцій, наведених в Законі України "Про основні засади забезпечення кібербезпеки України" коректними та суттєвими можна назвати лише 8 (стор. 53, 54).

При порівнянні їх з дефініціями, наведеними в інших джерелах НПБ сфери КБ, Кримінального кодексу України, ознак синонімічності серед дефініцій не виявлено. Аналіз на синонімічність дефініцій, синтезованих в ході даної наукової роботи, має бути здійснений одночасно їх аналіз на системність.

## Формування термінів, та визначень

Логічний алгоритм формування значення для терміну, дефініція (лат. definitio – визначення), є важливим засобом скорочення складних описів та окремих міркувань у наукових теоріях та галузях знань, чим виконує важливу функцію у науково-освітній та практичній діяльності. Враховуючи зазначене, для подальшої роботи необхідно ввести деякі умовні символи, означення яких наведено у таблиці 1:

Таблиця 1.

Таблиця умовних символів

| **Позначення** | **Означення** |
|---|---|
| $Dfd$ | дефінієндум – визначення будь-якого терміну |
| $Dfn$ | дефінієнс – зміст (денотат) і значення визначаючого поняття |
| $\in$ | належність |
| $\notin$ | неналежність |
| $\{\ \}$ | множина |
| $\equiv$ | тотожність |
| $=$ | однозначність, точність (денотат) |
| $K_o$ | термінологічна система предметної галузі – КО |
| $K$ | термінологічна система предметної галузі – КБ |
| $K_p$ | термінологічна система предметної галузі – криптографічний ЗІ |
| $T_p$ | термінологічна система предметної галузі– ТЗІ |
| $C_o$ | термінологічна система предметної галузі – комп'ютерні науки |
| $C_s$ | термінологічна система галузі предметної галузі – Cybersecurity |
| $C_d$ | термінологічна система галузі предметної галузі – Cyberdefence |

## Виклад основного матеріалу

До науково-технічних термінів висуваються наступні вимоги:

**Системність** (від грец. – з'єднання, утворення): основоположний принцип наукового пізнання і соціальної практики, сутність якого виявляється у застосуванні системного (комплексного) підходу в дослідженні складних об'єктів (систем) і орієнтує дослідження на розкриття їх цілісності та виявлення всіх типів зв'язків у ньому, зведення їх у єдину систему знань.

**Вмотивованість** (дефінієндуму) – структурно-семантична особливість слова, що дозволяє зрозуміти раціональність поєднання значення та звукової оболонки слова на основі лексичного та структурного співвідношення.

**Однозначність** – спроможність передати змістовне навантаження без додаткового застосування термінологічного словника.

**Точність** – високий ступінь відповідності об'єктивним даним, дійсності.

У терміносистемі сфери КБ одночасно існує й паралельно застосовується низка дефініцій, в яких одному дефінієндуму *( Dfd )* ставиться у відповідність декілька дефінієнсів *( Dfn )*:

$$Dfd \equiv \{Dfn\} \tag{1}$$

або навпаки, один дефінієнс розкриває значення різних дефінієндумів:

$$\{Dfd\} \equiv Dfn \tag{2}$$

Виконання даної роботи здійснюється за наступним алгоритмом, який демонструється Рис. 1.

Вибір термінів та їх дефініцій з множини ключового набору термінів термінологічних систем сфер КБ та кібероборони, а також суміжних галузей знань та формування множини усіх можливих (правдивих, ймовірно

правдивих, умовно-правдивих) дефініцій термінологічного апарату, які можуть бути розглянуті відносно їх належності до терміносистем галузей знань, що розглядаються представлені виразом 3.

$$\left\{ \begin{array}{l} Dfd = Dfn \in \left\{ K,\ K_p,\ T_p, C_o, C_s, C_d \right\} \\ Dfd \equiv Dfn \in \left\{ K,\ K_p,\ T_p, C_o, C_s, C_d \right\} \\ \left\{ Dfd \right\} = Dfn \in \left\{ K,\ K_p,\ T_p, C_o, C_s, C_d \right\} \\ Dfd \equiv \left\{ Dfn \right\} \in \left\{ K,\ K_p,\ T_p, C_o, C_s, C_d \right\} \end{array} \right\} \quad (3)$$

Збір максимальної кількості вживаних в професійному, науковому та соціальному середовищах конкретних дефініцій кожного терміну терміносистеми, включно з іноземних офіційних джерел міжнародних організації та країн-партнерів та формування множини усіх можливих ймовірно правдивих та умовно правдивих дефініцій термінологічного апарату, які можуть бути розглянуті щодо належності до терміносистем галузей знань, що розглядаються здійснюється за:

$$\begin{array}{l} \sum_1^n Dfd = Dfn \in \left\{ K, K_p, T_p, C_o, C_s, C_d \right\} \cup \\ \cup \sum_1^m Dfd \equiv Dfn \in \left\{ K, K_p, T_p, C_o, C_s, C_d \right\} \end{array} \quad (4)$$


Рисунок 1. Алгоритм дефрагментації предметної області дефініції

Здійснення виборки та аналіз кожної дефініції з множини (4) здійснюється на:

**системність**, тобто належність терміну до певної термінологічної системи, результат – виключення зайвих термінів;

$$Dfd \neq Dfn \notin \left\{ \begin{array}{l} \left\{ K,\ K_p,\ T_p, C_o, C_s, C_d \right\} \\ \left\{ K,\ K_p,\ T_p, C_o, C_s, C_d \right\} \\ \left\{ K,\ K_p,\ T_p, C_o, C_s, C_d \right\} \\ \left\{ K,\ K_p,\ T_p, C_o, C_s, C_d \right\} \end{array} \right\} \qquad (5)$$

відсутність синонімів, результат – виключення зайвих термінів, що в межах одній терміносистеми, забезпечує запобігання взаємному непорозумінню фахівців;

$$\{Dfd\} \equiv Dfn \notin \begin{Bmatrix} \{K,\ K_p,\ T_p, C_o, C_s, C_d\} \\ \{K,\ K_p,\ T_p, C_o, C_s, C_d\} \\ \{K,\ K_p,\ T_p, C_o, C_s, C_d\} \\ \{K,\ K_p,\ T_p, C_o, C_s, C_d\} \end{Bmatrix} \quad (6)$$

однозначність, тобто на тотожність тільки одного наукового або технічного терміну $Dfd$ та відповідного йому поняття $Dfn$, результат – виключення зайвих термінів:

$$\{Dfd \equiv Dfn\} \quad (7)$$

точність, тобто – ступінь відповідності об'єктивній дійсності. При цьому з'ясовується чому виникло занадто широке значення змісту (надлишковість) або занадто вузьке визначення та формується не менш ніж одна ймовірно правдива дефініція термінологічного апарату терміносистеми галузі знань, що розглядається:

$$\{\exists Dfd \equiv Dfn\} \quad (8)$$

вмотивованість, тобто спроможність передати змістовне навантаження без додаткового застосування термінологічного словника та формування не менш однієї правдивої дефініції термінологічного апарату терміносистеми галузі знань, що розглядається

$$Dfd \equiv Dfn \rightarrow Dfd = Dfn \quad (9)$$

Декомпозиція обраних для подальшої роботи термінів термінологічного апарату терміносистеми галузі знань, що розглядається як

$$Dfd \in \{K, K_o\} \cap Dfn \in \{K, K_o\} \quad (10)$$

Композиція однозначних нових дефініцій термінів. При чому, дефініція кожного нового словосполучення (складного терміну) має містити дефініційні ознаки кожного слова складного терміну, які мають формувати дефініцію складного терміну. При цьому складний термін має формувати нові властивості, притаманні тільки йому.

$$Dfd = Dfn \in \{K, K_o\} \quad (11)$$

Аналіз синтезованої нової єдиної ймовірно правдивої дефініції терміну на вмотивованість, точність, однозначність, відсутність синонімів, системність здійснюється порядком визначеним вище (вирази 5, 6, 7, 8).

Порівняльний аналіз на точність та вмотивованість синтезованої єдиної ймовірно правдивої дефініції терміну з аналогом міжнародної терміносистеми в даній сфері завершує процес формування єдиної правдивої дефініції терміносистеми галузі знань, що розглядається:

$$Dfd = Dfn \in \{K, K_o\} \equiv Dfd = Dfn \in \{C_s, C_d\} \quad (12)$$

## Висновки

Отже, враховуючи чисельні консультації, практичні навчання, конференції, семінари та тренінги, що займають значне місце серед різноманітних заходів програм взаємодії між Україною і НАТО та США у сфері КБ, було виявлено протиріччя базового термінологічного апарату. З метою вирішення вищезазначених протиріч законодавча та НПБ України потребує суттєвих змін. Необхідно провести реальну імплементацію міжнародних стандартів ISO/IEC 27k, NIS Directive, NIST CS Framework, зокрема щодо запровадження базового рівня відповідності вимогам з КБ, оцінювання ризиків, реагування на кіберінциденти і врегулювання інцидентів, відновлення сталого функціонування критичної інфраструктури держави у відповідності до кращих міжнародних практик.

## Перелік використаних джерел

1. Стратегія кібербезпеки України, введена в дію Указом Президента України від 26 серпня 2021 року № 447/2021, – Режим доступу https://www.president.gov.ua/documents/4472021-40013.

2. DOD Dictionary of Military and Associated Terms. As of January 2020. [Електронний ресурс]. – Режим доступу:

https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

3. Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности. – Женева:МСЕ, 2010. – С. 55. – [Електронний ресурс]. – Режим доступу: www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136

4. Рекомендації міжнародного союзу електрозв'язку. Мережі передачі даних, взаємозв'язок відкритих мереж та безпека. Безпека кіберпростору – кібербезпека. МСЕ-Х.1208 2014 р. ISO/IEC 27000. Режим доступу: [b-ISO/IEC 27000].

5. ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT). Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів.

6. NATO glossary of terms and Definitions (English and French). Edition 2019. Режим доступу: https://standard.di.mod.bg/ pls/mstd/MSTD.

7. Tallinn Manual on the International Law Applicable to Cyber Warfare. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Second Edition. Режим доступу: http://csef.ru/media/articles/3990/3990.pdf.

# АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ З МЕТОЮ ВИЯВЛЕННЯ ПРИХОВАНИХ C2 КАНАЛІВ ШПЗ

Д.В. Твердохлібов
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», НН Фізико-технічний інститут, Київ, Україна

В статті досліджено основні методи побудови звичайних і прихованих C2 (command and control) каналів ШПЗ (шкідливого програмного забезпечення). На прикладі open-source рішень, таких як C3 framework, Sliver та Covenant було проаналізовано знаходження індикаторів компрометації (IOC) у мережевому трафіку.

**Ключові слова:** ШПЗ, C2, індикатори компрометації, IOC, C3, Sliver, мережевий трафік

## Вступ

Однією із найпоширеніших технік атак є використання C2. Command and Control (C2) є відведеною тактикою у фреймворку Mitre ATT&CK [1], що складається з різних технік, кожна з яких описує різні способи забезпечення постійного зв'язку між «імплантами» (програмними агентами, які працюють на скомпрометованих робочих станціях та забезпечують можливість виконання команд та отримання результатів) та сервером командно-контрольного зв'язку [2]. C2 (Command and Control) фреймворк - це програмне забезпечення, що забезпечує централізовану платформу для управління та контролю мережею компрометованих комп'ютерів – ботнет. Його призначення полягає у тому, щоб дозволити злочинцям віддалено керувати скомпрометованими системами та використовувати їх для здійснення різних зловмисних дій, таких як викрадення чутливих даних, запуск DDoS-атак або поширення шкідливих програм. C2 зазвичай включає один або кілька каналів зв’язку, але залежно від атаки конкретні механізми можуть суттєво відрізнятися. Для наглядного визначення можливостей відомих C2 фреймворків було створено C2 Matrix [3].

## Основні види комунікації між C2 сервером і клієнтом

Загалом комунікація між клієнтом і командним сервером базується на застосуванні HTTP, DNS і TCP протоколів. У випадку комунікації між клієнтами ботнета всередині мережі часто використовується SMB.

З міркувань маскування, клієнти ботнету приймають і передають данні не постійно, а з певним інтервалом, таким чином зменшуючи об’єм трафіку. HTTP трафік зручний тим, що має величезну гнучкість, трафік зазвичай не блокується фаєрволами, данні можна передавати різними способами, наприклад, передавати данні різного призначення (початок сесії клієнта, обмін ключами

шифрування) форматовані різними енкодерами і по різнім url-шляхам [4].

Також при використанні HTTP трафіку доволі легко замаскувати командний сервер, використовуючи http-переадресацію, тобто запити не йдуть до сервера C2 зловмисника. Вони проходять через скомпрометовану веб-сторінку або фальшивий сайт-перенаправлення. Це зроблено для того, щоб при виявленні C2-трафіку було приховано адресу командного серверу.

Використання DNS у якості основного каналу комунікації зручне і доволі швидке, але такий канал дуже легко знайти у мережевому трафіку [5].

У якості штучного каналу можна використовувати WireGuard (як це робить Sliver) або OpenVPN. У такому випадку, C2-трафік маскується посеред VPN трафіку.

Тому часто зловмисники і red-team спеціалісти використовують штучні C2 канали використовуючи легітимні месенджери, пошту, файлообміники [6]. Наприклад, C3 фреймворк дозволяє будувати приховані канали через Discord, Slack, Mattermost, GitHub, Dropbox [8]. До того ж, він дозволяє будувати штучні канали всередині скомпрометованої мережі, використовуючи LDAP, UNC Share File [7].

**Знаходження основних індикаторів компрометації**

У випадку використання WireGuard у якості C2 каналу, сам факт наявності такого трафіку від кінцевих пристроїв у мережі є явним індикатором компрометації.

Для виявлення HTTP C2 каналу слід звернути увагу на великі об’єми HTTP трафіку, дивні патерни (наприклад, заголовок user-agent у запиті відрізняється від версії браузера встановленої в системі), url та імена файлів. Наприклад, для Sliver у стандартній конфігурації, файли з розширенням .woff використовуються для завантаження шелкодів.

При комунікації через DNS головними індикаторами є DNS запити до доменів з низькою репутацією. Крім того, DNS запити дозволяють знайти зразки ШПЗ, що використовують замасковані c2 канали через легітимні

месенджери, наприклад Slack. Звичайний легітимний месенджер буде робити запити на безліч субдоменів slack.com, наприклад slack.com, files.slack.com, api.slack.com, edgeapi.slack.com і так далі. В той час, ШПЗ, що використовує slack для комунікації з командним сервером, буде мати трафік лише на slack.com, або на files.slack.com для відправки файлів.

Для пошуку ШПЗ що використовує приховані C2 канали можна використовувати Event Tracing for Windows (ETW) і моніторити кількість мережевих з'єднань.

**Висновки**

Виявлення індикаторів компрометації для прихованих C2 каналів шкідливих програм, що використовують законні сервіси, такі як Slack, Discord та інші платформи, є критичним аспектом полювання на загрози. Зловмисники використовують легітимні сервіси для C2, щоб приховати свої дії та уникнути виявлення традиційними засобами безпеки. Щоб виявляти ці атаки з застосуванням C2, необхідно зосередитися на аналізі шаблонів комунікації в та виявленні аномалій в мережевому трафіку, які можуть свідчити про компрометацію мережі.

## Перелік використаних джерел


1. ATT&CK Matrix for Enterprise [Електронний ресурс] – Режим доступу: https://attack.mitre.org
2. Command & Control (C2) [Електронний ресурс] – Режим доступу: https://7h3w4lk3r.gitbook.io/the-hive/network-attacks-1/command-and-control
3. C2 Matrix [Електронний ресурс] – Режим доступу: https://www.thec2matrix.com/matrix
4. HTTP(S) C2 [Електронний ресурс] – Режим доступу: https://github.com/BishopFox/sliver/wiki/HTTP(S)-C2#under-the-hood
5. DNS C2 [Електронний ресурс] – Режим доступу: https://github.com/BishopFox/sliver/wiki/DNS-C2#under-the-hood

6. From C2 to C3: Hackers are getting esoteric when covering footprints, calling home [Електронний ресурс] – Режим доступу: https://thestack.technology/from-c2-to-c3/
7. C3 [Електронний ресурс] – Режим доступу: https://github.com/WithSecureLabs/C3
8. Attack Detection Fundamentals: C2 and Exfiltration - Lab #3 [Електронний ресурс] – Режим доступу: https://labs.withsecure.com/publications/attack-detection-fundamentals-c2-and-exfiltration-lab-3
9. Hunting for C3 [Електронний ресурс] – Режим доступу: https://labs.withsecure.com/publications/hunting-for-c3

# АНАЛІЗ ОСНОВНИХ НАПРАВЛЕНЬ В ДОСЛІДЖЕННІ МОДЕЛІ ФІЛЬТРАЦІЇ VEC ИСТІВ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

Д.В.Зібаров, О.В. Козленко
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», НН Фізико-технічний інститут, Київ, Україна

**Ключові слова:** BEC, електронна пошта, машинне навчання, аналіз пошти, підозріла активність.

## Вступ

Партнерські BEC, також відомі як Vendor email compromise (VEC) є цілеспрямованим типом атаки на компрометування робочої електронної пошти (BEC), в якому зловмисник імітує третю сторону – постачальник, аби щось вкрасти у клієнтів цього постачальника [1]. Ця форма спрямованої соціальної інженерії полягає в тому, що зловмисник використовує довіру до постачальників. Такий сценарій може використовувати підробку електронної адреси постачальника, викрадення облікових даних, тощо.

Системи виявлення та запобігання VEC можуть використовувати різні методи для захисту організації.

Наприклад, Agari пропонує рішення, яке включає в себе аналіз поведінки електронної пошти та інші методи, IronScales використовує комплексний підхід, щозаключається в аналізі усіх мета-даних за допомогою машинного навчання. Звісно, ніякий автоматизований підхід не може гарантувати стовідсоткову ймовірність виявлення, тому організації користуються послугами аналітиків для додаткового контролю за системою.

**Методи виявлення VEC:**

Основні методи виявлення:

1. Навчання з питань безпеки для співробітників. Дуже важливо, аби людина могла самостійно визначити небезпеку, якщо зловмисник зможе обійти фаерволл.
2. Абсорбційна спектроскопія – перевірка стандартів автентифікації електронної пошти (SPF, DKIM, DMARC), виявлення підроблених доменних імен.
3. Виявлення червоних прапорців: несподівані зміни в типовому контенті, зміни заголовків, помилки в листі, тощо.
4. Застосування готових рішень для захисту від фішингу. Одним з найбільш ефективних методів виявлення атак VEC – це комплексний аналіз заголовків електронної пошти, аналіз змісту та стилю написання автора за допомогою алгоритмів машинного навчання. [2]

Серед потенційних індикаторів VEC можуть бути: виглядаючі як оригінальні електронні адреси або імена користувачів, підозрілий (незвичний) поштовий сервер або IP-адреса, підозрілий текст листа (неочікувані запити на сплату, обмеження у варіантах відповіді). [3]

**Проблеми при виявленні BEC**

За 2022 рік атаки BEC еволюціонували від зламу пошти й обходу багатофакторної аутентифікації до імітування юридичної фірми та соціальної інженерії. [4] Тому систему виявлення потрібно постійно оновлювати щоб запобігти FP (false positive) та FN (false negative) реакціям. Аби робити правильні висновки щодо шкідливості окремого листа необхідно застосовувати комплексний підхід, який включає

повний аналіз заголовків та вмісту листа. Також необхідно правильно розставити ваги для кожного індикатора (наприклад, граматична помилка в тексті не так критична, як “look-a-like” адреса), таким чином після аналізу ми будемо мати список виявлених індикаторів з умовною сумою ваг, якщо ця сума більша за
певне число – ми можемо сказати, що лист шкідливий, а якщо вона висока, але недостатня – лист підозрілий і користувачу варто звернути увагу на його справжність.

