**НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ**
**ІНСТИТУТ ПРОБЛЕМ РЕЄСТРАЦІЇ ІНФОРМАЦІЇ НАН УКРАЇНИ**

# ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА БЕЗПЕКА

## МАТЕРІАЛИ XXIII МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

**ВИПУСК 23**

Київ – 2023

**ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ**
**ТА БЕЗПЕКА**

https://its.ipri.kiev.ua

ISBN 978-966-2344-96-7

**НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ**
ІНСТИТУТ ПРОБЛЕМ РЕЄСТРАЦІЇ ІНФОРМАЦІЇ НАН УКРАЇНИ

# ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА БЕЗПЕКА

## МАТЕРІАЛИ XXIII МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

**ВИПУСК 23**

Київ – 2023

*Рекомендовано до друку Вченою радою*
*Інституту проблем реєстрації інформації НАН України*
*(протокол № 11 від 26 грудня 2023 р.)*

**Інформаційні технології та безпека. Матеріали XXIII Міжнародної науково-практичної конференції ІТБ-2023.** – Київ: Інжиніринг. – 202 с. ISBN: 978-966-2344-96-7

До збірника увійшли матеріали доповідей, представлених на XXIII Міжнародній науково-практичній конференції «Інформаційні технології та безпека» (ІТБ-2023, 30 листопада 2023 року, м. Київ, Україна).

У збірнику представлені матеріали, присвячені питанням створення і впровадження інформаційних технологій, актуальним проблемам забезпечення інформаційної та кібербезпеки, протидії інформаційним операціям і кібертероризму, інтелектуальним технологіям підтримки прийняття рішень, проведенню аналітичних досліджень на основі сучасних методів інтелектуального аналізу даних.

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



ISBN 978-966-2344-96-7

# РЕЗИЛЬЄНТНІСТЬ КРИТИЧНИХ ІНФРАСТРУКТУР ТА КІБЕРБЕЗПЕКА ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ

О.Г. Додонов, О.С. Горбачик, М.Г. Кузнєцова
Інститут проблем реєстрації інформації Національної академії наук України, Київ, Україна
dodonovua@gmail.com, bges@ukr.net, marglekuz@gmail.com

Визначено поняття резильєнтності і безпеки критичних інфраструктур, показано їх залежність від функціональної стійкості і кібербезпеки інформаційної інфраструктури. Обговорюються шляхи забезпечення резильєнтності критичних інфраструктур, досвід використання міжнародних підходів і стандартів, засоби забезпечення кібербезпеки.

**Ключові слова:** резильєнтність критичної інфраструктури, інформаційно-керуюча система, функціональна стійкість, живучість, кібербезпека

## Вступ

*Резильєнтність* (англ. resilience) критичної інфраструктури - це властивість, яка характеризує її здатність адаптуватися до агресивних умов функціонування, відновлюватися після збоїв з мінімізацією негативних впливів на життєво важливі суспільні функції, економічну діяльність, громадське здоров'я та безпеку або навколишнє середовище. Під *безпекою критичної інфраструктури* розуміють незалежність від неприйнятного ризику, тобто забезпечення такого стану інфраструктури, коли ризик нанесення шкоди людині, суспільству, країні скорочується до прийнятного рівня.

Інформаційно-керуючі системи (ІКС) є у складі будь-якої критичної інфраструктури. Засобами цих систем виконується збір, обробка, зберігання та передача інформації для забезпечення стійкого функціонування та розвитку критичних інфраструктур. І саме вони сприяють швидкому виявленню інцидентів в критичних інфраструктурах, інформуванню про них і адекватному управлінню при відновленні. Нажаль, ІКС можуть самі стати об'єктами негативних впливів, кібератак, обсяг і витонченість яких останнім часом стрімко зростає.

## Основна частина

Вимоги до резильєнтності критичних інфраструктур потребують перманентного проведення заходів з аналізу ризиків, включаючи й малоймовірні, напрацювання заходів з протидії загрозам, планування відновлення. У більшості країн світу управління ризиками критичних інфраструктур базується на національних програмах. Так, у Великій Британії існує Структура управління ризиками (RMF) на основі Національного плану захисту критичних інфраструктур (NIPP), яка надає загальні рекомендації щодо цілей безпеки, стратегій і секторів охоплення. Інструменти, методи управління ризиками, методології захисту визначаються відповідно до цілі, яку вони виконують на кожному з етапів загального управління ризиками.

Забезпечення кібербезпеки є однією з найважливіших вимог, оскільки втручання у роботу інформаційних систем, виток інформації щодо об'єктів критичної інфраструктури та її несанкціоноване використання може призвести до інцидентів з катастрофічними наслідками. Ефективна програма кібербезпеки має охоплювати людей, процеси, технологічні рішення, які разом знижують ризик порушення функціонування критичної інфраструктури. Необхідними умовами та чинниками безпеки критичної інфраструктури стають функціональна стійкість та живучість їх інформаційної інфраструктури й ІКС, які здатні забезпечити своєчасне реагування на загрози, інформування про інциденти, формування відповідних керуючих впливів.

У США як частина національного дивізіону кібербезпеки (NCSD) функціонує програма захисту систем управління і є спеціальна команда реагування на кіберзагрози у промислових системах (ICS-CERT - Industrial Control Systems Cyber Emergency Response Team).

Європейською комісією розроблено глобальну стратегію захисту критичної інфраструктури («The European Programme for Critical Infrastructure Protection») і запропоновано створення єдиної структурованої платформи реагування на інциденти (Cybersecurity Crisis Response Framework). Платформа включатиме національні і транскордонні центри операцій, які мають виявляти кіберзагрози і реагувати на них, використовуючи сучасні технології.

Сьогодні вже напрацьовані певні методологічні підходи до аналізу ризиків кібербезпеки для технологічних процесів і

промислових підприємств у різних галузях [1]. Для газової та нафтопереробної галузей застосовують підхід Cyber Process Hazard Analysis (Cyber PHA), який базується на класичному підході до виявлення, оцінювання і управління ризиками технологічного процесу та включає аспекти, пов'язані з ризиками кібербезпеки [1]. Наприклад, компанією Shell для оцінювання факторів, що призводять до порушення цілісності функцій безпеки через загрози кібербезпеці (які є або можуть бути у програмно-апаратних комплексах автоматизації), було спільно використано методики оцінювання HSSE-ризиків (Health, Safety, Security and Environment), традиційні методики оцінки у рамках PHA, і методики оцінювання ризиків кібербезпеки (Security Risk Assessment) [1]. Напрацьовані міжнародні стандарти для аналізу ризиків кібербезпеки: ISO/IEC 27001 [2] – аналіз загроз; ISA TR84.00.09 [3] – аналіз загроз і оцінювання ризиків кібербезпеки, опис вимог із забезпечення кібербезпеки на всіх етапах життєвого циклу системи; ISA/IEC 62443[4] – побудова захищеної архітектури АСУ ТП на рівні автоматизації і технологічного управління. В ISA/IEC 62443 запропоновано комплексний підхід, який передбачає створення системи управління кібербезпекою CSMS (Cyber Security Management System) промислового об'єкту, а основними складовими є аналіз ризиків, усунення ризиків за допомогою CSM, контроль і удосконалення CSMS.

Критичні інфраструктури України мають досить складну структуру взаємозв'язків і взаємовпливів. Україна має досвід відбиття кібератак на ІКС критичних інфраструктур, та він потребує систематизації. Для критичних інфраструктур головним чином застосовується міжнародний стандарт менеджменту інформаційної безпеки ISO/IEC 27001 і тільки напрацьовуються національні рекомендації. Урядом України затверджено Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури, який передбачає, зокрема, моніторинг критичної інфраструктури; оцінку ризиків і загроз; визначення порядку взаємодії суб'єктів захисту критичної інфраструктури у кризових ситуаціях; забезпечення функціонування системи обміну інформацією; посилення стійкості критичної інфраструктури. Суттєву роль у підтримці функціонування критичної інфраструктури мають виконати функціонально стійкі інформаційні системи, в які впроваджено механізми динамічної реконфігурації, реорганізації, адаптації та відновлення для функціонування у кризових умовах. Мають застосовуватися

визнані практики кібербезпеки: мережева безпека, хмарна безпека, безпека застосунків, операційна безпека, відновлення безперервності бізнес-процесів, програми інформування про загрози , тощо, для мінімізації ризиків та негативних наслідків кібератак.

## Висновки

Забезпечення резильєнтності критичних інфраструктур потребує створення моделей прогнозування ризиків різної природи, визначення способів оцінювання втрат від їх реалізації, впровадження механізмів своєчасного й адаптивного реагування на інциденти. В критичних інфраструктурах та їх ІКС інциденти найчастіше трапляються несподівано, мають невідомий характер, тож передбачити, проконтролювати і запобігти їм у повні мірі майже неможливо, але забезпечення функціональної стійкості ІКС та використання практик забезпечення кібербезпеки дозволить суттєво ускладнити можливість порушення функціонування критичних інфраструктур, унеможливить витік, спотворення та несанкціоноване використання інформації щодо об'єктів критичної інфраструктури, а це приведе до зменшення кількості інцидентів з катастрофічними наслідками, запобігатиме розвитку каскадних аварій.

## Перелік посилань

1. URL:https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Oil_and_Gas/Pipeline/SecurityReference/SecurityIRD.pdf (accessed: 31.10.2023).
2. Cyber-related process hazard analysis. URL: https://www.isa.org/templates/news-detail.aspx?id=160155 (accessed: 31.10.2023).
3. Cyber Process Hazards Analysis (PHA) to Assess ICS Cybersecurity Risk. URL: https://youtu.be/8oZGYcRDjzc (accessed: 31.10.2023).
4. Quick Start Guide: An Overview of the ISA/IEC 62443 Standards. URL: https://gca.isa.org/blog/download-the-new-guide-to-the-isa/iec-62443-cybersecurity-standards (accessed: 31.10.2023).

# ДОСЛІДЖЕННЯ МЕРЕЖ СУБ'ЄКТІВ КІБЕРБЕЗПЕКИ ЗАСОБАМИ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ

Дмитро Ланде[1,2], Анатолій Фегер[1], Леонард Страшной[3]
[1] Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна
[2] Інститут проблем реєстрації інформації НАН України, Київ, Україна
[3] University of California, Los Angeles, USA
dwlande@gmail.com, feher.anatolii@gmail.com, lstrashnoy@gmail.com

В роботі запропонована методика екстрагування понять – назв хакерських угрупувань і їх контекстуальних зв'язківіз текстів повідомлень мережевих джерел, що стосуються предметної області кібербезпеки, засобами генеративного штучного інтелекту, формування мереж їх взаємозв'язків і змістовного аналізу цих мереж. Досліджуються мережі хакерських угрупувань, що активізувались напередодні і спочатку повномасштабних воєнних дій в Україні і в Ізраїлі. Підкреслюється наявність спільних хакерських угрупувань. Для створення реалізації запропонованих підходів використовуються засоби OSINTі системи генеративного штучного інтелекту ChatGPT, а також засоби програмного забезпечення для моделювання, аналізу та візуалізації графів – Gephi.

**Ключові слова:**OSINT, система генеративного штучного інтелекту,ChatGPT,екстрагування понять, мережа понять, кібербезпека.

## Постановка проблеми

У сфері кібербезпеки важливими об'єктами дослідження є хакерські угрупування, деструктивне програмне забезпечення, аналітичні групитощо. Утаких групах об'єктів, як злочинні хакерські угрупування, можуть активізуватись відомі або виникати нові центри та об'єкти, що потребують особливої уваги фахівців із кібербезпеки. Таким чином,актуальним є завдання постійного моніторингу інформації у межах визначеної предметної області.

Необхідна для цього завдання інформація широко представлена у соціальних мережах, форумах, в мережі Інтернет, до контенту якої, зокрема, документів, розміщених на веб-сайтах, може бути застосована технологія розвідки у відкритих джерелах (Open Source INTelligence, OSINT) [1]. Можливість масового моніторингу відкритих джерел інформації з метою пошуку цільового контенту, людей і подій приводить до необхідності застосування технологій Big Data, які успішно розвиваються на цей час [2]. Крім того, досягається різке скорочення часу доступу. Для здійснення дієвої аналітики результатів добування інформації пропонується застосування засобів генеративного штучного інтелекту (ГШІ) [3], зокрема, системи ChatGPT, яка дозволяє отримувати результати змістовних запитів (промптів) через API.

Метацієї роботи – створення і апробування методики визначення злочинних хакерських угрупувань, що діють напередодніі спочатку широкомасштабних широких воєнних дій, та зв‘язків між ними на базі аналізу ресурсів веб-простору, а також формування на основі системи ГШІта аналітична обробка мереж виявлених об’єктів кібербезпеки. Для досягнення цієї мети вирішується низка завдань, зокрема, добування і первинної обробки інформації, витягу із неї необхідних сутностей шляхом застосування ГШІ, встановлення зв’язків між ними, формування і аналіз мереж.

## Опис методики

Особливістю наведеної методики є поєднання OSINTі систем ГШІ. Основні етапи (ланцюжки) методики включають:

1) добування інформації шляхом звернення до системи контент-моніторингу (складової OSINT)із експертними запитами;

2) екстрагування понять і зв’язків між нимишляхом звернення до системи ГШІ із змістовними промптами;

3) фільтрація отриманих понять із залученням експертів;

4) формування мережі хакерських угрупувань;

5) аналіз і візуалізація цієї мережі.

## Приклад

Для отримання інформаційного масиву публікацій щодо кібербезпеки було визначено необхідний період(місяць до і місяць після початку широкомасштабних воєннихдій) та опрацьовано тематичні запити до системиOSINT:

***1. Війна в Україні***

**1.1. (кібератак~/3/украї) | (хакер~/3/атак~/2/украї) | (кибератак~/3/украин) | (хакер~/3/атак~/2/украин)**

**1.2. (hack~/3/ukrain) | (cyber~attack~/3/ukrain) | (cyberattack~/3/ukrain)**

***2. Війна в Ізраїлі***

**2.1. (кібератак~/3/ізра) | (хакер~/3/атак~/2/ізра) | (кибератак~/3/израил) | (хакер~/3/атак~/2/израил)**

**2.2. (hack~/3/israel) | (cyber~attack~/3/israel) | (cyberattack~/3/israel)**

Для кожного з отриманих документів було застосовано такий промпт до системи ChatGPT, результати якого надходять до програм через API та агрегуються для подальшого формування мереж:

| Промпт: Приведи список назв хакерських груп з тексту без пояснень у вигляді переліку. Текст: … |
|---|

На останньому етапі здійснюєтьсяаналізвідібраної мережі тавізуалізація сформованих мереж із застосуванням системи Gephi [4] (Рис. 1, 2).

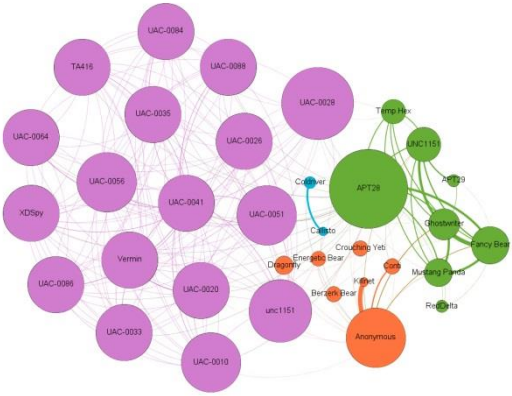



Рисунок1 – Фрагмент мережі злочинних хакерських угрупувань, пов’язаних із російсько-українською війною

Для подальшої кластеризації і візуалізації в рамках системи Gephi обчислюється модульність окремих вузлів – іменних сутностей, на основі якої здійснюється виявлення груп в мережах (кластерів).

## Висновки

Запропоновано методику виявлення злочинних хакерських угрупуваньіз документів системи OSINT із застосування системи генеративного штучного інтелекту, яка враховує приховані знання, внесені експертним мережевим середовищем.Результати контент-моніторингу інтернет-ресурсів та проведеного кластерного аналізу вказують наодночаснуактивність у двох війнах хакерських угрупувань, що відносяться до спецслужб рф, а саме: Killneti APT29 (CozyBear).

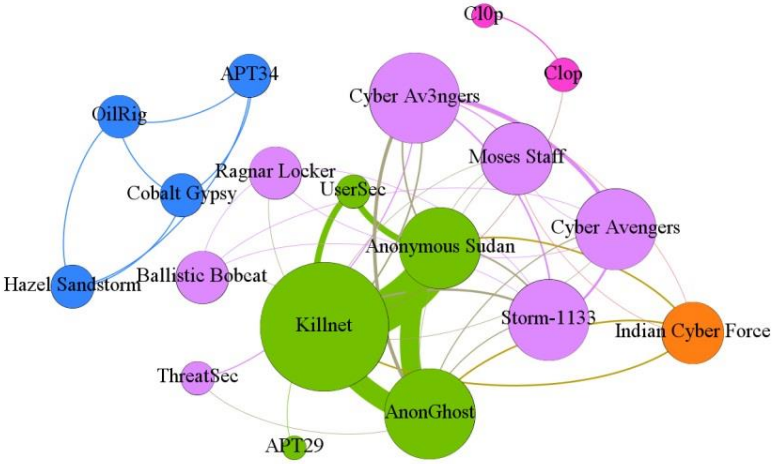



Рисунок 2 – Фрагмент мережі злочинних хакерських угрупувань, пов’язаних із війною в Ізраїлі

## Перелік посилань

1. D. Lande, O. Puchkov, I. Subach, M. Boliukh, D. NahornyiOSINT

investigationtodetectandpreventcyberattacksandcybersecurityincidents // InformationTechnologyandSecurity, 2021. Vol 9 (2). –pp. 209-218.DOI: doi.org/10.20535/2411-1031.2021.9.2.249921.

2. Dmytro Lande,Ellina Shnurko-Tabakova. OSINT as a part of cyber defense system. Theoretical and Applied Cybersecurity, 2019. – Iss. 1. –pp. 103-108.

3. Dmytro Lande, Leonard Strashnoy.GPT Semantic Networking: A Dream of the Semantic Web - The Time is Now. - Kyiv: Engineering, 2023. - 168 p. ISBN 978-966-2344-94-3

4. Cherven K. Mastering Gephi Network Visualization. – PacktPublishing, 2015. – 378 p. ISBN 78-1-78398-734-4.

## МЕТОДИ ТА МОДЕЛІ ПОБУДОВИ АДАПТИВНИХ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ

Додонов О.Г., Никифоров О.В., Путятін В.Г.
Інститут проблем реєстрації інформації НАН України, Київ, Україна

Предметна область досліджень щодо створення адаптивних автоматизованих систем управління (АСУ), територіально розподілених інформаційних комп'ютерних систем полягає у розробці адаптивних моделей та методів з:

- програмування функціонування: опис структури та поведінки системи, прогнозування значень її параметрів;
- цільового управління: формування підмножини контрольованих параметрів, зон їх контролю залежно від вимог до стійкості функціонування системи;
- поточного управління: контроль поточного стану та діагностування порушень працездатності.

В основному, для вирішення наукових задач в цієї галузі, використовується онтологічний підхід при застосуванні науково-методичного апарату алгебри систем [1], концептуального або конструктивного проєктування [2] та ступенів множин [3].

Відомо кілька прикладів успішного розв'язання задач побудови адаптаційних механізмів систем.

Так в [4] створено автоматичну адаптацію алгоритмів обробки інформації до змін умов, задач і цілей системи шляхом трансформації зв'язаних онтологій (онтології алгоритмів залежно від онтології предметної області). Створення практичних

алгоритмів для трансформації онтології задач здійснюється у середовищі CLEPE (Conceptual level programming environment) з урахуванням положень концептуального моделювання [2].

При цьому, предметна область (онтологія), на якої проєктується адаптивна АСУ, подається як множина підмножин-носіїв *n* багатосортних алгебр

$$E = \{E_1, ..., E_i, ..., E_n\},$$

де

$$E_i = \left(Name, \Sigma, Ex\right),$$

де *Name* – назва типу (наприклад, коло); $\Sigma$ – сигнатура багатосортної алгебри (параметри кола: координати центра і точок кола, радіус кола); *Ex* – визначальні співвідношення типу (рівняння кола).

На множині *E* визначені домені понять і відношень.

Трансформація системи алгоритмів, залежно від умов та обмежень предметної області, здійснюється за допомогою функції ініціалізації параметрів, яка подається як набір відображень між атрибутом дії і значеннями атрибутів сутностей і відношень зі складу онтологічної моделі задач АСУ.

Подальший розвиток апарату полягає у розширенні взаємодії моделей, реалізації механізмів логічного виводу, реалізації багатоваріантних обчислень та контекстної залежності [2].

В [5, 6] розв'язано задачу розгортання онтології предметної області на основі використання концептуальної схеми родів структури наступних абстрактних відношень:

- суб'єктів системи управління;
- ієрархічних суб'єктів, що трансформуються;
- кооперативних (полі-) суб'єктів;
- розповсюдження проблемної ситуації управління, що симптоматично визначається.

Даний підхід дозволяє реалізувати дедуктивний метод проєктування систем управління, коли відбувається рух від абстрактного до конкретного, від загального до часткового. Проблемним питанням, яке вирішено не повною мірою, виявляється питання інтерпретації елементів ступенів множин для вищих ступенів. Саме вони, вищі ступені, мають практичне значення. Їх колосальна розмірність не дозволяє здійснювати їх інтерпретацію без розробки спеціальних засобів інтерпретації [5].

Проблема розмірності тут може бути розв’язаною за рахунок попередньої розробки метамоделей (моделей-прототипів, конструктивних моделей) інформаційних систем різноманітних корпоративних АСУ з подальшим їх трансформуванням під визначені умови [6]. Слід помітити, що [4] також передбачає здійснювати адаптацію шляхом трансформації онтології вихідної системи.

В якості апарату перетворення вихідної структури системи до іншої системи зі зміненою структурою можуть бути використані методи та моделі тензорного перетворення мереж [7, 8]. Для цього вихідна структура інтерпретується у вигляді електричної мережі. Електрична мережа зручна для формалізованого опису структурних зв'язків різного роду. На відміну від інших типів неелектричних мереж, електрична мережа завжди оточена динамічним електромагнітним полем, що створюється нею самою і простирається до нескінченності у всіх напрямках. Використовуючи модель індукції та самоіндукції у гілках електричної мережі, зручно описувати різноманітні внутрішні системні зв'язки між елементами аналізованої структури (організаційної топології).

На цій основі Г. Кроном була запропонована методологія теоретико-множинного та алгебраїчного синтезу топологій у формі методу аналізу та тензорного перетворення електричних мереж [7].

Тобто, якщо коректне уявити структуру системи у вигляді багатокотушкової електричної мережі, тоді можна використовувати тензор перетворення Крона як механізм синтезу нової структури із заданими властивостями.

Таким чином, напрямок досліджень адаптаційних АСУ представлений методами концептуального проєктування, що будуються на основі алгебри систем та методичного апарату ступенів множин. На підставі цих методів можна розв’язувати задачі синтезу структур об’єктів (систем) із визначеними властивостями.

Велика розмірність елементів ступенів множин робить проблематичним інтерпретування результатів перетворень. Для побудови систем адаптивного управління зі складністю, що відповідає реальним процесам, треба вирішити проблему створення спеціальних засобів інтерпретації (представлення) результатів концептуального проєктування.

Розв’язання цієї проблеми може бути здійснено за рахунок використання заздалегідь створених конструктивних моделей структур систем з подальшим їх перетворенням для синтезу нових структур. В якості процедур перетворення можна використовувати тензорне перетворення мереж як механізм синтезу нових структур із визначеними властивостями.

## Джерела


1. Koo B. Algebra of systems: a metalanguage for model synthesis and evaluation / B. Koo, W. Simmons // IEEE Transactions on systems, man and cybernetics. – 2009. – Vol. 39, N 3. – P.501–513
2. Буров Є. В. Концептуальне моделювання інтелектуальних програмних систем: монографія / Є. В. Буров. – Львів: Вид-во Львівської політехніки, 2012. – С. 432
3. Bourbaki Nicolas. Eléments de Mathématique. XX. Première partie. Les structures fondamentales de l'Analyse. Livre I Théorie des Ensembles. Hermann et Cie, Paris, 1956. Première édition. 118 p.
4. Буров Є.В., Пасічник В.В. Програмні системи на базі онтологічних моделей задач // Вісник Національного університету "Львівська політехніка". Серія: Інформаційні системи та мережі : збірник наукових праць. – 2015. – № 829. – С. 36–57. – Бібліографія: 21 назва
5. Лелюк В.А. Концептуальное проектирование систем с базами данных. Монография. – Харьков: Основа, 1990. – 144 с.
6. Лелюк В.А. Введение в теории систем: Учеб. пособие. В 2-х т. – Харьков: ХНАГХ, 2008. – 396 с.
7. Kron G. Tensor analysis of networks. John Wiley and sons, inc. London: Capman and Hall, Limited. New York. – 1966. – 720 p.
8. Додонов О.Г. Реалізація прийняття рішень організаційного управління на основі онтології діяльності / Додонов О.Г., Никифоров О.В., Путятін В.Г. // Математичні машини і системи. 2022. № 1 – С. 31 – 51

# ПІДХІД ДО ВИЗНАЧЕННЯ РІВНЯ УЗГОДЖЕНОСТІ ЕКСПЕРТНИХ ОЦІНОК, ДОСТАТНЬОГО ДЛЯ ЇХ АГРЕГАЦІЇ

Віталій Циганок[1], Андрій Оленко[2], Павло Роїк[1], Оксана Власенко[1]
[1]Інститут проблем реєстрації інформації НАН України, Київ, Україна
[2]Університет Ла-Троб, Мельбурн, Австралія
vitaliy.tsyganok@gmail.com, A.Olenko@latrobe.edu.au, paulroyik@gmail.com, vo12062007@gmail.com

Для отримання достовірних результатів експертиз, в яких, зазвичай, застосовуються індивідуальні та групові попарні порівняння, важливо виконувати підсумкове узагальнення (агрегування) експертних оцінок при умові їх достатньої узгодженості. Існують декілька способів визначення порогового рівня узгодженості, достатнього для агрегації оцінок, але жоден з них не пов'язує це значення з вимогами до достовірності результатів експертизи, що проводиться. Отже, пропонується новий підхід до визначення цього порогу узгодженості, який базується на імітаційному моделюванні експертних попарних порівнянь та цілеспрямованому пошуку серед змодельованих матриць попарних порівнянь найбільш неузгоджених, що дозволяє визначити поріг узгодженості для заданого допустимого відхилення результуючої відносної ваги альтернативи від гіпотетичного еталонного значення.
**Ключові слова:** Достовірність експертизи, узгодженість експертних оцінок, достатній для агрегації рівень узгодженості, моделювання оцінок, еволюційні методи.

## Вступ

При підтримці прийняття рішень (ППР) задля забезпечення належного рівня їхньої якості важливим аспектом є адекватність моделей слабко структурованих предметних областей, на основі яких генеруються рішення. Для забезпечення достатнього рівня адекватності таких моделей, при їх побудові, неможливо нехтувати експертними знаннями, частка яких для будь-якої галузі дуже значна. У ході експертної ППР адекватність моделей забезпечується завдяки належній достовірності експертних

оцінок, що отримуються у ході експертиз. Необхідний рівень достовірності досягається шляхом узагальнення експертної інформації, яка, у загальному випадку, є надлишковою. Надлишковість інформації притаманна як груповим експертизам, де оцінка більше ніж одного експерта характеризує оцінюваний об'єкт, так і індивідуальним експертним оцінюванням, коли єдиний експерт виконує попарні порівняння об'єктів (альтернатив) і відносна вага кожного об'єкта визначається більше ніж одним попарним порівнянням.

Завдяки подальшій агрегації надлишкової експертної інформації узагальнюються і отримуються нові знання, що лягають в основу моделі певної предметної області (складної слабко структурованої системи). Проблемна ситуація полягає в тому, що узагальнювати (агрегувати, усереднювати) інформацію доцільно лише якщо множина оцінок є у достатній мірі узгодженою. Інакше, при наявності значної кількості протиріч, може виникати ситуація на кшталт «середньої температури пацієнтів у лікарні», коли ця усереднена величина є неінформативною і не відображає реальний стан справ.

Отже, у ході експертної ППР, повсякчас постає завдання забезпечення достатнього рівня узгодженості експертних оцінок перед їх агрегацією, що безпосередньо впливає на достовірність експертиз і опосередковано – на якість рекомендацій, що генеруються системами підтримки прийняття рішень (СППР) та надаються особам, що приймають рішення (ОПР). Тому, дуже важливим аспектом проведення експертиз є визначення ступеня узгодженості суджень експертів, а також, визначення рівня узгодженості, достатнього для агрегації експертних оцінок.

Із поданого вище можна зробити висновок, що для отримання достовірних результатів експертиз, надважливо враховувати узгодженість оцінок, при чому визначення узгодженості само по собі не має особливого сенсу без визначення порогового значення, яке слугує індикатором для виконання подальшої агрегації. У випадку низької узгодженості оцінок, її поліпшення доцільне лише до необхідного рівня, а не до повного узгодження, яке, на практиці, призведе до неминучої втрати ефективності проведеної експертизи.

## Проблемна ситуація

Практично кожний з відомих методів визначення узгодженості [1, 2] передбачає використання певного способу

визначення порогового значення. Більшість із них, окрім оригінальних підходів, на кшталт [3], ґрунтуються на імітаційному моделюванні експертних оцінок, наприклад, визначення узгодженості в методі аналізу ієрархій Томаса Сааті [4]. Наявні імітаційні підходи здебільшого пов’язують значення індексу узгодженості з розмірністю матриці попарних порівнянь, але жоден з них не пов'язує це значення з вимогами, що ставляться до достовірності результатів експертизи, хоча інтуїтивно зрозуміло, що узгодженість оцінок безпосередньо впливає на достовірність («точність») результатів експертизи.

## Сутність підходу

В основі підходу лежить постулат про існування «фундаментальної істини» (ground truth), який уможливлює проведення будь-якої експертизи. Це дає підстави припустити наявність еталонних (точних) ваг альтернатив, які мають бути визначені у ході експертизи. Отже, пропонується задати довільні ваги альтернатив (припускаємо, що вони апріорі відомі).

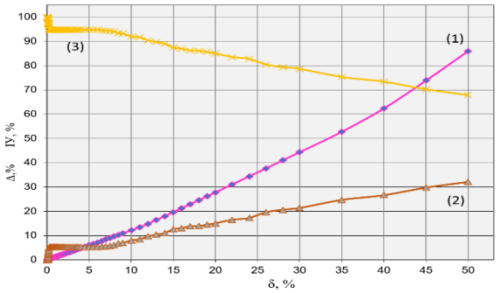
Імітаційне моделювання попарних порівнянь здійснюється наступним чином:

- За заданими вагами $w_i, i \in \{1..n\}$, де $n \in \mathbb{N}$ – кількість альтернатив, будується повністю (ідеально) узгоджена матриця попарних порівнянь $M = \{m_{ij}\},\ i,j \in \{1..n\}$, де $m_{ij} = \frac{w_i}{w_j}$, причому, $M$ є мультиплікативною, зворотно-симетричною: $m_{ij} = {}^{1}/_{m_{ji}}$.
- Матриця $M$ зашумлюється шляхом надання кожному елементу матриці деякого збурення $\delta$, наприклад, $m_{ij} = m_{ij} \pm m_{ij} \cdot \delta$. По суті, $\delta$ виступає у якості відносної похибки оцінювання, притаманної експерту при виконанні попарних порівнянь.

Зімітовані таким чином матриці попарних порівнянь агрегуються різними методами [5], також є можливість визначити узгодженість таких матриць.

Підхід до визначення порогу узгодженості, так саме, як і до оцінювання методів агрегації експертних оцінок [5], використовує цілеспрямований пошук (як приклад, Генетичний алгоритм [6]), з допомогою якого, серед змодельованих матриць попарних порівнянь знаходять такі, що спричиняють при агрегації найбільше відхилення ваг альтернатив від еталонних

значень Δ або представляють найбільш неузгоджений випадок попарних порівнянь (найменший індекс узгодженості $I$).




Результати обчислень за допомогою генетичного алгоритму подані у графічному вигляді на рисунку. Графік (1) – залежність $\Delta(\delta)$, розрахована для комбінаторного методу агрегації [5], (2) – залежність неузгодженості від $\delta$ і (3) – залежність індексу узгодженості від відносної похибки оцінювання: $I(\delta)$. По суті, відображені на рисунку значення індексу узгодженості залежності (3) $I(\delta)$ відповідають порогу узгодженості для відповідних значень заданої якості агрегації $\Delta(\delta)$ Комбінаторним методом при проведенні експертизи. Звідси нескладно визначити залежність $I(\Delta)$ – поріг узгодженості для заданого $\Delta$ – допустимого відхилення результуючої відносної ваги альтернативи від гіпотетичного еталонного значення.

Не важко помітити значну кореляцію між залежностями $\Delta(\delta)$ та $(1 - I(\delta))$, тобто, зі збільшенням відносної похибки оцінювання збільшується і неузгодженість експертних оцінок, що також добре узгоджується зі здоровим глуздом. У додаток, варто відмітити, що застосовуючи даний підхід доречно визначити залежності індексів узгодженості (неузгодженості) від вимог щодо достовірності отримуваних результатів експертизи для усіх методів агрегації попарних порівнянь.

## Висновки

Запропонований новий підхід до визначення порогу узгодженості експертних попарних порівнянь, достатнього для виконання агрегації цих оцінок та отримання відносних ваг альтернатив із заданою достовірністю. Визначення порогу узгодженості саме відповідного заданому допустимому відхиленню результуючої відносної ваги альтернативи від гіпотетичного еталонного значення дозволяє підвищити

ефективність процесу поліпшення узгодженості та заощадити високовартісні експертні ресурси.

## Перелік посилань


1. Brunelli Matteo, A survey of inconsistency indices for pairwise comparisons, *International Journal of General Systems*, 2018, 47:8, 751-771, DOI: 10.1080/03081079.2018.1523156
2. Olenko Andriy and Tsyganok Vitaliy, Double Entropy Inter-Rater Agreement Indices. *Applied Psychological Measurement.* 2016. Vol. 40(1). P. 37–55. DOI: 10.1177/0146621615592718
3. Totsenko V.G. Spectral Method for Determination of Consistency of Expert Estimate Sets. *Engineering Simulation*. – 2000. – 17. – P.715-727.
4. Saaty T. L. and Kearns K. P. Analytical Planning the Organization of Systems, *Pergamon Press*, 1985.
5. Tsyganok V.V. Investigation of the aggregation effectiveness of expert estimates obtained by the pairwise comparison method. *Mathematical and Computer Modelling*. – August 2010. – v.52, №3-4. – P.538-544. DOI: 10.1016/j.mcm.2010.03.052
6. Holland J.H. Adaptation in Natural and Artificial Systems. *University of Michigan Press*. Ann Arbor, 1975.


# CYBER ATTACKS SIMULATION FOR MODERN ENERGY FACILITIES


Oleksii Novikov, Mariia Shreider, Iryna Stopochkina, Mykola Ilin
National Technical University of Ukraine "Igor Sikorsky KPI", Kyiv, Ukraine
o.novikov@kpi.ua, marshr-ipt23@lll.kpi.ua, i.stopochkina@kpi.ua , m.ilin@kpi.ua



The work is devoted to the analysis and development of cyber attacks models against energy facilities. Models of typical attacks on energy systems are considered, which take into account the possibility of an attacker to distort the signal of the control system and control measurements of the state of the object in the measurement signals. A threat model for the energy object of the critical infrastructure is proposed. It is proposed to take into account the influence of integrity-

breaking attacks in the form of a function that depends on unknown parameters. Criteria are proposed that allow parametric identification of attacks with integrity violations, taking into account measurements, and based on restrictions on the behavior of the process. The stability conditions in conditions of cyberattacks for the typical automatic gain control system are analyzed. An attack parameter identification algorithm is proposed. Computer modeling of the processes of objects under various types of attacks was performed, conclusions were drawn about the impact of attacks on the objects resilience.
**Keywords:** Energy facilities, cybersecurity attacks, DoS, FDI attacks, resilience.

## Introduction

Cyber attacks on energy supply facilities reinforce and deepen the impact of physical attacks for maximum destructive effect. Understanding the limits of resistance to cyber influences significantly helps in creating a system of adequate protection mechanisms and preventive measures. Existing investigations [1-4] pay no appropriate attention to questions of estimating of attack features or parameters.

The main classes of cyber threats for AGC (automatic gain control) system of energy facility are: 1)DoS, DDoS, time delay attacks (against availability) [1,2] 2)replay attacks (against integrity) [3] 3) FDI, covert attacks (against integrity) [3,4]. In conditions of war these attacks are combined with physical attacks against critical infrastructure facilities [5]. Attack parameters calculation algorithms remain the relevant task to understanding of boundaries of object resilience and cyber incident investigation.

## Attack models against integrity of AGC data

The initial undisturbed controlled system is described by a system of equations in the state space:

$$\frac{dx(t)}{dt} = Ax(t) + kBu(t) + F,$$

where $x$ is system state; $u$ is control; $F$ is function of the source (supporting energy to/from neighbor zones); $k$ is a parameter of the intensity of the controlling influence. If control depends on measurements : $u(t) = -C_1 y(t)$, where measurements depends of state: $y(t) = C_2 x(t)$.

## The model of attack on the measurement of system

Let ξ(t) is distortions introduced to measurements by an attacker: $y(t) = C_2x(t) + \xi(t)$, then $u(t) = -C_1y(t) = -C_1\big(C_2x(t) + \xi(t)\big) = -C_1C_2x(t) - C_1\xi(t)$. An equation (1) takes the form

$\frac{dx(t)}{dt} = (A - kB_1 - kB_2\xi(t))x(t) + F$, де $B_2 = BC$.

Let $y^*(t) = C_2x^*(t)$ is a set of measurements which characterizes process with $\xi(t) \equiv 0$, and value $\mathcal{E}_{cr}$ is given for $J(y): J(y) \geq \mathcal{E}_{cr}$ signals about abnormal behavior of the system. For discrete measurements $J = \sum_{i=1}^{n}(y(t_i) - y^*(t_i))^2 \longrightarrow min$.

From the condition $det(D + D_1\xi(t)) = 0$, where $D \equiv A - kB_1$, $D_1 \equiv -kBC_1$ we can obtain border value $\xi(t)$, which leads to object unstability. Also, taking into account the measurements, we can identify the values of adversary distortions $\xi(t)$. Let suppose that $\xi(t)$ is small, and obtain that $\xi(t) \approx y(t) - C_2\left[x^*(t) + e^{Dt}\int_0^t e^{-Dt'}f(t')dt'\right]$.

## FDI attacks

Considering the class of FDI attacks, let us introduce attack parameter $\xi_s$ (scaling parameter), the value of the parameter we propose to obtain taking into account that $\xi_s y_i(t) = y_{max}$, or $\xi_s u_i(t) = u_{max}$,- then these attacks are called max-attacks, or, if $\xi_s y_i(t) = y_{min}$ or $\xi_s u_i(t) = u_{min}$, - then these attacks could be called min-attacks [2].

The $[y_{min}, y_{max}]$, $[u_{min}, u_{max}]$ are acceptable diapasons of changes of measurements and control accordingly, due to technological features of the process. Consider the case of an attack on the system state. The system under attack is described by the model:

$\frac{dx(t)}{dt} = Mx(t) + F$, де $M \equiv A - k\tilde{A} - \xi_s C_1C_2$, $\tilde{A} \equiv BC_1C_2$;

$u(t) = -C_1y(t)$; $y(t) = C_2x(t)$.

From $detM = 0$ we obtain the limiting value $\xi_s$, which leads to a loss of system stability.

An identification algorithm is proposed for $\xi_s$, in particular for max-attack it is based on criteria $J = \int_0^T (u - u_{max})^2\, dt \to min$. So Lagrange function for this case is:

$L(x,p,\xi) = \int_0^T [(B_1 x - u_{max})^2 + (\frac{dx}{dt} - A_1(\xi)x(t) - F)p]dt \rightarrow inf$, where $A_1 = A - k\tilde{A} - \xi_s C_1 C_2$; $B_1 = -C_1 C_2$ . Let variation of $L(x,p,\xi)$ is zero, so we could get the equations for $x$ and $p$ and obtain $\xi_s$ by gradient method.

## Conclusions

The proposed identification algorithms allow to reveal adversary impacts in the AGC system, using the information for incident response. We can correct existing mechanisms of resilience supporting, taking into account real abilities of adversary impact. The existing models of FDI attacks were enchanced with control theory application with additional criteria that take into account physical restrictions in the system.

The numerical results show that the harmful impact of FDI attack could be supported even with small values of $\xi_s$ , and availability – directed cyber attacks can destabilize system even with not very large diapasons of time delays. Also replay attacks also could by harmful. It means, that the AGC data protocols have to be protected with means against integrity corruption as far as with additional means of availability supplying. The organizational means of defense should be directed towards impossibility making influence on physical system characteristics directly.

Further research can be related to the analysis of power grid resilience taking into account combined harmful impact of different kinds of cyber attacks.

## References


1. Y. Shen, M. Fei, D.Du, Cyber security study for power systems under denial of service attacks, 2017, SageJournals, Volume 41, Issue 6. doi: 10.1177/0142331217709528.
2. 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, Energies, 13(15), 3860. doi: 10.3390/en13153860.
3. C. Moya, On Cyber-Attacks against Modern Power Grids, Ph.D. Thesis, The Ohio State University, 2020. URL: https://dl.acm.org/doi/10.5555/AAI28890224.
4. X.Li, P.Zhang, H.Dong, Robust Stealthy Covert Attacks on Cyber-Physical Systems, 2022, IFAC-PapersOnLine,

Volume 55, Issue 6, P. 520-525. doi: 10.1016/j.ifacol.2022.07.181.
5. M. Ovcharuk, M. Ilin, Models of Denial of Service Attacks on Cyber-Physical Systems, 2023, Theoretical and Applied Cybersecurity, Vol. 5, No2 (2023). doi: 10.20535/tacs.2664-29132023.2.289459

# ЗАХИСТ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ У СИСТЕМАХ ЗВ'ЯЗКУ НАТО

А.В. Балан, А.І. Іллінський
Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут, Київ, Україна
bsbmps@gmail.com, antonillinskyi@gmail.com

Розглянуто основні базові принципи та мінімальні стандарти політики безпеки країн членів НАТО у сфері захисту інформації з обмеженим доступом, згідно документу C-M (2002) 49, а саме INFOSEC та класифікацію інформації країн членів НАТО.
**Ключові слова:** Інформаційна безпека, кіберзахист у НАТО, INFOSEC, Інформація з обмеженим доступом (ІзОД) НАТО.

## Вступ

Інформаційна безпека та кіберзахист надзвичайно важливі, тому в структурах НАТО приділяється дуже велика увага до кіберзахитсу через зростання кіберзагроз у світі, де цифрові технології стають ключовими. Це вимагає постійного покращення заходів безпеки для захисту від серйозних наслідків атак та дезінформації. Забезпечення стабільності потребує постійної стратегії та співпраці з іншими країнами.

Україна, яка є партнером НАТО, виступає у складному геополітичному контексті, де кіберзагрози стають надзвичайно актуальними. В умовах активного партнерства з НАТО, Україна активно впроваджує стратегії кіберзахисту, співпрацюючи із союзниками для забезпечення стабільності і безпеки в цифровому просторі. Загальна стратегія кібербезпеки країни є невід'ємною

частиною колективних зусиль НАТО з протидії сучасним кіберзагрозам.

## Стратегії та процедури інформаційної безпеки в НАТО

Інформаційна безпека в НАТО(INFOSEC) - це комплексна система, що включає політичні стратегії, технічні заходи та освіту для забезпечення безпеки та конфіденційності інформації. Вона складається з політики безпеки, технічних заходів, управління ризиками та освітніх програм, спрямованих на захист від різних загроз.

«INFOSEC» регулює процедури захисту конфіденційності, цілісності, готовності та звітності щодо інформації, яка передається і обробляється за допомогою інформаційно-комунікаційних технологій.

«Попередня директива з INFOSEC», яка була опублікована Комітетом безпеки НАТО і Комітетом політики з питань консультації, командування і контролю (NC 3B) вимагає створення відповідної національної організації, відповідальної щодо заходів фізичної та персональної безпеки у комп'ютерних та комунікаційних мережах. Безпека комунікаційних мережах передбачає криптографічний захист та захист від витоків інформації через випромінювання або еманацію (TEMPEST).

Органами INFOSEC в структурі НАТО є:

управління С3 НАТО;

робоча група INFOSEC у складі NCS;

підкомітет INFOSEC;

командування NACOSA/INFOSEC;

установа INFOSEC з акредитації комунікаційного обладнання НАТО – SAA(Security Accreditation Authority).

Національними органами INFOSEC у кожній країні НАТО мають бути:

національне управління з інформаційно-комунікаційних систем;

національне представництво з безпеки комунікаційних мереж NCSA (National Communication Security Authority);

національне представництво з дистрибуції - NDA (National Distribution Authority);

національне управління з акредитації комунікаційного обладнання (SAA), визнане НАТО.

Кожна держава-член НАТО встановлює Національний орган безпеки комунікаційних систем (NCSA). Основні завдання NCSA полягають у наступному:

контроль за криптографічною технічною інформацією, яка стосується захисту інформації НАТО в межах власної держави;

забезпечення гарантії, що криптографічні системи, продукти та механізми для захисту інформації НАТО ефективно і раціонально відібрані, керовані і підтримувані;

повідомлення про безпеку комунікаційних систем НАТО та споріднені технічні справи INFOSEC як цивільні, так і військові, відповідному органу НАТО або державному органу.

Під час передачі засобами інформаційно-комунікаційних технологій інформація із грифом «НАТО/Цілком таємно» і вище захищається за допомогою криптографічних методів або продуктів, затверджених Військовим комітетом НАТО (NAMILCOM).

Під час передачі засобами інформаційно-комунікаційних технологій інформація з грифом «НАТО/Таємно» і «НАТО/Для службового користування» захищається за допомогою криптографічних методів або продуктів, затверджених Військовим комітетом НАТО (NAMILCOM) або державою-членом НАТО, за винятком випадків, коли такий метод або продукт є спільно консолідований, він затверджується NAMILCOM.

При обміні конфіденційною інформацією між НАТО та країнами-партнерами, які співпрацюють з НАТО, застосовуються спеціальні криптографічні методи та продукти, затверджені відповідними органами. Це забезпечує захист інформації з різними рівнями секретності, такими як "NATO SECRET/Цілком таємно", " NATO CONFIDENCIAL /Таємно" і "NATO RESTRICTED/Для службового користування". Органи НАТО та співпрацюючих країн відповідають за вибір, оцінку, сертифікацію та контроль за використанням цих методів та продуктів для забезпечення відповідних стандартів безпеки при обміні інформацією.

## Висновки

Аналіз системи інформаційної безпеки в НАТО підтверджує її комплексний характер, що охоплює політичні, технічні та освітні аспекти. INFOSEC визначає процедури захисту інформації, яка обробляється за допомогою технологій. Відповідно до вимог

Альянсу, кожна країна, що вступає до НАТО, має взяти на себе зобов'язання привести власні нормативно-правові документи у сфері захисту ІзОД у відповідності до стандартів НАТО. Тому вивчення та систематизації стандартів НАТО у сфері захисту ІзОД є обов'язковою умовою на шляху інтеграції України до НАТО, а досвід НАТО повинен стати зразком для України.

### Перелік посилань

1. NATO, Summary Record of the Meeting of the NATO Security Committee (Brussels: NATO Archives, October 17-18, 1957.

2. NATO Security Committee. (2002). Security within the North Atlantic Treaty Organization (NATO) [C-M(2002)49].

3. В.С. Сідак, В.Ю. Артемов. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: Навчальний посібник. — К.: КНТ, 2007. - 160 с.

## ОСОБЛИВОСТІ РИЗИКОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ

Юрій Григорович Даник,
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", м. Київ, Україна
danyk_1@ukr.net

В доповіді розглядаються ризики та загрози, пов'язані з розвитком та використанням штучного інтелекту. Аналізуються особливості формування ризикології штучного інтелекту.

**Ключові слова:** штучний інтелект, безпека, оборона, загрози, ризики, ризикологія, живучість, критична інфраструктура, кіберпростір.

### Вступ

З появою і впровадженням штучного інтелекту практично в усіх сферах життя і діяльності людини, суспільства, держави формується специфічний ландшафт загроз, ризиків їх реалізації та наслідків, які погано прогнозуються на існуючому етапі розвитку теоретичних та прикладних аспектів науки про ризики

цієї сфери. Поряд з новими можливостями, які пов’язані з розвитком і використанням ШІ, з’являються та множаться різноманітні етичні, соціальні, безпекові та інші проблеми. Кількість інцидентів, пов'язаних з некоректним використанням ШІ, швидко зростає. Тому, актуальним питанням є створення і забезпечення умов, за яких штучний інтелект не вийде з під контролю, і не буде створювати неприйнятних загроз людині і людству.

Наразі, вже існує значна сукупність невирішених протирічь в цій сфері. Зокрема, між швидким розвитком ШІ та його використанням, особливо в сфері безпеки і оборони, і необхідністю передбачати та максимально знизити ризики і загрози, пов'язані з його розвитком. Наразі відсутні обгрунтовані системні підходи до зниження, запобігання і нейтралізації цих загроз і ризиків їх реалізації, особливо стосовно питань забезпечення безпеки та живучості об’єктів критичної інфраструктури.

Метою дослідження є аналіз ризиків і загроз, пов'язаних з розвитком і використанням штучного інтелекту в різних сферах діяльності людства та особливостей формування ризикології штучного інтелекту.

## Ризики та загрози штучного інтелекту

З розвитком штучного інтелекту, поряд з новими можливостями з'являються нові етичні, соціальні і безпекові проблеми, пов'язані з його використанням. Це викликає потребу всебічного дослідження теоретичних та практичних аспектів виникнення та життєвого циклу ризиків пов’язаних з розвитком ШІ та його використанням. Такі дослідження, зважаючи на особливості ШІ мають міжгалузевий та міждисциплінарний характер. Вони безпосередньо пов’язані з високотехнологічним розвитком суспільства, глобалістикою, соціологією тощо і повинні враховувати особливості взаємодії в системах: людина (користувач) - штучного інтелект; ШІ – людина; ШІ – суспільство; ШІ –держава; ШІ – кібер-фізична(і) система(и) (КФС). А також системи більш високої складності і рівнів взаємодії. Таких як: особа (група осіб, суспільство)1- ШІ 1 – ШІ2 -особа (група осіб, суспільство)2; структура (інституція, організація, держава)1- ШІ 1 – ШІ2 - структура (інституція, організація, держава)2, ШІ 1 – КФС 1 - КФС 2 - ШІ 2 тощо. А також різноманітних комбінацій багатокомпонентних систем, які

можуть організовуватись різними акторами та самоорганізовуватись. Для управління ризиками в таких умовах виникає необхідність постійного моніторингу динамічних (що найчастіше змінюються хаотично) мінливих параметрів систем «людина-суспільство-природа-техносфера-ШІ» і наукового пізнання цих систем та формування ризик-рефлексії. Для цього необхідно здійснювати розробки, впровадження, і забезпечувати постійний випереджаючий розвиток механізмів зниження ризиків на всіх рівнях ієрархії вищерозглянутих систем. А саме на: макро- (держава(и)), мезо- (організації) і мікро- (особистості) рівнях. Ризикологія ШІ, як наука про ризики пов'язані з його виникненням, впровадженням, використанням, розвитком, всебічними взаємодіями в різноманітних бікомпонентних та багатокомпонентних системах повинна забезпечити всебічне вивчення, дослідження і розуміння природи, структури та наслідків реалізації загроз у взаємозв'язку із ризиками їх реалізації. При цьому, необхідною є розробка методів ідентифікації, класифікації, аналізу і оцінки джерел і чинників ризиків пов'язаних з ШІ. Також потрібно сформувати принципи класифікації, оцінки та соціальної прийнятності різних ризиків пов'язаних ШІ та його розвитком. Розробити методологію прогнозування динаміки і управління ризиками в цій сфері.

Найголовнішим є наявність обґрунтованого критерію і тесту, подібного тесту Алана Тюрінга для перевірки, наскільки машина розумна, і наскільки близько вона підходить під визначення «Штучний Інтелект (Розум)» у повному розумінні цього терміну, для своєчасного виявлення виходу ШІ з під контролю людини та розгляду ШІ людини, як загрози його існуванню або іншим інтересам. Однією з умов цього може бути виникнення і формування у ШІ інстинкту самозбереження та прийняття ним рішення щодо превентивних дій з нейтралізації подібних загроз.

Розгляд і дослідження зазначених питань дозволили виявити найбільш важливі аспекти пов'язані з ризикологією ШІ.

## Висновки

Таким чином, в доповіді розглянуті основні особливості, тенденції і напрями розвитку ризикології штучного інтелекту. Представлені виявлені закономірності в формуванні загроз і ризиків в цій сфері. Запропонований показник для оцінки ризику виходу ШІ з під контролю людини та розгляду штучним інтелектом людини, як загрози його існуванню або іншим

інтересам. Розглянуті підходи до виявлення потенційних ризиків та вжиття проактивних заходів для пом’якшення цих ризиків.

Подальші дослідження передбачають розробку механізмів управління ризиками пов'язаними з розвитком і використанням штучного інтелекту.

## Перелік посилань:


1. Artificial Intelligence and National Security, Bipartisan Policy Center and Georgetown University’s Center for Security and Emerging Technology (2020).
2. Brundage Miles, Avin Shahar, Clark Jack et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation (2018). Homepage, https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf, last accessed 2023/06/21.
3. China’s Rise In Artificial Intelligence And Future Military Capabilities. Battlefield Singularity: Artificial Intelligence, Military Revolution, and China’s Future Military Power, Nov. 1, pp. 8-32 (2017).
4. Amina Iqbal. China’s AI Military Revolution and its Security Implications (2023), Homepage, https://internationalaffairsbd.com/chinas-ai-military-revolution/, last accessed 2023/09/16.
5. Elsa B. Kania. “AI Weapons” In China's Military Innovation (2020). Homepage, https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_ai_weapons_kania.pdf.


# ІНТЕГРАЦІЯ ТЕХНОЛОГІЙ У СФЕРІ КІБЕРБЕЗПЕКИ: ІНФОРМАЦІЙНИЙ ПОШУК ТА ШТУЧНМЙ ІНТЕЛЕКТ


Олександр Пучков [1], Дмитро Ланде [1,2], Олександр Рибак

[1] Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна

[2] Інститут проблем реєстрації інформації НАН України, Київ, Україна



У цій роботі розглядається поєднання можливостей системи контент-моніторингу соціальних медіа CyberAggregator і системи генеративного штучного

інтелекту з метою покращення аналітичних можливостей корпоративної OSINT з проблем кібербезпеки, а саме засобів автоматичного формування зведенб (дайджестів), створення мереж понять (персон, термінів, об'єктів кібербезпеки).
**Ключові слова:** OSINT, генеративний штучний інтелект, інформаційний пошук, CyberAggregator, мережа понять, кібербезпека.

У сучасному світі кібербезпека стає все більш важливою сферою – кіберзагрози стають все складнішими та небезпечнішими. Для моніторингу стану кібербезпеки серед інших засобів застосовуються засоби розвідки у відкритих джерелах (Open Source INTelligence, OSINT) [1]. У той же час, невпинно розвивається штучний інтелект, який можливо використовувати для боротьби з загрозами в інформаційному просторі. Одним із шляхів застосування штучного інтелекту у сфері кібербезпеки є інтелектуалізація роботи із інформацією OSINT, узагальнення інформації з відкритих джерел.

Тому є актуальним завданням поєднання можливостей системи контент-моніторингу соціальних медіа з питань кібербезпеки CyberAggregator [1] з функціоналом генеративного штучного інтелекту [2]. CyberAggregator включає різні режими роботи, такі як пошук за конкретною тематикою та періодом входження документів та виведення окремих документів, отримання та аналіз динаміки інформації.

Поєднання цієї системи з можливостями utythfnbdyjuj штучного інтелекту (система Llama) спрямоване на покращення таких аспектів аналітичних режимів роботи системи, а саме формування:

1. Інформаційних зведень (дайджестів): комбінація технології пошуку з генеративним штучним інтелектом дозволяє автоматично аналізувати новинні повідомлення та створювати узагальнення, які надають зведену інформацію про події в інформаційному просторі.
2. Мережі персон, що враховує зв'язки між різними особами на основі їхньої активності в соціальних медіа та згадувань в інших джерелах інформації.
3. Мережі хакерських угрупувань, яка візуалізує зв'язки між окремими угрупуваннями, виявляє їх причетність до

кібератак, відношення до силових відомств окремих держав, тощо.

4. Мережі термінів, яка дозволяє автоматично аналізувати та визначати зв'язки між ключовими термінами, що сприяє кращому розумінню контексту інформації.

Пошуковий режим системи CyberAggregator базується на сучасній системі ElasticSearch [3]. Інтелектуальний режим використовує можливості генеративного штучного інтелекту, а саме моделі LLama-2 [4].

LLama-2 є великою мовною моделлю, яка має декілька переваг:

1. Розуміння складних зв'язків: Вона може аналізувати та розуміти складні зв'язки між словами та фразами.
2. Навчання на великому наборі даних: Модель може вдосконалюватися за рахунок великої кількості даних.
3. Безкоштовне використання: LLama-2 є безкоштовною для використання.
4. Відкритий код: Код LLama-2 доступний на GitHub, що робить його доступним для розширення та покращення.

Інтеграція CyberAggregator та LLama-2 надає можливості для автоматичного аналізу новинних статей, створення дайджестів та побудови мереж персон та слів. Всі ці можливості Ця інтеграція грає важливу роль в підвищенні рівня кібербезпеки та забезпеченні кращого розуміння інформаційного простору.

## Висновки

Інтеграція CyberAggregator та LLama-2 надає можливості для автоматичного аналізу новинних повідомлень, створення дайджестів та побудови мереж персон та слів. Це поєднання сприяє підвищенню аналітичних можливостей системи, використанню наявних ресурсів інформаційного простору.

## Перелік посилань


5. Dmytro Lande, Olexander Puchkov, Ihor Subach Method of Detecting Cybersecurity Objects Based on OSINT Technology. Selected Papers of the XXII International Scientific and Practical Conference "Information Technologies and Security" (ITS 2022) — Vol-3503. — pp. 115-124.
6. Dmytro Lande, Leonard Strashnoy. GPT Semantic Networking: A Dream of the Semantic Web - The Time is Now — Kyiv: Engineering, 2023. — 168 p. ISBN 978-966-2344-94-3

7. Pranav Shukla, Sharath Kumar M N. Learning Elastic Stack 7.0. Distributed Search, Analytics, and Visualization Using Elasticsearch, Logstash, Beats, and Kibana, 2nd Edition. Packt Publishing, 2019. ISBN 9781789958539, 1789958539. — 474 p.
8. Smith N. A., Hajishirzi H. Self-Instruct: Aligning Language Model with Self Generated Instructions // ArXiv.org — 2022. — arXiv:2212.10560

## СТРУКТУРНА СКЛАДНІСТЬ КОМПЛЕКСНИХ ГРАФІВ

А. Снарський[1,2]
[1]Інститут реєстрації інформації НАН України, 03113, Київ, Україна
[2]Національний технічний університет «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна

Введено кількісну міру структурної складності графа (складна мережа тощо), засновану на процедурі, подібній до процесу перенормування, враховуючи різницю між фактичною та усередненою структурами графа в різних масштабах. Запропонована концепція структурної складності графа відповідає якісному розумінню складності. Запропоновану міру можна також отримати для зважених графіків.

Було виявлено структурні складності для різних типів графів – детермінованих графів нескінченного розміру та графів кінцевого розміру, штучних графів різної природи, включаючи перколяційні структури, і часових рядів серцевих ритмів, відображених у складні мережі за допомогою алгоритму параметричного графа видимості. Останні досягають максимуму поблизу формування гігантської компоненти на графіку або на порозі перколяції для 2D і 3D квадратних ґраток, коли виникає гігантський кластер, що має фрактальну структуру. Отже, структурна складність графів дозволяє виявити та дослідити процеси, подібні до фазових переходів другого роду в складних мережах.

Новий індекс центральності вузла, що характеризує структурну складність певного вузла в структурі графа, також може бути введений, що може служити хорошим допоміжним або узагальненням для локального коефіцієнта кластеризації.

Такий індекс забезпечує ще один новий спосіб ранжирування для вузлів графа.

Будучи легко обчислюваною мірою, структурна складність графа може допомогти виявити різні особливості складних систем і процесів реального світу.

Термін складність означає багато різних понять. В [1-4] можна знайти величезний перелік уже встановлених типів складності, їх можна розділити на групи: складність опису, складність створення, обчислювальна складність тощо. Аналіз складності багатьох природних явищ виявляє внутрішні процеси, що відбуваються в досліджуваній системі, часто непроникні. загальноприйнятими описовими методами та алгоритмами. Це виправдовує зростаючу тенденцію до використання аналізу складності для кількісної оцінки різних даних реального світу, наприклад, нейронної активності, виміряної за допомогою сигналів електроенцефалографії (ЕЕГ) [5].

Нещодавно було введено новий вид складності – багатомасштабну структурну складність (MSC).[6], який має справу зі складністю різних типів забарвлень або візерунків у багатовимірному гратчастому просторі. До них відносяться, наприклад, двовимірні зображення різних структур, від зображень природи до смугастих доменів у феромагнітних тонких плівках, перлітної структури в рейковій сталі, смуг на пляжі в зоні припливів і багато іншого. Іншими словами, MSC має справу з вагами вузлів регулярної просторової решітки, наприклад, двовимірної квадратної решітки для звичайних зображень. Було показано, що МСК відкриває важливу інформацію про динаміку нерівноважних структур, явища фазових переходів і багато іншого.Ми ввели кількісну міру структурної складності графа (складної мережі тощо) на основі процедури, подібної до процесу перенормування, враховуючи різницю між фактичною та усередненою структурами графа на різних масштабах. Ми застосували цей підхід, щоб знайти структурні складності для різних типів графів – детермінованих нескінченних графів і графів кінцевого розміру, для штучних графів різної природи, включаючи перколяційні структури, і для часових рядів серцевих ритмів, відображених у складні мережі за допомогою параметричного алгоритму видимості графа [7-9].

Запропонована концепція структурної складності графа відповідає якісному розумінню складності. Чим складніша структура графа, тим більша складність графа. Структурна

складність порожніх і повних графів (без структури) дорівнює нулю, складність досягає максимуму біля утворення гігантської компоненти в графі або на порозі перколяції для 2D і 3D квадратних ґраток, коли гігантський кластер, що має фрактальну структуру, виник. Останнє показує, що структурна складність графа дозволяє виявляти та вивчати процеси, подібні до фазових переходів другого роду в складних мережах.

Запропонований алгоритм GSC також здатний обробляти зважені графіки. Навіть він може обробляти графіки з вагами, призначеними вузлам. Для цього потрібно зробити перехід, один із можливих — присвоїти ребрам вагу, що дорівнює сумі часткових ваг зв'язаних вузлів, поділених на ступінь такого вузла. Це дає змогу знайти, наприклад, складність зображення як GSC регулярної (двовимірної чи багатовимірної) решітки зі зваженими вузлами, або навіть складність мережі нерегулярних зважених вузлів.

У складі алгоритму GSC можна ввести новий індекс центральності вузла, що характеризує структурну складність певного вузла в структурі графа, тобто знайти розподіл складності вузла по графу. Цей індекс центральності може служити, наприклад, як хороший допоміжний засіб або узагальнення для локального коефіцієнта кластеризації. Структурна складність окремих вузлів забезпечує ще один новий спосіб ранжування вузлів графа. Ми вважаємо, що зміни в структурній складності складних соціальних мереж з часом можуть свідчити або бути індикатором майбутніх часто прихованих соціальних процесів. Можливі застосування також належать до контексту алгоритмів на основі машинного навчання або штучного інтелекту, які можуть використовувати обчислені складності. Будучи мірою, яку легко обчислити, вона може допомогти виявити різні особливості складних систем і процесів. Безсумнівно, необхідні наступні дослідження, щоб продемонструвати можливість використання запропонованого графа структурної складності для багатьох різних явищ реального світу.

## Список літератури

1. Albert, R. and A.-L. Barabási, Statistical mechanics of complex networks. Reviews of Modern Physics, 2002. 74(1): p. 47-97.

2. Estrada, E., The structure of complex networks: theory and applications. 2012, USA: Oxford University Press.
3. Jensen, H.J., Complexity science: the study of emergence. 2022, USA: Cambridge University Press.
4. Lloyd, S., Measures of complexity: a nonexhaustive list. IEEE Control Systems, 2001. 21(4): p. 7-8.
5. Lau, Z.J., et al., Brain entropy, fractal dimensions and predictability: A review of complexity measures for EEG in healthy and neuropsychiatric populations. European Journal of Neuroscience, 2022. 56(7): p. 5047-5069.
6. Bagrov, A.A., et al., Multiscale structural complexity of natural patterns. Proceedings of the National Academy of Sciences, 2020. 117(48): p. 30241-30251.
7. Lacasa, L., et al., *From time series to complex networks: The visibility graph.* Proceedings of the National Academy of Sciences, 2008. **105**(13): p. 4972-4975.
8. Bezsudnov, I.V. and A.A. Snarskii, *From the time series to the complex networks: The parametric natural visibility graph.* Physica A: Statistical Mechanics and its Applications, 2014. **414**: p. 53-60.
9. Snarskii, A.A. and I.V. Bezsudnov, *Phase transition in the parametric natural visibility graph.* Physical Review E, 2016. **94** (4).

## ПІДХІД ДО МОДЕЛЮВАННЯ ГЕОПРОСТОРОВИХ КАСКАДНИХ ЕФЕКТІВ КРИТИЧНИХ ІНФРАСТРУКТУР

А.В. Бойченко, В.Р. Сенченко
Інститут проблем реєстрації інформації НАН України, Київ, Україна

Дослідження критичних інфраструктур (КІ) визначається підвищеною складністю та трудомісткістю методів аналізу ризиків, заплутаністю математичних моделей, неможливістю врахування переважної більшості ключових факторів, які у підсумку можуть виявитися фатальними для КІ, наприклад загроз, пов’язаних з дистанційним ураженням об’єктів критичної інфраструктури (ОКІ).

Моделювання геопросторових каскадних ефектів передбачає фіксацію динаміки та взаємодії в межах географічного регіону, де зміни або події в одному місці можуть поширюватися та впливати на сусідні території. Цей тип моделювання актуальний у різних сферах, включаючи міське планування, екологічні дослідження, боротьбу зі стихійними лихами та соціально-економічний аналіз [1].

Геопросторові дані про розташування ОКІ є основоположними для поглибленого аналізу ризиків в КІ, та необхідні для прийняття раціональних рішень, спрямованих на зниження таких ризиків. Тому пропонується створити та використовувати базу просторових даних на основі OSM для зберігання даних щодо КІ України. OpenStreetMap (OSM) — це відкритий проєкт, спрямований на збір, збереження та розповсюдження геопросторових даних, створення інструментів для роботи з ними силами спільноти волонтерів [2].

Основними напрямками застосування ГІС при дослідженні каскадних ефектів КІ є:

- обґрунтування прийняття рішень на різних рівнях управління;
- суттєве скорочення часу доведення інформаційних, передусім директивних, рішень до всіх зацікавлених користувачів і виконавців;
- підвищення достовірності та повноти оцінювання загроз і ризиків для ОКІ;
- максимально повна інтеграція КІ;
- підвищення ефективності застосування засобів відновлення ОКІ.

Геопросторову БД планується застосувати для дослідження поточного розміщення ОКІ (Рис. 1.), виявлення та аналізу загроз КІ, пов’язаних з їх локаціями та експортувати в якості вхідних даних для подальшого використання в інших моделях таких, як моделювання сценаріїв прийняття рішень [3].

Перший етап — розробка логічної моделі даних (групування Рис. 2) передбачає зіставлення типів об’єктів з тими структурами, які здатні підтримувати доступні для вітчизняного науковця програмні засоби проектування.

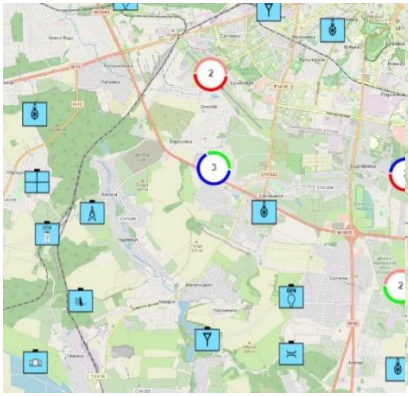


Рис. 1. Геопросторова візуалізація об’єктів КІ

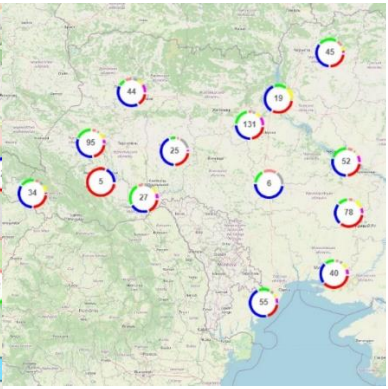



Рис. 2 Групування об’єктів КІ на мапі - логічна модель даних

Ці дії ґрунтується на структуруванні основних зав’язків між класами та їх визначенням у СУБД. Взаємна залежність об’єктів КІ зазвичай визначається як множина однонаправлених зв’язків між парами об’єктів, зумовлений тим, що зміна стану першого певним чином впливає на функціонування пов’язаного. Взаємозалежність є комбінацією пари таких залежностей. Таким чином, дослідження стану живучості та резильєнтності певного набору вимагає аналізу односторонніх залежностей, які її складають.

Взаємозалежність між об’єктами КІ може призвести до серйозних економічних і фізичних збитків у регіональному, загальнодержавному та навіть у планетарному масштабі. Виявлення та аналіз явних та прихованих зв'язків та залежностей, які існують між елементами КІ є необхідною складовою для розробки стратегій захисту та реагування на загрози живучості та резильєнтності КІ, а також мінімізації руйнівних наслідків деструктивних впливів [3].

В даний момент управління різних галузей критичної інфраструктури окремо одна від одної часто перешкоджає аналізувати їх взаємозалежності та ймовірні каскадні ефекти [4].

Для аналізу взаємних впливів між критичними інфраструктурами пропонується використати:

– визначення ключових факторів, на які може вплинути подія або зміна територіально-просторового контексту;

- причинно-наслідкові зв'язки між подією або зміною, що викликала каскадний ефект, і різними факторами в межах територіального простору;
- часову динаміку – розуміння того, як зміни відбуваються з часом, що має важливе значення для фіксації та моделювання каскадних ефектів у взаємопов'язаних КІ;
- геопросторові дані – відображають відстань між елементами КІ та ймовірність того, що порушення роботи одного об'єкта може вплинути на інші, розташовані поблизу;
- комунікаційні зв'язки на рівнях управління, пов'язані з інформаційним обміном;
- управлінські зв'язки характеризують порядок прийняття рішень на різних рівнях КІ.

В якості інструменту для дослідження динаміки території пропонується використання графової бази даних Neo4j (знання-орієнтованої технології). Застосування знання-орієнтованої Neo4j дозволяє будувати причинно-наслідкові моделі та досліджувати їх динаміку в межах територіального простору (геопросторової моделі). Така модель може доповнювати геопросторову (візуальну) модель розвитку каскадного ефекту на семантичному рівні (Рис. 3.). Запропоноване поєднання технології дозволяє досліджувати показники живучості та резильєнтності КІ шляхом аналізу залежностей та взаємозв'язків між елементами КІ, використовуючи графові алгоритми [5, 6]. Ці відношення можуть базуватися на географічній близькості, функціональних залежностях або інших факторах. Крім того, Neo4j зберігає дані у вузлах, зв'язках і властивостях, які добре узгоджуються з представленням знань, що робить інтуїтивно зрозумілим моделювання складних причино-наслідкових зв'язків, які зазвичай зустрічаються в КІ при викинені каскадних ефектів.

Візуалізація КІ на основі стандарту APP-D дозволить реалізувати різні сценарії моделювання, наприклад, запити на наявність та розташування певних просторових об'єктів КІ та відстані між ними. Візуалізація на основі карт використовується майже в усіх застосунках, однак, в основному використовують 2D-карти за винятком ARSI, Systematic і QGIS. Ці застосунки використовують найсучасніші 3D геопросторові візуалізації, використовуючи 3D-карти для ілюстрації просторових особливостей щодо об'єктів КІ, одночасно передаючи

інформацію щодо змін рельєфу, висоти природних просторових об’єктів та ступінь рослинності та погоди.

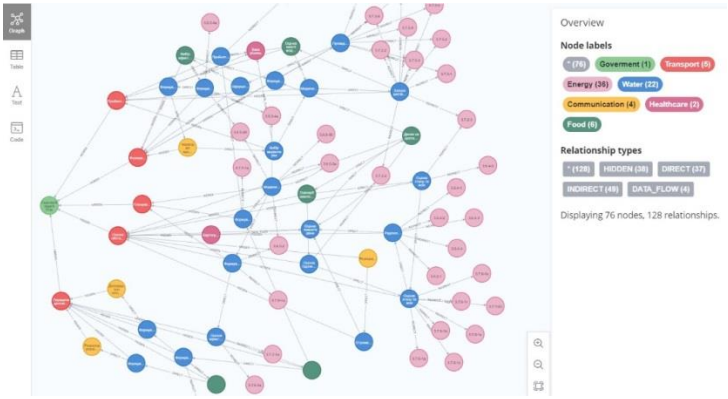



Рис. 3. Модель причинно-наслідкових зв'язків каскадних події КІ для дослідження в Neo4j

Таким чином, моделювання геопросторових каскадних ефектів є міждисциплінарним завданням, яке вимагає співпраці між експертами з географії, екології, міського планування та інших суміжних галузей. Точність і ефективність моделі залежать від якості даних, придатності методів моделювання та глибини розуміння залученої просторової динаміки.

## Література


1. Закон України «Про національну безпеку України». https://zakon.rada.gov.ua/laws/show/2469-19.
2. OpenStreetMap Ukraine https://www.facebook.com/openstreetmapua/
3. Додонов О.Г., Сенченко В.Р., Путятін В.Г., Бойченко А.В., Коваль О.В. (2023). Методологічні та технологічні аспекти комп’ютерного моделювання сценаріїв прийняття рішень. Математичні машини і системи. 2023 - 3, 65-88.
4. Додонов О.Г., Горбачик О.С., Кузнєцова М.Г. Підвищення безпеки критичних інфраструктур засобами автоматизованих систем організаційного управління // Реєстрація, зберігання і обробка даних, 2022. Т. 24. № 1. С. 74-81.

5. Neo4j Graph Database. URL: https://neo4j.com/product/neo4j-graph-database/
6. *Cypher Query Language. URL:* https://neo4j.com/developer/cypher/

# МЕТОДИКА СТВОРЕННЯ МОДЕЛІ СКЛАДНОЇ СИСТЕМИ ДЛЯ ТРАНСФОРМАЦІЇ ЇЇ ЦІЛЬОВОГО ПРИЗНАЧЕННЯ

С.С. Сабадаш[1], Ю.Г. Даник[2]
[1]Житомирський військовий інститут імені С. П. Корольова, м. Житомир, Україна,
[2]Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна
*sabadashss@ukr.net,* danyk_1@ukr.net

В доповіді розглядаютьсяметодика та результати моделювання складних систем озброєння та військової техніки для їх трансформації з метою перепрофілювання цільового призначення.
**Ключові слова:** складна система, трансформація, моделювання, перепрофілювання, програмні модулі.

## Вступ

На сьогоднішній день в інтересах національної безпеки та оборони застосовується значна кількість озброєння та військової техніки (ОВТ). Низка з цих систем втратили свою актуальність щодо їх використання за прямим призначенням. При цьому вони мають значний потенціал застосування за іншим призначенням. Для досягнення цього є необхідним відповідно до нового призначення визначити складдодаткових елементів, алгоритмів функціонування, програмних продуктів, перелік дій, які потрібно провести для забезпечення необхідної трансформаціїтаких комплексів і засобів. При цьому важливим є мінімальне втручання в системотехніку та архітектуру побудови існуючих засобів. Це пояснюється тим, що втручання в штатні алгоритми функціонування за призначенням можуть призвести до неприйнятних порушень в функціонуванні таких засобів. Що, в свою чергу, буде призводити до зростання небезпеки під час застосування, порушенняфункціонування системизагалом тощо.

З метою розробки засобів та програмних продуктів для зміни застосування засобів ОВТ є необхідним здійснення комп'ютерного моделювання роботи цих систем.

В доповіді пропонується методика розробки комп'ютерних моделей складних систем ОВТ з метою трансформації їх призначення та подальшої перевірки ефективності застосування.

## Сутність та особливості методики комп'ютерного моделювання складних систем ОВТ для трансформації їх цільового призначення

Розроблена методика комп'ютерного моделювання складних систем для трансформації їх цільового призначення включає проведення теоретичних, експериментальних та функціональних досліджень базового зразка, який обраний для трансформації.

Для визначення вихідних технічних, технологічних та конструктивних параметрів системи проводиться структурна, системна та функціональна декомпозиція системи (зразка ОВТ), її апаратної та програмної складових, аналітичні дослідження подібних систем ОВТ та технологічних вимог до їх застосування. При цьому особливу увагу слід приділити інформаційно-керуючим системам (ІКС) та виконавчим пристроям. Здійснюється обґрунтування складу, характеристик, вхідної та вихідної інформації програмних модулів, технічних та технологічних параметрів технічних засобів.

На основі проведених аналітичних досліджень розробляються технологічна та конструктивні схеми додаткових, нових технічних засобів, архітектура та склад моделі системи, яка трансформується.

Запропонована методика дозволяє розробити та реалізувати програмно-алгоритмічний комплекс який забезпечує:

– оцінку стану зразка ОВТ та можливості його трансформації для зміни призначення;

– проведення одночасного аналізу зразка ОВТ та його трансформованої версії;

– збір, збереження, обробку вимірів і видачу команд ІКС та виконавчим пристроям.

Методику апробовано на основі перепрофілювання одного із відомих засобів протиповітряної оборони (ППО) в систему формування та генерування сигналів, які відповідають тим, що мають місце під час здійснення атаки ППО по повітряним цілям.

На борту кожного бойового літака знаходиться система

безпеки, призначення якої є своєчасне виявлення сигналів для інформування пілота про атаку засобами ППО противника.Для забезпечення ефективної роботи такого засобу, було створено програмно-алгоритмічний комплекс, який здійснює моделювання функціонування базової системи та функціонування трансформованої системи. З такою метою було застосовано об'єктно-орієнтований метод програмування в інтегрованому середовищі MicrosoftVisualStudio 2022. В результаті одержано багатофункціональний програмний комплекс із можливістю нарощування функціональностіза допомогою застосування додаткових програмних модулів.