**Потенційні небезпеки**

Типові BEC/VEC листи зазвичай націлені на викрадення грошей (зміна платіжних даних, закуп подарункових карток, сплата фальшивих рахунків, тощо) або викрадення чутливих даних компанії (уточнення чогось з проханням надіслати це у відповідь). [5] За даними ФБР, BEC наразі є найдорожчим цифровим злочином. [6]

**Висновки**

Business email compromise і в тому числі vendor email compromise – серйозна проблема для сучасного бізнесу, котра може призвести до серйозних не тільки фінансових а й репутаційних втрат. Для запобігання витокам компанії зазвичай користуються сторонніми сервісами, що надають готові рішення для запобігання атак. Зазвичай для категоризації листа та виявлення потенційної небезпеки в ньому постачальники послуг безпеки аналізують вміст листа, дані відправника та заголовки цього листа.

**Посилання**

1. Business Email Compromise — FBI - https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise
2. Detection of Business Email Compromise Attacks with Writing Style Analysis | Request PDF (researchgate.net) – https://www.researchgate.net/publication/358062347_Detection_of_Business_Email_Compromise_Attacks_with_Writing_Style_Analysis

3. How to Prevent Vendor Email Compromise (VEC) Attacks (xorlab.com) – https://www.xorlab.com/en/blog/how-to-prevent-vendor-email-compromise-vec-attacks
4. 2022 Wrap Up - The Evolution of Business Email Compromise (BEC) (dacbeachcroft.com) – https://www.dacbeachcroft.com/ en/gb/ articles/2022/december/2022-wrap-up-the-evolution-of-business-email-compromise-bec/
5. What is Business Email Compromise (BEC)? | Microsoft
6. Security – https://www.microsoft.com/en-us/security/business/ security1/what-is-business-email-compromise-bec
7. What is Business Email Compromise (BEC)? And How To Prevent It | UpGuard – https://www.upguard.com/blog/business-email-compromise

# RSA-LIKE ALGORITHMS

Fedir Sokhatsky
Vasyl' Stus Donetsk National University
Vinnytsia, Ukraine

Some improvements are proposed for two algorithms: 1) for Euclid's extended algorithm: namely, for an algorithm for finding the linear representation of a gcd; and 2) for the RSA algorithm: for this aim, Fermat's theorem is generalized for square-free numbers (product of an arbitrary number of pairwise different prime integers), which allows constructing RSA-like algorithms: that is, algorithms based on square-free integers. Such algorithms are more reliable.
**Keywords:** Extended Euclidian algorithm, Fermat theorem, RSA algorithm, RSA-like algorithm, square-free integer, information protection, cybersecurity.

The reliability of the RSA algorithm increases if the basis of the algorithm is the product of $k$ prime numbers for $k > 2$. To construct such algorithms (i.e. RSA-like), Theorem 2 is proved. One of the subtasks of constructing RSA-like algorithms is

finding the inverse of integers. For this, the extended Euclid algorithm is used. A significant simplification of the algorithm is proposed here.

Let $a$, $b$ be integers, and $r_{n+1} = 0,\ r_0 \coloneqq a,\ r_0 \coloneqq b$ and

$$r_{i-1} = r_i q_i + r_{i+1},\ i = 1, 2, \dots n, \quad (1)$$

be Euclidian algorithm. The integers $y_1, y_2, \dots, y_{n-1}, y_n$ which defined by

$$\boldsymbol{y_n \coloneqq 1},\quad \boldsymbol{y_{n-1} \coloneqq -q_{n-1},\ y_i \coloneqq y_{i+2} - y_{i+1} q_i},\quad (2)$$
$$i = n-2, n-3, \dots, 2, 1,$$

will be called coefficients of linearity, and the integer $y_1$ be the main coefficient of linearity for $a$ and $b$.

**Theorem 1.** *Let a, and b be positive integers, $d \coloneqq gcd(a, b)$, (1) be Euclidian algorithm, and $y_i$ be defined by (2). Then*

1) $d = gcd(r_i, r_{i+1}),\ d = r_n,\ i = 0,1, \dots, n;$
2) $d = r_i y_{i+2} + r_{i+1} y_{i+1}, d = a y_2 + b y_1,$
$i = 0,1, \dots, n-2.$

**Corollary 1.** The integers $y_i$ and $y_{i+1}$ are coprime for all $i = 0,1, \dots n-1$. The calculation of the main coefficient of linearity $y_i$ needs not more than $4\log_2 a$ steps. $y_i$ is inverse to $b$ modulo $a$, if $a$ and $b$ are coprime and $a > b > 0$.

A *square-free integer* is an integer that is divisible by no square number other than 1. In other words, its prime factorization has exactly one factor for each prime that appears in it. Also, $n$ is square-free if and only if in every factorization $n = ab$, the factors $a$ and $b$ are coprime. Over 3/5 of all integers are square-free. The following simple theorem is a generalization of Fermat's theorem needed for the construction of RSA-like algorithms.

**Theorem 2.** *If n is square-free and $s \equiv 1\ mod\ \varphi(n)$, then $x^s \equiv x (mod\ n)$ for all integers x.*

**RSA-like algorithm:**

1) choose $s$ pairwise different prime numbers $p_1, \dots, p_s$;
2) find $n = p_1 \cdot \dots \cdot p_s$;
3) find $\varphi(n) = (p_1 - 1) \cdot \dots \cdot (p_s - 1)$;

4) find $k$ such that $k < \varphi(n)$ and $k$, $\varphi(n)$ are coprime;
5) find $\ell$ such that $k\ell \equiv 1\ (mod\ \varphi(n))$ (Theorem 1);

The pair $n,\ k$ of integers is the open key. $M^k$ modulo $n$ is the encrypt of information $M$. To renew $M$, $M^k$ is raised to the power $\ell$ modulo $n$: $(M^k)^\ell \equiv M^{k\ell} \equiv M$ (Theorem 2).

## Conclusion

The obtained results make it possible to simplify the construction of RSA algorithms and extend their set to the set of RSA-like algorithms increasing their reliability.

# ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙНУ ДЛЯ ПОБУДОВИ ІЄРАРХІЧНОЇ СТРУКТУРИ НА МНОЖИНІ ДЕРЖАВНИХ РЕЄСТРІВ З МЕТОЮ ЗАХИСТУ ВІД ПІДРОБКИ ІНФОРМАЦІЇ

Кондратенко М.С.
Інститут проблем моделювання в енергетиці ім. Г.Є.
Пухова НАН України, Київ, Україна

В роботі розглянуто питання безпеки зберігання даних в різних реєстрах, в тому числі державних. В першу увага була приділена атакам, спрямованим на підміну інформації у реєстрі, що на сьогодні є актуальною та реальною загрозою. Спосіб, запропонований в роботі базується на використанні результатів з відносно нового напрямку у галузі інформаційних технологій – технології блокчейну. В роботі пропонується побудова так званої каскадної структури реєстрів на блокчейнах, з використанням одного з найновіших протоколів консенсусу під назвою Proof-of-Proof (“підтвердження доведення”)[1]. Така каскадна структура реєстрів, при правильних параметрах її побудови та використання, забезпечує всі властивості правильного збереження інформації, такі як невідмовність, непідмінність, черговість розміщення в реєстрі тощо.

**Ключові слова:** Блокчейн, державний реєстр, бази даних, протоколи консенсусу, захист інформації.

На сьогодні в Україні відбувається активне формування та впровадження державних реєстрів у різних галузях життя країни. Державний реєстр ведеться уповноваженим органом держави з метою накопичення, обробки інформації та надання певним відомостям офіційного визнання. Враховуючи важливість інформації, що зберігається в реєстрах, а також обсяг персональної інформації в них, актуальним є питання захищеності цих даних. На сьогодні, як правило, реєстри (або бази даних, як їх технічне представлення) зберігаються централізовано на серверах та сховищах, які є власністю держави. Така централізована система все частіше стає уразливою до кібератак, оскільки вся інформація зосереджена в одному вузлі і зловмисникам варто отримати доступ до відповідного сервера чи бази даних для подальшої підміни інформації чи інших дій злочинного характеру. В цій ситуації на допомогу приходить відносно нова технологія під назвою блокчейн. Основна відмінність блокчейну від класичних баз даних полягає в тому, що бази даних використовують таблиці для зберігання інформації, а блокчейн – блоки, що пов'язані один з одним. Також важливо, що блокчейн – це децентралізована база даних (P2P – "Peer-To-Peer"), в якій вся інформація розміщується на великій кількості вузлів, які можуть знаходитись у будь-якій точці світу, при чому, в такій топології головний сервер відсутній [2]. Блокчейн – сучасна та прозора система. Кожен учасник може побачити інформацію про будь-який блок. Найбільшими перевагами даної технології є надійність, відмовостійкість та безпека. За невеликий проміжок часу її почали застосовувати для зберігання цифрових активів, захисту авторського права, ідентифікаційної інформації, голосування та інших даних. Варто зазначити, що блокчейн використовує криптографічні алгоритми для забезпечення роботи системи. Вони гарантують незмінність блоку транзакцій, що є важливим аспектом збереження даних, зокрнма і в державних реєстрах.

Все більше розвинутих країн починають використовувати блокчейн у державному секторі, збільшуючи надійність даних та зменшуючи значимість людського фактору, що знижує рівень корупції. На початку 2022 року влада Канади запустила систему, яка за допомогою блокчейну Ethereum стежила за прозорістю розподілу державних грантів. Тим часом Японія планує застосувати блокчейн у системі державних закупівель, а в Австрії цю технологію використовують для регулювання енергопостачань. Україна має досвід успішного використання блокчейн-технології у державному управлінні та демонструє готовність до її розвитку для боротьби з корупцією, забезпечення прозорості та ефективності в процесах прийняття рішень та покращення державного управління [3]. Завдяки своїй захищеності, прозорості та швидкодії, технологія блокчейн якнайкраще підходить для впровадження у сфері державних реєстрів.

Модель каскадних реєстрів, яка пропонується до розгляду, передбачає використання ієрархічної моделі блокчейнів, в якій на вершині ієрархії знаходиться єдиний державний блокчейн, якому, в свою чергу, підпорядковується мережа існуючих державних реєстрів, які ведуться на окремих блокчейнах. Блокчейни повинні передавати інформацію про кожен свій N-ний блок на головний блокчейн (mainchain). Безпосередньо головний блокчейн не буде містити інформацію про об’єкти реєстру та будь-які їх персональні дані, а лише хеш-коди відповідних блоків дочірніх реєстрів. Таким чином гарантується захищеність головного блокчейну від підміни інформації в ньому. Посилання на певні блоки за певним правилом є основним принципом взаємодії між блокчейнами та між окремими блоками. І саме розміщення посилань на певні блоки згідно певним правилам і визначає ієрархічну структуру між різними блокчейнами, кожен з яких буде забезпечувати функціонування та оновлення певного окремого реєстру.

У каскадних блокчейнах, на базі яких пропонується створювати каскадні реєстри, сайдчейни (SC) повинні надсилати інформацію про свої блоки до головного

блокчейну (МС). Безпосередньо МС не обов'язково має містити інформацію про об'єкти реєстру та будь-які їх персональні дані, а лише хеш-функції відповідних блоків з SC. Тепер пояснимо, як саме ідея протоколу PoP може бути використана для зберігання, обробки та обміну інформацією у однорангових децентралізованих системах.

Припустимо, що для зберігання локальної інформації (стосовно району, міста, області, тощо) використовуються багато різних незалежних однорангових систем, які організовані у блокчейни. Ці блокчейни ми вважатимемо сайдчейнами з усіма відповідними властивостями, зокрема з достатньо великою швидкістю виходу блоків. Щоб ці окремі децентралізовані системи могли безпечно взаємодіяти у плані обміну інформацією, над ними, вже на рівні держави, будується МС-блокчейн, єдиною функцією якого є створення своєчасних посилань на блоки всіх цих сайдчейнів. У такій моделі самостійність та де централізованість локальних мереж не порушиться, а їхні блоки будуть вважатись стабільними при зазначених вище умовах.

## Висновки

Запропонована модель побудови каскадних реєстрів з використанням технології блокчейн якнайкраще підходить для реалізації на множині єдиних державних реєстрів і в перспективі може значно підвищити показники надійності зберігання даних та їх захищеності, оскільки технологія блокчейн володіє всіма необхідними для цього властивостями.

## Перелік використаних джерел

1. Veriblock documentation. [Електронний ресурс]. – Режим доступу: https://www.veriblock.org/wp-content/uploads/ 2019/06/Proof-of-roof_and_VeriBlock_ Blockchain_Protocol_ Consensus_Algorithm_and_Economic_ Incentivization_v1.0.pdf

2. Moriah Fisher. Яка різниця між блокчейном і реляційною базою даних? [Електронний ресурс]. – Режим доступу: https://morioh.com/p/96c3e11795f2
3. Блокчейн у державному управлінні України. [Електронний ресурс]. – Режим доступу: https://psm7.com/uk/blockchain/blokchejn-u-derzhavnomu-upravlinni-ukra%D1%97ni-yak-liki-vid-korupci%D1%97-rejderstva-i-byurokrati%D1%97-dumka-ekspertiv.html

# БЕЗПЕЧНІ ДЕЦЕНТРАЛІЗОВАНІ СЕРЕДОВИЩА КОМУНІКАЦІЇ

Чорний А.Ю.
Навчально-науковий Фізико-технічний інститут КПІ
ім. Ігоря Сікорського, Київ, Україна

У статті розглядається проблема безпеки при передачі даних через Інтернет та можливі ризики, пов'язані з використанням централізованих сервісів. Пропонується децентралізований підхід як рішення цих проблем.
**Ключові слова:** Комунікація в мережі інтернет; Конфіденційні дані; Централізовані сервіси; Безпека даних; Приватність користувачів; Децентралізація; Безпека і конфіденційність

## Вступ

У сучасному світі, комунікація в мережі інтернет стала невід’ємною частиною життя для приблизно 65% населення Землі. Крім того інтернет є середовищем для передачі конфіденційних даних як і звичайних користувачів, так і бізнесу, чи навіть державних службовців. У разі компрометації конфіденційних даних, наслідки можуть призвести до втрати коштів або репутації. Тому з часом все більш швидко зростає попит на різні методи убезпечення даних що передаються через інтернет. У цій статті ми розглянемо проблеми передачі даних у мережі інтернет, і їх можливі рішення за допомогою децентралізованих систем комунікації.

## Загрози безпеки у сучасних середовищах комунікації в мережі інтернет

Однією з основних проблем безпеки централізованих інтернет сервісів є можливість несанкціонованого доступу до конфіденційної інформації користувачів. Коли дані зберігаються на центральному сервері, вони можуть бути скомпрометовані в результаті хакерських атак або витоку даних через внутрішній співробітників.

Крім того, централізовані сервіси використовуються для моніторингу активності користувачів, а це може порушувати приватність користувачів і створювати ризик переслідування або зловживання інформацією.

Інша проблема безпеки полягає в тому, що централізовані сервіси стають мішенню для атак на вузол, тобто атаки на сервер, що веде до недоступності сервісу або зниження його продуктивності. Також, централізовані сервіси можуть стати мішенню для DDoS атак, коли сервер перегружений великою кількістю запитів.

## Вирішення нагальних проблем комунікації за допомогою децентралізації

Децентралізація може допомогти вирішити проблеми безпеки і конфіденційності в інтернеті, оскільки вона дозволяє розподілити дані і функції між багатьма комп'ютерами, замість того, щоб зосереджувати їх в одному місці. Це зменшує ризик порушення безпеки даних або їх втрати через атаки хакерів, технічні неполадки або інші проблеми.

У децентралізованих системах кожен користувач контролює свої дані і не залежить від централізованих компаній або організацій, які можуть бути схильні до порушення конфіденційності даних. Крім того, децентралізовані системи можуть використовувати різні методи шифрування та автентифікації, що робить їх більш безпечними для збереження та передачі конфіденційної інформації.

Децентралізовані системи також можуть забезпечити більшу стійкість до відмов, оскільки вони розподілені між

багатьма комп'ютерами. Якщо один з комп'ютерів в децентралізованій мережі виходить з ладу, інші комп'ютери можуть продовжувати працювати, що запобігає зупинці всієї системи. Отже, децентралізація може допомогти вирішити проблеми безпеки і конфіденційності в інтернеті, зменшити ризик порушення безпеки даних або їх втрати через атаки хакерів, технічні неполадки або інші проблеми

## Висновки

Створення децентралізованих середовищ комунікації може стати вирішенням кількох наріжних проблем сучасного інтернету: скупчення великої кількості конфіденційних даних в одному місці, існування відстежуваного цифрового сліду користувачів і вразливість сервісів від точкових атак.

Поки жоден з сервісів що пропонують послуги з децентралізованої комунікації не набрав достатньої популярності щоб викликати зміну у попиті серед користувачів. Більшою мірою це пов’язано з нішевістю таких програмних продуктів, і відсутністю таких рішень що безкомпромісно перейшли на децентралізовану модель. В якості спроби вирішення цих проблем створено децентралізований сервіс комунікації що зберігає інформації користувачів, не вимагає і не провокує створення і розповсюдження цифрового сліду

## Перелік використаних джерел

1. Buchegger Sonja; Crowcroft Jon; Krishnamurthy Balachander; Strufe Thorsten Decentralized Systems for Privacy Preservation (Dagstuhl Seminar 13062) 2013

2. Michael Rogers; Trevor Perrin Security and Privacy in Decentralized Communication Systems. 2021.

3. Niklas Blum, Serge Lachapelle, Harald Alvestrand WebRTC: Real-Time Communication for the Open Web Platform

# ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В КІБЕРЗЛОЧИННОСТІ ТА МОЖЛИВОСТІ ЇЇ ЗАПОБІГАННЯ

Куцовол О.В.
Навчально-науковий Фізико-технічний інститут, КПІ ім. Ігоря Сікорського, Київ, Україна

Робота присвячена темі дослідження використання соціальної інженерії в кіберзлочинності. Розглянуто можливості та тактики для запобігання ризикам, які несе в собі соціальна інженерія в руках кіберзлочинців.
**Ключові слова:** оцінка ризиків, CI/CD, статичний аналіз, динамічний аналіз, SSDLC.

## Вступ

У сучасному цифровому світі, де технології безперервно розвиваються, ми стикаємося з ростом кіберзлочинності. Зловмисники постійно вдосконалюють свої методи, щоб здійснювати атаки на приватні дані, фінансові системи, урядові інституції та індивідуальних користувачів. Однак, одним з найбільш ефективних і хитрих методів, використовуваних зловмисниками, є соціальна інженерія..