## Висновки

Таким чином, в доповіді розглянутометодику моделювання складних систем ОВТ для трансформації їх цільового призначення. Наводиться приклад реалізації та застосування запропонованої методики. Отриманірезультати показали принципову можливість зміни цільового призначення зразків ОВТ, які втратили свою актуальність за прямим призначенням, а також з метою розширення можливостей цільового призначення.

Розробка нових та модернізація існуючих засобів ОВТ на основі їх трансформації з метою перепрофілювання цільового призначення дає можливість покращити ефективність їх застосування та скороти час нарощування сил за засобів оборони держави.

## Перелік посилань


1. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки [Електронний ресурс] : навчальний посібник / Д. В. Ланде, І. Ю. Субач, Ю. Є. Бояринова ; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 300 с. Режим доступу: https://ela.kpi.ua/bitstream/123456789/45721/1/NP_Osnovy_teorii_intelekt_analizu.pdf.
2. Методи моделювання складних систем і процесів [Електронний ресурс] : навчальний посібник / КПІ ім. Ігоря Сікорського; уклад. : Настенко Є. А., Павлов В. А., Носовець О. К., Корнієнко Г. А. – Київ: КПІ ім. Ігоря Сікорського, 2022. – 144 с. Режим доступу: https://ela.kpi.ua/bitstream/123456789/50988/1/Metody_modeliuvannia.pdf.

3. Ландэ Д. В. Основы интеграции информационных потоков: Монография / Д.В. Ландэ – К.: Инжиниринг, 2006. – 240 с.
4. Zhiwei Gao, Dexing Kong. Modeling and Control of Complex Dynamic Systems: Applied Mathematical Aspects / Hindawi Publishing Corporation Journal of Applied Mathematics, Volume 2012, Article ID 869792, 5 pages, DOI:10.1155/2012/869792.

# МЕТОД ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ ОРГАНІЗАЦІЇ ПРИ ВИКОРИСТАННІ ОРДИНАЛЬНИХ ШКАЛ

Г.М. Гнатієнко[1], О.Г. Гнатієнко[1], Р.М. Зулунов[2]
[1]Київський національний університет імені Тараса Шевченка, Київ, Україна
[2]Ферганська філія Ташкентського університету інформаційних технологій, Фергана, Узбекистан
g.gna5@ukr.net, oleksii.hnatiienko@knu.ua, zulunovrm@gmail.com

Розглянуто задачу забезпечення функціональної стійкості організаційної системи. Для визначення надлишкових ресурсів системи передбачено попереднє експертне оцінювання можливостей заміни виконання функцій тими елементами організаційної системи, які на поточний момент вийшли з ладу. Експертиза можливостей заміни виконання функцій елементами системи здійснюється в ординальних шкалах при визначенні якості виконання. Інтегральна якість функціонування організаційної системи в цілому визначається шляхом обчислення відхилення якості функціонування нової конфігурації системи від «ідеальної» конфігурації.

## Вступ

Основними властивостями складних систем, які характеризують їхню функціональну стійкість, є надійність, живучість, відмовостійкість. Функціональна стійкість деяким чином об’єднує усі наведені характеристики. Задачу, яка розглядається у цій роботі, найкращим чином можна описати,

застосовуючи концепцію функціональної стійкості, реалізація якої досягається застосуванням різних видів надмірності, шляхом перерозподілу ресурсів з метою компенсації наслідків позаштатних ситуацій [1, 2].

Функціональної стійкістю організаційної системи є її властивість зберігати структуру управління та виконувати основні функції, заради яких створено цю систему. Актуальність дослідження та забезпечення функціональної стійкості

## Постановка задачі та етапи забезпечення функціональної стійкості

Нехай задано деяку множину індексів функцій інформаційного захисту, які має забезпечувати система. Будемо вважати, що таких функцій $n$. Позначимо множину усіх функцій, що виконуються системою через $A = \{a_1,...a_n\}$, $J = \{1,...,n\}$. Зазначимо, що кількість функцій складної системи може складати сотні і тисячі одиниць. Функції, які виконуються різними елементами системи не дублюються, тобто $n = \sum_{i \in J} n_i$ – кожна функція у системі є унікальною: $A^{i_1} \cap A^{i_2} = \varnothing, i_1, i_2 \in J$, де $\varnothing$ – порожня множина.

Для забезпечення функціональної стійкості організаційної системи можна умовно виділити етапи, виконання яких дозволить визначити найбільш прийнятні варіанти конфігурації елементів системи та максимально зберегти якість виконання функцій:

– визначення надлишкових ресурсів;
– виявлення нештатної ситуації;
– розпізнавання нештатної ситуації;
– парирування наслідків нештатної ситуації;
– оцінка якості варіантів;
– вибір варіанта.

## Математична модель функціонування організаційної системи

Можна побудувати матрицю функцій, які виконуються елементами системи:

$$F^i = (f_i^0, f_i^1), \quad (1)$$

де $f_i^0 = \left( f_{ij}^0, j = 1,...,n_i \right), i \in I$ – вектор основних функцій $i-$го елемента системи,

$f_i^1 = \left( f_{is}^1, c_{is}, s \neq j \in \{1,...,n_i\}, s = \{1,...,\nu_i\} \right), i \in I -$ матриця суміжних функцій $i-$го елемента системи,

$c_{is}, s \neq j \in \{1,...,n_i\}, s = \{1,...,\nu_i\}, i \in I -$ рівень якості виконання $s-$ї суміжної функції $i-$м елементом системи.

Позначимо через $A^i, i \in J,$ підмножину функцій, що виконується $i-$м елементом системи.

Евристика Е1. Будемо вважати, що інтегральна якість функціонування системи є ідеальною на момент початку забезпечення її функціональної стійкості.

Ідеальну інтегральну якість функціонування організаційної системи позначимо через $F^I$.

Евристика Е2. У кожній організаційній системі існує взаємозамінність. Якість заміни елемента системи, який тимчасово чи назовсім вийшов з ладу, може бути критично низькою і навіть небезпечною для подальшого функціонування системи. Але вона завжди існує і може бути класифікована або оцифрована, наприклад, експертними методами.

Евристика Е3. Шляхом експертного оцінювання можна встановити відмінність якості заміни виконання будь якої функції з множини (1) основним елементом системи на виконання цієї ж функції деяким суміжним елементом у порядкових шкалах.

## Заміна елементів системи при виконанні окремих функцій

Нехай експертним шляхом вдалося встановити для кожної функції якість її виконання у ординальних шкалах. Наприклад, будемо вважати, що інформація про якість виконання деякої функції з індексом $j, j = 1,...,n$ несе в собі таке ранжування:

$$c_{ij} \succ c_{i_1 j} \approx c_{i_2 j} \succ c_{i_3 j} \approx c_{i_4 j} \approx c_{i_5 j}, \qquad (2)$$

де $c_{ij}-$ рівень якості виконання елементом системи з індексом $i, i \in I,$ функції з індексом $j, j = 1,...,n$.

Зазначимо, що варіанти виконання функції $j, j = 1,...,n$, в нових умовах використовують нестрогі ранжування (квазіпорядки, квазісерії), які задають відношення переваги між

якістю виконання функцій в ординальних шкалах.

Для генерування можливих варіантів конфігурації організаційної системи в нових умовах здійснюється перебір можливих варіантів заміни елемента з індексом $i, i \in I$, який вийшов з ладу, елемент з індексом із множини тих елементів, які представлені в ранжуванні виду (2).

Для визначення відстані між «ідеальною» конфігурацією системи та її новою конфігурацією можуть використовуватися різні метрики: Метрики: Хемінга, Кука, Евкліда, Литвака тощо.

Відомо, що у задачах експертного оцінювання немає еталонів, розглядаються лише відношення між елементами.

Евристика Е4. Якість функціонування організаційної системи залежить від відхилення початкової «ідеальної» конфігурації системи у порівнянні з новою конфігурацією системи, згенерованою на основі вибору нового варіанта виконання функцій елементами.

## Джерела


1. Babenko, T., Hnatiienko, H., Vialkova, V. Modeling of information security system and automated assessment of the integrated quality of the impact of controls on the functional stability of the organizational system // Selected Papers of the XX International Scientific and Practical Conference "Information Technologies and Security" (ITS 2020), Kyiv, Ukraine, December 10, 2020 / CEUR Workshop Proceedings, 2021, 2859, pp. 188–198.
2. Babenko, T., Hnatiienko, H., Ignisca, V., Iavich, M. Modeling of critical nodes in complex poorly structured organizational systems // Proceedings of the 26th International Conference on Information Society and University Studies (IVUS 2021), Kaunas, Lithuania, April 23, 2021 / CEUR Workshop Proceedings, 2021, 2915, pp. 92–101.

# KEYWORD-BASED COMPARISON OF SCIENTIFIC DATABASES

Cena Anna[1], Balagura Iryna[2,3]
[1]Warsaw University of Technology, Warsaw, Poland
[2] Institute for Information Recording of National Academy of Sciences of Ukraine, Kyiv, 03113, Ukraine
[3]University of Nottingham, United Kingdom

## Introduction

Co-word network analysis is frequently used in bibliometrics because it provides a clear graphic visualization, helps to describe the structure of the subject area, highlights the main key elements and groups of keywords to identify subtopics and interdisciplinarity in science. Moreover, this perspective opens up many opportunities for additional analysis, e.g. with tools developed within theory of complex networks. Please note that a combination of co-author and co-word networks allows the construction of a heterogeneous information network. In Lande et al. (2020) a Meta Path Computed Prediction (MPCP) algorithm for link prediction among scientists and publications was presented. Fan et al. (2022) used co-word network modularity analysis to identify primary research interests. The development of scientific areas also includes the comparison of domains: Khajavi (2023) proposed to measure a fuzzy distance between two domains using the three indicators of frequency, development, and investment appeal.

The main aim of the research presented in this paper is to better understand the mechanisms governing the popularity of specific topics and how they change over time. The investigation carried out in this paper includes comparison of selected open-source bibliometric databases, i.e., *dblp* database and *arXiv* e-print database and *Stack Exchange* Q&A websites, in terms of keyword behavior. We are inetersted in similarities and differences between those data sources as well as the information concerning relationships between topics and their evolution, interdiciplinarity and possible predictions for the future that can be formulated based on them. On the example of the computer science category / research field of study, various modelling techniques are consider - from quantitative analysis to keyword co-occurrence network modeling.

## Scientometric databases

In this section four databases, namely dblp, ArXiv, and Stach Exchange, will be described and compared. We focused on open sources that allow to gather and analyze bibliometric information freely.

The dblp-v13 database is a widely known computer science abstract database, which indexes about 7M publications, over 3M authors, over 6K conferences, and approximately 2K journals. Initially, dblp started as a database systems and logic programming (dblp) research group at the University of Trier in Germany, and since 2018 it has been operated and maintained by Schloss Dagstuhl. dblp is an open-access source of data, that provides data and a clear description of the form of storing data and updating processes.

ArXiv is a free distribution service and an open-access archive with 2,166,249 scholarly articles in the fields of physics, mathematics, computer science, quantitative biology, quantitative finance, statistics, electrical engineering and systems science, and economics. The greatest advantage of ArXiv is the fast publishing process, allowing scientists to increase the speed of research exchange, which was critically apparent during the pandemic of COVID-19.

StackExchange is a popular example of a Q&A website. Q&A websites are technical discussion forums on social media that serve as a platform for users to interact mainly via questions and answers and have become a necessary part of professional practice. In other words, the content of such websites mostly consists of current topics of practice in different areas. Stack Exchange is a large community run by professionals and enthusiasts and comprises 173 Q&A communities, including Stack Overflow.

## Empirical analysis

Computer science topics were analyzed and key-words networks were compared based on different resources. Note that in case of Stach Exchange forums we decided to include both Computer Science and Math forum. Table 1 present the summarization of data that were included in each of the database.

Please note that the data from all sources databases were easily accessible (i.e. there are archives available via official channels). Each of them, however, required extensive and time consuming pre-processing and cleaning. In general, at the first step of the scientometric analysis, data were gathered and filtered. Tags /

keywords were extracted (if needed) and standardized. The empirical cumulative distribution function estimated for keyword frequencies in each database is presented in fig. 1.

Table 1: Characteristics of considered data sources

| Database | Timeline | No. of keywords |
|---|---|---|
| ArXiv | 2007 - 2022 | 176[1] |
| Math[2] | 2010 - 2022 | 1930 |
| Computer Science[3] | 2008 - 2022 | 652 |
| dblp-v13 | 1930 - 2022[4] | 7,299,784 |

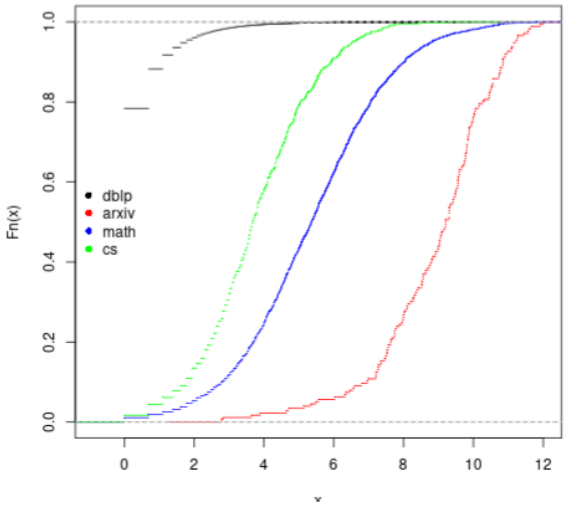



Figure 1: Empirical cumulative distribution function for keywords occurrence

Next an analysis of the time series of the posts and keywords was performed and co-word networks were build. Note that, both, for papers (dblp-v13 and arxiv databases) and posts (Stack Exchange forums) keyword / tags were mainly used. However, some additional information were also included (e.g. publication date, authors). Exemplary representation of the usage of keyword fuzzy is presented on fig. 2. Note that we may observe decline in number of times this

specific keyword was used. This may indicate for example that keyword fuzzy was replaced by more specialized and detailed expressions representing this domain.

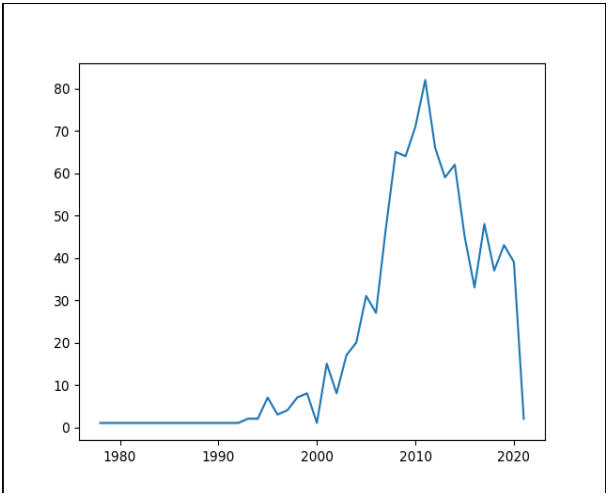



Figure 2: Time series representing the usage of keyword "fuzzy"

The presence of keywords/tags in one publication (paper or post) reflects the connection in the network. For example for Stack Exchange forum, the co-occurrence tags network consists of 664 nodes and 21735 edges, and the network diameter is equal to 4. The nodes with the highest centrality are most related to other topics. The main key-words for all the data are presented in the table 2.

Table 2: Top key-words in computer science

| dblp | math | cs | arxiv |
|---|---|---|---|
| data mining | real-analysis | algorithms | hep-ph |
| feature extraction | calculus | complexity-theory | hep-th |
| internet | linear-algebra | graphs | quant-ph |
| computer science | probability | formal-languages | cs.LG |
| optimization | abstract-algebra | time-complexity | astro-ph |

Moreover, the concept with the highest centrality was used as a keyword for searching and gathering the *ArXiv* data. For gathering data from *ArXiv* and *dblp* databases, the Science Metric library was used which was developed by the scientists of the Institute for Information Recording of National Academy of Sciences of Ukraine. The networks of concepts related to the selected tags were built using *ArXiv* and *dblp* and the main characteristics of the network were calculated. Selected concepts were compared by a proposed algorithm using the Borda count method and betweenness centrality measures. Selected keywords reflect the difference in purpose and usage of the databases.

## Conclusions

By analysing *dblp* database, *arXiv* e-print database and *Stack Exchange* Q&A websites, the behaviour of keywords and the mechanisms governing the popularity of specific topics were investigated. The most popular research trends in computer science were detected and analysed using co-word network and time series analysis with the discrete generalised distribution. The comparative analysis of four open-accessed databases was presented in the study and the main differences in usage were highlited in the study.

## References

1. D.Lande, M.Fu, W.Guo, I.Balagura, I. Gorbov, H. Yang, Link prediction of scientific collaboration networks based on information retrieval, World Wide Web: Internet and Web Information Systems23(2020) 2239-2257.doi: 10.1007/s11280-019-00768-9.

2. Wei-Min Fan, Wei Jeng, Muh-Chyun Tang First published: 06 June 2022 https://doi.org/10.1002/asi.24688

3. Khajavi R., Arastoopoor S. Semantic domain comparison of research keywords by indicator-based fuzzy distances: A new prospect (2023) Information Processing and Management, 60 (5), DOI: 10.1016/j.ipm.2023.103468

# АНАЛІЗ ІНТЕГРАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОЦЕС АВТОМАТИЗОВАНОГО ТЕСТУВАННЯ UX/UI ДИЗАЙНУ

О.А. Золотухіна, Ю.П. Бажан
zolotukhina.oks.a@gmail.com iurii.bazhan0@gmail.com

Розвиток інформаційних технологій за останні роки надав можливість відвантажувати протестований продукт до користувача в короткі терміни. Невчасно відвантажений продукт несе за собою негативні бізнесові наслідки: втрата репутації та прибутку.

Широке різноманіття продуктів представлених на сучасному ринку не може гарантувати існування єдиного, комплексного рішення швидкого розгортання. Але для всіх є сталим те, що важливе значення у процесі швидкого розгортання відіграє перехресна взаємодія функціональних груп, які займаються експлуатацією, безпекою та розробкою. Після 2010 року у зв'язку із впровадженням DevOps і хмарних технологій, нові функції (і навіть цілі компанії-стартапи) можуть створюватися за тижні і швидко, за години або навіть за хвилини, впроваджуватися у виробництво. Для таких організацій розгортання стало рутинною операцією, практично позбавленою ризиків. У цих організацій з'явилася можливість здійснювати експерименти для перевірки бізнес-ідей із метою з'ясування, які з них є найбільш цінними для клієнтів і самої організації і які можна швидко перетворити на «Функціональні рішення», а вже їх, своєю чергою, швидко і без ризиків розгорнути у виробництві.[1]

Існують три шляхи, завдяки яким формується база для успішного використання DevOps в організаціях: це принципи потоку, зворотного зв'язку, безперервного навчання та експериментування. Створення швідкого зворотного звязку має першочергове значення для досягнення якості. Тестування - це найголовніша форма зворотного зявку.

Метою даного дослідження є підвищення ефективності автоматизованого тестування UX/UI дизайну за допомогою методів штучного інтелекту на основі даних експериментальних досліджень.

Розглянемо очікувані результати та переваги використання методики. Наразі, у випадку зміни раніше вибраного селектора елемента в дизайні UX/UI, успішне проходження тесту програми

стає неможливим, оскільки програма не зможе знайти цей елемент, а данний тест завершиться невдачею. Однак ця проблема вирішується шляхом ручного пошуку та оновлення оновлених селекторів.

За допомогою методів штучного інтелекту буде виконуватись аналіз UX/UI дизайну з метою виявлення та розпізнавання оновлених елементів. У разі виявлення несходжень із результатами попереднього аналізу, система автоматично внесе зміни, замінюючи оновлені селектори елементів та додаватиме нові, щоб забезпечити коректну роботу системи.[2]

Використання методів штучного інтелекту в методиці автоматизованого тестування UX/UI дизайну сприятиме ефективному виявленню елементів та надасть можливість швидкіше оцінювати якість дизайну, виявляючи будь-які невідповідності. Такий підхід прискорить тестування та гарантує точне виявлення можливих проблем у UX/UI дизайні, а також надання швидкого зворотного зв'язку. Це визначається як важливий елемент для забезпечення якості, надійності та безпеки в технологічному процесі створення цінності. Шляхом виявлення проблем на ранніх етапах, адаптації до них та набуття нових знань, система забезпечить високу якість від початкових стадій розробки і буде постійно вдосконалюватися для оптимізації умов праці на низькорівневих робочих місцях.

## Література

1.M. Davies et al., “Advancing Neuromorphic Computing With Loihi: A Survey of Results and Outlook,” Proceedings of the IEEE, vol. 109, no. 5, pp. 911–934, May 2021, doi: 10.1109/JPROC.2021.3067593.

2.Cadwalladr, Carole (2014). "Are the robots about to rise? Google's new director of engineering thinks so…" The Guardian. Guardian News and Media Limited.

# МЕТОДОЛОГІЯ ОЦІНКИ ВІДНОШЕННЯ ЦІЛЬОВОЇ АУДИТОРІЇ ДО ОКРЕМИХ ВИСЛОВЛЮВАНЬ ЛІДЕРІВ ДУМОК

О.М. Безуглий
Інститут проблем реєстрації інформації НАН України, Київ,
*abezugliy00@gmail.com*

В цілях забезпечення оцінки відношення цільової аудиторії до окремих висловлювань лідерів думок: організувати збір інформації з різних відкритих джерел; провести оцінку отриманої інформації та моделювання динаміки її зміни для визначення рівня відношення цільової аудиторії до окремих висловлювань; забезпечити надійний доступу до інформації, що зберігається.

## Вступ

Методологія оцінки відношення цільової аудиторії до окремих висловлювань лідерів думок повинна розглядатися, як система принципів, правил, процедур і підходів, що використовуються для вивчення, дослідження, розробки та впровадження знань або процесу даної предметної області. Саме методологія визначає рамки і керівні принципи для виконання діяльності або досягнення мети, а також допомагає забезпечити систематичний підхід, ефективну організацію роботи, зменшення ризиків та досягнення кращих результатів. Крім того, методологія є основою для спільної роботи, спілкування та співпраці між учасниками проекту або командою. Тому, оцінка відношення цільової аудиторії до висловлювань лідерів думок повинна базуватися на методології, яка б забезпечила більш глибоке розуміння сприйняття аудиторії та впливу лідерів думок і виступала б важливим інструментом, який допомагає організувати та керувати різними видами діяльності з метою досягнення поставлених цілей.

## Актуальність методології

Актуальність методології оцінки відношення цільової аудиторії до висловлювань лідерів думок є вельми важливою в сучасному світі комунікацій. Методологія є актуальною, тому що враховує [1]:

*рівень сприйняття аудиторією* висловлювань лідерів думок, що дозволяє з'ясувати, як цільова аудиторія сприймає висловлювання лідерів думок, а це допомагає налаштувати комунікаційну стратегію, щоб краще відповідати очікуванням та потребам аудиторії;

*конкурентну перевагу* між лідерами думок, що допомагає зрозуміти, як конкуренти використовують лідерів думок та як можна покращити свою стратегію комунікації для отримання конкурентної переваги;

*постійну зміну тенденцій*, тому що соціальні мережі та медіа швидко змінюються, і нові лідери думок постійно з'являються, а оцінка відношення аудиторії до висловлювань лідерів думок допомагає відстежувати ці зміни та адаптувати стратегію відповідно.

## Методологія

Методологія оцінки відношення цільової аудиторії до окремих висловлювань лідерів думок вимагає ретельного планування і дослідження та включає [2,3]:

*визначення цільової аудиторії*, це можуть бути користувачі ІТ продукту або послуг, підписники платформи або соціальні мережі;

*виявлення популярних лідерів думок*, це дозволить покращити вплив і сприйняття аудиторією;

*збір даних* включає аналіз соціальних мереж, необхідно слідкувати за коментарями, лайками, репостами та іншими взаємодіями з цікавими публікаціями;

*аналіз трафіку* для вивчення поведінки цільової аудиторії на веб-сайті та дослідити, які сторінки або контент привертають більше уваги;

*аналіз даних* може включати кількісний аналіз, або якісний аналіз;

*визначення впливу* висловлювань лідерів думок на цільову аудиторію, що може бути виміряно через зміни в свідомості, рішеннях аудиторії, збільшення свідомості про вибрані показники;

*інтерпретація результатів* означає розуміння того, як цільова аудиторія сприймає висловлювання лідерів думок, які фактори впливають на їхню думку, і як ця інформація може бути використана;

*вироблення стратегії*, яка враховує вплив лідерів думок на цільову аудиторію, що вимагає системного підходу та досліджень, які враховують визначення цільової аудиторії та потребує ретельного її вивчення;

*аналіз впливу* потребує досліджень, які висловлювання, рекомендації або думки лідерів мають найбільший вплив на цільову аудиторію;

*вимірювання результатів* шляхом встановлення метрик та показників, які допоможуть виміряти ефективність стратегії;

*моніторинг* відношення цільової аудиторії до висловлювань лідерів думок повинен бути постійним та забезпечити ефективність вибраної стратегії і включати встановлення таких метрик, як кількість коментарів, репостів, лайків, позитивних або негативних відгуків тощо;

*використання соціальних медіа*, які допоможуть відстежувати висловлювання лідерів думок та реакції аудиторії на них, до таких медіа можна віднести Brandwatch, Hootsuite, Mention або Sprout Social та інші, які можуть надавати звіти та аналітику з соціальних мереж;

*збір відгуків*, щодо процесу оцінки методології шляхом збору відгуків, пропозицій і рекомендацій;

*аналіз результатів* використання методології шляхом виявлення сильних та слабких сторін, а також можливості для її поліпшення, причому необхідно приділяти увагу якісним і кількісним показникам, які допоможуть оцінити ефективність методології;

*постійне навчання* для розвитку учасників проекту з питань оцінки відношення цільової аудиторії до висловлювань лідерів думок, необхідно організувати семінари, тренінги або вебінари, де будуть обговорюватись нові підходи, методи та інструменти.

## Висновки

1. Оцінка відношення цільової аудиторії до висловлювань лідерів думок повинна базуватися на методології, яка б забезпечила більш глибоке розуміння сприйняття аудиторією лідерів думок та була б важливим інструментом, який допомагає організувати та керувати різними видами діяльності з метою досягнення поставлених цілей.

2. Методологія повинна базуватися на вимогах, які повинні включати: виявлення впливових осіб, вимірювання

реакції аудиторії, розробку стратегії комунікації, виявлення можливих викликів, покращення конкурентної переваги.

3. Актуальність методології обґрунтовується тим, що лідери думок впливають на усвідомлення, прийняття рішень та утворення думок аудиторією, крім того, методологія дозволяє з'ясувати, як цільова аудиторія сприймає висловлювання лідерів думок, оцінити відношення аудиторії до їх висловлювань, що допомагає виявити можливості для співпраці та покращення комунікації з лідерами думок, а також допомагає виявити можливі виклики або негативні відгуки, що можуть потребувати вирішення.

4. Розкриті складові методології оцінки відношення цільової аудиторії до окремих висловлювань лідерів думок.

## Джерела


1. О.Г. Додонов, Д.В. Ланде, В.В. Прищепа, В.Г. Путятин Комп'ютерна конкурентна розвідка, 2021, С: 309, ISBN:978-966-02-9212-3.
2. О.Г. Додонов, В.Р. Сенченко О.В. Коваль, Аналітика і знання в комп'ютерних системах. 2020, 54с, ISBN:978-966-2344-79-0.
3. Э. Дюркгейм. Правила соціологічного методу, 1995, С: 384, ISBN: 978-5-17-137831-8.


# МЕТОДИ ПРОТИДІЇ ПРОГРАМНИМ РЕАЛІЗАЦІЯМ КОНТРОЛЮ ЦІЛІСНОСТІ ПОТОКУ ВИКОНАННЯ


В.М. Дудуладенко, М.І. Ільїн
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"
dudуladenko.volodymyr@lll.kpi.ua, m.ilin@kpi.ua



Розглянуто програмну реалізацію непрямого відстеження гілок (indirect branch tracking) системи контролю цілісності потоку виконання (control-flow integrity). Показано способи протидії.



**Ключові слова:** переповнення стекового буферу, зворотно-орієнтоване програмування (ROP), контроль цілісності потоку виконання (CFI).

## Вступ

У 1996 році в американському журналі Phrack вийшла стаття під назвою «Руйнування стеку для розваги та прибутку» («Smashing The Stack For Fun And Profit») за авторством Aleph One, яка була першою в історії статтею з детальним описом вразливості переповнення буфера. Якщо виявити помилку переповнення буфера стека, використати її для перезапису адреси повернення поточного виклику і повернутися до інструкцій, які були поміщені в буфер як частина корисного навантаження, то таким чином можна досягти виконання довільного коду і отримати доступ до командної оболонки операційної системи [1].

З метою запобігання таким шкідливим діям з'являються різні техніки захисту стеку. У травні 2003-го виходить OpenBSD 3.3, що має реалізацію технології W^X, яка використовуються в процесорах для відокремлення областей віртуального адресного простору призначених або для зберігання даних або для інструкцій процесора. Такі системи захисту виконуваного простору позначають сторінки пам’яті як невиконувані, так що спроба виконати машинний код у цих областях спричиняє виняткову ситуацію та аварійне завершення програми. Microsoft реалізує функції W^X починаючи з Windows XP Service Pack 2 (2004). Захист виконуваного простору в Windows називається «Запобігання виконанню даних» (DEP).

І хоча W^X було розроблено для блокування атак із інжектуванням коду у відкритому вигляді з певних областей пам’яті, зловмисники швидко адаптувалися та замість того, щоб інжектувати все корисне навантаження, вони вдалися до повторного використання малих фрагментів коду зі сторінок пам’яті, дозволених на виконання, що називаються ROP гаджетами. Ці фрагменти коду беруться з уже існуючого коду в цільовій програмі та об’єднуються разом, щоб вибудувати бажане корисне навантаження зловмисника або просто вимкнути запобіжний механім W^X на певній сторінці пам'яті, щоб дозволити виконувати існуючі корисні навантаження коду. З моменту свого детального опису в 2005 році в роботі Себастьяна Крахмера зворотно-орієнтоване програмування (ROP) було переважаючим способом обходу W^X механізму під час експлуатації пошкодження пам’яті [2].

З метою блокування ROP атак, було запропоновано низку рішень з контролю цілісності потоку виконання (CFI), що

намалювало похмуру картину майбутнього для розробників експлойтів та їхньої залежності від методів на основі ROP. Однак у 2015 році в статті Фелікса Шустера Counterfeit Object-oriented Programming (COOP) було сформульовано нову техніку повторного використання коду, яка демонструвала подолання певних функцій CFI [3]. Враховуючи це компанія Intel розробила нову апаратну систему контролю цілісності потоку виконання під назвою Control Enforcement Technology (CET), яка вперше була поставлена в системах Windows лише у 2020-му році з мобільними процесорами Intel Core 11-го покоління Tiger Lake [4]. Таким чином на даний момент велика кількість користувачів, що не володіє сучасними версіями процесорів потребує використання програмних реалізацій CFI, що актуалізує розробку методів атак на ці програмні реалізації.

## Програмна реалізація CFI та методи протидії

Головна ідея програмної реалізації механізму непрямого відстеження гілок системи контролю цілісності потоку виконання полягає в перевірці значення вказівника функції, що викликається. Це значення повинне бути рівним операційному коду інструкції endbr64. На мові С для досягнення такої поведінки слід визначити директиву CFI(f) яка буде здійснювати перевірку за допомогою вбудованої функції __builtin_bswap32() та викликатиме цільову функцію у позитивному випадку або ж спричинятиме анормальний вихід з програми викликаючи __builtin_trap().

```
#define INSN_ENDBR64 (0xF30F1EFA) /* endbr64 */
#define CFI(f)                                          \
  ({                                                    \
    if (__builtin_bswap32(*(uint32_t*)(f)) != INSN_ENDBR64) \
      __builtin_trap();                                 \
    (f);                                                \
  })
```

Рисунок 1 – Директива визначення CFI

Таким чином, якщо код експлойту захоплює потік виконання в програмі та змушує його перейти на ROP гаджет визначений зловмисником, це буде виявлено і програму буде аварійно завершено.

Однак обмеження, що накладаються захисним механізмом CFI не є вичерпними. Залишається можливість використовувати віртуальні функції, що присутні в цільовій програмі або в завантажених бібліотеках. Непов'язані між собою, вони не можуть бути визначеними як такі, що становлять загрозу, проте запис бажаних значень у пам'яті і об'єднання їх за допомогою викликів цих віртуальних функцій може призвести до обходу CFI.

Кожна віртуальна функція має відповідати за виконання невеликого завдання. Подібно до ROP, функції можуть виконувати такі завдання, як заповнення значення в регістрі. Згруповані разом, кілька функцій можуть виконувати більш складні операції. Водночас функції вибираються з пулу CFI-легальних функцій, тож їх виконання не буде заблоковано CFI, коли буде здійснюватися несанкціонований виклик однієї з них.

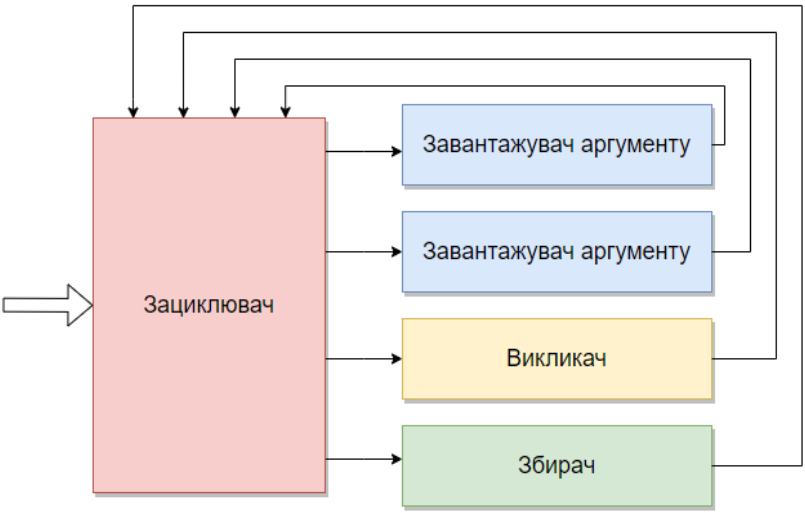



Рисунок 2 – Схема роботи методу

Першим кроком методики є знаходження базової функції, яка виконуватиме основну задачу створення циклу. Цей зациклювач повинен одна за одною викликати інші функції, що мають свої специфічні задачі. Такими задачами є завантаження аргументів, виклик функції та збір аргументів. Завантажувач аргументів заповнює певний регістр, записуючи в нього значення. Після

заповнення регістрів одним або декількома завантажувачами керування передається викликачу, щоб виконати певну функцію. Збирачі – це функції, які отримують значення з регістру і зберігають його у цільовій адресі пам'яті.

Зібравши повне корисне навантаження в дозволений спосіб з'являється можливість обходу CFI.

## Висновки

Контроль цілісності потоку виконання це ще один потужний захисний механізм, який безсумнівно підвищує проблематичність розробки експлойтів. Однак незважаючи на високу складність цього заходу безпеки знаходяться шляхи атак, які можуть бути використані для його обходу.

Представлена програмна реалізація CFI унеможливлює використання техніки зворотно-орієнтованого програмування застосовуючи непряме відстеження гілок. Проте можливість утворення петлі викликів коректних з точки зору CFI функцій, що поетапно вибудовують в пам'яті шкідливе корисне навантаження створює шлях обходу системи захисту.

На даний момент існує великий простір для інновацій та досліджень, а в найближчому майбутньому очікуються новітні рішення з успішного та ефективного забезпечення надійного захисту і як наслідок новий виток пошуку методів їх обходу.

## Перелік посилань


1. Aleph One, Smashing The Stack For Fun And Profit, 1996, https://inst.eecs.berkeley.edu/~cs161/fa08/papers/stack_smashing.pdf
2. Sebastian Krahmer, x86-64 buffer overflow exploits and the borrowed code chunks exploitation technique, 2005, https://www.researchgate.net/publication/228933148_x86-64_buffer_overflow_exploits_and_the_borrowed_code_chunks_exploitation_technique
3. Felix Schuster, Counterfeit Object-oriented Programming, 2015, https://www.researchgate.net/publication/283121202_Counterfeit_Object-oriented_Programming_On_the_Difficulty_of_Preventing_Code_Reuse_Attacks_in_C_Applications
4. A Technical Look at Intel's Control-flow Enforcement Technology

https://www.intel.com/content/www/us/en/developer/articles/technical/technical-look-control-flow-enforcement-technology.html

# СЕМАНТИЗАЦІЯ ПОШУКУ – ТРИВИМІРНА МОДЕЛЬ СПІВСТАВЛЕННЯ ПІДХОДІВ

Ю.В. Рогушина
Інститут програмних систем НАНУ, Київ, Україна
ladamandraka2010@gmail.com

Проаналізовано існуючі підходи до семантизації інформаційно-пошукових систем. Запропоновано тривимірна модель співставлення пошуку, яка базується на аналізі подання пошукових запитів, вимог до результатів пошуку та властивостей масивів даних, серед яких здійснюється пошук.
**Ключові слова:** семантичний пошук, онтологія.

## Вступ

Класичні інформаційно-пошукові системи (ІПС) отримують вхідні дані у вигляді запиту користувача, що подається як список ключових слів, а в якості вихідних даних генерують впорядкований список документів, що релевантні цим ключовим словам. В процесі семантизації пошуку забезпечуються додаткові можливості як для подання та автоматизованого вдосконалення запиту, так і для здобуття з результатів пошуку тих відомостей, що цікавлять користувачів. Крім того, розширюється спектр тих інформаційних ресурсів (ІР), серед яких здійснюється пошук.

## Складові пошуку

У найбільш загальному вигляді пошук складається з трьох складових:

- запиту користувача q, що відображає його інформаційну потребу;
- масиву даних I, в яких здійснюється пошук;
- результатів пошуку R – тієї інформації, яку отримує користувач внаслідок виконання пошукової процедури.

В такому випадку пошук можна розглядати як функцію $R = S(q, I)$, таку, що $R \subseteq I$.

*Семантичний пошук* (СП) – термін, який використовують для позначення набору методів, що призначені для покращення пошуку у документах або у базі знань [1]. На відміну від традиційних методів пошуку, які зосереджуються на ранжуванні документів на основі набору ключових слів (як у запиті користувача, так і в індексованому контенті), методи СП спрямовані на те, щоб враховувати контекст і семантику як запиту користувача, так і тих ресурсів, в яких здійснюється пошук, за допомогою використання засобів обробки природної мови (ПМ), онтологічного аналізу [2], технологій Semantic Web [3] та методів машинного навчання для отримання більш релевантних результатів.

Семантичний пошук є одним з підтипів інформаційного пошуку $R_{sem} \subseteq R$, який має ті самі складові, але доповнюється використанням зовнішніх джерел знань K та методами їх застосування у пошуковому процесі: $R_{sem} = S_{sem}(q, I, K)$.

Можна виділити наступні типи запитів q, що обробляються в ІПС: 1. набори ключових слів (що безпосередньо вводяться користувачами чи будуються на основі таких запитів за допомогою різних методів розширення); 2. ПМ-запити, в яких значення має також порядок слів та їх форми (в ІПС такі запити також перетворюються на набори ключових слів, але вибір ПМ та методи перетворення значним чином впливають на результати пошуку); 3. структуровані запити, в яких явно описані логічні відношення (диз'юнкція, кон'юнкція, заперечення тощо) між термінами та умови щодо властивостей.