Застосування соціальної інженерії в кіберзлочинності має серйозні наслідки для користувачів, організацій та суспільства в цілому. Вона може спричинити фінансові втрати, порушення конфіденційності та приватності, пошкодити репутацію, а навіть призвести до крадіжки особистої ідентичності. Щоб бути ефективними в запобіганні таким атакам, ми повинні розуміти та усвідомлювати ризики, пов'язані з соціальною інженерією

## Використання соціальної інженерії

Соціальна інженерія - це процес використання маніпулятивних технік та психологічних стратегій з метою впливу на інших людей і отримання від них потрібної інформації або досягнення певних цілей. Вона може мати

як позитивні, так і негативні аспекти. В ході дослідження було проаналізовано різноманітні методи соціальної інженерії, які використовуються зловмисниками. До них належать:

1. Фішинг: це метод, коли зловмисники створюють підроблені веб-сторінки або електронні листи, що імітують легітимні організації або особи, з метою отримання особистих даних, таких як паролі, номери кредитних карток тощо.
2. Виманювання: зловмисники використовують маніпуляцію та психологічний тиск, щоб отримати конфіденційну інформацію від людей..
3. Інженерія довіри: зловмисники використовують соціальні мережі та інші джерела, щоб зібрати інформацію про своїх потенційних жертв.
4. Викидання інформації: зловмисники шукають слабкі місця в системах безпеки, де можна отримати доступ до важливої інформації. Вони можуть використовувати соціальну інженерію, щоб отримати доступ до користувачів з високими привілеями або зламати систему через маніпуляцію персоналом.

На жаль, раз за разом, використовуючи соціальну інженерію , зловмисники досягають своїх цілей. І в сучасному світі яскраво постало питання про те, яким же чином можна захиститися від соціальної інженерії та чи є можливості їй запобігти.

## Можливості запобігання

Забезпечення захисту та від соціальної інженерії вимагає комплексного підходу та впровадження різноманітних засобів безпеки. Однак, більшість з порад, зазвичай стосується атак на великі компанії. В той час в кожній компанії працює сотні-тисячі осіб, кожен з яких може потрапити під вплив соціальної інженерії з боку зловмисників. Поглянемо на можливості запобігання для окремого індивіду:

1. Уникати надання особистих, фінансових або конфіденційних даних невідомим особам або через ненадійні канали комунікації.
2. Уникати клікати на посилання або відкривати вкладення в ненадійних електронних листах, повідомленнях або на соціальних мережах.
3. Публікувати мінімум особистої інформації на своїх профілях у соціальних мережах. Зловмисники можуть зібрати та використати цю інформацію для маніпуляції.
4. Встановлювати унікальні та складні паролі для своїх онлайн-акаунтів і використовувати двофакторну аутентифікацію, коли це можливо.
5. Регулярно оновлювати всі свої програми, включаючи операційну систему, браузери та інші застосунки.
6. Перевіряти ідентичність осіб, які звертаються до вас з проханнями про інформацію або дії, особливо якщо це нещодавні знайомі.

Таким чином, великі компанії мають проводити тестування по виконанню своїми співробітниками даних вимог, і лише потім відштовхуватися від них в бажанні захистити конфіденційність та цілісність власної інформації.Запобігання соціальній інженерії вимагає пильності, освіти та вживання заходів безпеки як на індивідуальному, так і на організаційному рівнях.

## Висновки

В цій роботі проведено дослідження використання соціальної інженерії, а також запропоновано можливості запобігання соціальній інженерії на індивідуальному рівні такі як обережне розкриття особистої інформації, уникання підступних посилань та вкладень, використання міцних паролів та двофакторної аутентифікації.

## Перелік використаних джерел

1. "The Art of Deception: Controlling the Human Element of Security" by Kevin D. Mitnick and William L. Simon

2. "Unmasking the Social Engineer: The Human Element of Security" by Christopher Hadnagy

# ПОБУДОВА МЕТОДИКИ ОЦІНКИ РИЗИКІВ БЕЗПЕКИ В ПРОЦЕСІ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Сернова А.Р.
Навчально-науковий Фізико-технічний інститут
КПІ ім. Ігоря Сікорського, Київ, Україна

Робота присвячена темі кількісної оцінки ризику на різних етапах розробки програмного забезпечення. Розглянуто методи виявлення вразливостей та загроз та метод підрахунку числового значення при застосування різних методик досліджень.
**Ключові слова:** оцінка ризиків, CI/CD, статичний аналіз, динамічний аналіз, SSDLC.

## Вступ

У світі сучасних технологій та стрімкої інформатизації всіх галузей життя, розробка програмного забезпечення поставлена на такий конвеєр, що кількість нових продуктів, які потрапляють щодня на ринок, злічується навіть не десятками. В той самий час пріоритетом розробки є дизайн, логічна структура коду, швидкодія – все те, чого потребує команда розробки та споживач саме зараз, а питання безпеки відступає на другий план.

Для успішного забезпечення і «безпечності» готової продукти, елементи кібербезпеки необхідно впроваджувати на усіх етапах життєвого циклу, а значить і робити оцінку ризиків для подальшого прийняття рішень щодо управління безпекою.

## Життєвий цикл програмного забезпечення

Класичний підхід SDLC не передбачає впровадження механізмів кібербезпеки, але альтернативно було

розроблено SSDLC (secure SDLC). Він не передбачає нових етапів, тільки висуває додаткові процедури на кожному з існуючих шести.

1. Планування: аналіз розповсюджених для даної задачі ризиків.
2. Аналіз: визначення вразливостей обраних мов програмування та фреймворків. Формування документації.
3. Дизайн: аналіз взаємодії з користувачем.
4. Розробка: огляд коду та статичний аналіз.
5. Тестування: тестування інструментами автоматизації DevSecOps.
6. Інтеграція: отримання репортів при виході з середовища тестування.

Таким чином, бачимо, що аналіз на наявність ризиків, їхня оцінка та приорітизація відбуваються неперервно на кожному кроці, але в залежності від етапу акцент робиться на різні техніки дослідження.

## Методи досліджень

Задамо функції реалізації ризику при застосуванні конкретної групи технік дослідження:

$$R_1 = f(x_1, x_2, x_3, x_4) - \text{статичний аналіз};$$
$$R_2 = f(y_1, y_2) - \text{динамічний аналіз};$$
$$R_3 = f(z) - \text{експертний аналіз};$$
$$R_4 = f(n) - \text{формальна верифікація};$$

Перетворимо відому формулу обрахунку ризику на таку, що враховує залежність імовірності реалізації загрози від кількості застосованих технік, де $W$ характеризує сукупність застосованих технік.

$$R = V * P = V * \frac{1}{W};$$

Таким чином функції оцінки ефективності методики дослідження будуть виглядати так:

$$f_1 = V * \frac{1}{x_1 + x_2 + x_3 + x_4};$$
$$f_2 = V * \frac{1}{y_1 + y_2};$$

$$f_3 = V * \frac{1}{z};$$
$$f_4 = V * \frac{1}{n};$$

де

$$x_i, y_i, z, n, m = \begin{cases} 1.1, \text{якщо техніка застосована;} \\ 0.001, \text{якщо техніка не застосована.} \end{cases}$$

Примітка: 1.1 та 0.001 – значення, які береуться, щоб показати відносну оцінку ризику.

Загальний ризик реалізації конкретної атаки тоді є $\sum_{i=1}^{5} f_i$. Розглянемо ризики CI/CD ланцюга [2], техніки їх дослідження та задамо формальне описання ризику наявності уразливостей протягом життєвого циклу. За допомогою програмної реалізації вище поданого методу дамо оцінку кожному ризику:

| Етап | Загроза | Техніка дослідження | | | | | | | | Оцінка ризику |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Експертний аналіз | Статичний аналіз | | | | Динамічний аналіз | | Формальна верифікація | |
| | | | Синтаксичний | Символьне виконання | Розповсюдження залежностей | Контекстуально-залежний | Розповсюдження залежностей | Динамічне тестування | | |
| Source | Недостатній контроль потоків | | | | | | | | | 25009 |
| | Неадекватне управління | | | | | | | | | 15018 |
| Build | Poisoned pipeline execution (PPE) | | | | | | | | | 10016 |
| | Ненадійна конфігурація | | | | | | | | | 10018 |
| Test | Недостатня гігієна конфіденційності | | | | | | | | | 25.75 |
| | Неузгоджене використання | | | | | | | | | 1016 |
| Deploy | Використання уразливостей ланцюга залежностей | | | | | | | | | 31.8 |
| | Некоректна перевірка цілісності артефактів | | | | | | | | | 25004 |

Витрати при реалізації ризику V умовно покладені рівні для кожного ризику, тому оцінка показує співвідношення для різних атак.

## Висновки

В цій роботі запропоновано метод отримання кількісної відносної оцінки ризику, що при поєднані з відомими методологіями, наприклад DREAD дає змогу винести вердикт про ступінь безпечності програмного продукту на різних кроках його розробки.

Виконано порівняння ступені небезпечності різних етапів CI/CD конвеєру.

## Перелік використаних джерел


1. Secure software development lifecycle (SSDLC): https://dpa-analytics.ru/secure-software-development-lifecycle-SSDLC-DevSecOps.
2. OWASP Top 10 CI/CD Security Risks: https://owasp.org/www-project-top-10-ci-cd-security-risks/.


# ОСОБЛИВОСТІ МОДЕЛЮВАННЯ ЗАГРОЗ ДЛЯ KUBERNETES ЗА ДОПОМОГОЮ ДЕРЕВ АТАК


О.Д. Бенда
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»,
НН Фізико-технічний інститут, Київ, Україна



**Ключові слова:** Kubernetes, моделювання, дерева атак, загрози.


## Вступ

Kubernetes, як найпопулярніша система оркестрації контейнерів, відіграє ключову роль у розробці програмного забезпечення. Його здатність управляти великим обсягом динамічних ресурсів сприяє продуктивності, але також створює серйозні виклики в контексті безпеки. Нажаль, разом з ростом популярності Kubernetes зростає й кількість потенційних загроз для безпеки. Розробка надійних моделей для візуалізації і передбачення цих загроз є важливим викликом. Один із наліпших способів моделювання цих загроз - використання дерев атак.

Дерева атак – це графічне представлення всіх потенційних шляхів, які атакуючий може використати для досягнення своєї цілі.[1] В даній моделі атаки на систему

представляються у формі деревоподібної структури, де кореневий вузол є кінцевою метою, а різні способи досягнення цієї мети виражені у вигляді ієрархій подій і листових вузлів. Вузли «АБО» використовуються для представлення альтернативних шляхів, а вузли «І» використовуються для представлення різних кроків у досягненні однієї й тієї ж мети.

## Моделювання загроз для Kubernetes за допомогою дерев атак

Створення дерев атак може виконуватись декількома методами. Найефективніше з усіх підходів показують себе двоє:

***"Знизу вверх"*:** у цьому підході побудова дерева починаєте зі списку всіх потенційних атак або експлойтів, які зловмисник може використовувати для компрометації системи, що й буде листовими вузлами. Після ідентифікації всіх цих атак вони групуються на основі цілей вищого рівня, досягненню яких вони сприяють, створюючи гілки і, нарешті, з'єднуючись з кореневим вузлом, який і є кінцевою ціллю атаки.

Цей підхід може бути вичерпним і детальним, але він може пропустити деякі стратегії на вищому рівні або не враховувати певні вектори атак, які не були зафіксовані в початковому списку потенційних експлойтів.

***"Сценарний (Зверху вниз)":*** у підході за сценарієм створення дерева починається з кінцевої цілі атаки (кореня дерева), яке потім розділяється на підцілі або кроки, які потрібно виконати, аби досягти кінцевої цілі, допоки не досягне листових вузлів, які є окремими експлойтами або атаками.

Цей підхід може бути більш стратегічним і допомагає зрозуміти, як взаємодіють різні атаки, але він може не бути таким детальним у врахуванні всіх можливих експлойтів на нижньому рівні, як підхід "знизу вверх".

Окрім вибору підходів, при створенні дерев атак особливу увагу треба приділити глибокому аналізу цілей, загроз та сценаріїв атак. Керуючись численними джерелами

в сфері безпеки, включаючи звіти організацій, таких як MITRE[2], CIS та Microsoft[3] варто зазначити такі найбільш типові сценарії атак:

- Privilege Escalation;
- Denial of Service;
- Malicious Code Execution;
- Cryptojacking
- Malicious Container Abuse;
- Resource Hijacking

## Специфіка моделювання загроз для Kubernetes

Для складної системи, такої як Kubernetes, яка використовується для керування контейнеризованими додатками в масштабі, моделювання загроз може допомогти виявити проблеми безпеки, які можуть вплинути на її розгортання.

Ось кілька конкретних найкращих практик, використання яких обов'язкове, коли мова йде про моделювання загроз для Kubernetes:

- Ідентифікація активів;
- Розуміння архітектури та компонентів Kubernetes;
- Механізми аутентифікації та авторизації;
- Розуміння роботи контейнерного середовища;
- Використання мережних політик;
- Пріоритезація ризиків;
- Зменшення ризиків.

Важливо пам'ятати, що, у зв'язку з динамічною природою системи, моделювання загроз для Kubernetes – це процес повторюваний. Із кожною новою функцією моделі повинні оновлюватися, нові вразливості будуть неодмінно з'являтися, не враховуючі нові експлойти під старі функції.

## Висновки

Враховуючи важливість Kubernetes в сучасних середовищах розробки ПЗ, нагальним є використання ефективних інструментів для моделювання потенційних загроз безпеки. Дерева атак являють собою надзвичайно потужний інструмент для візуалізації й моделювання

потенційних векторів атаки. Зокрема, методи "знизу вверх" та "сценарний" дозволяють розглядати проблеми з різних перспектив, хоча кожен з них має свої переваги та обмеження.

Типові сценарії атаки в Kubernetes, такі як підвищення привілеїв, відмова в обслуговуванні, виконання шкідливого коду, криптоджекінг, зловживання шкідливими контейнерами та використання ресурсів, вимагають вдумливого розгляду в контексті дерева атак.

Відносно специфіки моделювання загроз для Kubernetes, слід зауважити важливість забезпечення глибокого розуміння архітектури Kubernetes, механізмів аутентифікації та авторизації, мережевих політик та інших компонентів системи. На основі цієї інформації, можна ідентифікувати активи, пріоритезувати ризики та розробити стратегії для їх зменшення.

## Перелік використаних джерел


1. Bobbio A. A methodology for qualitative/quantitative analysis of weighted attack trees / A. Bobbio, L. Egidi, R. Terruggia. // IFAC Proceedings Volumes. – 2013. – №46. – С. 133.
2. Containers Matrix [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://attack.mitre.org/matrices/enterprise/containers/.
3. Threat Matrix for Kubernetes [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://microsoft.github.io/Threat-Matrix-for-Kubernetes/


# КОМПЛЕКС І СИНЕРГІЯ КІБЕРДІЙ У СУЧАСНИХ КОНФЛІКТАХ


Даник Ю.[1], Ланде Д.[1], Шестаков В.[2]

[1] Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського”, м. Київ, Україна

[2] Національна академія Служби безпеки України, м. Київ, Україна

**Анотація.** У доповіді розглянуто окремі види кібердій як складових кібер операції. Показано, що синергія кібердій відбувається у разі їх комплексного застосування за єдиним замислом, узгодженими за місцем та часом реалізації.
**Ключові слова:** кібердії, кібероборона, кібербезпека, ризики, технології конфліктів і війни.

**Вступ**

Конфлікти сучасності стають комплексним протиборством різних технологій, у тому числі, інформаційних. При цьому, значна роль досі належить використанню форм, способів і засобів збройної боротьби війн попередньої епохи [1]. Однак стійкою світовою тенденцією є перенесення протиборства в кіберпростір [2].

Сторони конфлікту здійснюють потужні кіберінформаційні дії. Так, протягом 2022 року за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було зареєстровано в 2,8 разів більше кіберінцидентів, ніж в 2021 році, геолокація джерел яких асоційована з росією збільшилась на 26% [3]. Відзначається, що з початку вторгнення рф в Україні активно розвивається громадянський кіберсупротив. За координації фахівців суб'єктів кібербезпеки і кібероборони силами волонтерів та активістів громадянського суспільства шляхом комплексного і системного ведення за єдиним замислом і планом різноманітних, але, в першу чергу, інформаційних, інформаційно-психологічних, когнітивних та кібердій. реалізуються атаки, які спрямовані на: порушення систем управління державою та її сектором безпеки і оборони; дискредитацію ключових акторів та маніпуляцію репутацією, викривлення сприйняття осіб і дій військово-політичного керівництва держави особовим складом збройних сил, населенням та світовою спільнотою.

Водночас, однією з проблем функціонування сил оборони України в умовах існуючих та потенційних загроз є неспроможність ефективно реагувати на зростаючу кількість загроз у кіберпросторі [4].

Тому стає наукове протиріччя – розвиток інформаційних технологій спричиняє ускладнення інформаційних і кіберзагроз, веде до синергії різноманітних інформаційних та кібердій, що потребує пошуку шляхів адекватного реагування на такі загрози та зниження ризиків їх реалізації.

Метою доповіді є представлення ймовірного комплексу кібердій та можливий результат їх синергії, який може бути реалізовано у військових конфліктах сучасності.

**Основний матеріал**

Суттєвим стримуючим чинником на шляху комплексного вивчення синергії кібердій при їх взаємному впливі і взаємодії за їх паралельно-послідовного ведення за єдиним замислом і планом так і за їх відсутності в першу чергу виступає дефініційна невизначеність та відсутність таксономічної моделі. Базові поняття наведено в [5]. Тому далі розкривається авторське бачення сутності та змісту окремих категорій, показуються їх спільні та відмінні риси.

Дослідження показали, що, як правило, кібердії є комплексними, узгоджені з інформаційним, інформаційно-психологічними та когнітивними впливами, проводяться за єдиним замислом і планом у формі кібероперації [5, 6].

У доповіді розкривається сутність та описується найбільш ймовірний сценарій проведення кібероперації.

Доводиться, що операція в кіберпросторі складається з чотирьох основних компонентів: кіберпротиборство, кібероперація в мережах, операція з кіберпідтримки, операція з кіберобізнаності.

Обґрунтовується, що у багатьох випадках ефективність кібероперацій на порядок вище ефективності операцій із застосуванням засобів вогневого ураження або значно підвищує ефективність інших операцій. Високий показник ефективності кібероперації пояснюється тим, що сучасні засоби кібервійни досягли такого рівня бойових можливостей, який гарантує їм внесення радикальних змін у сутність збройного протиборства.

Враховується, що у визначеній зоні (районі) воєнних дій здійснюється формування з наявних засобів локального інформаційно-кібернетичного простору.

Обґрунтовується, що синергетичний ефект матиме місце тільки тоді, коли інформаційні та кібернетичні дії здійснюються за єдиним задумом і планом та узгоджуються за завданнями в часі та просторі.

У доповіді приведено приклади, кількісні і якісні оцінки синергії, урахування яких сприяє виробленню ефективних заходів кібероборони.

**Висновки**

За результатами досліджень можна стверджувати, що синергетичні ефекти виникають внаслідок взаємодії інформаційних та кібердій Розкрито типовий сценарій проведення кібероперації. Доведено, що синергетичний ефект матиме місце у випадку, коли інформаційні та кібердії реалізуються за єдиним задумом і планом, узгоджуються за завданнями в часі та просторі.