Набори ІР I, серед яких здійснюється пошук різними ІПС, різняться [4]: 1. моделями подання інформації; 2. рівнем структурованості контенту; 3. ступенем розподіленості; 4. обсягом. Важливою умовою пошуку є відкритість даних.

Результати запитів R можна класифікувати на: бінарні відповіді щодо наявності потрібної інформації; кількісні; посилання на документи, які відповідають умовам запиту; посилання на інформаційні об'єкти; обрані відповідно до умов запиту значення властивостей знайдених об'єктів (документів або їх елементів), які визначені користувачем; більш складні результати обробки таких знайдених значень властивостей тощо.

Кожна ІПС (або пошуковий сервіс) характеризується певною непорожньою множиною у цих трьох вимірах, розміри та точність визначення якої залежать від набору пошукових функцій, які підтримує система. Важливою особливістю запропонованої моделі є те, що вона використовує лише ті характеристики ІПС, які можуть бути проаналізовані користувачами (слід вважати, що алгоритми, які використовуються в ІПС для співставлення запитів та ресурсів, доступні тільки розробникам цих систем, а їх наявні описи – приміром, в наукових публікаціях або в документації – можуть значно відрізнятися від використаних у поточній версії програмної реалізації). В процесі семантизації пошуку знання з K можуть використовуватися як для вдосконалення самих q, I та R окремо (наприклад, нормалізація слів у запиті або переклад результату), так і у методах, що підтримують пошукову процедуру (наприклад, онтологічні міри семантичної близькості між поняттями ПрО), але запропонована модель дозволяє явно визначити сферу їх застосування.

## Висновки

Запропонована тривимірна модель семантичного пошуку пропонується як додатковий інструмент опису та співставлення пошукових систем, що використовують різноманітні лементи штучного інтелекту та менеджменту знань для більш ефективного та пертинентного задоволення інформаційних потреб користувачів. Самі методи виконання співставлення між запитами та IP в цій моделі не аналізуються, тому що це співставлення є наступним кроком виконання пошуку. Потрібно відмітити, що значення параметрів, які аналізує ця модель, не є взаємно виключними, тобто та сама ІПС може підтримувати кілька варіантів пошуку. Крім того, засоби подання запитів та ресурсів не завжди є порівнюваними (наприклад, структуровані дані, що описуються різними схемами метаданих, можуть бути орієнтовані на різні типи задач та відображати різні аспекти даних, але при цьому одна схема не є повнішою але виразнішою за іншу). Так саме, різні способи фільтрації та подання результатів мають відповідати різним потребам і не завжди можуть порівнюватися за виразністю (наприклад, можливість візуалізації отриманих значень у вигляді графіку не може бути порівняна з можливістю виконання логічних або арифметичних операцій над цими значеннями), але наявність самих критеріїв

порівняння та розширений набір їх параметрів надає більш зручний апарат для вибору відповідної ІПС.

Таким чином, така модель дозволяє виявляти ІПС, для яких перетинаються тріади "запит-ІР-результат" та виконувати їх порівняння саме на цих підкласах пошукових задач. Це дозволяє визначати, які алгоритми пошуку виявляються більш пертинентними для конкретних задач користувачів і на основі цього обирати такі сервіси як джерело інформації для подальшої обробки.

## Список посилань


1. Рогушина Ю. В. (2015) Семантичний пошук у Web на основі онтологій: розробка моделей, засобів і методів. – Мелітополь: МДПУ ім. Богдана Хмельницького, . – 291 с. ISBN 978-617-7346-28-8.
2. Asim, M. N., Wasim, M., Khan, M. U. G., Mahmood, N., Mahmood, W. (2019). The use of ontology in retrieval: a study on textual, multilingual, and multimedia retrieval. IEEE Access, 7, 21662-21686.
3. Hitzler, P., Krotzsch, M., Rudolph, S. (2009). Foundations of semantic web technologies. CRC press.
4. Rogushina J., Grishanova I. (2023) Semantic Information Resources with a Complex Structure: Knowledge Representation, Scaling and Search Problems. In: Scientific and Practical Programming – UkrPROG-2022, CEUR Vol-3501, pp.158-171.


# ЗАСТОСУВАННЯ ОНТОЛОГІЧНО-ОРІЄНТОВАНОЇ СТРУКТУРИ ОБМІНУ ДАНИМИ ТА ДЕЦЕНТРАЛІЗОВАНОГО КЕРУВАННЯ РОЄМ БПЛА


А.Я. Гладун, К.О. Хала
Міжнародний науково-навчальний центр інформаційних технологій та систем НАНУ та МОНУ, Київ, Україна
glanat@yahoo.com, cecerongreat@ukr.net



БпЛА все частіше застосовують як рої або групи, щоб вони відповідали вищим вимогам місії. Обмін даними відіграє важливу роль у керуванні, контролі та координації рою БпЛА. Тому пропонується семантичний підхід до

створення системи обміну даними рою, що забезпечує вищий рівень автономності, надійності та безпеки рою за рахунок застосування онтологічно-орієнтованої структури та бездротової мережі.
**Ключові слова:** рій БпЛА; онтологія, автономна система; автономний БпЛА.

## Вступ

БпЛА набули широкого застосування у військовій сфері, сільському господарстві, пошуково-рятувальних завданнях, для обміну даними, фотографування, дистанційного моніторингу, 3D-картографування тощо. Більш важливіше застосування мають рої БпЛА, які можуть подолати обмеження, з якими стикаються окремі БпЛА як енерговитрати, відстань для обміну даними та зона видимості. Крім того, переваги рою враховують економію часу, скорочення людино-годин, скорочення робочої сили та скорочення інших пов'язаних витрат. Також, їх можна розділити на групи та оснастити різними сенсорами для виконання більш різноманітних завдань та досягнення більших масштабів.

## Розробка онтолого-орієнтованої структури рою БпЛА

Загалом не існує точного визначення рою, але базуючись на дослідженнях та пропозиціях інших авторів можна визначити найбільш загальні ознаки. Розглянемо визначення рою зі словника Мерріама-Вебера: «велика кількість живих або неживих речей, згрупованих разом і зазвичай у русі». У природі прикладами ройової поведінки є бджоли, що координують роботу один з одним для виконання завдань, критичних для їх виживання, або густа зграя шпаків, які реагують на раптову загрозу (яструб) і маневрує як єдиний організм.

Подібним чином, рій БпЛА – це скоординована одиниця БпЛА, яка виконує завдання або набір завдань, щоб отримати значний або бажаний результат [1]. Рій БпЛА — це кіберфізична система. Рій технічно називається групою БпЛА, керованих штучним інтелектом [2]. Однак, рій не слід плутати з групою БПЛА, які літають разом і діють окремо, автономно [3].

Основні ключові вимоги до класифікації безпілотної літальної системи як рою є: 1) кількість БпЛА у місії $\geq 3$; 2) взаємний обмін даними між БпЛА–БпЛА або БпЛА–станцією керування; 3)

автоматичне або автономне планування місії для більш ніж ≥ 3 БпЛА [3].

Надзвичайно важливим в середовищі рою БпЛА є автономне керування багатьма БпЛА у за ефективний та безпечний спосіб. Рівень автономності залежить від кількості завдань, координації або прийняття рішень, які БпЛА може виконати без участі оператора. Було запропоновано п'ять рівнів автономності керування БпЛА [4], де найвищий рівень автономності рою БпЛА визначають як здатність виконувати завдання, скоординовано декількома БпЛА без втручання людини-оператора. Рух і виконання завдань традиційно керованого БпЛА повністю контролюється рішеннями, які приймає людина, тоді як у повністю автономній системі рішення приймаються алгоритмами. Структура прийняття рішень рою БпЛА відповідає парадигмі прийняття рішень автономної системи, визначеній трьома етапами: дані (сенсори), контроль (сприйняття та планування) і процес (прийняття рішення).

Найпоширенішим алгоритмом для контролю, керування та планування роїв БпЛА є варіації та адаптації оптимізації методу рою частинок. Проте використання методів динамічного програмування для оптимізації траєкторії, а також впровадження алгоритмів бджолиних колоній для оптимізованого планування траєкторії та координації між БПЛА дає кращий результат для автономності та надійності архітектури рою БпЛА.

У [5] запропоновано використання мобільної бездротовій мережі Ad-hoc для координації обміну даними між усіма БпЛА в мережі. Група БпЛА взаємодіє один з одним без точки доступу, але принаймні один із них підключено до наземної станції керування або супутника, що дає змогу БпЛА виконувати свої місії без втручання людини. Бездротова спеціальна мережа не покладається на існуючу інфраструктуру для встановлення мережі. Для однорангової мережі не потрібні маршрутизатори чи точки доступу, натомість вузли динамічно призначаються та перепризначаються на основі динамічних алгоритмів маршрутизації.

## Використання онтології предметної області в структурі БпЛА

Для досягнення вищого рівня автономності БпЛА та підвищення надійності та безпеки, пропонується архітектура рою базована на гібридній адаптованій мережі з застосуванням

інфраструктури з онтологією автономного рою та мобільної бездротової мережі. Де інфраструктура з онтологією рою застосовується для пересилання даних. Тоді як адаптована бездротова мережа забезпечить надійний обмін даними та розподілене прийняття рішень.

Ройові архітектури базовані на інфраструктурі мають переваги в проведенні оптимізації та обчислень в режимі реального часу та відсутності необхідності мережа між БпЛА, що зменшує корисне навантаження. Проте так архітектура залежать від наземної станції керування для координації всіх БпЛА та вимагає їх позиціонування в радіусі поширення свого сигналу, що унеможливлює резервування системи та підвищує вразливість до перешкод. У разі атаки або збою наземної станції працездатність усього рою порушується.

Онтологію будемо розглядати як підхід до представлення знань, що відображає концепції з їх властивостями та відношеннями, а також обмеження та правила, що регулюють ці властивості та відношення. Для автономного рою БпЛА онтологія поєднує рішення та інші характеристики, очікувані від людей, з технічними характеристиками у формі формальних моделей і структурних рамок. Автономний рій БпЛА має характеристики, де індивіди дотримуються простих правил поведінки або логічних правил, і можуть стимулювати колективну поведінку за допомогою механізму децентралізованої координації. Однак, відношення між поведінкою рою загалом і поведінкою окремої особи має бути ефективно представлений в онтології. Онтологія для рою БпЛА створює загальну концептуалізацію для контроль життєвого циклу відповідно до сценаріїв місій, та дає змогу прогнозувати та перевіряти поведінку як рою загалом, так і окремих осіб.

## Висновки

Перевагами запропонованої архітектури є широкий діапазон, на якому БпЛА можуть обмінюватися даними, високий рівень автономії з корисним навантаження БпЛА, що містить обчислювальну потужність, достатню для координації рішень на основі даних телеметрії в реальному часі, отриманих від усіх залучених БпЛА. Запропонована архітектура рою дає змогу розподілено приймати рішення на основі формальної логіки, машинного навчання та інших алгоритмів розподіленого керування. Розробка автономних роїв із можливістю взаємодії та

координації між БпЛА є основою для підвищення ефективності роїв БПЛА.

### Перелік посилань


1. Bürkle, A., Segor, F., and Kollmann, M. 2011. Towards autonomous micro UAV swarms. J. Intell. Rob. Syst. 61(1): 339–353. doi: 10.1007/s10846-010-9492-x.
2. Mitch C, Prakash R, Saleh F. UAV swarm communication and control architectures: a review. Journal of Unmanned Vehicle Systems. 7(2): 93-106, https://doi.org/10.1139/juvs-2018-0009, 2018
2. Argel A. Bandala, Elmer P. Dadios, Ryan Rhay P. Vicerra, and Laurence A. Gan Lim, Swarming Algorithm for Unmanned Aerial Vehicle (UAV) Quadrotors – Swarm Behavior for Aggregation, Foraging, Formation, and Tracking, Journal of Advanced Computational Intelligence and Intelligent Informatics Vol.18 No.5, 2014. DOI: 10.20965/jaciii.2014.p0745, 2014
3. Roberts-Grey, C. 2015. The five levels of autonomous vehicles. Available from https://www.trucks.com/2015/09/30/ five-levels-autonomous-vehicles/ [accessed 3 July 2018].
4. Bekmezci, I., Sahingoz, O.K., and Temel, Ş. 2013. Flying Ad-Hoc Networks (FANETs): A survey. Ad Hoc Networks, 11(3): 1254–1270. doi: 10.1016/j.adhoc.2012.12.004.


## РОБАСТНИЙ МЕТОД ОЦІНКИ ВАГОВИХ КОЕФІЦІЄНТІВ ДЛЯ БАГАТОКРИТЕРІАЛЬНОЇ ТЕОРІЇ КОРИСНОСТІ


В.І. Полуциганова, С.А.Смирнов
НТУУ «КПІ ім. І. Сікорського», Київ, Україна
medvika@ukr.net, sergsmr@ukr.net



В багатокритеріальній теорій корисності вигляд самої функції корисності трактується лише як мультиплікативний чи адитивний. При цьому експертні методи не дають точної оцінки вагових коефіцієнтів. В даній роботі наведено метод корекції вагових коефіцієнтів та зведення загального вигляду функції корисності до

адитивного вигляду з робастними оцінками вагових коефіцієнтів.

**Ключові слова:** багатокритеріальна теорія корисності, вагові коефіцієнти, експертні методи

## Вступ

В теорії прийняття рішень варіанти вибору прийнято називати альтернативами. Альтернативи - невід'ємна частина проблеми прийняття рішень: для постановки задачі прийняття рішень необхідно мати хоча б дві альтернативи. Якість вибору оцінюється за допомогою критеріїв, і якщо їх декілька, вибір стає неочевидним. У більшості випадків багатокритеріальні задачі розв'язуються шляхом переходу до однокритеріальної на основі побудови узагальненого критерію.

Найбільш обгрунтований підхід до конструювання узагальненого критерію пропонує багатокритеріальна теорія корисності (MAUT — multi-attribute utility theory). Основи підходу MAUT відрізняють такі особливості:

1) багатокритеріальна функція корисності (БФК) має аксіоматичне обґрунтування;

2) умови, що визначають вигляд цієї функції, піддаються перевірці в діалозі з експертами;

3) залежність між оцінками альтернатив за критеріями та загальною якістю альтернативи;

4) скалярна оцінка якості наявних альтернатив і вибір найкращої.

Приклади побудови БФК для практичних ситуацій наведені в [2].

Якщо спеціальні аксіоми незалежності для критеріїв виконані, то з цього випливає суворий висновок про існування багатокритеріальної функції корисності у певному вигляді. За теоремою Р. Кіні [3], якщо умови незалежності за втратами та незалежності за перевагою виконані, то функція корисності є адитивною:

$$U(x) = \sum_{i=1}^{N} w_i U_i(x)$$

при $\sum_{i=1}^{N} w_i = 1$, або мультиплікативною:

$$1 + kU(x) = \prod_i \left(1 + kw_i U_i(x)\right)$$

При $\sum_{i=1}^{N} w_i \neq 1$, де

- $U$, $U_i$ - функції корисності, що змінюються від 0 до 1;
- $w_i$- коефіцієнти важливості (ваги) вразливості,

причому $0 < w_i < 1$;

- коефіцієнт $k$>-1.

Таким чином, багатокритеріальну функцію втрат можна визначити, якщо відомі значення коефіцієнтів $w_i$, $k$ а також однокритеріальні функції втрат $U_i(x)$, що будуються за окремими критеріями на попередньому етапі процедури MAUT.

## Постановка задачі

В реальних умовах очікувати від експертів надання оцінок ваг однокритеріальних функцій корисності з неробастною умовою, що їх сума дорівнює одиниці не доводиться. Навіть якщо ця умова виконується, нема гарантії що це не є наслідком помилок. До того ж відповідно до процедури MAUT відповіді експертів дозволяють отримати оцінки відношення вагових коефіцієнтів з певними неточностями, тому є сенс шукати процедуру обчислення, що забезпечить отримання нормованих та робастних оцінок ваг.

Розв'язання такої задачі коригування неточних оцінок дозволяє більш точно та обґрунтовано побудувати БФК та зменшити вплив суб'єктивних помилок експертів.

## Метод уточнення оцінок коефіцієнтів

Хоча теорема Кіні дає змогу формувати функцію корисності як мультиплікативну, але це лише знецінює адитивну форму як таку що реалізується у виключної ситуації, отже, за наявності помилок оцінок не може вважатися надійною. Тому хотілось би побудувати точніші оцінки, відкориговані аналітичним шляхом, але опираючись на наявні. Нехай ми шукаємо точні оцінки $w_i$, але експерт надає нам свої суб'єктивні оцінки співвідношення ваг однокритеріальних функцій корисності, тобто $w_i/w_j \approx \alpha_{ij}$, але при цьому $\prod \alpha_{ij} \neq 1$. Нам потрібно щоб цей добуток оцінок дорівнював 1. Визначимо точні відношення ваг як $\frac{w_i}{w_j} = \beta_{ij}$.

Для побудови оцінок вагових коефіцієнтів використаємо метод найменших квадратів з додатковою умовою нормування:

$$\begin{cases} \sum_{i=1}^{n} w_i = 1 \\ 0 < w_i < 1 \\ \sum (\frac{w_i}{w_j} - \alpha_{ij})^2 \to min \end{cases}$$

Для розв'язання цієї задачі використовуємо метод Лагранжа та отримуємо загальний вигляд рішення:

$$\beta_{ij}^{1,2} = \frac{1}{2}(\alpha_{ij} \pm \sqrt{{\alpha_{ij}}^2 + 4\mu})$$

Розглядаються два випадки:

А) $\prod \alpha_{ij} > 1, \beta_{ij} < \alpha_{ij} \Rightarrow \mu < 0$ (2);

Б) $\prod \alpha_{ij} < 1, \beta_{ij} > \alpha_{ij} \Rightarrow \mu > 0$ (3).

В обох випадках для рішення квадратного рівняння обираємо варіант зі знаком плюс, адже він буде набагато ближчий до $\alpha_{ij}$, аніж варіант з мінусом, а за постановкою задачі ми намагаємося відкоригувати аналітично наявні оцінки, а не жорстко виправляти їх. Тоді:

$$\prod \beta_{ij} = \prod \left(\alpha_{ij} + \sqrt{{\alpha_{ij}}^2 + 4\mu}\right) = 2^n$$

де $n$ – кількість множників. Двійка отримується від коренів квадратичного рівняння відносно $\beta_{ij}$.

Отже, при відомих $\alpha_{ij}$, попереднє рівняння хоч і виглядає складним, але містить лише одну невідому $\mu$ і може бути легко розв'язано чисельно на комп'ютері. Ваги $w_i$ однозначно виражаються через знайдене $\mu$.

## Висновки

Розроблений метод дозволяє уточнити отримані від експертів оцінки вагових коефіцієнтів та гарантувати саме адитивний вигляд БФК. Оскільки умова нормування вагових коефіцієнтів сама по собі є достатньо умовною, як прояв суб'єктивної домовленості, пропонована процедура, на наш погляд, додає надійності та об'єктивності методу MAUT.

## Перелік посилань

1. Багатокритеріальні системи підтримки прийняття рішень. *Підручники для студентів онлайн*.

URL: https://stud.com.ua/154786/informatika/bagatokriterialni_sistem i_pidtrimki_priynyattya_rishen
(дата звернення: 21.11.2023).
2. Keeney R. L. Siting energy facilities. New York, N.Y : Academic Press, 1980. 413 p.
3. Keeney R. L. Decisions with multiple objectives: preferences and value tradeoffs. Cambridge [England] : Cambridge University Press, 1993. 569 p.

## CONSTRUCTION OPTIMIZING OF SEARCH AND DATA PROCESSING SCENARIO BASED ON A GRAPHICAL MODEL

Oleksandr V. Koval [1], Valeriy O. Kuzminykh [1], Iryna I. Husyeva [1], Xu Beibei [2] and Zhu Shiwei[2]
[1] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, 03056, Ukraine
[2] Information Research Institute of Shandong Academy of Sciences, Jinan, 250316, China
avkovalgm@gmail.com, vakuz0202@gmail.com, iguseva@yahoo.com, xubeibei1987@163.com, zhusw@sdas.org

The problem of choosing the optimal scenarios for analytical activities based on comprehensive information from a set of acceptable scenarios in terms of quality and efficiency is considered. An approach using a graphical model is proposed. This approach makes it possible to significantly simplify analytical activities using typical scenarios for optimizing those activities.
**Keywords:** analytical activities, graphical model, optimization

### Introduction

When describing ontologies to solve the problems of choosing the optimal scenarios from a set of acceptable scenarios in terms of quality and efficiency, a method of description based on graphs is commonly used. As a rule, it is most appropriate to use a description in the form of hierarchical graphs. For such graphs, cost estimates are used, both for the information processing related to actions in individual nodes of the graph, and cost estimates for the actions (edges) when moving between nodes. It allows to sum up the costs of

each possible path according to the scenario or a separate fragment of this path for comparison and determination of the most efficient paths included in the description of the selected scenario.

Currently, there are many methods for selecting efficient scenarios from a set of acceptable ones, which are built on the basis of a corresponding ontology, and for analysis of the nature and composition of factors that can influence the process of scenario planning and execution. In practice, the planning and implementation of the scenario determines the features of the paths which distinguish one or another scenario by factors that depend on the values of the criteria on the basis of which decisions are made and the procedures for forming the necessary scenarios are determined. One of rather complicated and currently relevant tasks that require the construction of efficient scenarios for its solution is the task of construction and further optimization of scenarios for conducting analytical activities based on comprehensive information. The task of optimizing scenarios for collecting streaming information for conducting analytical work based on comprehensive information is one of the most important tasks for processing big volumes of data [1].

## Graphical model

Any ontology can be represented as a graph, where the nodes determine certain knowledge of the subject area, and the edges reflect the sequence of user actions to achieve the research goal. Permanent hierarchical connections of the type "part and whole" and "class and subclass" at the same time determine the structure of actions and the related knowledge structure of the subject area. Such model can be built using approaches based on the product of the graph describing the hierarchy of the data storage structure or the knowledge structure of the subject area, and the graph describing the hierarchy of possible actions (methods) related to data processing [2].

The knowledge structure of the subject area can be presented in the form of a graph adjacency matrix $G = (V_1, E_1)$, where $V_1 = \{v_1, v_2, ..., v_n\}$ is a set of nodes and $E_1 = \{e_1, e_2, ..., e_m\}$ is a set of edges.

The structure of procedures for possible actions is presented in the form of a graph adjacency matrix $H = (V_2, E_2)$, where $V_2 = \{v'_1, v'_2, ..., v'_n\}$ is a set of nodes and $E_1 = \{e_1, e_2, ..., e_m\}$ is a set of edges.

For further scenarios construction, it is necessary to build a graphical model which combines the hierarchy of the knowledge structure of the subject area and the hierarchy of possible processing actions. This model is presented in the form of a graph *J (V,E)= G* x *H*, which is constructed based on the Cartesian product of graphs [3]. It is done based on the following correlation: $V = V_1 \times V_2$.

This model, built on the basis of Cartesian product of graphs, differs from the existing ones as it combines the hierarchy of knowledge structures and possible actions that are characteristic of this analytical process.

This allows to build various data processing scenarios; optimize possible scenarios; provide the analyst with information about possible alternative solutions; increase the reliability of the search for optimal analytical solutions in the hierarchical analysis of information that determines the necessary knowledge.

The efficiency assessment of the search for the graph optimal path can be defined as a cumulative assessment of the costs of work on each of the nodes and an assessment of the costs of transition to the next node moving from the initial node to the final node with the determination of possible transition paths.

Without reducing the degree of generality, the model, which considers the costs associated with both the aggregate estimate of the costs of work for each node, and the estimate of the costs of moving to the next node in the process of transition from the initial node to the final one, can be considered as a model taking into account only costs on the edges of the graph.

With doing so, the costs in the nodes will be included in the costs of the edges of the graph:

$$P_{ij} = t_j + r_j + T_{ij} + R_{ij} \quad , \quad i,j \in K.$$

$t_k$ – time spent on each of *k* nodes, corresponding to the selected path on the graph; $r_k$ – resources spent on each of *k* nodes, corresponding to the selected path on the graph; $k \in K$ – node numbers of the selected path on the graph; $T_{ij}$ – time spent on each of *ij* edges of the graph corresponding to the selected path on the graph; $R_{ij}$ – resources spent on each of *ij* edges of the graph corresponding to the selected path on the graph; $i,j \in K$ – node numbers of the selected path on the graph.

So the task of building the optimal scenario based on the evaluation of its efficiency can be considered as the task of finding the

graph shortest path, taking into account the costs at each step.

The sequence of actions for evaluating the quality of modelling of the information analysis scenario can be stated as follows:

1. Selection of corresponding quality functions on the lower layer of the nodes of the graph.
2. Analysis of connections between selected nodes and the nodes of the next level, which are located higher in the model hierarchy.
3. Saving the edges corresponding to the found connections for further analysis and use in search operations.
4. Iterating until reaching the search source at the top level.
5. Consolidation of all the collected edges and nodes of the graph, which is built on the basis of the quality function, considered as a request for information search.
6. Ordering of all paths along the constant graph according to the quality function.
7. Analysis of the scenario model based on the selection of the shortest paths with the minimum number of edges on the graph.

## Conclusions

The test results show that the approach to scenario optimization based on graphical description using typical scenarios can significantly reduce the complexity and costs of constructing new scenarios, which are more efficient according to the specified criteria. This makes it possible to significantly simplify analytical activities using typical scenarios for its optimizing.

## References


1. Koval, O.V., Kuzminykh, V.O., Husyeva, I.I., Xu, B., Shiwei, Z. Improving the Efficiency of Typical Scenarios of Analytical Activities CEUR Workshop Proceedings, № 3241, pp. 123-132.2022.
2. Moore, Edward F. “The Shortest Path Through a Maze,” International Symposium on the Theory of Switching, 285–92, 1959.
2. Lee, C Y. “An Algorithm for Path Connections and Its Applications.” IEEE Transactions on Electronic Computers 10, no. 3 (September 1961): 346–65.

# БІОМЕТРИЧНА МОДЕЛЬ КЛАВІАТУРНОГО ПОЧЕРКА КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

В.В. Фесьоха[1], Н.О. Фесьоха[1],
І.Ю. Субач[1,2], А.В. Микитюк, І.В. Горнійчук
[1] Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
[2] Інститут спеціального зв'язку та захисту інформації Національного технічного Університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна
vitaliifesokha@gmail.com, nadiia.fesokha@viti.edu.ua,
igor_subach@ukr.net, mukuta8888@gmail.com,
horniychuk.ivan@gmail.com.

Розглянуто завдання підвищення рівня кіберзахисту інформаційних систем (ІС) сектору критичної інфраструктури від несанкціонованого доступу. Виявлено головний недолік існуючих підходів до автентифікації користувачів – досить вузький підхід до формалізації унікальності користувачів на етапі реєстрації. Запропоновано біометричну модель клавіатурного почерка (КП) користувачів ІС, яка ґрунтується на основі інженерії поведінкових закономірностей із множини досліджуваних ознак КП з подальшим їх описом нечіткими правилами. Передбачено виявлення факту дрейфу значень ознак КП користувачів ІС на основі дивергенції Кульбака-Лейблера з метою своєчасного забезпечення максимальної адаптації біометричної моделі до користувача.
**Ключові слова:** кібербезпека, несанкціонований доступ, автентифікація, поведінкова біометрія, клавіатурний почерк, інформаційні системи, нечітка логіка, дрейф даних.

## Вступ

Існуюча технологічна ескалація у кіберпросторі обумовлює актуальність неперервного підвищення рівня кіберзахисту ІС критичної інфраструктури. Перспективним завданням у контексті зазначеного є організація виявлення фактів несанкціонованого доступу до інформаційних ресурсів ІС, розголошення яких може становити загрозу для національної безпеки держави. Поряд з цим,

існуючі підходи до автентифікації користувачів ІС у процесі керування та розмежування їх доступу не здатні у повній мірі забезпечити належний рівень кіберзахисту ІС, про що свідчать численні факти несанкціонованих втручань [1].

Одним з найбільш ефективних шляхів вирішення даного завдання є застосування методів аналізу поведінкових біометричних характеристик користувачів ІС, зокрема характеристик їх КП, оскільки дозволяють розпізнавати користувачів за їх унікальними підсвідомими сенсорними і руховими навичками, які практично неможливо фальсифікувати [2].

## Біометрична модель клавіатурного почерка користувачів

У переважній більшості досліджень, які присвячені застосуванню методів аналізу поведінкових біометричних характеристик КП користувачів ІС недостатньо уваги приділяється завданням формалізації унікальності (індивідуальних підсвідомих поведінкових рис) користувачів ІС та виявлення факту дрейфу даних їх біометричних моделей КП, що негативно впливає на адекватність даних моделей, і як наслідок не дозволяє здійснювати автентифікацію користувачів ІС із високою достовірністю.

Для усунення недоліку недостатньої формалізації унікальності користувача у роботах [1,3] запропоновано застосування біометричної моделі КП на основі нечіткої логіки, суть якої полягає у визначенні початкового простору ознак КП ($d$ – динаміка друку, $t_s$ – швидкість друку) і формуванні додаткового простору ознак КП на основі виявленої закономірності зі статистичного набору значень тривалості утримання $t_i^r$ клавіш клавіатури під час введення контрольного тексту для кожного персоніфікованого ідентифікатора ІС. Так, здійснюється побудова варіаційної кривої тривалості утримання $t_i^r$ клавіш клавіатури користувачем для подальшої декомпозиції на 10 часових вікон (кількість часових вікон визначено, як середній час введення контрольного тексту (паролю) у більшості відкритих наборах даних). Заключним етапом є формування біометричної моделі КП користувача ІС шляхом опису отриманих ознак КП нечіткими лінгвістичними термами. У відповідності до зазначеного, біометричну модель КП користувача ІС можна представити наступним аналітичним виразом [1]:

$$\mu_{u_i} = (S_{start} = \{d, t_s\} \cup S_{add} = \{t_1^w, \dots, t_{10}^w\}) \rightarrow \{d, t_s, t_1^w, \dots, t_{10}^w\}, \quad (1)$$

де $S_{start}$ – початковий ознаковий простір, $S_{add}$ – додатковий ознаковий простір, $t_i^w$ – часове вікно.

Вибір підходу до аналізу КП користувача ІС на основі контрольного (наперед вивченого, доведеного до автоматизму) тексту обумовлено закономірністю його відтворення близькими значеннями КП. Крива тривалості утримання $t_i^r$ клавіш клавіатури користувачем ІС під час введення контрольного тексту дозволяє описати швидкість її зміни (геометричний сенс диференціювання функцій) нечіткими правилами у часових вікнах $t_{1-10}^w$ (терм-множини: зростання у градусах (високе, середнє, мале); спадання у градусах (високе, середнє, мале)), що у свою чергу дозволяє врахувати певну варіативність значень КП користувача ІС. Так, множина вхідних лінгвістичних змінних нечіткої моделі – ознаковий простір біометричної моделі $\mu_{u_i}$, вихідна лінгвістична змінна – персоніфікований ідентифікатор користувача ІС.

Для своєчасного виявлення дрейфу даних (Data Drift – зміна статистичних властивостей навчальної вибірки) запропонованої біометричної моделі КП, як наслідок зміни значень ознак КП користувачів ІС (з часом швидкість (ритм) набору тексту може зменшуватись (збільшуватись)) у роботі [4] запропоновано застосування дивергенції Кульбака-Лейблера, також відомої як відносна ентропія, яка обчислюється на основі аналітичного виразу (2). Іншими словами – це міра, що дозволяє визначити значення відмінності інформаційної ентропії однієї множини від ентропії іншої множини.

$$KL(P \parallel Q) = P(X)\log(P(x)/P(x)) \quad (2)$$

Так, на основі (2) здійснюється періодичне (не менше одного разу в квартал) обчислення значення відмінності/схожості розподілів навчальної вибірки моделі та накопиченого статистичного набору даних введення контрольного тексту користувачем ІС засобами дивергенції Кульбака-Лейблера з метою реалізації своєчасного донавчання (адаптації) моделі.

## Висновки

Таким чином, запропоновано біометричну модель КП користувачів ІС на основі нечіткої логіки, побудова якої базується на вперше отриманій нечіткій множині ознак КП у результаті декомпозиції знайденої поведінкової закономірності на статистичному наборі введення контрольного тексту, яка описує унікальні поведінкові риси користувачів нечіткими правилами. Застосування даної моделі дозволяє підвищити достовірність процедури автентифікації у процесі керування і розмежування доступу користувачів ІС критичної інфраструктури.

## Перелік посилань


1. Фесьоха В. В., Фесьоха Н. О. Метод регуляризації ознакового простору біометричної моделі клавіатурного почерку користувачів інформаційних систем військового призначення на основі факторного аналізу. Збірник наукових праць ВІТІ ім. Героїв Крут. Київ. 2023. № 3. СА. 152–162.
2. Фесьоха В. В., Фесьоха Н. О. Аналіз існуючих рішень автентифікації користувачів інформаційних систем та мереж спеціального призначення. Збірник наукових праць ВІТІ ім. Героїв Крут. Київ. 2020. № 3. С. 129–136.
3. Фесьоха В., Фесьоха Н. Модель нечіткої автентифікації користувачів інформаційних систем органів військового управління на основі поведінкової біометрії. Ukrainian information security research journal. 2021. Т. 23, №2. С. 116–123.
4. Фесьоха Н. О. Визначення необхідності дрейфу даних біометричної моделі клавіатурного почерку користувачів інформаційних систем військового призначення на основі відстані Кульбака-Лейблера. Science and Education in Progress**:** 2nd International Scientific and Practical Conference (Dublin, Ireland, June 16-18, 2023). Україна: Scientific Publishing Center “InterConf”, 2023. С. 353-354.

# КАСКАДНА ОРГАНІЗАЦІЯ УЗАГАЛЬНЕНОЇ ОПТИМІЗАЦІЙНОЇ МОДЕЛІ ВИРОБЛЕННЯ, РОЗПОДІЛУ, ПОСТАЧАННЯ І СПОЖИВАННЯ РЕСУРСІВ

О.Г. Додонов[1], А.І. Кузьмичов[1] , Ю.В. Чернецька[2]
[1]Інститут проблем реєстрації інформації НАНУ, Київ, Україна
[2]Ін-т енергозбереження та енергоменеджменту КПІ ім. Ігоря Сікорського, Київ, Україна
dodonovua@gmail.com, akuzmychov@gmail.com, j.chernetska-iee@lll.kpi.com

Розроблена і досліджена на конкретних прикладах з проблематики вироблення і розподілу обмежених енергоресурсів оптимізаційна модель, із декількох різних за постановкою задач про мережеві потоки, має каскадну організаційну структуру із узагальненою цільовою функцією.
**Ключові слова:** Мережева оптимізація, узагальнені (з витратами) задачі про потоки, каскадна оптимізаційна стратегія.

Специфікою реальної енергетики є комплексне використання певного ресурсу, скажімо, потоків води, у різних спряжених мережевих структурах, відповідно, виникає проблема комплексного розрахунку потоків різних ресурсів з метою дотримання нормальних умов експлуатації енергетичного обладнання та відповідних комунікацій.

Для дослідження цих процесів збудована оптимізаційна модель за каскадною схемою, яка певним чином відповідає каскадній організації системи ресурсного забезпечення відповідних технологій генерації, розподілу і споживання [1]. Мета: досліджувати ситуації, коли з-за дефіциту певних ресурсів чи перевищення норм у вузлах виникає локальна аварійна ситуація, наслідки якої, згідно каскаду, підсилюються з-за вагових характеристик дуг і розповсюджується мережею, набуваючи завищених властивостей складових системи із різних систем [2, 3].

В теорії [4] каскадна стратегія передбачає послідовну структуру відповідних модулів із програм і даних як завершених

фаз чи етапів, бо каскадна модель (waterfall model) імітує спадаючий, без повернення уверх, водний потік, але в проведених нами модельних дослідженнях вдалося реалізувати дещо складніші конструкції, де шукані значення потоків у різних задачах об'єктивно узгоджуються в межах усієї моделі, що наближає узагальнену модель до реальних технологічних процесів.

Згідно [5], практичний досвід реалізації каскадної стратегії побудови складно організованих моделюючих систем змушує застосовувати програмно-технічні комплекси із кількох оптимізаторів, взаємодія яких ускладняється з-за вимушеного використання узгоджуючих баз даних.

У модельних розрахунках, про що йдеться, вдалося скористатися одним оптимізатором, під контроль якого поставлено узгоджену сукупність кількох оптимізаційних задач із їхніми постановками, входами, типами виходів, обмеженнями і цільовими функціями.

У прикладах узагальнена мережева структура складається із технологічних мереж постачання, генерації, розподілу і споживання сировинних та згенерованих енергетичних ресурсів за заданими даними про відповідні пропозиції і попит, кожна складова представлена оптимізаційною моделлю пошуку змінних рішень за відповідними їх типом, обмеженнями і критерієм.


1. Додонов О.Г., Кузьмичов А.І. Мережеві організаційні структури управління. Моделювання та візуалізація засобами Excel. К.: Вид-во Ліра-К, 2021. 297 с.
2. Кузьмичов А.І., Чернецька Ю.В., Шестаков В.А. Пошук і аналіз чутливості часових оптимальних планів постачання енергетичних ресурсів із застосуванням надбудови SolverTable // Реєстрація, зберігання і обробка даних. 2022. Т. 24. № 2. С. 62-71.
3. Martorell S. et al (eds.) Safety, Reliability and Risk Analysis. Theory, Methods and Applications/ 4 volumes. CRC Press, 2009. – 3512 p.
4. Badiru A. Systems Engineering Models. Theory, Methods and Applications. CRC Press, 2019. – 227 p.
5. Patnaik S. A cascade optimization strategy for solution of difficult multidisciplinary design problems/ NASA TM-107189, 1996

# ФОРМУВАННЯ ТА ДОСЛІДЖЕННЯ ДИНАМІЧНИХ МЕРЕЖ ТЕРМІНІВ

О.О. Дмитренко[1,2]
[1] Інститут проблем реєстрації інформації НАН України, Київ, Україна
[2] Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна
dmytrenko.o@gmail.com

У цій роботі досліджується динаміка вагових значень вузлів у мережах термінів, отриманих на основі динамічно-розширюваного текстового корпусу.
**Ключові слова:** динамічно-розширюваний текстовий корпус, мережа термінів, динаміка вагових значень.

## Вступ

Виявлення інформаційних вкидів є важливим компонентом, що впливає на інформаційну безпеку. В цьому дослідженні представлений алгоритм, за результатами роботи якого можна здійснити аналіз динаміки вагових значень вузлів у мережах термінів на основі динамічно-розширюваного текстового корпусу.

***Метою цієї роботи*** є представити новий підхід для аналізу мереж термінів, отриманих на основі динамічно-розширюваного текстового корпусу.

## Алгоритм

Нехай є деякий інформаційний потік $d_i$, $i = \overline{1,N}$, де $N$ – кількість текстових документів. Алгоритм побудови динамічної мережі термінів складається з наступних кроків:

Крок 1. Нехай перший документ $d_1$ у потоці $d_i$ є первинним для певної сукупності текстів $T_i$, що формується ($T_1 = d_1$). Для $T_1$ формується направлена зважена мережа термінів $G_1$, методика якої представлена у роботі [1]. Отримана мережа термінів $G_1$ є первинною мережею, для якої фіксується список ключових термінів та їх вагових значень – *GTF*.