Показано, що завдання завчасного виявлення, оцінювання та прогнозування синергетичних ефектів вирішується на основі розробленої та розкритої в доповіді методології. Обґрунтовано, що розроблена методологія виступає ефективним регулятором нелінійних процесів, які

виникають унаслідок взаємодії інформаційної та кібернетичної компонент.

## Перелік використаних джерел


1. Danyk Yuriy, Shestakov Valery. Ways of reducing civilian casualties during wars and armed conflicts of modern times. High-tech aspects. The actual problems of the world today. London, 2019. Vol. 2. pp. 15 – 30.
2. Стратегія кібербезпеки України. Затверджено Указом Президента України від 26.08.2021 № 447/2021.
3. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. 2022. URL: https://scpc.gov.ua/api/docs/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1.pdf
4. Стратегічний оборонний бюлетень України. Затверджено Указом Президента України від 17.09.2021 №473/2021.
5. Даник Ю., Грищук Р., Основи кібернетичної безпеки : Монографія, за заг. ред. Ю. Г. Даника, Житомир: ЖНАЕУ, 2016, 636 с.
6. Даник Ю. Г., Грищук Р. В. Синергія інформаційних та кібернетичних дій // Труди університету. Київ, 2014. – № 6 (127). – С. 132–143.


# МОДЕЛЮВАННЯ КІБЕРАТАК НА ЕНЕРГЕТИЧНІ СИСТЕМИ


Шрейдер М.О., Стьопочкіна І. В.
Фізико-технічний інститут,Київ, Україна Навчально-науковий Фізико-технічний інститут КПІ ім. Ігоря Сікорського, Київ, Україна



В роботі розглянуто модель системи автоматичного керування генерацією електроенергії в умовах існування кібернетичних впливів, які можуть призвести до наявності спотворення сигналів та їх затримки. Увагу зосереджено на

DDoS атаках, які спричиняють затримки в системі. Проаналізовано їхній вплив на роботу системи, запропоновано превентивні заходи, які дозволяють пом’якшити наслідки..

**Ключові слова:** Енергомережі, AGC, затримки часу, DDoS, моделювання.

## Вступ

Системи керування генерацією електроенергіїє сучасним елементом об’єктів критичної інфраструктури , від яких значною мірою залежить процес постачання електроенергії. Кібератаки на такі системи можуть загрожувати її нормальному функціонуванню. Серед типових кібератак можна вказати атаки типу “розподілена відмова в обслуговуванні”, які призводять до затримок, а також атаки типу replay – коли сигнали та дані перехоплюються зловмисником і транслюються у зручнийдля атаки час.

Важливою складовою в процесі попередження негативних наслідків є моделювання кібератак, яке дозволяє зрозуміти вразливості системи, виявити впливи, які призведуть до втрати системою своїх нормальних якостейта оцінити наслідки деяких атак.

На основі отриманих результатів можна розробляти заходи захисту системи. Серед них є впровадження технічних засобів та організаційних заходів захисту, зокрема - унеможливлення безпосереднього доступу до комунікаційних ліній системи ззовні, створення резервного обладнання для запобігання затримкам та перевантаженню, створення резервних копій даних для контролю цілісності.

## Система AGC

Одним з компонентів енергетичної системи є системи автоматичного керування генерацією електроенергії AGC (Automatic Generation Control).За допомогою моделі цієї системи і можна представити поведінку електромережі.

Її основна роль полягає у забезпеченні балансу між виробництвом та споживанням електричної потужності в реальному часі.

Принцип роботи AGC базується на неперервному моніторингу та регулюванні генерації електроенергії (Рис.1.)


Рисунок 1. Принцип роботи AGC

Модель AGC описується за допомогою динамічної системи (1-5) і дозволяє передбачити поведінку системи в певний момент часу. Вона виступає в якості середовища для здійснення атак.

Модель можна описати за допомогою наступних рівнянь:

$$x'(t) = Ax(t) + Bx(t) + F\Delta d(t), \quad (1)$$
$$y(t) = Cy(t), \quad (2)$$
$$ACE(t) = Dy(t), \quad (3)$$
$$p'(t) = ACE(t), \quad (4)$$
$$u(t) = -K(f(t) + p(t)), \quad (5)$$

де (1) - рівняння стану, (2) - рівняння спостереження, (3)- рівняння похибок, (4)- рівняння стану контролера, (5)- рівняння керуючого сигналу.

## Атаки на систему AGC та результати

Загалом система існує не ізольовано і може виходити в мережу для передачі вимірюваних даних в центр керування, де відбуваються розрахунки та аналіз отриманих даних, на вихід йде сигнал керування. В ціймережі на неї і може бути здійснена кібератака.

Однією з найбільш результативних кібератак може бути DDoS. Результатом цієї атаки на систему є перевантаження комунікаційної мережі, по якій передаються дані.

Це, в свою чергу, призводить до затримок передачі даних (Рис. 2). Такі затримки впливають на функціонування системи в режимі реального часу, адже без актуальних

даних система не може оперативно реагувати на зміни частоти та регулювати генерацію електроенергії.

Довжина таких затримок впливає на критичність ситуації,адже чим довші затримки, тим більш ймовірно, що це призведе до нестабільності енергосистеми.

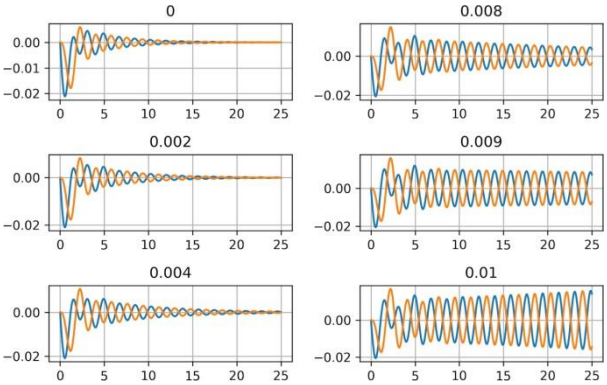


Рисунок 2.

З графіків можна побачити, що граничне допустиме значення затримки лежить в межах від 0.009 до 0.01.

## Висновки

Моделювання кібератак на систему AGC відіграє важливу роль в безпеці цієї системи, адже дозволяє визначити, чи може енергомережа бути дестабілізована, яким чином і як система буде себе поводити, коли якась її частина функціонує некоректно. На основі відповідної моделі може працювати система моніторингу, яка збиратимереальні дані і співставлятиме їх із результатами моделювання атаки, роблячи висновки про ступінь критичності поточної ситуації.

## Перелік використаних джерел

1. P. Kundur, Power System Stability and Control. McGraw-Hill Inc., 1994

2. C. Moya, On Cyber-Attacks against Modern Power

Grids, 2020
3. P. L. Goethals, N, M. Scala, D. T. Bennett, Mathematics inCyber Research, 2022
4. A. M. Mohan, N. Meskin, H. Mehrjerdi, A Comprehensive Review of the Cyber-Attacks and Cyber-Security on Load Frequency Control of Power Systems, 2020

# РОЗРОБКА РЕКОМЕНДАЦІЙ ПІДВИЩЕННЯ АНОНІМНОСТІ ВІДПОВІДІ ГОЛОСУЮЧИХ УСИСТЕМІ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

Тараканов Є.О., Даник Ю.Г.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», НН Фізико-технічний інститут, Київ, Україна

У роботі пропонується комплексний підхід до аналізу та оцінки захищенності голосуючих в системах електронного голосування з метою забезпечення їх надійності, анонімності та захищенності від куберзагроз. Через зростаючу актуальность кібербезпеки, яка грає важливу роль у захисті застосунків, ця робота включає дослідження існуючих методик, та розробку рекомендацій для підвищення рівня анонімності виборців у системі електронного голосування.

**Ключові слова:** анонімність, цифровий підпис, кібервразливість, електронне голосування, методика,аналіз, рекомендації.

## Вступ

У зв’язку зі зростанням передових технологій та цифровізацією, а особливо період карантину у всьому світі, люди все більше переходять в дистанційний форматроботи. У доповіді розглянуто тему електронного голосування, а саме захист анонімності голосуючих, зроблю дослідження

та висуну рекомендації стосовно покращення системи цифрового виборчого процесу.

Розробка мого застосунку буде спиратися на публікацію [1], в якій розглянуті вразливості та проблеми, а також їх вирішення у системі електронного голосування із використанням блокчейн технологій.

**Електронний цифровий підпис, та його використання**

Найголовнішим засобом захисту саме анонімності в електронному голосуванні в нас являється саме електронний цифровий підпис. Це так би мовити аналог звичайного підпису, але в цифровому форматі. Його використовують для автентифікації та перевірки цілісності інформації, повідомлення, документу.

Електронний підпис це унікальний набір даних, що генерується за допомогою криптографічного алгоритму і включає в себе публічний ключ власника підпису, що дозволяє перевірити автентичність документа за допомогою публічного ключа [2]. (Рис. 1)

**Реалізація застосунку системи електронного голосування**

Враховуючи те, що більшість систем електронного голосування є прозорими, тобто реалізовані таким чином, що самі користувачі зашифровані (це робиться за допомогою методу шифрування електронного цифрового підпису), але їх вибір можна побачити. Тому я вирішив розробити аналог системи голосування із використанням анонімності відповіді голосуючих.