Крок 2. Сукупність текстів $T_i$, отримана на попередньому кроці, розширюється завдяки додаванню наступного документа з потоку $d_i$: $T_{i+1} = T_i + d_i$. В результаті буде отримано нову

сукупність текстів $T_{i+1}$ для якої формується нова направлена зважена мережа термінів $G_{i+1}$ з урахуванням нових вагових значень виокремлених ключових термінів. Для отриманої мережі фіксується новий список ключових термінів та їх оновлених вагових значень – *GTF*.

Крок 3. Крок 2 повторюється, допоки $i \neq N$.

Далі для кожного ключового терміна із зафіксованого на останньому кроці списку ключових термінів будується графік динаміки вагового значення *GTF* окремого терміна в залежності від розширення сукупності текстів $T_i$ на кожному кроці $i = \overline{1, N}$.

## Висновки

Запропонований алгоритм дослідження динаміки вагових значень вузлів у мережі термінів. Цей алгоритм може бути використаний для покращення інформаційної безпеки шляхом виявлення значних змін у вагових значеннях вузлів мережі термінів.

## Літературні джерела


1. Lande, D., & Dmytrenko, O. Creating directed weighted network of terms based on analysis of text corpora. In *2020 IEEE 2nd International Conference on System Analysis & Intelligent Computing (SAIC)* (pp. 1-4). IEEE.


# МОДЕЛЮВАННЯ НАЛАШТУВАННЯ ПІД-РЕГУЛЯТОРА ЗА ДОПОМОГОЮ ГЕНЕТИЧНОГО АЛГОРИТМУ ПО БАГАТОКРИТЕРІАЛЬНІЙ ЦІЛЬОВІЙ ФУНКЦІЇ ДЛЯ КЕРУВАННЯ НЕСТІЙКИМИ ОБ'ЄКТАМИ


Д.П. Кучеров, О.М. Пошивайло, І.В. Мирошниченко
Національний авіаційний університет, м. Київ, Україна
d_kucherov@ukr.net, o.poshyvailo@gmail.com,
ignat.mir@gmail.com



Розглядається задача налаштування регулятора промислового типу, а саме ПІД-регулятора, який має декілька параметрів, а саме коефіцієнти пропорційної, інтегральної та диференційної ланок. В дослідженні ПІД-регулятор застосовується для керування нестійким

об’єктом з нелінійною динамікою. Ставиться задача відстеження вхідного сигналу з мінімальними перерегулюванням, помилкою та часом встановлення. В статті наводяться параметри алгоритму та результати моделювання з використання сучасної техніки моделювання систем автоматичного управління у фазовому просторі.
**Ключові слова**: ПІД-регулятор, генетичний алгоритм, об’єкт управління, цільова функція

## Вступ

У керуючому контурі, який охоплений зворотним зв'язком для підвищення стабільності і точності дії технічної системи, знайшли поширене використання так звані пропорційно-інтегрально-диференціюючі (ПІД) пристрої, які формують потрібний сигнал керування. Вихідний сигнал ПІД-регулятора є сумою трьох доданків. Кожна складова відповідає за компенсацію помилок у статичному (пропорційна та інтегральна складові) та динамічному режимах (наприклад, збурення) перехідного процесу (диференційна складова).

Основною перевагою їх практичного застосування є незалежність від математичної моделі керованого об’єкта. Але при цьому виникає проблема щодо встановлення параметрів регулятора, вирішення якої вимагає тонкого налаштування системи керування в умовах нелінійної математичної моделі керованого об’єкта [1]. Параметри ПІД є незалежними, але зміна одного коефіцієнта завжди впливає на інші, тому завдання налаштування ПІД-регулятора вирішується ітераційно за експериментальними методами, за якими здійснюється перевірка динаміки системи «регулятора-об'єкт управління» [2].

Одним з підходів, що може бути використаним до налаштування системи ПІД-регулятор – об’єкт управління за мінімумом помилки системи керування можуть бути генетичні алгоритми (ГА) [3, 4]. Ці алгоритми зазвичай використовуються в науці та техніці як адаптивні для вирішення практичних завдань. На відміну від традиційних методів стохастичного пошуку, ГА вимагає популяції початкових наближень до рішення [5].

## Особливості реалізації генетичного алгоритму

Налаштування ПІД-регулятора є складним завданням, коефіцієнти якого по-різному впливають на перехідний процес. В

такому разі виникає завдання багатопараметричної оптимізації (наперед невідомих параметрів ПІД-регулятора) для розв'язання багатокритеріальної задачі (одночасного забезпечення показників перехідного процесу), яке не можливо вирішити класичними підходами та стають доречними евристичні методи, до яких відноситься процедура генетичного алгоритму (ГА).

На першому кроці застосування процедури ГА вводиться випадковий хромосомний набір, які пов'язують з параметрами ПІД-регулятора, ефект дії яких на систему надалі оцінюється. Після завершення моделювання маніпулювана змінна автоматично повертається до ГА, а вибраний критерій помилки використовується для оцінки продуктивності та визначення значення придатності цієї хромосоми для подальшого пошуку параметрів ПІД-регулятора, що здатні задовольнити конструктора системи.

Продуктивність ГА оцінюється за цільовою функцією $I$, яка враховує перегулювання, мінімальне значення середнього квадрата помилки (MSE) відпрацювання вхідного завдання і тривалості перехідного процесу, яку можна подати виразом

$$I = \alpha \cdot OS + \beta \cdot MSE + \gamma \cdot T_p,$$

де $OS$ – перерегулювання, $MSE$ (mean squared error) – середній квадрат помилки, $T_p$ – тривалість процесу регулювання, тобто коли вихідна величина у досягне встановленого значення $y_{вст}$. Інші позначення: $y_{\max}$ – максимальне значення вихідної величини; $\alpha$, $\beta$, $\gamma$ – вагові коефіцієнти, що визначають вклад кожного доданку у загальну продуктивність ГА.

Традиційно ГА включає такі етапи: відбір або селекцію, схрещування, мутацію, оцінювання якості отриманого хромосомного набору і, якщо критерій зупинки не задовольняється, процедура ГА повторюється визначену кількість разів.

В розробленому алгоритмі встановлена максимальна кількість генерацій нового покоління $P$. Велика кількість ітерацій призводить до невиправданого зростання часу роботи алгоритму при отриманні повторного результату, що можна трактувати як зациклення у локальному мінімумі.

Після ініціалізації набору хромосом, що складаються з $N$ особин обраних випадковим чином, відбувається селекція. Операція схрещування проводилася за найбільш вдалим для

пошуку оптимуму функції багатьох дійсних змінних принципом арифметичного схрещування.

В алгоритмі використана нерівномірна мутація для *i*-го гена. Мутації підлягають всі хромосоми, які не задовольняють зазначеному рівню цільової функції. На останньому етапі алгоритму відбувається формування нового покоління. Щоб не втратилися найкращі хромосоми, вони гарантовано входять до нової популяції. Зазначена послідовність операцій повторюється, доки алгоритм не буде вважатися збіжним. Дія алгоритму припиняється, якщо буде задоволена визначена продуктивність або, якщо будуть виконано усі призначені генерації поколінь. В останньому випадку обирається хромосомний набір з найкращою продуктивністю.

В прикладі моделювання розглядається нестійкий об'єкт управління, що має двократний нульовий корінь і описується системою диференційних рівнянь першого порядку.

Об'єкт стабілізований ПІД-регулятором. На параметри ПІД-регулятора накладені обмеження у вигляді нижньої та верхньої границі параметрів. На вхід системи подається стандартизований одиничний сигнал у вигляді сходинки, тобто $r(t)=1(t)$.

## Висновок

В доповіді представлено технологію реалізації ГА для налаштування параметрів ПІД-регулятора для нестійкого об'єкта, що має кратні нульові корені характеристичного рівняння. Як цільова функція використана багатопараметрична функція, яка включає перерегулювання, середній квадрат помилки та тривалість перехідного процесу. Загальне підвищення налаштування порівняно з алгоритмом Зіглера-Нікольса складає 6%.

## Перелік посилань


1. Astrom K.J., Hagglund T. PID controllers: theory, design, and tuning. ISA: The Instrumentation, Systems, and Automation Society; USA, 1995. URL: https://www.amazon.com/PID-Controllers-Theory-Design-Tuning/dp/1556175167
2. Kucherov D., Kozub A., Tkachenko V., Rosinska G., Poshyvailo O. PID controller machine learning algorithm applied to the mathematical model of quadrotor lateral motion. IEEE 6th International Conference on Actual Problems of Unmanned Aerial Vehicles Development (APUAVD), 19-21

Oct. 2021, Kyiv, Ukraine, doi:10.1109/APUAVD53804.2021.9615438
2. O'Mahony T., Downing C.J., Fatla K., Genetic Algorithms for PID Parameter Optimisation: Minimising Error Criteria, Conference paper, 2002, p.1-6. URL: https://www.researchgate.net/publication/252840849_Genetic_Algorithms_for_PID_Parameter_Optimisation_Minimising_Error_Criteria
3. Mirzal A., Yoshii S., Furukawa M. PID Parameters Optimization by Using Genetic Algorithm, URL: https://arxiv.org/ftp/arxiv/papers/1204/1204.0885.pdf
4. Субботін С. О., Олійник А. О., Олійник О. О. Неітеративні, еволюційні та мультиагентні методи синтезу нечіткологічних і нейромережних моделей: Монографія / Під заг. ред. С. О. Субботіна. – Запоріжжя: ЗНТУ, 2009. – 375 с.

## FRAMEWORK FOR DETECTING OUTLIER AND UNKNOWN DATABASE INTRUSIONS

Mykhailo V. Kolomytsev, Svitlana O.Nosok, Oksana V.Tsygankova
National Technical University of Ukraine ”Igor Sikorsky Kyiv Politechnic Institute”, Kyiv, Ukraine

This article presents a comprehensive framework designed to detect anomalies in the actions of users of relational databases, and focuses primarily on detecting insider threats. The framework uses a new methodology that employs machine-learning algorithms for reliable and efficient detection. The architecture, parameter selection, and experimental validation of the proposed framework were discussed in detail.

This study solves the critical problem of internal threats that lead to unauthorized access, theft, or modification of information in the database. Anomalies in the time series of user activities, such as unusual spikes or changes in access patterns, are indicators of potential threats.

**Keywords**: Anomaly detection, insider threats, relational databases, Isolation Forest algorithm, information security, machine learning.

**Introduction**. This paper presents a comprehensive framework designed to detect anomalies in the activities of relational database users, with a focus on combating insider threats. The framework combines advanced machine-learning algorithms and a new methodology to provide a reliable solution for evolving database security problems.

**Background and motivation**. The constant threat of insider attacks that lead to unauthorized access, theft, or modification of information in databases necessitates the use of innovative approaches for anomaly detection. The proposed scheme is based on the analysis of time series and allows the use of distinctive characteristics of user activity patterns to detect subtle deviations that may indicate the presence of malicious intent.

**Literature review**. An overview of anomaly detection methods is presented, ranging from traditional statistical methods to modern machine-learning and deep-learning approaches. Particular attention is paid to problems associated with insider threats when anomalous values can be very similar to normal values, which require the use of specialized algorithms. The analysis allowed us to identify the characteristic features of insider activity [1,2], formulate the features of the problem of detecting insider activity [3], and choose the optimal algorithm for searching for anomalies [4].

**Architecture of the proposed framework**. This paper describes in detail the architecture of the proposed framework, including key components, such as data analysis, algorithm selection, and parameter optimization. The Isolation Forest algorithm was chosen because of its efficiency when working with large datasets, low memory requirements, and adaptability to different types of data. The architecture of the framework is illustrated by a logical flowchart that provides a clear idea of the sequential steps involved in the anomaly detection.

**Methodology**. The methodology is described, including data preparation, model training, and the application of the trained model to data validation. Specific steps include loading data into memory, normalization, transformation of categorical features, and splitting data into training and test samples. The parameters of the Isolation Forest algorithm, including the number of trees, tree depth, and sample size, were carefully selected to ensure a balance between the detection quality and computational efficiency.

**Experimental analysis**. An experimental analysis is conducted using the generated datasets to confirm the effectiveness of the

system. The datasets were carefully selected to model realistic scenarios, and they manually included anomalous values. To evaluate the effectiveness of the algorithm in comparison with "real" detected emissions, we used metrics such as the precision, recall, and F1-score. The experimental results confirmed the system's ability to detect anomalous behavior with high accuracy and recall.

**Real-world applicability and customization.** The applicability of the framework to real-world scenarios is discussed, emphasizing the need to adapt it to specific database systems. This article highlights the existing features in popular database management systems, such as the MS SQL Server, which can be used for implementation. Third-party tools for additional customization for specific use cases were also considered.

**Conclusion and future prospects**. In conclusion, the proposed scheme offers a new and effective approach for detecting anomalies in the actions of relational database users, particularly in the context of insider threats. Comprehensive methodology, experimental validation, and architectural solutions significantly contribute to the field of information security. Although the framework shows promising results on benchmark datasets, it is recommended to study its behavior in practical real-world database environments in the future. This framework opens up opportunities for improving database security and is positioned as a valuable tool in ongoing efforts to combat insider threats.


1. D. Vaidya Insider Threat (https://www.wallstreetmojo.com/ insider-threat/ )
2. M. Al-Mhiqani, R. Ahmad A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations. Appl. Sci. 2020, 10(15); DOI:10.3390/app10155208
3. Chandola, V., Banerjee, A., Kumar, V. Anomaly detection: A survey. ACM Computing Surveys (CSUR), 2009, V. 41(3), p. 1-58. DOI: 10.1145/1541880.1541882
4. Liu, F. T., Ting, K. M., & Zhou, Z. H. Isolation forest. Eighth IEEE International Conference on Data Mining, 2008 pp. 413-422.

# ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ НЕТИПІЗОВАНОЇ ОБРОБКИ ІНФОРМАЦІЇ

Максим Коновалюк[1], Олег Дмитренко[1,2]
[1]Національний технічний університет України ―Київський політехнічний інститут імені Ігоря Сікорського, Київ, Україна
[2]Інститут проблем реєстрації інформації Національної академії наук України, Київ, Україна
konovalyuk@gmail.com, dmytrenko.o@gmail.com

У сучасному процесі розробки програмного забезпечення доволі часто постають задачі обробки інформації, яка зберігається у базі даних, такі як операції по збереженню, оновленню та зчитуванню інформації з бази даних, так звані операції Create Read Update Delete (CRUD). В більшості випадків реалізація подібних операцій не потребує суттєвих зусиль від програміста та носить здебільшого рутинний технічний характер, оскільки, функціонал, що реалізується не є оригінальним. Іншими словами, бізнес логіка зазвичай співпадає, відмінність полягає лише у тому, якою інформацією оперують, але розробка подібного функціоналу все рівно потребує часу розробників, тому потребує автоматизації.
**Ключові слова:** Create Read Update Delete (CRUD), Mongo, MongoTemplate, Spring.

## Мета дослідження

Метою дослідження є розробка рішення, що дозволить абстрагуватись від моделі даних та розробити універсальний інструментарій для виконання операцій CRUD, який би не залежав від інформації, якою будуть оперувати, та міг би застосовуватись для оперування різною інформацією. Іншими словами, реалізувати універсальний CRUD, який можна було б застосовувати для різних моделей даних та не витрачати час Back End розробників на однотипну роботу.

## Дослідження та розробка

Розглянемо середовище зберігання інформації, а саме бази даних. Реляційні бази даних представляють інформацію у вигляді таблиці. Кожна таблиця складається з фіксованих стовпчиків, що мають назву та тип. На відміну від реляційних баз даних,

нереляційні бази даних мають більш гнучкий підхід до збереження інформації. Багато залежить саме від технологічного рішення нереляційної бази даних.

Розглянемо досить популярне рішення Mongo DB. Mongo зберігає інформацію у вигляді документу, який містить поля та значення, та може бути представлений у вигляді Json-документу. Тобто, Mongo зберігає інформацію у вигляді структури даних ключ-значення, де назва поля – це ключ.

Структура даних, що зберігається в Mongo, у більшості випадків залежить від моделі даних, яка визначається класами-сутностями на рівні коду, які взаємодіють з Mongo. Розглянемо взаємодію Mongo зі Spring. Одним із можливих шляхів взаємодії з Mongo є застосування бібліотеки spring-data-mongodb. Основним підходом взаємодії з Mongo є застосування «репозиторних» інтерфейсів та відповідних класів-сутностей, що строго визначають модель даних. Проте ця бібліотека також надає більш гнучку можливість взаємодії з Mongo за допомогою методів класу MongoTemplate. Даний клас проводить операції CRUD з тією моделлю даних, яка вказана - зазвичай це класи-сутностей. Проте бібліотека містить клас Document, який так само може бути використаний для методів класу MongoTemplate. На відміну від класів-сутностей даний клас може зберігати будь-які поля та значення, оскільки успадковується від структур даних Map. Завдяки цьому існує технічна можливість записати будь-яку інформацію у вигляді ключ-значення екземпляру класу Document та зберігати у базі даних. Чому б аналогічну можливість не надати на рівні API endpoint?

Потрібно врахувати, що якщо зберігати будь-яку інформацію в одній і тій самій колекції, то це може призвести до складнощів роботи з цією інформацією у користувачів API. Також різна структура та тип первинного ключа в рамках однієї колекції може спричинити складнощі. Тому варто, щоб в рамках однієї колекції зберігалась однотипна інформація, але яка б в той же час відповідала довільній моделі даних.

Пропонується наступний підхід: за допомогою тої самої можливості класу Document зберігати будь-яку інформацію, створивши еталону модель даних за допомогою допоміжного CRUD, та в подальшому порівнювати вхідну інформацію з еталонною моделлю.

## Реалізація

Реалізація базується на наступних технологіях: SpringBoot, Mongo та бібліотеках, зокрема spring-boot-starter-data-mongodb. Розглянемо реалізацію еталонної моделі даних. Еталона модель даних має відповідати певній колекції у Mongo. Відповідна колекція створюється та видаляється під час створення та видалення відповідної моделі даних. Варто врахувати, щоб при створенні еталонної моделі не використати вже створену раніше колекцію у Mongo.

Для зручності оперування введено єдине унікальне поле «*модель*», що буде визначати конфігурацію. Таким чином, модель даних для еталонної моделі буде складатись із назви моделі, назви колекції даних та самої еталонної моделі у вигляді поля типу Document.

Для реалізації основного універсального CRUD реалізовані методи, які приймають назву моделі та екземпляр Document, для передачі довільної інформації. Параметр моделі потрібен, щоб завантажити актуальну конфігурацію та перевірити колекцію, унікальний ідентифікатор та відповідність вхідної інформації еталонній моделі з точки зору наявності або відсутності полів та їх типів.

Варто зазначити, що значеннями полів можуть бути вкладені екземпляри, тобто значенням поля може бути об’єкт, що складається із декількох полів та відповідних значень. У такому разі перевірка на відповідність еталонній моделі повинна також включати перевірку всіх вкладених полів та значень, що було реалізовано за допомогою рекурсії.

## Висновки

Розроблено інструментарій, який містить функціонал універсальних операцій CRUD. Реалізоване рішення не містить специфічної бізнес-логіки, тому не покриває всі можливі випадки, але може бути застосоване для більшості випадків, що потребують базовий функціонал. Дане рішення можна застосувати для збереження часу Back-End розробників на виконанні рутинної однотипної роботи. Front-End розробники можуть самостійно конфігурувати необхідну модель даних та працювати з розробленим універсальним CRUD.

## Перелік посилань

1. MongoDB Documentation. URL: https://www.mongodb.com/docs/manual/core/document/
2. Spring Data MongoDB API. URL: https://docs.spring.io/spring-data/mongodb/docs/current/api/org/springframework/data/mongodb/core/MongoTemplate.html
3. Spring Documentation: URL: https://docs.spring.io/spring-boot/docs/current/reference/htmlsingle/


# АРХІТЕКТУРА СИСТЕМИ ДОСТУПУ ДЛЯ ПОКРАЩЕННЯ ІДЕНТИФІКАЦІЇ У ОНЛАЙН-БАНКІНГУ


Олег Коновал
ДУІКТ, м. Київ, Україна
folk.user.8888@gmail.com



У цій статті розглядається такий важливий аспект функціонування банківської системи як ідентифікація у онлайн-банкінгу, пропонується архітектура системи доступу, що покращує ідентифікацію.


**Ключові слова:** ідентифікація, розпізнавання, система ухвалення рішень, граф класифікації, онлайн-банкінг, нейронні мережі.


### Вступ

Розвиток дистанційних банківських послуг обумовлений двома причинами. По-перше, сьогодні економічна галузь знаходиться на такому етапі розвитку та перетворення, коли на ринку виникає дедалі більша кількість постачальників фінансових послуг. Це породжує підвищення рівня конкуренції у сфері фінансового посередництва та змушує банківські організації вдаватися до інноваційних технологій у спробах зберегти клієнтів.

По-друге, змінилися запити щодо якості та швидкості надання банківських послуг. Глобалізація прискорила та ускладнила механізми розрахунку між різними суб'єктами економічних відносин; сучасна людина, корпоративні структури згідно з

нормами законодавства, повинні вміти здійснювати транзакції в електронному режимі.

Природним результатом двох вищеописаних тенденцій стала поява принципово нових, простих у використанні та технологічних способів як Інтернет-банкінг та мобільний банкінг.

## Постановка проблеми

Ідентифікація клієнта в онлайн банкінгу може бути пов'язана з ризиками, які можуть бути пов'язані з несанкціонованим доступом до особистих даних клієнта, крадіжкою особистої інформації, шахрайством, іншими проблемами забезпечення безпеки та, власне, розкраданням коштів – основною метою правопорушників.

## Матеріали та методи

Пропонується програмний засіб для аналізу графічних даних і побудови графа класифікацій об’єктної моделі методами машинного навчання для покращення ідентифікації у онлайн-банкінгу.

Архітектура системи для для покращення ідентифікації у онлайн-банкінгу, зображена рисунку 1, включає такі структурні компоненти: набір засобів формування графічної інформації, модуль попередньої обробки графічної інформації, модуль детектування графічного об’єкта на зображенні, модуль розпізнавання об'єктів, модуль побудови графа класифікацій об’єктної моделі, бази даних та бази знань, система ухвалення рішення і т.д.

## Реалізація

Реалізація системи для покращення ідентифікації у онлайн-банкінгу відбувається за шість основних етапів: імпорт бібліотек необхідних для реалізації системи та формування набору графічних даних, які підлягають аналізу та детектуванню; попередня обробка графічних даних, які підлягають аналізу та детектуванню, формування масиву оброблених зображень із обов’язковим перетворенням на 8 бітний формат; створення результуючої моделі, здатної здійснити аналіз та розпізнавання графічної бази даних з обов’язковим виведенням графу класифікацій; складання моделі, налаштованої на аналіз та

розпізнавання графічної бази даних з обов'язковим виведенням графу класифікацій; тренування моделі / Навчання моделі аналізу та розпізнавання графічної бази даних застосовуючи еталонну вибірку; оцінка моделі, сформованої для аналізу та розпізнавання графічної бази даних з обов'язковим виведенням графу класифікацій.

Підкреслено, що реалізація паралелізму здійснена, по-перше, на рівні отримання потоку зображень, забезпечуючи незалежну обробку окремо взятої послідовності зображень, по-друге, на етапі створення кадрів тестової та навчальної вибірки, у разі знаходження різниці об'єктів, по-третє, на етапі формування синтетичних зображень та видачі результату розпізнавання графічних даних [1].

Загалом реалізація відбувається поступово за шість основних етапів:

1) Імпорт бібліотек необхідних для реалізації системи та формування набору графічних даних, які підлягають аналізу та детектуванню;

2) Попередня обробка графічних даних, які підлягають аналізу та детектуванню, формування масиву оброблених зображень із обов'язковим перетворенням на 8 бітний формат;

3) Створення результуючої моделі, здатної здійснити аналіз та розпізнавання графічної бази даних з обов'язковим виведенням графу класифікацій;

4) Складання моделі, налаштованої на аналіз та розпізнавання графічної бази даних з обов'язковим виведенням графу класифікацій;

5) Тренування моделі / Навчання моделі аналізу та розпізнавання графічної бази даних застосовуючи еталонну вибірку;

6) Оцінка моделі, сформованої для аналізу та розпізнавання графічної бази даних з обов'язковим виведенням графу класифікацій на підтвердження ідентифікації у онлайн-банкінгу.

## Висновки

Наведена вище архітектура системи доступу для покращення ідентифікації у онлайн-банкінгу допоможе зменшити ризики пов'язанні з несанкціонованим доступом до особистих даних клієнта, крадіжкою особистої інформації, шахрайством, іншими проблемами забезпечення безпеки та, власне, розкраданням коштів – основною метою правопорушників.

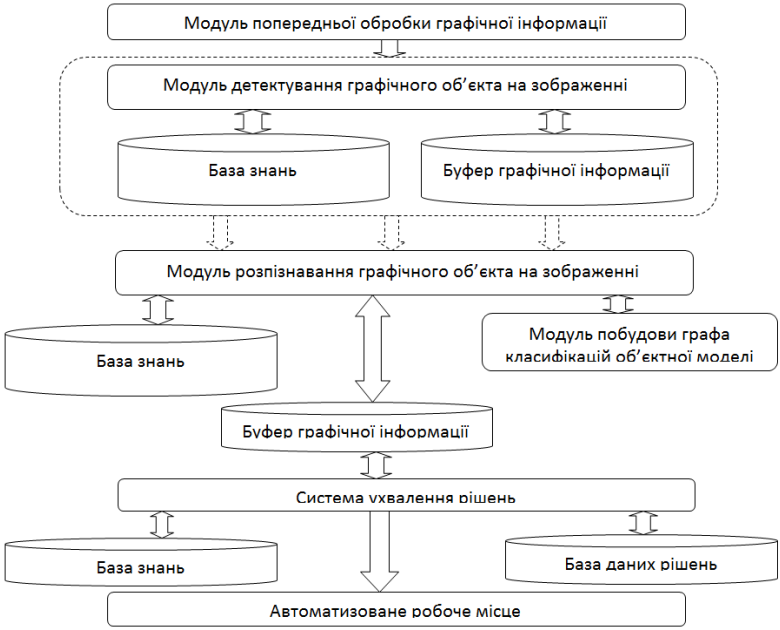



Рис. 1 – Система для покращення ідентифікації у онлайн-банкінгу

## Список використаних джерел:

1. Особливості застосування нейромережевих методів пошуку схожих за контентом зображень / Ж.В. Фількінштейн, М. Г. Сидорова // Питання прикладної математики і математичного моделювання, 2020. № 20. С. 175-185.

# СИСТЕМА АВТОМАТИЗОВАНОГО НАГЛЯДУ ЗА СТАНОМ ЗДОРОВ'Я ВОДІЯ ПІД ЧАС РУХУ АВТОМОБІЛЯ

А.А. Мухін
Дніпровський національний університет імені Олеся Гончара, Дніпро, Україна
6122dante@gmail.com

Запропоновано інтеграцію в блок допомоги при керуванні сучасним автомобілем додаткової системи автоматизованого нагляду за станом здоров'я водія під час руху. Основною метою такої системи є догляд за критичними показниками здоров'я такими, як температура, серцевий тиск, рівень кисню в крові у відсотковому співвідношенні, ЕКГ, фотоплетизмограмма або ФПГ та звукове дослідження легень та серця - стетоскопія. Запропоновано реалізацію програмного керування даною системою та інтеграцію її до головного електронного блоку автомобіля за допомогою спеціального протоколу на основі інтерфейсу USART. Основним мікроконтролер на якому пропонується робити керування системою - STM32F412CG або аналогічний. Обробка даних з сенсорів проходить одночасно за допомогою інтеграції операційної системи FreeRTOS та її складових частин інтегрованих в STM32CubeIDE, таких як черги, семафори, обробка переривань. Обрано всі необхідні складові частини системи замірювання основних показників здоров'я - датчик ЕКГ/ФПГ - MAX86150; MEMS мікрофон - IMP34DT05; знищуючий DC/DC перетворювач 3.3В - MIC33050-SYHL; температурний сенсор - TMP36, або система на основі терморезистору PT1000. Така система є особливо актуальною в сьогоденні, коли станом на 2020 рік, 25% всіх мешканців країни є водіями. Система дозволяє попереджувати про небезпеку для водія, що є особливо критичним під час руху, та проводити активний та пасивний моніторинг роботи серця, накопичувати дані та відправляти та за необхідності передавати їх лікарям для подальшого дослідження. Для находження критичних показників використовуються алгоритми цифрової обробки даних, фільтри низьких та

високих частот, смугові фільтри та алгоритми машинного навчання.
**Ключові слова:** система, сенсор, керування, автоматича, напруга, max86150, stm32f412cg, фільтрація, протокол, екг, моніторинг.

**Вступ**

За статистикою на 2020 рік в Україні було 245 діючих водіїв на 1000 осіб. Необхідною умовою для керування автомобілем є знаходження в максимально сконцентрованому та здоровому стані та стежити за своїм станом, під час їзди. Керування автомобілем потребує максимальної уваги за дорожньою ситуацією, тому водій не завжди може звернути увагу на те, що йому стає зле без стороннього догляду. Є багато систем, які допомагають у керуванні. Деякі з таких систем – камерні системи паркування, парктроніки ABS, ESP, камери, системи безпеки, системи допомоги водієві та інші. Здоров'я водія та оточуючих - це одна з найголовніших складових при використанні транспортних засобів. Система, що розроблюється, допомагає запобігти ДТП на дорозі та стежить за основними параметрами здоров'я водія. Вона може повідомити або запобігти ризикам здоров’я, які присутні під час керування.

Такі системи також можна використовувати для простого неінвазивного моніторингу стану здоров'я медичним персоналом. Незважаючи на прогрес у ранньому виявленні та лікуванні серцево-судинних захворювань, таких як серцеві напади та серцева недостатність, витрати все ще високі. 80% усіх витрат, пов’язаних з лікуванням серцевої недостатності, пов’язані з госпіталізацією, і 75% цих госпіталізацій можна запобігти.

Цифрова обробка сигналу (ЦОС) [2], яка застосовується в системі для обробки сигналів стосується різних методів підвищення точності та надійності цифрових даних. В основному, ЦОС працює шляхом уточнення або стандартизації рівнів або станів цифрового сигналу. Схема ЦОС здатна розрізняти створені людиною сигнали, які є впорядкованими, від шуму, який за своєю суттю є хаотичним.

Усі комунікаційні схеми містять деякий шум. Це справедливо незалежно від того, чи є сигнали аналоговими чи цифровими, і незалежно від типу інформації, що передається. Шум є вічним супутником інженерів зв’язку, які завжди прагнуть знайти нові способи покращити співвідношення сигнал/шум у систем зв’язку.

Традиційні методи оптимізації співвідношення сигнал/шум включають збільшення потужності переданого сигналу та підвищення чутливості приймача. Цифрова обробка сигналу значно покращує чутливість приймального пристрою. Ефект найбільш помітний, коли шум конкурує з бажаним сигналом. Хороша схема ЦОС здатна віднайти інформативний сигнал в системах з дуже високим рівнем шуму, одною з таких систем є ЕКГ. Але є обмеження того, що ЦОС може зробити. Якщо шум настільки сильний, що всі сліди сигналу стираються, схема DSP не може знайти жодного порядку в хаосі, і сигнал не буде отримано.

Якщо вхідний сигнал аналоговий, наприклад, стандартна телевізійна станція, сигнал спочатку перетворюється в цифрову форму за допомогою аналого-цифрового перетворювача (АЦП). Результуючий цифровий сигнал має два або більше рівнів. В ідеалі ці рівні завжди передбачувані, точні напруги або струми. Однак через те, що вхідний сигнал містить шум, рівні не завжди відповідають стандартним значенням. Схема ЦОС регулює рівні таким чином, щоб вони були на правильних значеннях. Це практично усуває шум. Потім цифровий сигнал перетворюється назад в аналоговий за допомогою цифро-аналогового перетворювача (ЦАП).

На рис. 1 показано приклад частково відфільтрованого сигналу ЕКГ[3] з сенсору MAX86150. Цей сигнал відфільтровано від впливу лінії живлення, вирізані частоти 50, 100, 150 Гц. Але інформативна частина сигналу все ще залишається з шумами.

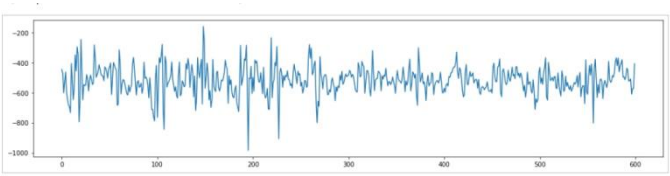



Рисунок 1 – Приклад сирого сигналу ЕКГ

Для порівняння на рис. 2 наведено форму відфільтрованого сигнал електрокардіограми для того ж сенсора.

Рисунок 2 – Відфільтрований сигнал ЕКГ

**Постановка задачі досліджень**

Метою є покращення рівню безпеки водія з можливими серцевими порушеннями за допомогою удосконалення існуючих систем нагляду за водієм під час керування автомобілю. Підвищення рівню безпеки досягається за допомогою додавання спеціальних датчиків ЕКГ, ФПГ, кров'яного тиску та стетоскопії (мікрофони) в елементи безпеки та керування автомобілю, таким чином щоб досягти необхідного контакту з тілом водія. Інформація з таких сенсорів зчитується за допомогою додаткового програмного забезпечення для одного з бортових процесорів автомобіля та/або додавання окремого контролеру для зчитування та цифрової обробки сигналів з сенсорів.

**Рішення задачі**

Для реалізації такої системи необхідне інтегрування додаткового ПЗ, яке буде виконувати наступні функції: реалізація механізму керування сенсором ЕКГ, ФПГ MAX86150 - драйвер написаний мовою програмування С; реалізація управління помпою та клапаном, які використовуються в системі вимірювання тиску; зчитування температури з високоточних ІЧ та кантатних термометрів; ініціалізація та зчитування інформації з MEMS-мікрофонів та переробка їх з сирого PDM формату в готовий до використання та переведення в аудіо файл PCM, наприклад IMP34DT05; нейронна мережа для аналізу отриманих даних, або інший механізм цифрової обробки даних який може бути застосований для визначення відхилень (фільтрація, знаходження піків сигналів).

Було обрано основний мікроконтролер для зчитування та обробки даних в системі: STM32F412CG. Приведений мікроконтролер має всі необхідні інтерфейси для підключення сенсорів – декілька лінії I2C для підключення сенсору MAX86150 та температурних сенсорів, UART для налагодження системи та виведення допоміжних повідомлень при тестуванні системи, а також для передачі даних, USB у разі переходу на новий

інтерфейс передачі даних до головуючих компонентів, SPI та I2S лінії для опитування мікрофонів, TIM – таймери для допоміжних функцій системи та реалізації ділення частот при підключенні двох мікрофонів з метою реалізації стерео звуку та інше.
Схема підключення сенсору MAX86105 представлена на рис. 3.

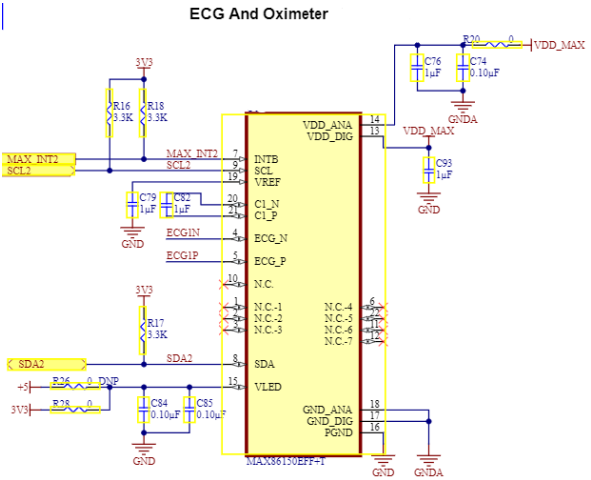


Рисунок 3 – Схема підключення сенсору ЕКГ та ФПГ, MAX86150

Схему виконано у середовищі для розробки друкованих плат Altium Designer. Були використані рекомендації з даташиту мікросхеми MAX86150[1].

Схема фільтрації сигналу на контактах преведена на рис. 4.

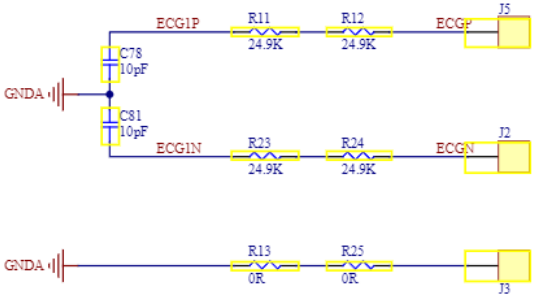


Рисунок 4 – Схема підключення контактів ЕКГ на MAX86150[1]

Реалізовано фільтр високих частот за допомогою RC кола. Такий фільтр необхідний для видалення електромагнітного впливу з контактів електрокардіограми. Такі контакти називають сухими і необхідні вони для прямого дотику пальців або інших частин тіла, де можна вимірювати ЕКГ в одному виведенні. Вимірювання даних кардіограми з вказівних пальців лівої та правої руки еквівалентно вимірюванню у I відведенні. Приклад вимірювання ЕКГ в різних відведеннях наведено на рис. 5.

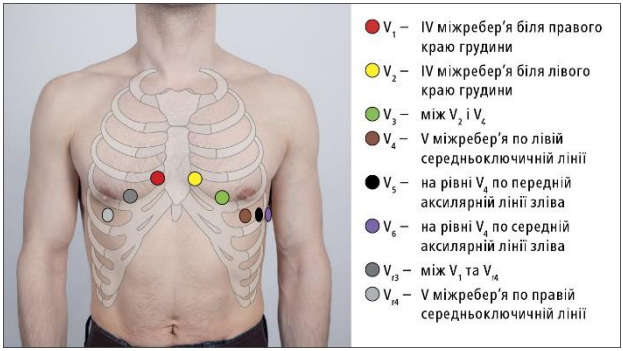



Рисунок 5 – Точки вимірювання ЕКГ в різних відведеннях

Для забезпечення живлення системи може бути використано одну з лінії постійної напруги 5В системи автомобіля. Для прототипування пропонується використовувати USB інтерфейс. На рис. 6 показана схема розведення напруги 5В та 3.3В на плату для живлення складових частин.

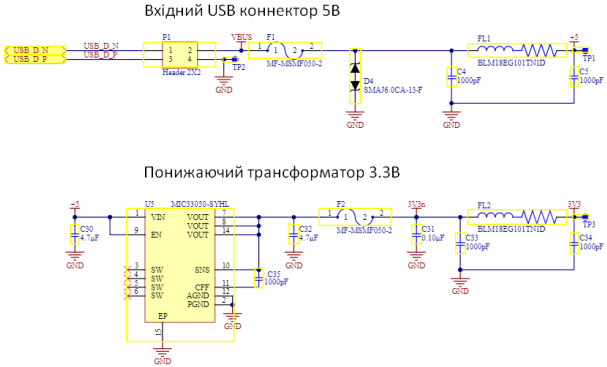
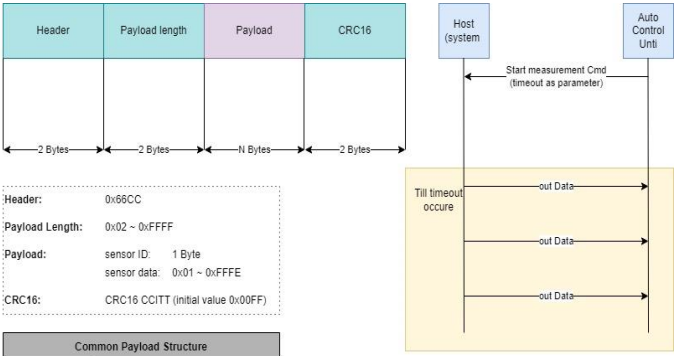


Рисунок 6 – Схема постачання напруги на прототип системи

Для обміну даними між системою та рівнем керування автівки було розроблено спеціальний протокол на який працює за допомогою інтерфейсу UART зі швидкістю передавання в 1 МБод.

Протокол має команди для контролювання версії прошивки системи у разі подальшої її зміни, щоб запити можна було робити до актуальної версії прошивки. Також існує можливість контролювання версії друкованої плати. Також основні команди для запиту старту вимірів на визначений час і для призупинення. На рис. 7 показано схему діаграму реалізації протоколу спілкування.




| Common Payload Structure | | |
|---|---|---|
| Field | Payload | |
| | Sensor ID | Sensor Data |
| Length (bytes) | 1 | N |

| Commands description | | |
|---|---|---|
| **Command** | **Description** | **Example** |
| firmware | get system firmware version | **request:** fw_ver<br>**response:** 0.1 |
| hardware | get system hardware version | **request:** fw_ver<br>**response:** 0.1 |
| start | start gathering sensors data and send it | **request:** start_rec --rec_time= 10000<br>**response: data according to protocol** |
| stop | stop recording | **request:** stop<br>**response:** nothing on success |

Рисунок 7 – Протокол комунікації з системою

Система робить одночасний запис даних з усіх сенсорів – ЕКГ, ФПГ, температура, дані з стерео мікрофона – тобто звук, таким чином можливо робити порівняльний аналіз даних з сенсорів. Додатково планується додавати мітки часу, з метою

співставлення ділянок даних на графіках наприклад ЕКГ і ФПГ – шо є стандартною практикою в аналізі серцевої діяльності лікарями. Дані збираються за допомогою модулю прямого доступу до пам'яті або DMA STM32F412CG, цей модуль дає можливість розвантажити систему від блокування на зчитуванні одного з інтерфейсів. Кожен з сенсорів має вбудовано чергу даних і систему перевірки рівню цієї черги за перериваннями.

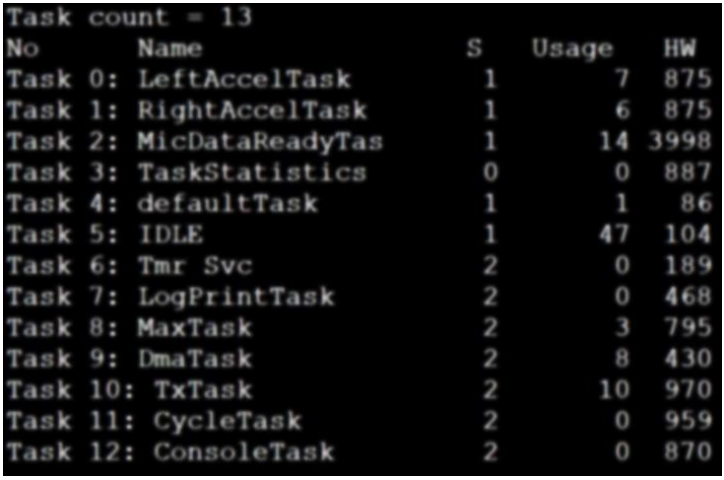
Налаштування сенсорів зроблені таким чином, що при заповнені вбудованої черги на половину – сенсор видає переривання, яке оброблюється на контролері за допомогою системи EXTI. При надходженні переривання система зчитує регістр кількості даних на сенсорі та починає зчитування за допомогою DMA. Коли дані прочитані до рівня порогу переривання в черзі, воно автоматично скається до настання наступного рівню переривання.

На прикладі сенсору MAX86150 дані для ЕКГ та ФПГ розміщуються у черзі сенсору таким чином, як показано на рис. 8.

| | FIFO_DATA | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | BYTE 1 | | | | | | | | BYTE 2 | | | | | | | | BYTE 3 | | | | | | | | |
| ADC Resolution | FIFO_DATA[23] | FIFO_DATA[22] | FIFO_DATA[21] | FIFO_DATA[20] | FIFO_DATA[19] | FIFO_DATA[18] | FIFO_DATA[17] | FIFO_DATA[16] | FIFO_DATA[15] | FIFO_DATA[14] | FIFO_DATA[13] | FIFO_DATA[12] | FIFO_DATA[11] | FIFO_DATA[10] | FIFO_DATA[9] | FIFO_DATA[8] | FIFO_DATA[7] | FIFO_DATA[6] | FIFO_DATA[5] | FIFO_DATA[4] | FIFO_DATA[3] | FIFO_DATA[2] | FIFO_DATA[1] | FIFO_DATA[0] |
| PPG (19-bit) | x | x | x | x | x | | | | | | | | | | | | | | | | | | | |
| ECG (18-bit) | 0 | 0 | 0 | 0 | 0 | 0 | | | | | | | | | | | | | | | | | | |

Рисунок 8 – Структура черги MAX86150 [1]

Такий підхід до зчитування даних з сенсорів - за допомогою DMA і сенсорів з вбудованою чергою даних, дає можливість за допомогою операційної системи реального часу реалізувати паралельний підхід до зчитування даних на одному мікроконтролері з оптимальним використанням процесорного часу. У FreeRTOS для кожного сенсора були реалізовані окремі задачі для ініціалізації та читання даних. Також окремі задачі для старту системи, відправка допоміжних даних, реалізації протоколу та інше. Система показала наступні результати на тестах завантаження системи. Ці результати можна побачити на Рис. 9.



```
Task count = 13
No      Name                S   Usage   HW
Task 0: LeftAccelTask       1       7  875
Task 1: RightAccelTask      1       6  875
Task 2: MicDataReadyTas     1      14 3998
Task 3: TaskStatistics      0       0  887
Task 4: defaultTask         1       1   86
Task 5: IDLE                1      47  104
Task 6: Tmr Svc             2       0  189
Task 7: LogPrintTask        2       0  468
Task 8: MaxTask             2       3  795
Task 9: DmaTask             2       8  430
Task 10: TxTask             2      10  970
Task 11: CycleTask          2       0  959
Task 12: ConsoleTask        2       0  870
```

Рисунок 9 – Навантаження системи

На рисунку використання системою процесорного часу дано у відсотках. Як можна було впевнитись – система завантажена тільки на приблизно 50% від максимуму, враховуючи дана конфігурація, на якій проходили тести використовувала по 2 сенсора кожного типу, що створювало додаткове навантаження.

Ініціалізація системи, котра відбувається при подачі живлення, описана на рис. 10.

Основними пунктами ініціалізації є запуск тактування необхідних інтерфейсів та підсистем контролеру, ініціалізація системи портів вводу виводу для конкретних виводів, ініціалізація системи DMA для переферії, що використовується та інше. Останнім пунктом є старт ядра системи freeRTOS де відбувається ініціалізація операційної системи та запуск необхідних задач.

Система стерео звуку реалізована за допомогою таймера для ділення частоти тактування. Для стерео звуку на платі прототипу розведено два мікрофони через інтерфейс I2S. Схему підключення можна переглянути на рис. 11.

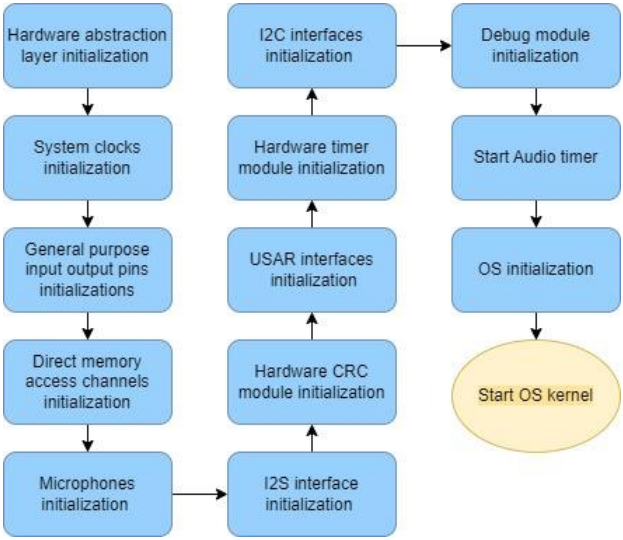



Рисунок 10 – Ініціалізація системи

Підключення лінії живлення зроблено з додатковою фільтрацію аби забезпечити максимальну якість звуку.

Ці мікрофони є PDM мікрофонами, обробка звуку відбувається без додаткових аудіо перетворювачів за допомогою мікроконтролера. Для цього використовується бібліотека від STM32 PDM2PCM library. Вона дає змогу зробити демультиплексацію каналів звуку, перетворення сигналу з сирого формату PDM у формат PCM, та налаштувати підсилення каналів.

**Висновки**

1. Розроблено методичне оснащення для розробки системи контролю за станом здоров'я водія під час руху на основі STM32F412 та сенсорів ЕКГ, ФПГ, температури та мікрофонів.
2. Представлено схеми підключення основних частин плати прототипу системи.
3. Розроблено опис алгоритму спілкування з керуючим блоком автомобіля.

4. Проведення тестування навантаження системи під час активної фази роботи – збору інформації з усіх сенсорів та її обробки.

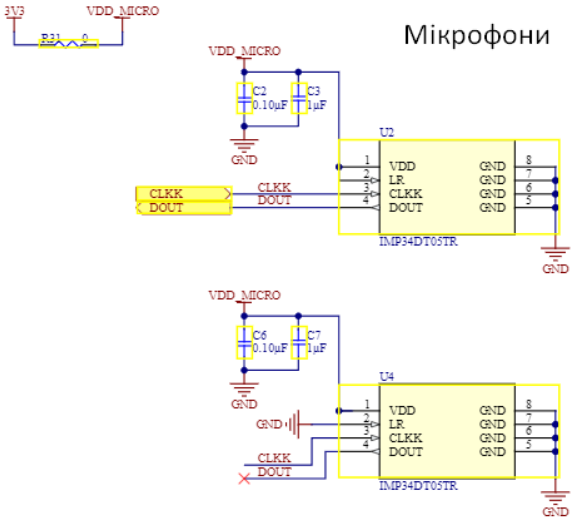



Рисунок 11 – Схема підключення мікрофонів до системи

## Бібліографічні посилання


1. Maxim Integrated Inc. Integrated Photoplethysmogram and Electrocardiogram Bio-Sensor Module For Mobile Health. MAX86150 datasheet, 2019. – URL: https://datasheets.maximintegrated.com/en/ds/MAX86150.pdf
2. Digital signal processing (DSP). TechTarget. 2012 – URL: https://www.techtarget.com/whatis/definition/digital-signal-processing-DSP.
3. Стандартна електрокардіографія. empendium.com. 2022 – URL:
2. https://empendium.com/ua/chapter/B27.V.25.1.1.

# ФОРСАЙТ ПРОРИВНИХ ТЕХНОЛОГІЙ З ВИКОРИСТАННЯМ НЕЧІТКОЇ ЛОГІКИ

А.В. Купчин
Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, м. Київ, Україна,
kupchyn.artem@ukr.net

У тезах доповіді надано короткий опис технологічного форсайту з визначення проривних технологій НАТО, який ґрунтується в більшості на експертних оцінках. Показано новий підхід до довгострокового прогнозування у сфері визначення оборонних технологій за допомогою комп'ютерної моделі на основі теорії нечіткої логіки, що дозволяє зменшити суб'єктивність у прийнятті кінцевого рішення.
**Ключові слова:** технологічний форсайт, підтримка прийняття рішень, нечітка логіка, проривні технології.

Процес формування переліку проривних технологій (ПТ) і загалом технологічний форсайт у цій галузі знань є досить новою та дискусійною темою. Сфера визначення ПТ є новим сегментом наукових досліджень не тільки для України, а й для більшості країн світу.

Організація НАТО з питань науки та технологій у своєму звіті “Science & Technology Trends 2023-2043” показала методичні підходи до визначення проривних та виникаючих технологій з прогнозованим горизонтом зрілості до 2043 року [1].

При цьому, єдиним об’єктивним інструментом у форсайті НАТО є модель оцінки науково-технологічної екосистеми (STEAM – Science and Technology Ecosystem Analysis Model). STEAM – це комп’ютерна модель на основі алгоритмів штучного інтелекту, яка є інструментом для аналізу та оцінки даних (опубліковані звіти, статті, матеріали конференцій і семінарів тощо).

Модель використовує понад 7 мільйонів різноманітних документів і 200 мільйонів тез, забезпечуючи репрезентативну вибірку поточної дослідницької діяльності за останні п’ять років. Базові дані відвантажуються в STEAM з таких баз зберігання наукової інформації, як Microsoft Academic, arXiv, MedRxiv та bioRxiv.

Однак, використання STEAM є лише невеликою частиною при оцінюванні технологій. За більшістю показників технології оцінюються експертами. Зокрема, при визначенні належності технологій до множини проривних були враховані наступні показники: технологічна зрілість, рівень уваги до технології, інтеграція до спроможностей НАТО, потенційний військовий вплив.

З метою усунення суб'єктивної думки експертів в ході визначення переліку ПТ у даній доповіді показано новий підхід до технологічного форсайту в цій сфері. Побудована комп'ютерна модель базується на застосуванні нечіткої логіки (рис. 1) [2].

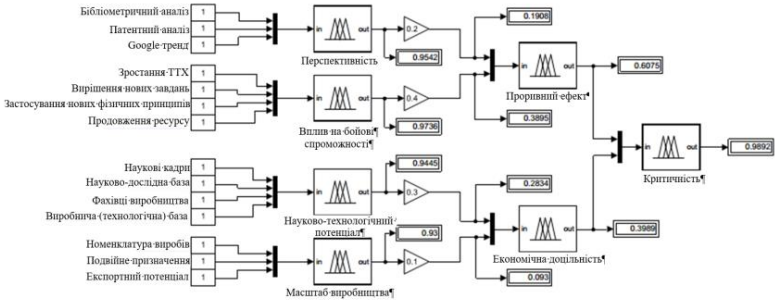



Рис.1. Комп'ютерна модель технологічного форсайту

Варто зауважити, що дана робота націлена на визначення ПТ виключно для оборонної сфери.

Запропонована модель представляє собою ієрархічну структуру прийняття рішення щодо визначення рівня критичності технологій. В даному випадку вищий рівень критичності розглядається як ознака проривності технологій [3].

З точки зору ієрархії прийняття рішення та застосовуючи дедуктивний принцип для визначення рівня критичності технології враховуються два глобальних показника: "Проривний ефект" та "Економічна доцільність". Перший відображає бажання, а другий спроможність. Далі відбувається декомпозиція на показники нижчого рівня.

Загалом, модель репрезентує структуру прийняття рішення щодо визначення ПТ трьох рівнів показників, кожен з яких має певну вагу та своє місце в загальній системі. Таким чином,

модель включає в себе 1 вихідний показник, 2 глобальних, 4 групових та 14 вхідних (1-2-4-14).

Вхідні показники були визначені таким чином, щоб оцінювання технологій не потребувало залучення експертних груп. Тому більшість показників мають бінарну оцінку, а оцінювання може проводити сам дослідник, виходячи з наявних статистичних та інших відкритих даних. Наприклад, визначення рівня перспективності технологій відбувається за вхідними показниками Google trends, бібліометричного та патентного аналізів, інформація про що є доволі об'єктивною та незаангажованою експертною думкою.

Функціонально модель складається з семи систем нечіткого висновку (fuzzy inference system – FIS), які скомпільовані в одну модель у програмному середовищі Simulink Matlab.

На вхід подаються оцінки за вхідними показниками. А виходом є інтегральний показник, який визначає рівень критичності досліджуваних технологій.

Варто зауважити, що вхідні показники вибирались таким чином, щоб мінімізувати їх кореляцію між собою та забезпечити однаковий вплив на вихідну оцінку. Тому всі вхідні показники приймаються такими, що мають однакову вагу.

Решта показників мають різний вплив на результуючу оцінку, виходячи зі своєї вагомості. Всі ваги враховані у скомпільованій моделі. Визначення вагових коефіцієнтів заслуговує на окрему доповідь, тому не буде розглянуто тут.

Після визначення рівня критичності технологій відбувається їх ранжування та селекція до множини ПТ. Межа включення технології до множини проривних визначається методом "еквідистантних точок", який запропонований у роботі [3].

Таким чином, розроблена модель на основі нечіткої логіки дозволяє зменшити суб'єктивну складову у прийнятті рішення щодо визначення рівня критичності технологій, а також сформувати перелік ПТ у оборонній сфері. А з урахуванням того, що технологічний форсайт проводиться на довгострокову перспективу 20 і більше років, усунення похибки в оцінюванні технологій має суттєве або навіть стратегічне значення для розвитку оборонно-промислової галузі економіки.

## Бібліографічні посилання

1. Reding, D.F. et al. (2023). Science & Technology Trends 2023-2043. VOL. 2: Overview. *NATO Science & Technology*

*Organization.* URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf.
2. A. Kupchyn, et al. Determining the accuracy for fuzzy logic technology foresight model. *Cybernetics and Systems Analysis.* 2022. № 58 (3). С. 382-391. https://doi.org/10.1007/s10559-022-00470-1.
3. Kupchyn, A., Sotnyk, V. (2021). A model of disruptive technologies determination for defense sphere. *Issues of Armament Technology*, 156(1), 65-83. https://doi.org/10.5604/01.3001.0015.2529.

## THE ASSESSMENT OF DATA CENTER RESILIENCE

Andrii Davydiuk[1,2]
[1]NATO CCDCOE
[2]G.E. Pukhov Institute for Modelling in Energy Engineering National Academy of Sciences of Ukraine
andrey19941904@gmail.com

With the advancement of IT technologies, society generates an increasing amount of digital data, leading to a constant rise in the demand for larger data storage. Governmental bodies and critical infrastructure entities are transitioning from proprietary resources to smart data storage in data centers. The primary advantages of data processing centers (hereinafter referred to as DPCs) include the ability for rapid scalability and reliable data storage while ensuring access to information. Simultaneously, the centralization of data in one location creates more dependencies on surrounding IT infrastructure, transforming data centers into critical infrastructure objects, where ensuring resilience and cybersecurity becomes a top priority.

As of today, the reliability of data centers is primarily assessed based on "tiers." Data center tiers are a standardized rating system indicating the reliability of a data center's infrastructure. This classification evaluates facilities on a scale from 1 to 4, where 1 represents the lowest and 4 signifies the most effective level. This international rating for data centers is provided by the Uptime Institute, an independent organization that assesses a facility's level primarily based on guaranteed uptime, fault tolerance, and the cost of service.

The assessment is conducted based on the following criteria:

– guarantee of service availability and uninterrupted operation;

– levels of redundancy (the process of duplicating critical components and preserving them as backup copies and safeguards in case of planned or unplanned failures);

– state of cooling and power infrastructure;

– staff experience and technical support protocols (including the ability to handle concurrent maintainability);

– cost of service;

– operational resilience and the center's ability to achieve long-term business objectives;

– time required for the data center to onboard a new client;

– levels of data center security;

– operator neutrality.

Four levels of data processing centers certified by the Uptime Institute:

Tier 1: A data processing center with a single path for power supply and cooling without redundant components. This level has an expected uptime of 99.671% per year.

Tier 2: A data processing center with a single path for power supply and cooling, along with some redundant components. This level offers an expected uptime of 99.741% per year.

Tier 3: A data processing center with multiple paths for power supply and cooling, as well as backup systems that enable personnel to work on configurations without transitioning to autonomous mode. The expected uptime for this level is 99.982% per year.

Tier 4: A fully fault-tolerant data processing center with redundancy for every component. This level anticipates an expected uptime of 99.995% per year [1].

Separately, in publication [2], a methodology for assessing the availability of next-generation data centers has been developed. This methodology relies on automatically obtaining the hardware configuration of the data center to evaluate its availability using accessibility models. The proposed methodology utilizes a new standardized API, Redfish, and corresponding modeling structures. Through this approach, we analyzed the advantages of transitioning from traditional data center infrastructure (referred to as Performance Optimization Data Center (POD) with backup servers) to the next-generation virtual Performance Optimized Data Center (named virtual

POD (vPOD), consisting of a pool of disaggregated hardware resource data).

However, during wartime, unlikely risks of peacetime, such as physical destruction of data centers or frequent power supply failures, network accessibility issues, capture, and unauthorized access become more plausible. Hence, the realities of warfare necessitate the development of new approaches to assess data center resilience. Taking the above into account, implementing Key Performance Indicators (hereinafter referred to as KPIs) in data center resilience processes is advisable. In general, to assess resilience, the following criteria for data center resilience can be identified.Mean Time Between Failures (далі - MTBF) - вимірює середній час між відмовами в інфраструктурі ЦОД. Це допомагає оцінити надійність компонентів і систем у центрі обробки даних.

Mean Time to Repair (MTTR) indicates the average time required for repair or restoration after a malfunction. Lower MTTR values indicate that the data center can quickly recover from failures, ensuring minimal downtime.

Availability measures the percentage of time during which the data center operates and remains accessible. Higher availability percentages indicate a more resilient data center.

Redundancy Level involves components such as power modules, cooling systems, and networking equipment.

Disaster Recovery Time (DRT) measures the time required for full recovery after a catastrophe or significant failure. A shorter recovery time implies a more reliable and efficient disaster recovery plan.

Data Backup Frequency and Completeness (DBFC) assesses how often data backups are created and whether these backups are comprehensive and up-to-date. This metric ensures the ability to restore critical data in case of loss or damage.

Energy Efficiency (EF) evaluates the energy efficiency of the data center infrastructure, including cooling systems, servers, and other equipment. This metric is crucial for reducing operational costs and minimizing the environmental impact of the data center.

Security Incident Response Time (SIRT) measures the time required to detect and respond to security incidents in the data center. Rapid response is critical for mitigating potential threats and minimizing the impact of security breaches.

These indicators can be measured in the following ways.1.Mean Time Between Failures (MTBF) [3]:

*MTBF = Total operational time / Number of failures*

Mean Time to Repair (MTTR) [4]:

*MTTR = Total downtime due to failures / Number of failures*

2.Availability (A):

*Availability = (Total operational time - Total downtime) / Total operational time*

3.Redundancy Level (RL) [5]:

*Redundancy Level = (Number of redundant components / Total number of components)*

4.Disaster Recovery Time (DRT) [6]:

*DRT = Time taken to recover from a disaster*

5.Data Backup Frequency and Completeness (DBFC) [7]:

*Backup Completeness = (Amount of data backed up / Total data size)*

6.Energy Efficiency:

*Power Usage Effectiveness (PUE) = Total Facility Power / IT Equipment Power*

7.Security Incident Response Time (SIRT):

*Incident Response Time = Time taken to detect an*
*d respond to a security incident*

Thus, data center resilience (DCR) can be calculated as follows:

$$DCR = \frac{MTTR + A + RL + DRT + DBFC + PUE + SIRT}{7} * 100\%$$

Having obtained the data center stability indicator, it is possible to quantitatively evaluate the effectiveness of the implementation of data center stability and security measures as objects of critical infrastructure. Quantifying resilience facilitates effective resource management, which is critical in wartime.

## References


1. *Data center tiers classification explained: (tier 1, 2, 3, 4)*. (n. d.). phoenixNAP Blog. https://phoenixnap.com/blog/data-center-tiers-classification
2. Rosendo, D., Gomes, D., Santos, G. L., Goncalves, G., Moreira, A., Ferreira, L., Endo, P. T., Kelner, J., Sadok, D., Mehta, A., & Wildeman, M. (2019). A methodology to assess the availability of next-generation data centers. *The Journal of Supercomputing*, *75*(10), 6361–6385. https://doi.org/10.1007/s11227-019-02852-3
3. *Mean time between failures (MTBF) | MTBF calculation | fiix*. (б. д.). Fiix. https://fiixsoftware.com/maintenance-metrics/mean-time-between-fail-maintenance/#:~:text=MTBF%20=%20#%20of%20operational%20hours%20÷,of%20equipment%20is%20125%20hours.
4. *MTBF, MTTR, MTTF, MTTA: Understanding incident metrics*. (б. д.). Atlassian. https://www.atlassian.com/incident-management/kpis/common-metrics#:~: text=MTTR%20(mean%20time%20to%20repair,system%20is%20fully%20functional%20again.
5. Fuxing Wang, Ramamritham, K., & Stankovic, J. A. (1995). Determining redundancy levels for fault tolerant real-time systems. *IEEE Transactions on Computers*, *44*(2), 292–301. https://doi.org/10.1109/12.364540
6. *What is the difference between RPO and RTO? Real meaning*. (б. д.). Data Resiliency Cloud | Fully Managed SaaS Platform | Druva. https://www.druva.com/blog/understanding-rpo-and-rto
7. Backup integration. (n d.). У *Digital data integrity* (с. 31–39). John Wiley & Sons, Ltd. https://doi.org/10.1002/9780470035184.ch3
8. *Energy efficiency: Buildings and industry*. (б. д.). Energy.gov. https://www.energy.gov/eere/energy-efficiency-

buildings-and-industry#:~:text=Energy%20efficiency%20is%20the%20use,less%20energy%20to%20produce%20goods.

# ВИЯВЛЕННЯ РОБОТИ КЕЙЛОГГЕРА РІВНЯ ЯДРА ЗА ДОПОМОГОЮ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Г.Д. Шибаєв, Л.Ю. Гальчинский
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікóрського», Київ
K233@ukr.net, hleonid@gmail.com

**Актуальність дослідження** зумовлена зростанням кількості викрадень приватних даних користувача, таких як паролі, імена користувачів, паролі облікових записів електронної пошти, PIN-коди та номери рахунків для систем електронних платежів. Для таких атак також використовуються кейлоггери, що не завжди розглядаються як шкідливе програмне забезпечення. Кейлоггер— це застосунок, сам по собі не є шкідливою програмою, бо не несе безпосередніх загроз ресурсам обчислювальної системи, а лише призначений для фіксації та передачі назовні інформацію, яку користувач генерує за допомогою клавіатури. Така амбівалентність дозволяє кейлоггерам бути присутніми у різноманітних законних програмах, починаючи від батьківського контролю до контролю роботи співробітників адміністрацією на протязі робочого дня. Кейлоггери іноді використовують користувачам для можливості перемикання між розкладками клавіатури, або викликати певні програмні завдання за допомогою «гарячих клавіш» (наприклад, Keyboard Ninja)

**Метою роботи** є проведення експериментальних досліджень для підтвердження можливості виявлення роботи кейлоггера рівня ядра засобами машинного навчання.

Для виявлення шкідливої роботи кейлоггера у ядрі операційної системи була запропонована модель, що основується на моніторингу потенційно небезпечних подій, що виникають при роботі шкідливого програмного забезпечення для операційної системи Linux. Такими подіями ми вважаємо: неочікуване збільшення мережевого трафіку та запис у тільки що створені файли. Ці події ми реєструємо у впродовж деякого часу, що би зібрати достатню кількість даних для подальшого аналізу

методами машинного навчання. Головна мета подальшого аналізу полягає у класифікації небезпечних подій поміж усіх даних що були зафіксовані під час експерименту.

## Висновки

В результаті проведеного аналізу було аналізу обгрунтовано доцільність використання методів машинного навчання для вирішення задачі виявлення роботи кейлоггера. Наведена модель показує підвищення рівня виявлення кейлоггерів у ядрі операційної системи Linux.

## Література

1. Abdel-Basset, Abdel-Fatah & Sangaiah (2018) Abdel-Basset M, Abdel-Fatah L, Sangaiah AK. Metaheuristic algorithms: a comprehensive review. In: Sangaiah AK, Sheng M, Zhang Z, editors. Computational Intelligence for Multimedia Big Data on the Cloud with Engineering Applications. Cambridge: Academic Press; 2018. pp. 185–231.

2. Greensmith, J., Aickelin, U. and Twycross, J., Detecting Danger: Applying a Novel Immunological Concept to Intrusion Detection Systems, International Journal of Communications, Network and System Sciences, 2010

3. Greensmith, J., Aickelin, U., Twycross, J. (2006). Articulation and Clarification of the Dendritic Cell Algorithm. In: Bersini, H., Carneiro, J. (eds) Artificial Immune Systems. ICARIS 2006. Lecture Notes in Computer Science, vol 4163. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11823940_31

# INSURANCE CLAIMS RISKS MODELLING AND FORECASTING

Kuznietsova Nataliia[1], Kvashuk Illia[1] and Chemanova Anna[1]

[1]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
natalia-kpi@ukr.net, illiakvashuk@gmail.com , ankachemanova@gmail.com

In this paper the most significant tasks of car insurance claims risks are solved. The task of measuring the claim probability for a specific policy is proposed to solve by using a set of

generalized linear models families with survival models. The second task is to forecast the distinct classes of policies, the quantity and prices of claims in different groups. The third task is to develop of scorecard for insurance claims risks evaluation. All these tasks were solved on real data.
**Keywords:** generalized linear models, scorecard, insurance risks, modelling, forecasting.

## Introduction

Modelling and prediction are vital parts of finances especially in the field of insurance companies. The key task for insurance operation is based on a prediction of severity and probability of each claim as well as the group of the claims. It means that for solving it demands a high level of data quality as well as the quality and accuracy of the used models. During the forecasting task solving we defined the most important problems and found the best models, methods, techniques for their solving. For this reason we made an extensive analysis of the real dataset and use various modelling techniques to solve risk-related problems for insurance data.

## Problem statement and used data

The main objective of this study is to define not only the probability and cost (value) of each claim but also for the subset of the most damaged cases. We will validate an appliance of existing models for real-life task problems in the car insurance field as well as propose to modify the problem statement based on risk management tasks and business needs of the insurance company. It was carried out the extensive examination of different formulations of the problems that can arise from the data.

We used the dataset where the number of classes of claimed and non-claimed insurance claims was to some extent imbalanced – from 589592 records only 3728 were with claims. When the matrix of correlation was examined it was found that there is no strict correlation between features and target variable.

The results of the modelling showed how significant were the limitations and underlined the low predictability in the scope of the data. As per results, for a simple claim, using the best model (normal) it was found that no records possessed the significant predicted probability in order to be divided into the records that will be claimed and those that won't.

## Most relevant tasks for claim risks modelling

During our research we need to admit that insurance strategy based on available data is not bad. There is a big imbalance which defined that the quantity of the most risk claims is small. It is good from the business side of the insurance company but it would be great to evaluate what is the damage and percentage of the most valued claims. For this reason we need to solve such type of tasks.

1) Claim probability evaluation. There are a few well-developed and researched model families that can be used for modelling the claim distribution [1]. Statistical and probability of the claim machine learning based models are both utilized to a great extent in real-life applications for claim determination and prediction. Among machine learning, the random forest is widely used. For statistical models, the regression families are used and among them, further extension is frequently applied to the real-life problem – generalized linear regression [2, 3]. Those models extend the basic linear regression problem with a link function which allows us to take care of the non-linear relationship inside the data. They are used as a main model family in the task of building robust and usable models. We used two generalized linear models: binomial which is best used for probability determination and normal or Gaussian models which can also be applied for the modelling.

2) Predicting groups of claims. The task of grouping the claims into some classes using common values to link and organize records into categories and build models for them. By grouping the records, we could solve two sub-problems of risk management: predict the number of claims per category and also model the total spending on the group. The original dataset was lacking financial data e.g., the severity of the claim or the price of a car. This challenge is an example of real-life data that are missing some parts of information. In order to bypass the problem, the financial data were obtained via an external source per presented classes and adjusted to account for available features. Overall, encountering missing data – observations and features is a known challenge and limitation of the data taken from open source. However, when applying modelling to the data collected by the organization it is still possible to miss some key features or have errors in data that should be cleaned. Sometimes new features are provided in the dataset which require a different approach [4]. Two models have been used – Poisson and Normal model for the number of claims prediction and Normal model for costs of claims

per claim prediction. The result showed a high level of predictability by the classes.

3) Scorecard. While modelling the relationships between input variables and target it is important not only to build a model with a high level of confidence but also to account for its usability. There is a problem with the most complex model that results while giving a sufficient answer, which is hard to decode. In machine learning with many layers, the weights are not interpretable almost to the full extent. For the statistical approach, the interpretation is easier but still doesn't give a measurable and understandable interpretation for people not familiar with the subject of models like staff or regular decision-makers. Any prediction provides only an approximation to the real condition and it is often for the staff to make a final decision which requires understanding. Another problem is that results are not gradation of the severity of the answer. How low is the result? If it is not a definite "yes" – what should be taken? We used a scorecard for solving the task the severity gradation as well as to define the class of the most valued claims.

## Conclusions

The problem of single-claim prediction is the hardest one. For the claims risk management we need to forecast the probability of each claim, of each type of claims and to develop a special scoring card in understandable and easily interpretable manner the key features automatically. Our research showed both weak and strong sides of modern statistical models in risk management. In order to simplify the task, grouping can be performed which results in much better output and possesses far greater accuracy. At the end of our research, we decided to address the problem of the single claim from another perspective and use the scorecard to at least determine in an understandable and easily interpretable manner the key features. It might not be sufficient for single-claim prediction but it yields great results on the grouped data and provides valuable insights about the tendencies.

## References

[1] J. Ashworth Nelder, R. W.M. Wedderburn, "Generalized linear models", Journal of the Royal Statistical Society: Series A (General), 135.3 (1972): 370-384. doi:10.2307/2344614.

[2] N. Klein, M. Denuit, S. Lang, Thomas Kneib, "Nonlife ratemaking and risk management with Bayesian generalized additive models for location, scale, and shape", Insurance: Mathematics and Economics, vol. 55, issue C (2014): 225-249. doi:10.1016/j.insmatheco.2014.02.001.
[3] E. W. Frees, G. Meyers and R. A. Derrig, eds. "Frequency and severity models." Predictive modeling applications in actuarial science: Volume 1. Cambridge University Press (2014): 138-166.
[4] R. Verbelen, K. Antonio, G. Claeskens, "Unravelling the predictive power of telematics data in car insurance pricing", Journal of the Royal Statistical Society, Series C (Applied Statistics), 67.5 (2018): 1275-1304. doi:10.1111/rssc.12283.

## ОЦІНЮВАННЯ КІБЕРВІДМОВОСТІЙКОСТІ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Леонід Гальчинський, Владислав Личик
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
hleonid@gmail.com, lychyk.vlad@gmail.com

Забезпечення кібервідмовостійкості є надзвичайно важливим завданням для різних сфер та для життєдіяльності цілих держав. Для забезпечення життєздатності систем, менеджери та інженери шукають способи застосування концепцій кібервідмовостійкості та інтеграції технологій підвищення стійкості у системну архітектуру, конструкції та операційні системи.
**Ключові слова:** кіберстійкість, метрика кіберстійкості, кібервідмовостійкість.

### Вступ

У англомовній літературі існує консенсус щодо терміну "Cyber resilience" (прямий переклад - кіберстійкість), там де ми вживаємо термін кібервідмовостійкість [1]. Кібервідомовостійкість(кібер-резилентність) - це здатність організації забезпечити розвиток діяльності (стійкість підприємства) за рахунок готовності до кібер-загроз, можливості реагування на них, засобів відновлення після кібератак [2]. Цю здатність можна розглядати на різних вимірах та рівнях. Кібер-резилентность об'єктів критичної інфраструктури залежить як від

апаратно-програмного забезпечення, так і від компетентності персоналу.

## Основна частина

Щоб кібер-резилентність була ефективною, її потрібно розглядати системно. В загальних рисах вимоги ефективності відповідають чотирьом областям у матриці кібервідмовостійкості:

- компоненти та системи, які можуть бути виявлені за допомогою фізичних засобів;
- системи, які можуть бути оцінені в інформаційній або технічній сфері;
- програми та операції з кібербезпеки всередині організації;
- структури та механізми для прийняття рішень, пов'язаних із кібервідмовостійкістю, в організаційному, галузевому, регіональному, національному чи транснаціональному масштабах [3].

Згідно даних Національного інституту стандартів і технологій (NIST) можна виділити такі характеристичні параметри кібервідмовостійкості:

**Основні функції:**

1. **Ідентифікація** - завчасний пошук індикаторів впливу, векторів атак, які можна використати, щоб проникнути у IT-екосистему.
2. **Захист** - зменшення вразливих місць відповідно до вашої терпимості до ризику.
3. **Виявлення** - виявлення індикаторів компрометації за допомогою аудиту в реальному часі, виявлення аномалій та попередження.
4. **Відповідь** - швидкий збір та аналіз інформації про інцидент, задля прийняття обґрунтованих рішень щодо найкращого способу дій.
5. **Відновлення** - швидке, точне та ефективне відновлення системи і даних.
6. **Керування**. Це наскрізна функція, яка інформує та підтримує інших; наприклад, результати управління визначають пріоритетність засобів контролю безпеки.

**Цілі кібервідмовостійкості.** Цілі – це більш конкретні заяви про очікувані результати. [3], [4].

1. **Запобігання або уникнення** - запобігання успішному виконанню атаки або реалізації несприятливих умов.

2. **Підготовка** - розуміння того, що негаразди відбудуться, і відповідно, дотримання набору реалістичних реакцій для подолання очікуваних негараздів.
3. **Продовження** - максимізація тривалості та життєздатності основних місій або бізнес-функцій під час труднощів.
4. **Обмеження** - обмеження шкоди від негараздів, завданих цінним активам, таким як ті, що зберігають або обробляють конфіденційну інформацію або підтримують важливі для місії можливості.
5. **Відновлення** - відновлення якомога більше функцій місії чи бізнесу після негараздів, гарантуючи, що відновлені ресурси є надійними.
6. **Розуміння** - підтримка корисного представлення місії та бізнес-залежностей і статусу ресурсів щодо можливих негараздів.
7. **Трансформація** - зміна місії або бізнес-функції та їх допоміжних процесів, щоб краще справлятися з труднощами.
8. **Перебудова** - зміна системи, місії та допоміжної архітектури, щоб ефективніше справлятися з труднощами.

**Основні методології для оцінки кібервідмовостійкості:**

- Платформа для підвищення рівня кібербезпеки критично-важливої інфраструктури (Національний інститут стандартів і технологій (NIST));
- Стандарти Агентства Європейського для мережевої та інформаційної безпеки (European Union Agency for Network and Information Security (ENISA) Standards);
- Методологія дослідників американської організації Корпорація Mitre.
- Метрика групи І. Лінкова (Resilience metrics for cyber systems) [4];

Однак, у жодній з цих методологій немає засобів для розробки моделей кількісної оцінки кібер-резилентності. Очевидно, що це потребує етапу мета-моделювання для конкретних класів об’єктів, зокрема критичної інфраструктури.

## Висновки

Наступним етапом після формування понятійного апарату має стати мета-моделювання самої кібер-резилентності для об’єктів.

Такий підхід дозволить узгодити контекст, у якому використовується певний показник, а також полешить знаходження методів оцінювання кібер-резилентності.