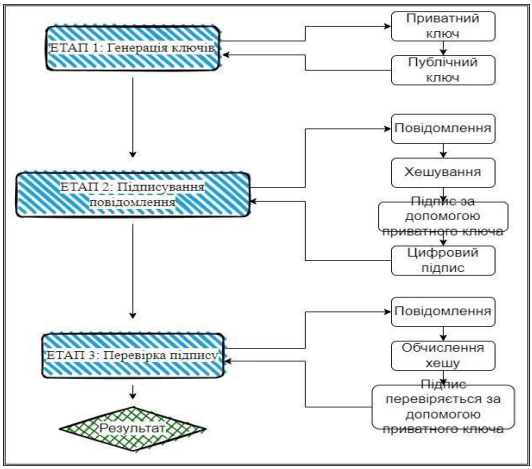


Рисунок 1. Алгоритм електронного цифрового підпису

Оскільки люди довіряють системі цифрового виборчого процесу, то чому б тоді повністю не закрити систему та наприкінці голосування отримати фінальний результат. Тим паче, що маючи повну статистику електронного голосування із відповідями, можна вплинути негативно на думку людей, що не проголосували, оскільки вони будуть вважати свій вибір марним.

У власному аналогу застосунку електронного голосування я використовую хешування SHA3-256, алгоритми шифрування RSA, ключі довжиною 4096 біт.

Ось як буде виглядати відповідь людини, яка обере варіант А (Рис. 2).

```
А проголосував за А.
Signature :  b'\x8ew3\xf1\x16\x864_\x8d\x07\xc3\xcf\x15\xb1,\xeb\x8a\xc6\xbb\
tg\'\xea\x85V\x8a\xad\xf1#:6\x9d:\\F\xbd\x98\xddx\x89<\xcb\xaf\xde\xaf\xba=\x
dc\'u\xeej\r\x1a\xffE\xd5\xbc8\xf8\x04!\xac\'\xee\xe3\xf2\xec\n`\xd8`l\xae\x0
3\xb4\xd2\xa5Wh\x05\x85FQ\xd0Y\x9d\xab,r\xa3\xe6t]\t?\x00\x8a\xbe\xd6K\xd3\x9
```

Рисунок 2 шифрування підпису виборця

Таблиця 1

| (біт) | Час генерування ключа (с) | Час підпису повідомлення(с) | Час перевірки підпису (с) |
|---|---|---|---|
| 2048 | 0,770496189594 | 0,05074018239 | 0,001000106 |
| 4096 | 10,311133027076 | 0,21675568819 | 0,003001213 |

На Рис. 2 зображена не вся довжина повідомлення, а тільки лише частина. Також перевірено обчислювальну здатність, а саме час генерації ключів та перевірки цифрового підпису. Хоча швидкість обробки запитів різниться, але потужності новітніх комп'ютерних ссистем вистачить для переходу довжини ключа із 2048 біт на 4096 біт. Це покращить складність обчислень та дасть більше стійкості

**Висновок**

Оскільки у доповіді розглянуто аналог застосунку електронного голосування, то його можна вдосконалювати, використовувати разом з електронним цифровим підписом, який ідентифікує людей та додавати до повноцінної системи виборчого процесу. Запевняю, щосаме анонімність відповіді голосуючих збільшить присутність людей на виборах та зменшить спекулятивний момент, адже у голосуванні дуже важливо, щоб прийняли участь як можна більше виборців.

# СТЕКІНГ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ У ЗАДАЧІ ВИЯВЛЕННЯ ШКІДЛИВИХ ПОСИЛАНЬ

Хукаленко Є. О.
Навчально-науковий Фізико-технічний інститут,
НТУУ «КПІ ім. Ігоря Сікорського», Київ, Україна

Робота присвячена темі виявлення шкідливих посилань у мережі інтернет. Розглянуто підходи до виявлення

шкідливих посилань та запропновано метод на основі стекінгу, що покращує точність наявних рішень.

**Ключові слова:** машинне навчання, стекінг, URL, кібербезпека.

**Вступ**

З підвищенням загрози шкідливих посилань у великих масштабах, виявлення та захист від цих загроз стає надзвичайно важливим завданням в галузі кібербезпеки. У даному дослідженні розглядаються методи та алгоритми для виявлення шкідливих посилань, а також застосування стекінгу моделей машинного навчання у задачі виявлення шкідливих посилань, досліджуючи переваги та ефективність такого підходу. Отримані результати мають потенційну користь для розробників програмного забезпечення та власників веб-сайтів, оскільки вони допоможуть підвищити безпеку користувачів мережі.

**Задача виявлення шкідливих посилань**

Сформулюємо задачу виявлення шкідливих URL-адрес як завдання двокласного передбачення: «зловмисний» і «безпечний». Зокрема, враховуючи набір даних із T URL-адресами $\{(u_1, y_1), \ldots, (u_T, y_T)\}$, де $t = 1, \ldots, T$ представляє URL-адресу з навчальних даних, а $y_t \in \{1, -1\}$ - відповідну мітку.

Суть автоматичного виявлення шкідливих URL-адрес полягає в двох аспектах:

1. Представлення ознак: отримання відповідного представлення: $u_t \rightarrow x_t$, де $x_t \in \mathbb{R}^d$ — d-вимірний вектор ознак;
2. Машинне навчання: вивчення функції класифікації $f$: $\mathbb{R}^d \rightarrow \mathbb{R}$, що прогнозує мітку класу для будь-якої URL-адреси x.

Ціль машинного навчання для задачі виявлення шкідливих посилань – максимізувати точність прогнозування.

**Розробка методу на основі стекінгу**

У даному дослідженні пропонується поєднати переваги існуючих алгоритмів та підходів до виділення ознак з URL-адрес шляхом використання методу стекінгу моделей. Стекінг передбачає навчання алгоритму, який комбінує прогнози кількох інших алгоритмів машинного навчання. Спочатку всі інші алгоритми навчаються за допомогою доступних даних, а потім алгоритм комбінатора навчається робити остаточний прогноз, використовуючи передбачення інших алгоритмів як додаткові вхідні дані. Стекінг зазвичай демонструє кращу продуктивність, ніж будь-яка окрема навчена модель [1].

Пропонується створити стекінг таким чином: окремо відбираємо лексичні ознаки URL, окремо мережеві (дані з dns/whois), для кожної групи ознак обираємо найкращі моделі, третьою моделью в стекінгу буде модель Transformer, яка є найкращим існуючим рішенням[2].

Моделі порівнюються за метриками AUC, Preecision і Recall, процедура валідації – крос-валідація з параметром k=5. Результати для лексичних характеристик наведені в таблиці нижче, як видно по результатам найкращою моделью для лексичних характеристик є модель kNN.

| Алгоритм | AUC | Precision | Recall |
|---|---|---|---|
| kNN | 0.813 | 0.820 | 0.811 |
| Naïve Bayes | 0.801 | 0.800 | 0.801 |
| Decision Tree | 0.761 | 0.753 | 0.766 |
| Random Forest | 0.810 | 0.805 | 0.815 |
| SVM | 0.705 | 0.696 | 0.715 |
| XGBoost | 0.805 | 0.789 | 0.813 |
| Logistic Regression | 0.764 | 0.723 | 0.786 |

Аналогічно порівняємо моделі для мережевих ознак. Як видно із результатів в таблиці – найкращою моделью для мережевих ознак є модель XGBoost.

| Алгоритм | AUC | Precision | Recall |
|---|---|---|---|
| kNN | 0.851 | 0.871 | 0.831 |
| Naïve Bayes | 0.826 | 0.813 | 0.847 |
| Decision Tree | 0.803 | 0.798 | 0.808 |
| Random Forest | 0.860 | 0.844 | 0.876 |
| SVM | 0.789 | 0.795 | 0.781 |
| XGBoost | 0.872 | 0.874 | 0.872 |
| Logistic Regression | 0.801 | 0.790 | 0.810 |

Наступним кроком є вибір моделі, що буде модел'ю стекінгу. Процедура вибору так ж як і раніше. У цьому стекнгу приймають участь три моделі: модель transormer навчана тільки на тексті URL-адрес, модель kNN для лексичних характеристик і модель XGBoost для мережевих харакетристик.

Результати стекінгу трьох моделей різними моделями верхнього рівня наведено в таблиці. Найкращою моделью стекінгу визначено логістичну регресію із приростом AUC у 3% відносно найкращої моделі першого рівня.

| Алгоритм | AUC | Precision | Recall |
|---|---|---|---|
| kNN | 0.901 | 0.905 | 0.891 |
| Naïve Bayes | 0.891 | 0.890 | 0.893 |
| Decision Tree | 0.910 | 0.905 | 0.915 |
| SVM | 0.897 | 0.889 | 0.906 |
| Logistic Regression | 0.927 | 0.930 | 0.926 |

**Висновки**

У цій роботі було проаналізовано різні підходи до виявлення шкідливих URL-адрес і запропоновано метод виявлення шкідливих посилань на основі стекінгу трьох моделей, що має вищу точність за існуючі рішення.

## Перелік використаних джерел

1. Wolpert D. Stacked generalization / David Wolpert // Neural Networks. – 1992
2. Pingfan X. A Transformer-based Model to Detect Phishing URLs / X. Pingfan. – 2021

# ЗМІСТ

Наукове видання

# ТЕОРЕТИЧНА ТА ПРИКЛАДНА КІБЕРБЕЗПЕКА

Перша Всеукраїнська
науково-практична конференція,
присвячена 100-річному ювілею
академіка В. М. Глушкова

Матеріали конференції

(Українською та англійською мовами)

*В авторській редакції*
*Надруковано з оригінал-макета замовника*

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Свідоцтво про державну реєстрацію: серія ДК № 5354 від 25.05.2017 р.
просп. Перемоги, 37,
м. Київ, 03056

Підп. до друку 09.05.2023. Формат 60 × 84 1/16. Папір офс. Гарнітура Times.
Спосіб друку – електрографічний. Ум. друк. арк. 15,58.
Обл.-вид. арк. 13,03. Наклад 100 пр. Поз. 23-3-3-004. Зам. № 23-061.

Видавництво «Політехніка» КПІ ім. Ігоря Сікорського
вул. Політехнічна, 14, корп. 15
м. Київ, 03056
тел. (044) 204-81-78