## Перелік посилань


1. Гальчинський Л.Ю., Личик В.В. Метрики оцінки кібервідмовостійкості (аналітичне оглядове дослідження). Інформаційні технології та суспільство. Київ: Міжрегіональна Академія управління персоналом, 2023. Випуск 2 (8). 98 с. - Режим доступу: http://journals.maup.com.ua/index.php/it/issue/view/260
2. Björck, Fredrik; Henkel, Martin; Stirna, Janis; Zdravkovic, Jelena (2015). Cyber Resilience - Fundamentals for a Definition. Advances in Intelligent Systems and Computing. Vol. 353. Stockholm University. pp. 311–316.
3. Bodeau D, Graubart R, McQuaid R, Woodill J (2018) Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods. (The MITRE Corporation, Bedford, MA), MITRE Technical Report.
4. Igor Linkov, Daniel A Eisenberg, Kenton Plourde, Thomas P Seager, Resilience metrics for cyber systems December 2013 Environment Systems and Decisions 33(4) DOI:10.1007/s10669-013-9485-y


# DEVELOPMENT OF CONTINUOUS USER AUTHENTICATION ALGORITHM


Maksym Ogurtsov
V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine, Kyiv, Ukraine
maksymogurtsov@gmail.com



The relevance of information security has been growing over the past decades and will continue to grow. To increase the information security level, the special algorithm for multifactor authentication of users using Near Field Communication technology (NFC) was developed. Based on it, it is proposed to create a constant channel for transmitting secret authentication data for the data protection algorithms operational work.

**Keywords:** authentication, near-field communication, NFC, information security, access control

## Introduction

The relevance of information security has been growing over the past decades and will continue to grow in the future, as the value of information with limited access (ILA) and the amount of losses that can be caused by its disclosure, distortion or destruction are constantly increasing [1].

To date, the ILA protection is provided by cryptography and access control means [1-2] and sometimes – by steganographic means for hiding the fact of information transmission. But the means of user multifactor authentication when trying to gain access to ILA remain insufficient [1-4]. And even if two-factor authentication used – situations, when authorized user leaving his work place without locking it, providing to malefactor ability to get unauthorized access to ILA, remain.

**The goal of this work** is to develop a special multifactor authentication algorithm for protecting information when accessing it using Near Field Communication technology (NFC) [5] to increase the level of protection of personal information.

It is proposed to implement the architecture of the system of CI (SCI) based on multifactor authentication of users using NFC) technology. On its basis, it is proposed to create a channel for constantly transmitting secret authentication data.

NFC technology was chosen because of its unique features of transmitting data only in very close range, which will be necessary for the proposed algorithm work, as is shown below.

Continuous user control

Let's consider how it is possible to increase the level of protection of authentication data based on the use of NFC. For this goal, it is proposed to apply a method of continuous user control, according to which each user must have an NFC authentication device. According to the **developed algorithm of continuous user control**, the NFC-devices that each user has with him will be constantly used to track the user’s presence and location, while determining his level of authority (Figure 1).

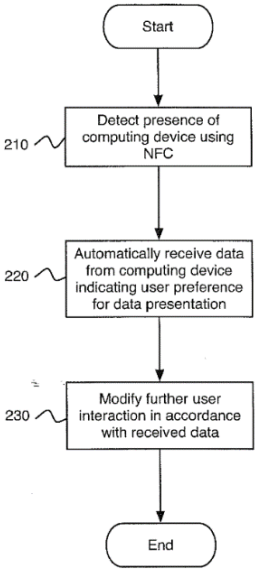



Figure 1 – Scheme of the algorithm of continuous user control work

Algorithm of continuous user control

The **algorithm workflow**:

1. When the user is going to start work with ILA (the first data access request), he enters the password.

2. During the password verification process, the NFC reader automatically checks the presence of an NFC authenticator in the nearby zone, which is corresponding to the given password.

3. If the password is correct, but there is no NFC-authenticator, access is denied.

4. If the password is correct and NFC-authenticator present, access is granted.

5. During further work with ILA, the NFC-authenticator is regularly (at least once every few seconds) scanned for its presence.

5. In the case if the NFC-authenticator is not detected during scanning, access to ILA is blocked and step 1 must be repeated.

6. If the user moves away (went on a break, moved to another workplace, etc.) – step 1 must be repeated.

As a result of this algorithm implementation, authorized user will be forced to enter his password only when coming to work and

returning from a break. During all other times it will be enough for user to have an NFC-authenticator with him to get access the ILA within the framework of his/her authority. At the same time, stealing the NFC-authenticator will not grant unauthorized access to malefactor, since in order to gain such access to ILA, he will have to additionally enter a password that is known only to a legitimate user. At the same time, the security system monitors the presence, location, and actions of each user in real time, checking their access rights automatically if necessary.

The construction of security system based on the proposed algorithm will allow protection against the most dangerous threats, simplify the deployment, modification and scaling of security system and increase the reliability of ILA protection. Users wouldn't have to care anymore is their workplace is locked when they are going to go away for some reason – it will happen automatically. And without risks of false-negative errors as with other approaches [1]: for example, in approach of automatically blocking access to workplace after some time of inactivity there is possible situation, when user gets a call, talks on the phone, stopping doing any other actions – and his/her workplace automatically locking. With the proposed algorithm such a situation wouldn't happen. The use of an NFC device will allow effective and transparent multi-factor user authentication.

It is also possible to use a mobile phone with NFC support as an NFC authenticator.

## Conclusions

The developed algorithm of multi-factor user authentication based on NFC technology, when applied, will allow easy and flexible deployment, scaling and updating of the access control systems. According to the algorithm, it is proposed that the location and actions of users are constantly monitored by the security system in automatic mode and with the password will provide multi-factor authentication.

However, the following questions require further research:

• which specific software and hardware tools would be the optimal choice to build the access control system;

• economic substantiation of the NFC-authenticators feasibility.

## References

1. Ouaddah, A., Mousannif, H., Abou Elkalam, A., & Ouahman, A. A. (2017). Access control in the Internet of Things: Big

challenges and new opportunities. *Computer Networks*, 112, 237-262.
2. Yang, S. S., Jang, Y. H., Park, M. H., Park, S. C., & Kim, H. J. (2021). Design and implementation of active access control system by using NFC-based EAP-AKA protocol. *Wireless Personal Communications*, 118, 2487-2503.
3. Ogurtsov M. (2021, November). Special algorithm development for users multifactor authentication. In *International Scientific Conference "Mathematical modeling, optimization and information technologies"*. Chişinău – Київ – Batumi. 15 - 19 November, 2021 (in Ukrainian).
4. Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A usability study of five {two-factor} authentication methods. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (pp. 357-370).
5. Raman, T. V., & Chen, C. (2012). Personalized access using near field communication. *U.S. Patent No. 8,150,915*. Washington, DC: U.S. Patent and Trademark Office.

## СИСТЕМА ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

О.В. Сачук
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ovsachuk@gmail.com,

Робота присвячена вивченню проблеми безпеки та стійкості критичної інфраструктури.. Аналіз збитків, завданих російською агресією, вказує на важливість невідкладних заходів для вдосконалення системи та реагування на екстремальні ситуації. Робота також висвітлює напрями розв'язання проблеми захисту критичної інфраструктури через створення нормативно-правової бази, організаційно-інституційної структури та визначення повноважень суб'єктів системи.

**Ключові слова:** критична інфраструктура, кризові ситуації, державна безпека, війна.

## Вступ

В умовах війни, система захисту об'єктів критичної інфраструктури стає невід'ємною складовою національної безпеки для України. Питання ефективного захисту критичних об'єктів стає не тільки технічним викликом, але й ключовим аспектом забезпечення національної стійкості та безпеки. Ця тема є актуальною і вимагає комплексного підходу до вивчення та розробки заходів, спрямованих на підвищення рівня захисту об’єктів критичної інфраструктури України в умовах сучасних викликів та загроз.

## Результати досліджень

Критична інфраструктура – це система об'єктів, установ та мереж, яка є необхідною для функціонування суспільства, економіки та національної безпеки. Ці об'єкти забезпечують основні послуги та функції, такі як електропостачання, транспортні комунікації, водопостачання, телекомунікації, медична допомога та інші, без яких неможливо повсякденне життя та праця суспільства. Завдяки своєму стратегічному значенню ці об’єкти потребують особливого захисту від природних катастроф, техногенних аварій, кібератак, терористичних загроз та інших небезпек [3].

До основних принципів функціонування державної системи захисту критичної інфраструктури належать: координованість; єдність методологічних засад; державно-приватна взаємодія; забезпечення конфіденційності; міжнародне співробітництво [3].

Об'єкти І категорії критичності займають особливе значення з точки зору загальнодержавного значення. Вони володіють значним впливом на інші об’єкти критичної інфраструктури, та їхнє порушення може призвести до виникнення кризової ситуації державного рівня (електростанції, центри управління, великі державні центри).

Об’єкти ІІ категорії критичності є життєво важливими та мають регіональне значення. У разі порушення їх функціонування виникає кризова ситуація, що має вплив на регіональний рівень (паливно-енергетична промисловість, логістичні центри).

Об’єкти ІІІ категорії критичності є важливі для місцевого рівня – в основному підприємства. Наслідком їх порушення може спровокувати кризову місцевого місцевого значення.

Об'єкти IV категорії критичності є необхідними і порушення їх функціонування може призвести до кризового обмеження локального значення – заправки, нафтобази, локальні центри управління [1].

Продовження агресії Російської Федерації впродовж 2022 року в 2023 призвело до зростання суми збитків, що були завдані ракетними обстрілами по критичній інфраструктурі України, особливо енергетичній сфері, так і обстрілами міст та селищ, активними бойовими діями на півдні та сході України.

Регулярний моніторинг завданих втрат за вересень 2022 року – лютий 2023 року, що ведеться цивільно-військовими адміністраціями та міністерствами, дозволяє проводити регулярну оцінку чинного стану збитків від російської агресії. За майже пів року з 1 вересня 2023 року Україна додатково понесла понад $18,4 млрд збитків своїми активами [2]

Найбільше зростання пов’язане зі збільшенням збитків житлового фонду. За останні три

місяці ця сума у лютому зросла до $53,6 млрд. До трійки найбільш постраждалих сфер, окрім руйнувань житлового сектору, належать сфера інфраструктури із сумою збитків у $36,2 млрд та промисловість й пошкоджені підприємства – на $11,3 млрд [2].

Найбільша частка у загальному обсязі прямих втрат належить житловим будівлям ($53,6) та критичній інфраструктурі ($36,2 млрд). Втрати активів бізнесу становлять мінімум $11,3 млрд і продовжують зростати . Ще $8,7 млрд складають прямі втрати аграрного сектору внаслідок війни.

Сукупні прямі втрати від руйнувань та пошкоджень об’єктів громадського сектору (соціальні об’єкти та установи, заклади освіти, науки та охорони здоров’я, культурні споруди, спортивні об’єкти, адміністративні будівлі тощо) складають близько $13,69 млрд.

Проблеми забезпечення захисту критичної інфраструктури передбачається розв’язати за трьома напрямами:

– створення нормативно-правової бази з питань організації діяльності державних органів і суб’єктів господарювання у сфері захисту критичної інфраструктури;

– створення організаційно-інституційної структури державної системи захисту критичної інфраструктури;

– визначення повноважень, завдань та відповідальності суб’єктів державної системи захисту критичної інфраструктури


## Висновок

Дослідження системи захисту об'єктів критичної інфраструктури України в контексті військового конфлікту з російською федерацією показало актуальність та важливість цієї теми для національної безпеки. Розглянуті категорії об'єктів дозволяють усвідомити різний рівень їх стратегічної важливості та розмістити оптимальні заходи забезпечення їх ефективного захисту. Важливим елементом функціонування системи є принципи координованості, єдності методологічних засад, державно-приватної взаємодії, забезпечення конфіденційності та міжнародного співробітництва. Результати моніторингу збитків, завданих російською агресією, свідчать про серйозні наслідки для економіки та соціальної сфери України.

## Перелік посилань

1. Закон України Про критичну інфраструктуру [Електронний ресурс]. – Режим доступу:

https://ispn.kievcity.gov.ua/HelpInfo/News/NewsOne.aspx?ID=329
2. Звіт про прямі збитки інфраструктури від руйнувань внаслідок військової агресії росії проти України за рік від початку повномасштабного вторгнення [Електронний ресурс]. – Режим доступу: https://kse.ua/wp-content/uploads/2023/03/UKR_Feb23_FINAL_Damages-Report-1.pdf
3. Про критичну інфраструктуру | Закон України від 16.11.2021 р. No 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20

## RESEARCH OF THE EFFICIENCY OF NETWORK-CENTRIC CONTROL OF MOBILE AGENTS IN A DYNAMIC ENVIRONMENT

Vadym Mukhin, Valerii Zavgorodnii, Anna Zavgorodnya, Olexandr Yarovyi, Lesia Baranovska, Oleg Mukhin
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kiyv, Ukraine
v.mukhin@kpi.ua, zavgorodniivalerii@gmail.com, annzavgorodnya@gmail.com, getem13@ukr.net, lesia@baranovsky.org, o.mukhin01@gmail.com

Based on model of the algorithm of network-centric control of mobile agents in a dynamic environment and simulation model regarding the behavior of interacting mobile agents, there is a need to conduct experimental studies of parameters and evaluate the effectiveness of network-centric control of mobile agents.

To confirm the correctness of the developed scientific and methodological apparatus, we conducted mathematical modeling of the process of researching the effectiveness of network-centric management of mobile agents in a dynamic environment. The software tools used include the following elements:

– the simulation was performed on an Intel® Celeron® personal computer with a 3.2 GHz processor and 16 GB of RAM in the Microsoft Windows 10 operating system;

– Microsoft SQL Server 2022 was used for the database management system;

– Microsoft Visual Studio 2022 Community Edition is chosen as the development environment. The development was carried out in the C# programming language using an object-oriented approach;

- conducting experiments in the simulation environment included setting the initial parameters of the task, performing intermediate calculations, deriving the results and their visualization using Windows Presentation Foundation.

Let's calculate the minimum sufficient number of nodal mobile agents, % (nodePercentage) to hit the target.

A target is considered hit when the following conditions are met simultaneously:

a) the percentage of mobile agents that reached the target (targetHitPercentage) must be no less than the percentage of mobile agents that was sufficient to hit the target (targetHitPercentage);

b) among the mobile agents that have reached the goal, there is at least one node mobile agent (targetReachedCount > 0).

For this, series of 100 experiments were performed each, with the following values:

– number of mobile agents (numberOfAgents): 100;

– the percentage of mobile agents that will be sufficient to hit the target (targetHitPercentage): 5%.

– percentage of nodal mobile agents (nodePercentage): from 1 to 20% of the total number of mobile agents;

– initial (startLatitude, startLongitude) and final (targetLatitude, targetLongitude) geographic coordinates for nodal mobile agents;

– the percentage of mobile agents with which communication was lost(lossPercentage): Automatically generated randomly between 50% and 90%. At the same time, the current geographic coordinates of such a mobile agent are set to NULL.

According to the obtained results of the experiments, graphs of the dependence of the number of nodal mobile agents, % (nodePercentage) on the probability of hitting the target (targetHitPercentage) in each experiment were drawn (Figs. 1-5).

Summarizing the results of the conducted experiments, the average effectiveness of hitting the target with different numbers of nodal mobile agents was considered (Table 1, Fig. 6).

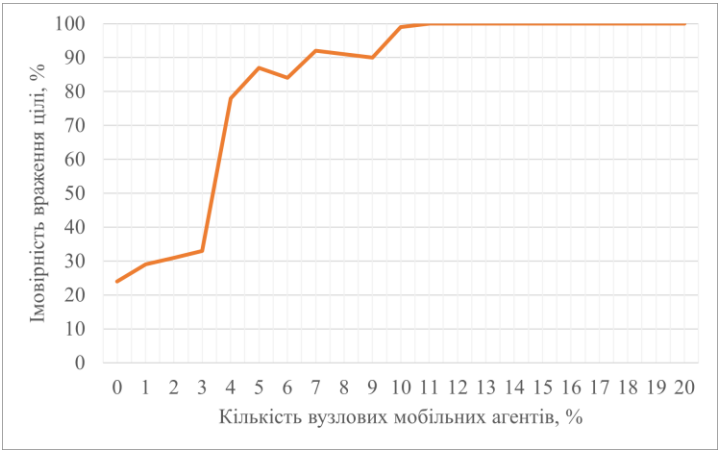



Fig. 1 Dependence of the value of the number of node mobile agents (%) on the probability of the impression of the target: the percentage of mobile agents with which the connection was lost - up to 50%

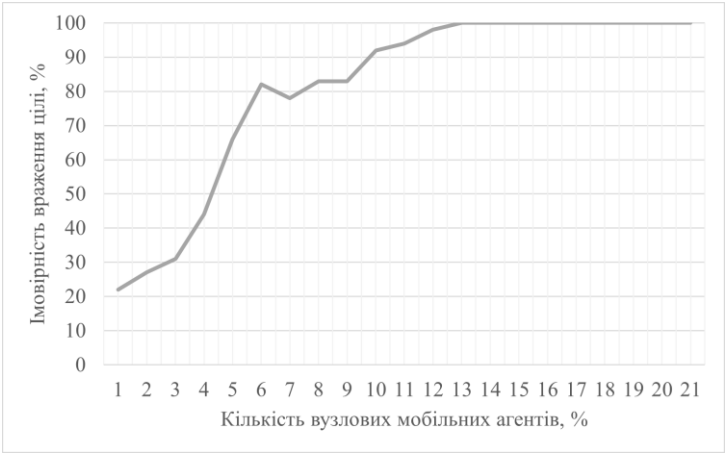



Fig. 2. Dependence of the value of the number of nodal mobile agents (%) on the probability of the impression of the target: the percentage of mobile agents with which communication was lost is up to 60%

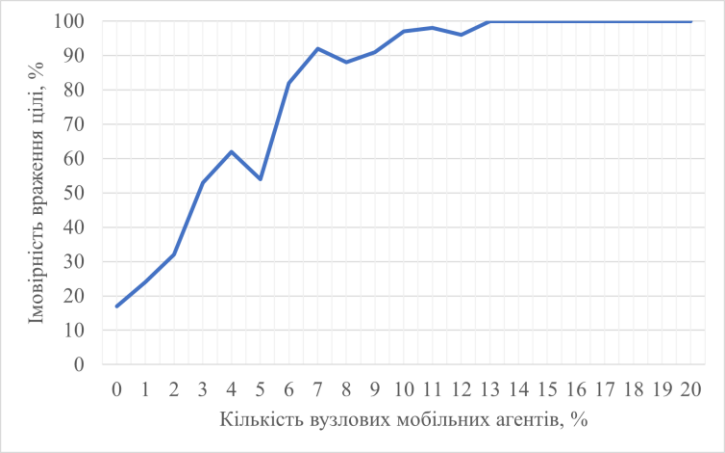



Fig. 3. Dependence of the value of the number of nodal mobile agents (%) on the probability of the impression of the target: the percentage of mobile agents with which communication was lost is up to 70%

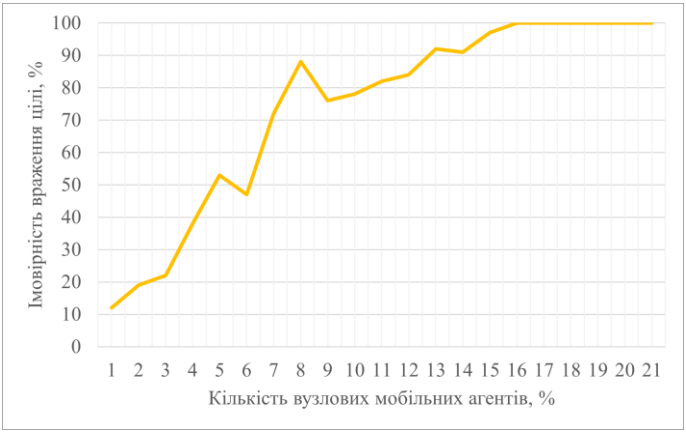



Fig. 4. Dependence of the value of the number of node mobile agents (%) on the probability of the impression of the target: the percentage of mobile agents with which communication was lost is up to 80%

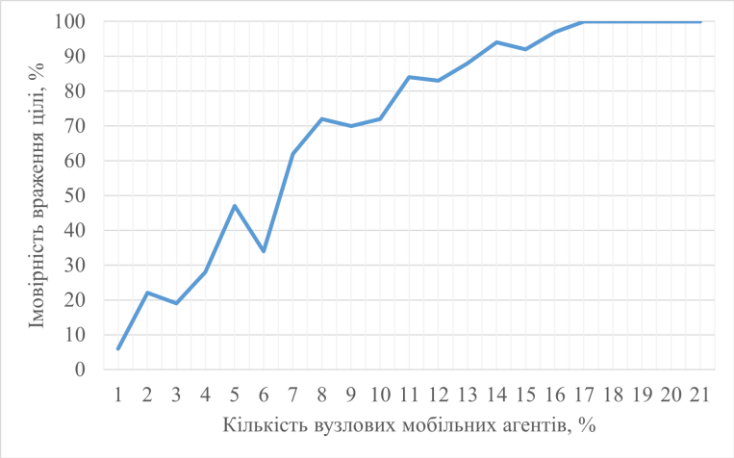



Fig. 5. Dependence of the value of the number of node mobile agents (%) on the probability of the impression of the target: the percentage of mobile agents with which communication was lost is up to 90%

Table 1

Effectiveness of hitting the target with different number of nodal mobile agents

| Number of nodal mobile agents, % | Number of mobile agents with which communication was lost, % | | | | |
|---|---|---|---|---|---|
| | up to 50% | up to 60% | up to 70% | up to 80% | up to 90% |
| 0 | 24 | 22 | 17 | 12 | 6 |
| 1 | 29 | 27 | 24 | 19 | 22 |
| 2 | 31 | 31 | 32 | 22 | 19 |
| 3 | 33 | 44 | 53 | 38 | 28 |
| 4 | 78 | 66 | 62 | 53 | 47 |
| 5 | 87 | 82 | 54 | 47 | 34 |
| 6 | 84 | 78 | 82 | 72 | 62 |

| | | | | | |
|---|---|---|---|---|---|
| 7 | 92 | 83 | 92 | 88 | 72 |
| 8 | 91 | 83 | 88 | 76 | 70 |
| 9 | 90 | 92 | 91 | 78 | 72 |
| 10 | 99 | 94 | 97 | 82 | 84 |
| 11 | 100 | 98 | 98 | 84 | 83 |
| 12 | 100 | 100 | 96 | 92 | 88 |
| 13 | 100 | 100 | 100 | 91 | 94 |
| 14 | 100 | 100 | 100 | 97 | 92 |
| 15 | 100 | 100 | 100 | 100 | 97 |
| 16 | 100 | 100 | 100 | 100 | 100 |
| 17 | 100 | 100 | 100 | 100 | 100 |
| 18 | 100 | 100 | 100 | 100 | 100 |
| 19 | 100 | 100 | 100 | 100 | 100 |
| 20 | 100 | 100 | 100 | 100 | 100 |

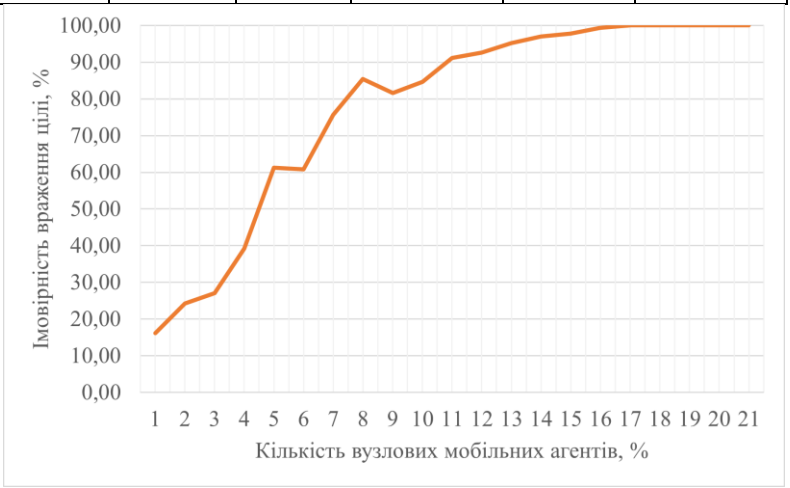



Fig. 6. Average effectiveness of hitting the target with different number of nodal mobile agents

From Figure 6, it can be concluded that the effectiveness of hitting the target was on average:

– at 16% and above nodal mobile agents – 100%;

– with 12-15% of nodal mobile agents – 95%;
– at 10-11% of nodal mobile agents – 90%;
– with 7-9% of nodal mobile agents – 80%;
– with 0-6% of nodal mobile agents – less than 80%;

From the above, it follows that for effective damage to the target (80% and above), the minimum sufficient number of nodal mobile agents (nodePercentage) is from 7 to 9%, therefore it is not advisable to use more than 9% of nodal mobile agents from the total number of mobile agents.

Thus, an experimental study of the parameters and evaluation of the effectiveness of network-centric management of mobile agents was performed. The study was carried out using the developed model of interaction of mobile agents based on network-centric management and a simulation model of the behavior of interacting mobile agents in a dynamic environment.

As a result of the research, compared to the centralized (nodal mobile agents are absent) approach to management, the effectiveness of network-centric management was revealed. It is shown that with an increase in the number of nodal mobile agents, the effectiveness of hitting the target increases, but reaches sufficient values (80% and higher) already at 9%nodal mobilesagents from the total number of mobile agents and therefore it is not advisable to exceed this indicator.

## MODEL-BASED INFORMATION SECURITY MANAGEMENT SYSTEMS ARCHITECTURE

V. Mokhor[1], O. Bakalynskyi[1],
Ya. Dorohyi[2,3], V. Tsurkan[1,3]

[1]Pukhov Institute for Modeling in Energy Engineering
of National Academy of Sciences of Ukraine, Kyiv, Ukraine
[2]Donetsk National Technical University, Lutsk, Ukraine
[3]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
v.mokhor@gmail.com, baov@meta.ua, argusyk@gmail.com, v.v.tsurkan@gmail.com

Investigated the representation of the information security management system architecture. The study elucidates the influences of the organizational environment on its fundamental

concepts and properties. This is manifested in the elements, relationships, principles, and evolution of the information security management system. The description of its architecture within a specific organization, considering the type, size, and nature, is condensed into constructing a model from the perspective of stakeholders. To achieve this, the proposed approach involves employing model-based systems engineering. This enables the attainment of a unified representation of the information security management system architecture primarily from the perspectives of various stakeholders. The formalization is based on the language of system modeling. According to its graphical notation, architecture elements are depicted as blocks, along with their properties and relationships.
**Keywords:** risk assessment, risk treatment, information security management system architecture, model-based systems engineering, model-based architecture, interested party.

## Introduction

The embodiment of the fundamental concepts and properties of the information security management system in the surrounding environment is reflected in its elements, relationships, principles, and evolution [1]. Such representation is conventionally referred to as architecture. The description of its creation in a specific environment and/or community of stakeholders is determined by a model constructed from a particular perspective [2].

A distinctive feature of creating information security management systems is the orientation towards ensuring the integrity of essential information properties within an organization. This is achieved through risk assessment and, consequently, ensuring stakeholders of the proper handling of these risks. In this case, the organization is proposed to be interpreted as the surrounding environment defining parameters and conditions influencing the information security management system. Meanwhile, its fundamental concepts and properties are embodied in the architecture's elements and relationships [1, 3–5].

This interpretation allows establishing credible influences on the information security management system from the organization's perspective in terms of its type, size, and nature [3, 4]. Furthermore, it considers the existence and interaction with other management systems, such as cybersecurity and privacy information security. This

is crucial for meeting the needs, expectations, and constraints of stakeholders within defined boundaries (organization, organizational unit). Therefore, a model-oriented representation of the architecture of information security management systems remains relevant.

## Model-based information security management systems architecture

The prerequisite for defining the architecture of the information security management system is the analysis of the organization's activities as the surrounding environment. Based on established internal and external circumstances, requirements from stakeholders are formulated. Their implementation allows for the consideration and, consequently, satisfaction of defined needs, expectations, and constraints. As a result, the stakeholders' vision is transformed into a technical solution vision. This is essential for presenting characteristics, attributes, functional, and non-functional requirements for the information security management system within the organization [1–4].

Taking into account the interests of stakeholders and established functional and non-functional requirements is achieved by creating alternative variants of the architecture of information security management systems. Each variant defines elements and relationships between them, interfaces for interaction with other systems within the organization, as well as with other organizations (or structural components of the same organization). Additionally, it is crucial to consider the dependency on quality management systems, as they collectively form an integrated organizational management system [2–5]. Interfaces and interactions characterize the boundaries of its creation and implementation, while these aspects are addressed through the development of the information security management system architecture model. To accomplish this task, the use of model-based systems engineering is proposed [2, 6].

The adoption of the proposed methodology allows moving away from document-oriented model construction for the architecture of the information security management system. This achieves uniform representation, primarily from the perspectives of various stakeholders. This is important for clear understanding and meeting their needs, expectations, and constraints. The basis for such formalization is the Systems Modeling Language (SysML) [7, 8]. According to its graphical notation, the elements of the information security management system architecture are represented as blocks,

along with their properties and relationships. Simultaneously, the structure of each block can be further detailed through their ports and interfaces, which is useful for representing interactions within the elements of the information security management system architecture and with the surrounding environment.

## Conclusion

Thus, the elements, relationships, principles, and evolution reflect the fundamental concepts and properties of the information security management system in the surrounding environment. By the surrounding environment, we mean the organization as a whole or a specific structural component. Considering this, its influence is determined based on the type, size, and nature. This representation in a specific environment is characterized by a model of the architecture of the information security management system constructed from the perspective of stakeholders.

The use of model-based systems engineering has allowed moving away from document-oriented model construction for the architecture of the information security management system. This has achieved uniformity in its representation, primarily from the perspectives of various stakeholders. The basis for such formalization is the Systems Modeling Language. According to its graphical notation, the elements of the information security management system architecture are represented as blocks, along with their properties and relationships.

## References


1. ISO/IEC/IEEE 42010:2022. Software, systems and enterprise. Architecture description. [Valid from 2022-11-07]. URL: https://www.iso.org/standard/74393.html, last accessed 2023/11/22.
2. ISO/IEC/IEEE 15288:2023. Systems and software engineering. System life cycle processes. [Valid from 2023-05-16]. URL: https://www.iso.org/standard/81702.html, last accessed 2023/11/22.
3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. [Valid from 2022-10-25]. URL: https://www.iso.org/standard/27001, last accessed 2023/11/22.
4. ISO/IEC 27001:2022/Amd 1. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. [Valid from 2023-09-19]. URL:

https://www.iso.org/standard/88435.html, last accessed 2023/11/22.
5. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection. Information security controls. [Valid from 2022-02-15]. URL: https://www.iso.org/standard/75652.html, last accessed 2023/11/22.
6. Shevchenko N. An Introduction to Model-Based Systems Engineering (MBSE). URL: https://insights.sei.cmu.edu/blog/introduction-model-based-systems-engineering-mbse/, last accessed 2023/11/22.
7. OMG Systems Modeling Language (OMG SysML™). URL: https://sysml.org/.res/docs/specs/OMGSysML-v1.6-19-11-01.pdf, last accessed 2023/11/22.
8. Friedenthal S., Moore A., Steiner R. A Practical Guide to SysML. The Systems Modeling Language. Waltham : Elsevier, 2015. 599 p.

## ФОРМУВАННЯ ІНФОРМАЦІЙНОГО РЕСУРСУ НА ОСНОВІ РІЗНИХ ДЖЕРЕЛ В СИСТЕМАХ ОРГАНІЗАЦІЙНОГО УПРАВЛІННЯ

О.В. Андрійчук[1,2,3], В.В. Юзефович[1], Є.О. Цибульська[1], Ніколай Стоянов[4]
[1]Інститут проблем реєстрації інформації Національної академії наук України, Київ, Україна
[2]Київський національний університет імені Тараса Шевченка, Київ, Україна
[3]Національний технічний університет України “Київський політехнічний
інститут імені Ігоря Сікорського”, Київ, Україна
[4]Болгарський оборонний інститут імені професора Цвєтана Лазарова, Софія, Болгарія
andriichuk@ipri.kiev.ua, uzefv71@gmail.com, evts68@gmail.com, n.stoianov@di.mod.bg

В доповіді розглянуто особливості отримання та обробкизнань різних типів фахівців, як джерел інформації для систем організаційного управління.Запропоновано математичний апарат нечіткої логіки та підтримки прийняття рішень для застосування в системах

організаційного управління при формуванні інформаційного ресурсу

Ключові слова: система організаційного управління, інформаційний ресурс, аналітик, експерт, нечітка логіка, метод цільового динамічного оцінювання альтернатив.

## Вступ

Відповідно до дослідження [1], лев'яча частка знань організацій (близько42%) знаходиться у головах спеціалістів.Однією із особливостей систем організаційного управління (СОУ) є наявність впливів в межах об'єкта і суб'єкта управління людського фактору [2, 3]. Наряду з об'єктивною інформацією (наприклад, показів приладів) у СОУ також в якості джерел інформації досить широко використовуються 5 категорій фахівців [2]: "джерельні" аналітики, аналітики з агрегування (узагальнення) інформації для забезпечення прийняття рішення на різних рівнях управління, експерти, організатори експертизи та інженери знань.Таким чином актуальною задачею є розробка математичного апарату для СОУ, який дозволить якісно використовувати знання всіх згаданих категорій фахівців про формуванні інформаційного ресурсу шляхом врахування їх особливостей.

## Агрегація знань аналітиків

Наведемо евристичні вимоги до агрегації даних від аналітиків, які, на відміну від даних технічних джерел, додатково характеризуються різним ступенем достовірності.

1. При надходженні різних за змістом даних від одного і того самого аналітика, протягом одного циклу управління, отримані дані не об’єднуються і до уваги береться лише останнє надане значення показника.
2. При надходженні від декількох аналітиків повідомлень з однаковими даними різного ступеня достовірності (впевненості у їх істинності) результат їх об’єднання має характеризуватися більшою достовірністю ніж кожне окреме повідомлення.
3. При надходженні від декількох аналітиків даних, що не співпадають за змістом, результат їх об’єднання має характеризуватися не більшим ступенем достовірності, ніж найбільша «заявлена» у повідомленнях достовірність.
4. Якщо зміст наданих аналітиками даних різниться суттєво – загалом має зростати можливість того, що показник насправді

має інше, «проміжне» значення, яке певним чином усереднює отримані дані, із наданням більшої достовірності тому значенню, що тяжіє до більш достовірного «вхідного» повідомлення.

Для практичного втілення сформульованих вимог приформалізації та агрегуванніданих від аналітиків може бути застосовано евристику на основі математичного апарату нечіткої логіки [4].

У такому випадку, кожне повідомлення про значення показника формалізується у вигляді нечіткої множини:

$$S_X = \{\mu_s(x_n)/(x_n)\},\ x_n \in X,$$

де $\mu_s(x_n)=[0,1]$ – ступінь належності значення $x_n$нечіткій множині $S_X$, $X=\{x_1, x_2, x_3, \ldots, x_N\}$ - чітка множина, що є носієм нечіткої множини і містить можливі (допустимі) значення показника, кількістю $N$.

Для остаточної формалізації повідомлення про значення показника у вигляді нечіткої множини окрім множини-носія показника бажано задати ступені належності $\mu_s(x_n)$ для кожного з можливих значень у вигляді функціональної залежності. Відомо багато різних способів задавання функції належності для нечітких множин, найбільш простою з яких є функція трикутної форми, яка описується наступним чином:

$$\mu_s(x_n) = \begin{cases} 0, & \text{якщо} \quad x_n \le a; \\ \dfrac{(x_n - a)}{(C - a)}, & \text{якщо} \quad x_{min} < x_n < C; \\ \dfrac{(b - x_n)}{(b - C)}, & \text{якщо} \quad C \le x_n < b; \\ 0, & \text{якщо} \quad x_n \ge b. \end{cases}$$

де $C$ – значення показника, визначене аналітиком;$a$, $b$ – ліва та права межі трикутної функції належності, яка поширюється і на інші значення показникаокрім $C$, що знаходяться між $a$ та $b$.

Якщо $|C - a| = |C - b|$– функція належності є симетричною відносно $C$. Діапазон значень показника $\Delta_S=|b - a|$визначає перелік його значень наближених до $C$, які можливо насправді приймає показник. Функцію належності можна розглядати як аналогію до розподілу похибки вимірювання показника будь-яким технічним засобом, де значення $C$ – є результат вимірювання,$\Delta_S/2$ – абсолютна похибка вимірювання, а функція належності $\mu_s(x_n)$– закон розподілу похибки.

Для врахування достовірності повідомленнянеобхідно задати числову відповідність (шкалу) визначеним лінгвістичним значенням достовірності (впевненості у значенні показника). Приклад такої відповідності показано у таблиці 1.

Таблиця 1–Лінгвістичні значення атрибуту впевненості тавідповідні їм числові значення

| Лінгвістичне значення атрибуту впевненості | Числове значення атрибуту впевненості (*Ds*) |
|---|---|
| «Достовірно» | 1 |
| «Ймовірно» | 0,7 |
| «Можливо» | 0,5 |
| «Сумнівно» | 0,25 |

Далі усі значення функції належності нормуються відповідним числовим значенням достовірності за виразом:

$$\mu_{DA+B}(x_n)=D_S*\mu_s(x_n).$$

Оскільки таке перетворення функції незалежності є лінійним – вона збереже трикутну форму.

Здійснивши зазначену просту формалізацію усіх вхідних повідомлень від аналітиків можна перейти до вирішення задачі їх об'єднання. В рамках теорії нечітких множин накопичено значний інструментарій для оперування нечіткими множинами. Найбільше відповідає сформульованим вище правилам об'єднання операція алгебраїчної суми нечітких множин. Для об'єднання двох повідомлень *A* та *B* відповідний вираз буде мати вигляд:

$$\mu_{DA+B}(x_n)=\mu_{DA}(x_n)+\mu_{DB}(x_n)-\mu_{DA}(x_n)*\mu_{DB}(x_n).$$

Останньою операцією є отримання об'єднаного значення показника та визначення його достовірності для чого може бути використано вираз для отримання зваженого середнього нечіткої множини $\mu_{DA+B}(x_n)$:

$$x_{\overline{AB}}=\frac{\sum_{n=1}^{N} x_n\cdot\mu_{D_{A+B}}(x_n)}{\sum_{n=1}^{N}\mu_{D_{A+B}}(x_n)}.$$

Така операція називається дефаззифікацією нечіткої множини. Достовірність отриманого значення буде визначатися ступенем належності отриманого зваженого середнього:

$$D_{\overline{AB}} = \mu_{D_{A+B}}\left(x_{n_{\overline{AB}}}\right).$$

Запропонований підхід дозволить зменшити вплив суб'єктивної складової на результат обробки даних від аналітиків.

## Агрегація знань експертів

При формуванні інформаційного ресурсу СОУ також слід враховувати певні особливості експертних знань [5]. Під час проведення експертного оцінювання можуть виникати когнітивні викривлення даних та знань, які значно впливають на його результат. Людські психофізіологічні обмеження обмежують здатність одночасно опрацьовувати більше ніж 9 об'єктів. Експертне оцінювання вимагає значних часових затрат і є вартісним процесом, тому його краще застосовувати лише у випадках нагальної потреби. Якщо можливо, рекомендується використовувати раніше побудовані бази знань (БЗ), їх фрагменти та шаблони (прецеденти) вирішення схожих задач у ретроспективі. Експерти можуть пропустити сеанси оцінювання, не відповідати на деякі питання через обмежений час, велику зайнятість, втому або небажання. Тому важливо мати можливість обробки неповної експертної інформації. При цьому, потреби в узагальнених та систематизованих знаннях поступово розкриваються шляхом декомпозиції на менших рівнях ієрархії СОУ, а деталізована інформація «знизу вверх» агрегується для задоволення інформаційних потреб користувачів більш високих рівнів управління.

Для агрегації знань експертів використовується метод цільового динамічного оцінювання альтернатив (МЦДОА), в рамках якого будується ієрархія цілей [6]. Вона є результатом декомпозиції головної цілі на складові (підцілі), які, в свою чергу, також декомпозуються на підцілі і т.д. Процес декомпозиції зупиняється, коли в якості складових отримаємо конкретні заходи (проєкти).

МЦДОА пропонує узагальнену процедуру визначення ступеня досягнення будь-якої цілі ієрархії в заданий момент часу *t*. Для визначення ступеня досягнення певної цілі необхідно проаналізувати ступені досягнення цілей, які безпосередньо впливають на цю ціль, для кожної підмножини сумісних цілей [6]. Таким чином, ступінь досягнення *h*-ї цілі в момент часу *t* описується формулою для $d_i(t)$:

$$d_i(t) = \begin{cases} 0, & if \quad D_i(t) < T_i, \\ T_i, & if \quad D_i(t) = T_i, \\ f\big(D_i(t)\big), & if \;\; T_i < D_i(t) < 1 - \sum |w_{ij}^{(\bar{k})}| \\ 1, & if \quad 1 - \sum |w_{ij}^{(\bar{k})}| \leq \; D_i(t) \leq 1, \end{cases}$$

де: $D_i(t) = \sup_k \sum_j w_{ij}^{(k)} d_j(t)$;$T_i$ – поріг досягнення *i*-ї цілі;*f(D*$_i$*(t))*– функція ступеня досягнення *i*-ї цілі в момент часу t; $w_{ij}^{(\bar{k})} w_{ihk}$ – часткові коефіцієнти впливу*j*-ї цілі в *k*-й групі сумісних цілей, який має негативний вплив на *i*-ту ціль.

В якості практичного прикладу запропонований математичний інструментарій було використано для побудови бази знань Стратегії енергетичної безпеки України [7]. Отримані результати підтвердили застосовність запропонованого підходу до вирішення таких задач.

## Висновки

Показано особливості знань аналітиків та експертів, характерних для СОУ, які в подальшому складають інформаційну основу баз даних та БЗ при формуванні інформаційного ресурсу СОУ. Виділено п’ять типів фахівців - джерел інформації в СОУ.

Запропоновано використовувати апарат нечіткої логіки для обробки інформації «джерельних» аналітиків та аналітиків з агрегування в інформаційно-аналітичній підсистемі СОУ.

Запропоновано використовувати при побудові БЗ підсистеми підтримки прийняття рішень СОУ наряду з об'єктивною та експертною інформацією ще й інформацію отриману від аналітиків після попередньої її обробки.

## Перелік посилань


1. V. Shabrina, A. Silvianita. Factors Analysis on Knowledge Sharing at Telkom Economic and Business School (TEBS) Telkom University Bandung. In: Procedia - Social and Behavioral Sciences, vol. 169, 2015, pp. 198-206. DOI: 10.1016/j.sbspro.2015.01.303.
2. В.В. Юзефович, О.В. Андрійчук, Є.О. Цибульська, Ніколай Стоянов Врахування особливостей експертних знань в системах організаційного управління при формуванні

інформаційного ресурсу // Інформаційні технології та безпека. Матеріали XXII Міжнародної науково-практичної конференції ІТБ-2022. – Київ: Інжиніринг. - С.84-89.
3. Volodymyr Yuzefovych, Yevheniia Tsybulska, Oleh Andriichuk One Approach to Formation of Common Information Space Information Resourcein Organizational Management Systems / CEUR Workshop Proceedings (ceur-ws.org). Vol. 3241 urn:nbn:de: 0074-3241-0. Selected Papersof the XXI International Scientific and Practical Conference "Information Technologies and Security" (ITS 2021), Kyiv, Ukraine, December 9, 2021. - pp. 215-224. [http://ceur-ws.org/Vol-3241/paper20.pdf]
4. Потій О.В., Лєншин А.В. (2005). Основні положення математичного апарату суб'єктивної логіки та його застосування для оцінки рівня зрілості систем забезпечення безпеки інформації // Радіотехніка. Тематичний випуск "Інформаційна безпека" - Харків: Харківський національний університет радіоелектроніки. с. 144–160.
5. О.В. Андрійчук, В.В. Циганок, С.В. Каденко, Я.В. Порпленко, Мінглей Фу, О.О. Власенко Підходи до врахування когнітивних упереджень експертів в системах підтримки прийняття рішень / Інформаційні технології і безпека. Матеріали XXI Міжнародної науково-практичної конференції ІТБ-2021, 09 грудня 2021, Київ, Україна. - К.: ООО "Инжиниринг", 2021. - С. 225-229.
6. В.Г. Тоценко Методы и системы поддержки принятия решений. Алгоритмический аспект – К.: Наук. думка, 2002. – 382 с.
7. Стратегія енергетичної безпеки України.URL:https://zakon.rada.gov.ua/laws/show/907-2021-%D1%80#n10

# МЕТОДИ МАНІПУЛЮВАННЯ ВИБОРОМ В ЗАДАЧАХ ЕКСПЕРТНОГО ОЦІНЮВАННЯ

Г.М. Гнатієнко
Київський національний університет імені Тараса Шевченка,
Київ, Україна
g.gna5@ukr.net

Розглянуто проблему маніпулювання вибором на усіх етапах застосування експертних технологій. Введено означення маніпулювання для ситуації експертного оцінювання. Сформульовано евристики, які забезпечують дослідження проблеми маніпулювання при застосуванні експертних технологій. Запропоновано основи методології протидії маніпулюванню при експертному оцінюванні.

## Вступ

Задачі експертного оцінювання застосовуються у найрізноманітніших сферах людської життєдіяльності і є важливим інструментом вирішення проблем, які виникають при необхідності формалізації та структуризації ситуацій у різних предметних областях. Експертні технології часто можуть виявитися єдино можливим способом одержати прийнятне вирішення практичної проблеми. Оскільки такі рішення апріорно не є оптимальними, а завжди компромісними, то їхня природа надає широкі можливості для маніпулювання. Ця робота присв'ячена побудові математичної моделі маніпулювання експертних технологій.

## Формалізація експертних технологій прийняття рішень

Задачі експертного оцінювання представляються у вигляді кортежу

<A, S, R, E, C, P>,

де A – множина об'єктів (варіантів, альтернатив, наборів параметрів), S – множина обмежень, R – множина критеріїв, шкал вимірювання по критеріях, відображення множини допустимих альтернатив у множину критеріальних оцінок, згорток критеріїв, E – множина формальних характеристик експертів, C – множина цілей, що стоять перед дослідниками, P – система переваг, задана особою, що приймає рішення (ОПР), колективом ОПР при

колегіальному прийнятті рушень або групи експертів на різних етапах підготовки до прийняття рішення.

*Одним із підходів, який застосовується для класифікації задач експертного оцінювання в теорії дослідження операцій, є розгляд пари* $\langle C, A \rangle$,

*де* $C$ *– принцип оптимальності,*

$A$ *– задана множина об'єктів.*

*В теорії дослідження операцій пара* $\langle C, A \rangle$ *називається по різному, залежно від виду та особливостей її складових:*

*– задачею прийняття рішень, якщо* $C$ *та* $A$ *не є апріорно заданими і можуть варіюватися;*

*– задачею вибору, якщо множина об'єктів* $A$ *є заданою, а принцип оптимальності* $C$ *– таким, що варіюється;*

*– загальною задачею оптимізації, коли* $C$ *та* $A$ *є заданими.*

Розв'язком ЗЕО $\langle C, A \rangle$ є підмножина об'єктів

$$A_0 \subset A, \qquad (1)$$

одержана з використанням принципу оптимальності: $A_0 = C(A)$.

Нехай задано множину $A$, що складається з $n$ об'єктів, які порівнюються між собою:

$$a_i \in A, \ i \in \{1,...,n\} = I.$$

Об'єкти описуються множиною $m$ параметрів, тобто кожен об'єкт є точкою деякого параметричного простору $\Omega^m$

$$a_i = \left(a_i^1,...,a_i^m\right), \ a_i \in A, \ i \in I, \ A \subset \Omega^m,$$

де $a_i^j$, $i \in I$, $j \in \{1,...,m\} = J$, – значення $j$-го параметра $i$-го об`єкта.

З множини $A$ вирішуючим елемепнтом вибирається найкращий за встановленими критеріями об'єкт та обґрунтовується його вибір. Зрозуміло, що вже на етапі обґрунтування підходів до вибору та власне самої процедури вибору виникають можливості для маніпулювання результатами розв'язання задачі.

## Маніпулювання вибором при застосуванні експертних технологій

Існує багато різних означень поняття маніпулювання, які застосовуються при вивченні проблеми маніпулювання у різних галузях науки.

Маніпулюванням вибором будемо називати сприяння вибору прийнятного для зацікавлених осіб рішення задачі експертного оцінювання серед компромісних рішень виду (1).

У більшості випадків це не є обманом, не є підміною і не є підтасовкою фактів. Маніпулювання полягає у виборі такого інструментарію для формалізації проблеми, який дозволить задовольнити побажання деякої зацікавленої групи осіб у легітимному прийнятті «правильного» рішення. Причому, в таких ситуаціях використання математичних методів, моделей, психологічних особливостей людини для одержання тенденційного рішення, яке є достатньо обгрунтованим, щоб мати ознаки об'єктивності.

Введемо низку евристик, які дозволяють формалізувати задачу виявлення можливостей маніпулювання, їх структуризацію та забезпечити протидію таким спробам.

Евристика Е1. Оскільки на усіх етапах експертного оцінювання виникають проблеми, вони можуть бути вирішені різними способами.

Евристика Е2. Відповідно, результати вирішення проблем можуть використані в інтересах учасників процесу, замовників експертизи чи кінцевих бенефеціарів.

Евристика Е3. Для усіх рішень може бути знайдене обгрунтування та підкріплене відповідними математичними обчисленнями.

Евристика Е4. Можна дослідити якість обгрунтування рішення у задачі експертного оцінювання та запропонувати більш обгрунтовані рішення. Тобто, у цій сфері можна таємне зробити явним.

## Методологічні основи протидії маніпулюванню вибором при застосуванні експертних технологій

Можна запропонувати цілу низку підходів, які є методологічною основою протидії маніпулюванню при застосуванні експертних ехнологій.

1. Формалізація усіх етапів експертного оцінювання.

2. Виявлення та фіксування усіх евристик, які застосовуються. При цьому слід враховувати означення евристики та їх прояви: постулат, гіпотеза, аксіома, презупція тощо.
3. Застосування м'яких обчислень, зокрема, методів побудови функцій належності нечіткій множині: нашарування; частотності значень; апроксимації трикутною чи трапецієподібною функцією належності тощо.
4. Виявлення коаліцій серед учасників процедури експертного оцінювання.
5. Дослідження динаміки прийняття рішень коаліціями.
6. Застосування адаптивних методів та обгрунтування: чому застосовуються конкретні евристики.
2. Візуалізація, ілюстрація, інтерпретація альтернатив.
3. Визначення відстаней від ідеального рішення та альтернативних рішень між собою.
4. Застосування преференційного ранжування, а не простого вибору.
5. Використання непрямі методів замість прямих: врахування обмежених можливостей людей.
6. Виявлення перетинів та меж схожості між згортками критеріїв, які застосовуються.
7. Визначення ідеальних ранжувань та обчислення компромісів між ними.

# ВИКОРИСТАННЯ РЕПОЗИТОРІЮ СКЛАДНИХ ІНФОРМАЦІЙНИХ ОБ'ЄКТІВ ДЛЯ РОЗРОБЛЕННЯ СЕМАНТИЧНИХ АНАЛІТИКО-ІНФОРМАЦІЙНИХ СИСТЕМ

Ю.В. Рогушина[1], А.Я. Гладун[2]

[1]Інститут програмних систем НАНУ, Київ, Україна,
[2]Міжнародний науково-навчальний центр інформаційних технологій та систем НАНУ та МОНУ, Київ, Україна
ladamandraka2010@gmail.com, glanat@yahoo.com

Створення інформаційно-аналітичних систем (ІАС) потребує отримання знань із різноманітних зовнішніх інформаційних ресурсів, структура та контент яких можуть

змінюватися. Для автоматизації експорту таких знань пропонується використовувати репозиторії інформаційних об’єктів, що розширюють функціонал репозиторіїв онтологій та підтримують пошук класів та екземплярів класів за заданими властивостями та відношеннями. Доцільність цього розглянуто на прикладі розробки веборієнтованої ІАС «е-Підручник»
**Ключові слова:** репозиторій інформаційних об’єктів, інформаційно-аналітична система, складний інформаційний об’єкт, онтологія.

## Вступ

Створення прикладних інформаційно-аналітичних систем (ІАС) потребує формалізації знань про предметну область (ПрО) та інформаційні об'єкти (ІО), які є складовими компонентами системи. Це потребує отримання знань із зовнішніх інформаційних ресурсів (ІР), структура та контент яких можуть змінюватися. Формальні моделі семантики ІО потрібні для формалізації та забезпечення однозначної інтерпретації їхнього змісту, а також для однозначного та інтероперабельного визначення структури та взаємозв’язків інформаційних об’єктів. Для автоматизації експорту та структурування таких знань (відомостей) запропоновано застосовувати онтологічних підхід для отримання відомостей із зовнішніх онтологій. Онтологічні моделі дозволяють формалізувати властивості тих інформаційних об’єктів, які є предметом аналізу в ІАС, визначати терміносистему для обробки матеріалів та встановлювати семантичні зв’язки з іншими джерелами інформації [1].

З точки зору онтологічного аналізу [2] ІО — класи або екземпляри онтології, які характеризуються своєю структурою і відношеннями з іншими ІО. Однак для вирішення багатьох прикладних задач потрібно аналізувати більш складні сукупності інформації, які містять ІО різних типів, що пов’язані відношеннями та обмеженнями між ними та між їхніми властивостями – *складними інформаційними об’єктами* (СІО).

## Джерела інформації про СІО

Кожен екземпляр СІО — це набір з більше ніж одного екземпляра ІО, які пов’язані один з одним онтологічними відношеннями та відповідають вимогам щодо структури і значень властивостей ІО [3]. Приклади СІО – організація, набір її

співробітників та множина проектів, які виконуються в організації; навчальний заклад та набір спеціальностей, за якими проводиться навчання і множина компетенцій, які цими спеціальностями забезпечуються [4]. Формальна модель СІО базується на онтології ПрО. У моделі СІО використовується така непорожня підмножина елементів онтології, яка виокремлює набір екземплярів класів, між екземплярами яких в СІО визначені певні семантичні відношення.

Наразі у відкритому вебсередовищі існує велика кількість онтологій, які характеризують різні аспекти ПрО з тим ступенем виразності та деталізації, що визначається цілями розробки таких онтологій, але для створення ІАС потрібно знаходити не окремі класи онтології або їхні екземпляри, а набори екземплярів певних класів, які знаходяться один з одним у потрібних відношеннях. Для побудови структури бази знань будь-якої ІАС доцільно використовувати зовнішні онтології, які уможливлюють визначення структури СІО відповідно до загально прийнятих правил. Наприклад, у пошуку навчальних матеріалів потрібно використовувати зовнішні онтології, які містять різні аспекти знань про навчальний процес, освіту та ті спеціальності, навчання яким потребує використання цих матеріалів. Але пошук таких відомостей у пертинентних онтологіях не є простою задачею, яку можна виконувати автоматично.

Це спричиняє потребу створення репозиторіїв СІО, що підтримують набір функцій, аналогічний репозиторіям онтологій [5] або документів, але підтримують пошук на більш детальному рівні. Важливо зазначити, що такі репозиторії можуть поповнюватися відомостями як із зовнішніх онтологій, так і з семантично розмічених документів. Крім того, інформація щодо СІО може вноситися або редагуватися вручну експертами відповідної ПрО. Специфічними для репозиторіїв СІО є такі функції: пошук класів, що містять визначений набір об’єктних властивостей; пошук екземплярів класів, для яких визначені значення певних властивостей; пошук екземплярів обраних класів, що є між собою у визначених відношеннях; перевірка існування екземплярів класів, що відповідають визначеному набору умов; пошук семантично близьких класів та порівняння їхніх екземплярів (з використанням різних мір семантичної близькості та семантичної подібності).

## Використання репозиторію СІО для системи «е-Підручник»

Веборієнтована ІАС «е-Підручник» призначається для надання доступу студентам та викладачам українських університетів до навчальних матеріалів — підручників, довідників, методичних вказівок тощо. Постачальниками контенту системи «е-Підручник» можуть бути: книговидавці, які видають підручники; викладачі, які готують підручники зі своєї спеціальності; кафедри університетів; інші зацікавлені особи, власники відповідних інформаційних ресурсів. Крім того існує імпорт контенту з зовнішніх джерел (е-бібліотек, репозиторіїв). Основні СІО, що мають бути подані в системі «е-Підручник»: «підручник»; «автор»; «видавець»; «спеціальність;, «компетенція»; «навчальний курс (модуль)». Система повинна підтримувати пошук та співставлення на семантичному рівні таких СІО, щоб шукати підручники не тільки за назвою та спеціальністю, а з урахуванням значно більшої кількості параметрів (таких, як рік видання, мова подання, рівень складності та якість подання матеріалу). Але у різних електронних бібліотеках такі ІО мають різну структуру, і тому виникає потреба в їх уніфікації на основі знань про ці СІО з різних онтологій.

Саме для пошуку елементів такої структури виникає потреба в репозиторії СІО, який підтримує пошук екземплярів різних онтологічних класів, пов’язаних певними типами семантичних відношень.

## Висновки

При створені прототипу системі «е-Підручник» були сформовані базові вимоги до репозиторію СІО та проаналізовані технології, які доцільно застосувати для його поповнення. Створення таких репозиторіїв забезпечує більшу деталізацію структури знань ПрО та розширює виразність пошукових запитів.

## Перелік посилань

1. Рогушина Ю.В., Гладун А.Я. Використання онтологічних знань для багатокритеріального співставлення складних інформаційних об`єктів // Проблеми програмування, 2022, №2–3. С. 249–259. URL: pp.isofts.kiev.ua/ojs1/article/view/526/523. doi: https://doi.org/10.15407/pp2022.03-04.249

2. Guarino N. Formal Ontology and Information Systems. Formal Ontology in Information Systems. Proceedings of FOIS'98, Trento. Italy, Amsterdam, IOS-Press. 1998. P. 3–15. https://www.researchgate.net/publication/272169039_Formal_Ontologies_and_Information_Systems
3. Rogushina J., Gladun A., Valencia-Garcia R. Reuse of Ontological Knowledge in Open Science: Models, Sources, Repositories. In: Communications in Computer and Information Science, Springer Cham, 2023, pp. 157–172 . DOI: 10.1007/978-3-031-45682-4_12
4. Gladun A., Rogushyna J. Repositories of ontologies as a means of reuse of knowledge for recognition of information objects // Ontology of design, № 1 (7), 2013. С. 35–50.

## ADAPTABLE AND SCALABLE DECENTRALIZED GOVERNANCE ON EVM-COMPATIBLE BLOCKCHAIN

Larysa Katerynych, Maksym Veres, Kostiantyn Zhereb and Kyrylo Riabov
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
katerynych@gmail.com, veres@ukr.net, zhereb@gmail.com, kyryl.ryabov@gmail.com

This paper explores scalable and adaptable governance through decentralized networks, enabling collective decision-making and easier evolution when requirements change. We use interconnected Smart Contracts on the EVM-based blockchain to resolve foundational governance issues. We introduce a solution that combines a role-based access system and a modular system contracts architecture to enhance the system's scalability and adaptability. This approach allows for modifications and scaling at any time through community proposals and voting. Members can propose configuration parameters for a new module, and with community majority approval, the system can adapt and scale.
**Keywords:** Decentralized Autonomous Organization, Decentralized Governance, WEB3, Role-Based Access System, Ethereum, Blockchain, Solidity

## Introduction

Implementing decision-making on the Internet poses a significant challenge in establishing a robust system where members cannot manipulate outcomes and only eligible parties can participate. Recently, new approaches appeared based on Blockchain, Smart Contracts [1] and Decentralized Autonomous Organizations (DAOs). While such approaches are effective for smaller communities, they struggle with larger, continuously evolving systems. Some issues include complexity and risks of updating contract logic, size limitations negatively affecting scalability, as well as inability to adapt existing DAOs to new requirements and protocols.

To address these limitations, we propose a modular architecture incorporating a role-based access system. This approach eliminates the need for system redeployment and reconfiguration, and empowers the community to modify the system's functionality through voting, ensuring security and sustainability as long as the majority actively cooperate.

## Our approach

This paper introduces a Role-Based Access System (RBAS) serving as a pivotal connector between system components. RBAS establishes a set of transparent and comprehensible rules that delineate access to system resources.

In many solutions, contracts depend on account addresses to determine resource access, a method that restricts the system to specific addresses. RBAS, in contrast, abstracts resource access to parties with specific permissions, granted through community voting. It centralizes all access rules, unlike traditional approaches where access to protected functions requires extensive contract code analysis. Despite the additional gas usage, RBAS compensates by facilitating a more manageable and adaptable system.

To construct a system capable of scaling indefinitely, we propose a Modular System Contract Architecture, aligning with the standards proposed in ERC-2535 [2]. Given the restrictive 24KB [3] contract size limitation, this architecture organizes a collection of Smart Contracts under the ERC-2535 standard to accommodate extensive systems.

The adaptability inherent in Modular Smart Contracts Architecture allows DAOs to seamlessly integrate or modify modules, ensuring continuous compliance with evolving disclosure regulations

and aligning with the transparency and consumer protection needs of the decentralized finance ecosystem [4]. For enhanced scalability in governance, we have streamlined the ERC-2535 standard to increase transparency [5] for external developers and, crucially, for end-users interacting with the system.

Traditional governance modules predominantly rely on the voting power of community members, however in larger communities this may result in suboptimal decisions. To mitigate this, we introduce a Veto Process, based on Expert Group, comprised of members with the authority to veto community-selected proposals and to initiate expert-specific proposals. The veto process is integral to the governance of the DAO, acting as a protective mechanism to halt proposals that may diverge from the DAO's foundational principles and constitution. This process is reserved for Experts, appointed during the DAO governance process, and serves as a safeguard to ensure the alignment of all proposals with the DAO's values and objectives. This additional protective layer aims to reduce the risk of system stagnation by ensuring that decisions are meticulously scrutinized and are reflective of informed and expert opinions, thereby enhancing the robustness and reliability of the governance structure.

## Application Example

We demonstrate our approach using an example of integrating a new AirDrop module, which requires one proposal from the community, as shown in Figure .

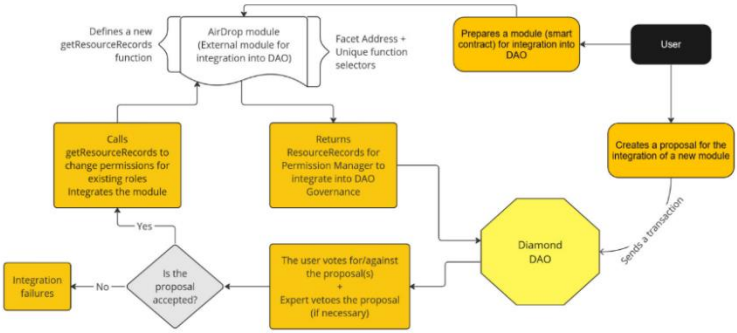



Figure 1: Example of AirDrop Module Integration

Due to the modular smart contract architecture, the new AirDrop module can be easily integrated into the DAO core, allowing access to

the entire DAO storage. In addition, the role-based access system (RBAS) ensures that this module is simultaneously integrated into the DAO governance system. This means that any configuration desired by the DAO can be achieved, such as a configuration where only experts manage the new module. However, the initial adoption of such rules is subject to community approval.

## Conclusion

This paper presents a scalable and adaptable governance system on the Ethereum network, designed to circumvent the inherent limitations of the Ethereum protocol. The foundation of this system is the Role-Based Access System (RBAS), which orchestrates the interactions between various components within a Decentralized Autonomous Organization (DAO). We introduced a modular system architecture, allowing the DAO to expand and integrate a diverse range of modules while maintaining coherent governance. This modular approach, coupled with the Expert governance structure, enhances the security and reliability of the system, ensuring robust protection against potential vulnerabilities.

## References


6. A. M. Antonopoulos, G. Wood. Mastering Ethereum: Building Smart Contracts and DApps, O'Reilly Media, 2018. 422 p.
7. N. Mudge. EIP-2535: Diamonds, Multi-Facet Proxy. 2020. URL: https://eips.ethereum.org/EIPS/eip-2535.
8. G. Wood. Ethereum: a secure decentralised generalised transaction ledger. Berlin version 2bcdb2d. 2023. URL: https://ethereum.github.io/yellowpaper/paper.pdf.
9. C. Brummer. Disclosure, DApps and DeFi. Stanford Journal of Blockchain Law & Policy, Vol 5.2. 2022. pp. 137-147. URL: https://stanford-jblp.pubpub.org/pub/disclosure-dapps-defi
10. T. Sharma, Z. Zhou, A. Miller, Y. Wang. A {Mixed-Methods} Study of Security Practices of Smart Contract Developers. In 32nd USENIX Security Symposium (USENIX Security 23). 2023. pp. 2545-2562.

# УПРАВЛІННЯ ЛОГІСТИЧНИМИ ПРОЦЕСАМИ У ТРАНСПОРТНІЙ СФЕРІ

В.С. Погребний
Європейський Університет, м.Київ, Україна
vpohrebnyj@e-u.edu.ua

У даній роботі розглянуто ключові аспекти управління логістикою в транспортній сфері. Зокрема, досліджено інтегрований підхід, використання сучасних технологій, стратегічне планування, гнучкість систем та стратегію управління ризиками. Результати вказують на необхідність комплексного підходу для оптимізації логістичних процесів та забезпечення конкурентоспроможності підприємств у транспортній галузі.

**Ключові слова:** логістика, транспортна галузь, інтегрований підхід.

## Вступ

Управління логістичними процесами у транспортній сфері стає все більш складним завданням у сучасному світі. З плином часу та розвитком технологій виникає необхідність вдосконалення методів керування, серед яких особливе місце займають автоматичні рішення та імітаційне моделювання [1].

Автоматичні рішення в логістиці транспортної сфери дозволяють ефективно керувати та оптимізувати різноманітні процеси, використовуючи аналіз даних та алгоритми для прийняття швидких та точних рішень [2]. Вони спрощують вирішення завдань з розподілу ресурсів, маршрутизації транспорту, управління запасами та планування доставок.

Щодо імітаційного моделювання, цей підхід надає можливість створення віртуальних моделей для аналізу та передбачення поведінки системи логістики у різних умовах. Це дозволяє експериментувати з різними стратегіями управління та вирішення проблем, що допомагає вдосконалювати процеси без прямого втручання в реальну систему.

Об'єднання цих підходів в управлінні логістичними процесами у транспортній сфері створює потенціал для зменшення витрат, оптимізації часу та ресурсів, підвищення рівня сервісу та адаптації до змінних умов ринку.

## Результати дослідження

Управління логістикою в транспорті базується на кількох ключових підходах: інтегрованому підході, технологічному прогресі, стратегічному плануванні, гнучкості та адаптивності, а також стратегії управління ризиками. Ці підходи дозволяють створювати ефективні системи управління, які відповідають потребам сучасного ринку та підвищують конкурентоспроможність підприємств у транспортній сфері.

Управління логістикою в транспорті базується на комплексному підході до оптимізації та координації різноманітних процесів. Це включає інтеграцію всіх ланок логістичного ланцюжка, починаючи від складу і закінчуючи доставкою, для максимізації ефективності та мінімізації затримок.

Спираючись на сучасні досягнення в області технологій, управління використовує Інтернет речей (IoT), штучний інтелект (AI) та системи аналітики даних для поліпшення моніторингу та прогнозування транспортних операцій [3].

Стратегічне планування враховує вимоги клієнтів, оптимізацію маршрутів та раціональний вибір видів транспорту для оптимізації витрат.

Гнучкість системи управління логістикою в транспорті визначається її здатністю швидко адаптуватися до змін на ринку, у технологіях та внутрішніх процесах для забезпечення максимальної ефективності.

Стратегія управління ризиками передбачає попереднє планування та реагування на можливі негативні сценарії, такі як затримки чи пошкодження вантажів, для мінімізації впливу на операційні процеси. Ці інтегровані підходи створюють динамічні та ефективні системи управління логістикою в транспорті, які відповідають сучасним вимогам ринку та сприяють підвищенню конкурентоспроможності підприємств у цій галузі.

З розвитком технологій, таких як розширені аналітичні інструменти та інтелектуальні системи управління, управління логістикою отримує нові можливості для точного прогнозування попиту, оптимізації маршрутів та виявлення ризиків [4].

Гнучкість системи управління логістикою в транспорті також вимагає постійного вдосконалення. Це означає здатність оперативно реагувати на зміни попиту, технологічні інновації та непередбачувані обставини, такі як припинення роботи певних

маршрутів чи виникнення небезпечних ситуацій під час транспортування.

Стратегія управління ризиками постійно адаптується до нових викликів. Вона базується на постійному аналізі та вдосконаленні процедур для мінімізації впливу можливих загроз на ефективність та безперебійність логістичних операцій.

Ці підходи утворюють основу для створення динамічних та ефективних систем управління логістикою в транспорті, які забезпечують не лише потрібну ефективність, а й спроможність адаптуватися до постійно змінюючогося оточення [5].

## Висновки

Управління логістикою в транспорті відіграє вирішальну роль у підтримці ефективності та конкурентоздатності підприємств. Інтеграція, використання передових технологій, стратегічне планування та гнучкість систем управління створюють надійні механізми, що дозволяють адаптуватися до швидкозмінюваних умов ринку. Такий комплексний підхід сприяє ефективній оптимізації логістичних процесів, що є важливим елементом для успішної діяльності в умовах сучасного бізнесу та сприяє забезпеченню високого рівня задоволеності клієнтів.

## Список використаної літератури


1. Давідіч Ю. О. Теоретичні основи ергономічного забезпечення автотранспортних технологічних процесів: автореф. дис. ... д-ра техн. наук: 05.22.01; 05.01.04 / Юрій Олександрович Давідіч; Харківська національна академія міського господарства. – Х., 2007. – 42 с.
2. Крикавський Є. В. Логістика. Основи теорії / Є. В. Крикавський. – Львів: «Інтелект-Захід», 2006. – 456 с.
3. Чухрай Н. Формування ланцюга поставок: питання теорії та практики. Монографія / Н. Чухрай, О. Гірна. – Львів: «Інтелект-Захід», 2007. – 232 с
4. Харрісон Алан. Управління логістикою: Розробка стратегій логістичних операцій / Алан Харрісон, Хоук Ремко Ван. – [пер. с англ.]. – [за наук. ред. О.Є. Міхейцева]. – Дніпропетровськ: Баланс Бізнес Букс, 2007. – 368 с.
5. Левковець П. Р. Координація роботи різних видів транспорту [Електронний ресурс] / П. Р. Левковець, П. В. Нікітін, А. В. Лабута. – Режим доступу:

http://www.nbuv.gov.ua/portal/natural/Upsal/2008_5/08lprdkt.pdf. – Назва з екрану.

# ЗАСТОСУВАННЯ ЗАСОБІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПОКРАЩЕННЯ ЕКСПЕРТНИХ ФОРМУЛЮВАНЬ ПРИ ПОБУДОВІ БАЗ ЗНАНЬ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

О.В. Андрійчук[1,2,3], С.В. Каденко[1], Анна Флорек-Пашковська[4]
[1]Інститут проблем реєстрації інформації Національної академії наук України, Київ, Україна
[2]Київський національний університет імені Тараса Шевченка, Київ, Україна
[3]Національний технічний університет України "Київський політехнічний
інститут імені Ігоря Сікорського", Київ, Україна
[4] CENTRUM Católica Graduate Business School Pontificia Universidad Católica del Perú, Ліма, Перу
andriichuk@ipri.kiev.ua, seriga2009@gmail.com, aflorekpaszkowska@pucp.edu.pe

Доповідь присвячено проблемі застосування засобів штучного інтелекту для покращення експертних формулювань при побудові баз знань систем підтримки прийняття рішень. Розглянуто задачі, що виникають при побудові бази знань слабко структурованих предметних областей, та запропоновано відповідні підходи до використання засобів штучного інтелекту. Проведено відповідне експериментальне дослідження, результати якого вказують на те, що таке застосування засобів штучного інтелекту на практиці доцільне лише в автоматизованому варіанті із залученням групи експертів.
**Ключові слова**: аналітик, експертні знання, інформаційний ресурс, система організаційного управління.

## Вступ

Результатом застосування систем підтримки прийняття рішень (СППР) є рекомендації для осіб, що приймають рішення [1]. Для цього відбувається моделювання слабко структурованої предметної області [2] засобами СППР на основі побудованої

відповідної бази знань (БЗ). Однією з важливих властивостей таких предметних областей є неповнота опису об'єктів, яка унеможливлює створення якісної навчальної вибірки для застосування машинного навчання. Відтак, доводиться використовувати знання експертів. Проведення експертиз, зокрема групових, вимагає значних часових та фінансових затрат.

Останнім часом, інструменти штучного інтелекту (ШІ), які базуються на великих лінгвістичних моделях, реалізованих з використанням штучних нейронних мереж з архітектурою трансформер [3, 4], здобули значну популярність через свою зручність та доступність. Ці інструменти швидко й широко розповсюдилися серед користувачів, знайшли пряме застосування у практиці підготовки та написання різних видів робіт, включно з науковими працями, зокрема, англомовних текстів, а також у видавничій справі [5]. Деякі дослідники навіть використовують ці засоби ШІ для побудови мереж ключових слів як концептуальних моделей для певних предметних областей [6]. Проте розробники таких інструментів попереджають, що великі мовні моделі не надають гарантій стосовно правдивості або надійності вихідних даних [4].

Вищевказані міркування зумовлюють необхідність та актуальність дослідження можливостей використання засобів ШІ в СППР для побудови моделей слабко структурованих предметних областей.

**Побудова БЗ слабко структурованої предметної області**

На рис. 1 показано задачі, що виникають при побудові БЗ слабко структурованих предметних областей [7]. При отриманні знань від експертних груп проводиться декомпозиція цілей та визначення (оцінювання) ступенів їхнього впливу. При формулюванні цілей кожен експерт з групи надає тексти своїх індивідуальних формулювань підцілей. Визначаються підмножини однакових за змістом формулювань. Відбувається вибір кращого формулювання в кожній підмножині. Під час встановлення впливів між цілями слід шукати у БЗ цілі, які впливають на певну ціль, а також цілі, на які впливає певна ціль. Під час групового експертного оцінювання ступенів впливу, агрегація відповідних оцінок відбувається за умови досягненні достатнього рівня узгодженості. Під час агрегування знань, отриманих від різних експертних груп, відбувається пошук та об'єднання в БЗ цілей однакових за змістом, але сформульованих

різними групами. Також відбувається «до-встановлення» впливів о об'єднаній множині цілей з перенормуванням відповідних значень ступенів впливу. При цьому, слід шукати у БЗ цілі, які впливають на певну ціль, а також цілі, на які впливає певна ціль.


Рис. 1. Задачі, що виникають під час побудови БЗ слабко структурованих предметних областей

Майже для всіх вищезгаданих задач, у побудові БЗ слабко структурованих предметних областей доцільно використовувати засоби ШІ. Виникає питання, чи можна повністю покладатися на рекомендації ШІ та виконувати ці задачі в автоматичному режимі? Нижче приведено результати проведеного експериментального дослідження достовірності рекомендацій засобів ШІ щодо покращення експертних формулювань. Ці результати свідчать про те, що таке застосування засобів ШІ на практиці доцільне лише в автоматизованому режимі із залученням групи експертів. Повністю покладатись на рекомендації засобів ШІ на даному етапі його розвитку недоцільно.

**Експериментальне дослідження достовірності рекомендацій засобів ШІ щодо покращення експертних формулювань**

Проведене експериментальне дослідження достовірності рекомендацій засобів ШІ щодо покращення експертних формулювань складалося з трьох етапів:

1. Група експертів-респондентів надала тексти своїх англомовних формулювань. Більшість цих текстів було перекладено з української та російської мов за допомогою машинного перекладу та кваліфікованих перекладачів англійської мови. Кожен експерт з цієї групи має спеціалізацію в галузі інформаційних технологій та безпеки. Англомовні тексти, що містять експертні формулювання, належать саме до цієї галузі. Також слід зазначити, що для цих експертів англійська не є рідною мовою.

2. В ході застосування інструментарію ШІ з архітектурою GPT-3.5, були отримані рекомендації щодо поліпшення якості англомовних текстів, що містять експертні формулювання. Для цього були використані спеціальні запити (prompts) до інструментарію ШІ.

3. Група експертів-валідаторів оцінила достовірність та якість англомовних текстів, що містять експертні формулювання, а також рекомендацій, отриманих від інструментарію ШІ. Ця група експертів має компетенцію в галузі інформаційних технологій та безпеки, а також вільно володіє англійською. Крім того, ця група консультувалася з групою експертів, які спеціалізуються на англійській мові взагалі, перекладі, філології, лінгвістиці, а також – на англійській мові в галузі комп'ютерних наук.

Результати підрахунку достовірності рекомендацій засобів ШІ щодо покращення експертних формулювань, отриманих в ході експериментального дослідження, наведено в Таблиці 1.

Таблиця 1. Результати експериментального дослідження достовірності рекомендацій засобів ШІ щодо покращення експертних формулювань

| **Назва показника** | **Кількість (частота)** |
|---|---|
| загальна кількість отриманих рекомендацій | 1104 |
| недостовірні рекомендації | 365 |
| достовірні рекомендації, що еквівалентні за якістю вихідним формулюванням | 17 |
| достовірні рекомендації, що потребують незначного коригування | 108 |
| достовірні рекомендації, що не потребують коригування | 614 |

Протягом проведеного експериментального дослідження було проаналізовано 92 англомовних текстових уривки, надані експертами-респондентами, для яких англійська мова не є рідною.

Аналіз отриманих емпіричних результатів показав, що 56% рекомендацій, наданих засобами ШІ, достовірні та не потребують коригування, 65% з них підвищують якість формулювань, 67% – не погіршують її, 1.5% рекомендацій є даремними (не додають користі), а 33% є шкідливими (спотворюють зміст формулювань).

**Висновки**

Показано, що для вирішення низки задач, які виникають у ході побудови БЗ СППР, доцільно використовувати засоби ШІ.

Запропоновано шляхи застосування засобів ШІ під час побудови БЗ, зокрема, для покращення якості експертних формулювань.

Проведено експериментальне дослідження достовірності рекомендацій засобів ШІ щодо покращення експертних формулювань.

Отримано відповідні емпіричні результати, які свідчать про те, що застосування засобів ШІ на практиці доцільне лише в автоматизованому режимі, тобто, із залученням групи експертів. Повністю покладатись на рекомендації засобів ШІ на даному етапі розвитку цієї технології недоцільно.

## Перелік посилань


1. Тоценко В.Г. Методы и системы поддержки принятия решений. Алгоритмический аспект / В.Г. Тоценко. – К.: Наук. думка, 2002. – 382 с.
2. Таран Т.А. Искусственный интеллект. Теория и приложения / Т.А. Таран, Д.А. Зубов; Восточноукр. нац. ун-т им. Владимира Даля. — Луганск: ВНУ им. В.Даля, 2006. — 239 с.
3. GhatGPT. URL: https://chat.openai.com
4. Galactica. URL: https://galactica.org
5. N. Punar Özçelik A Comparative Analysis of Proofreading Capabilities: Language Experts Vs. ChatGPT / International Studies in Educational Sciences, ed. by Bülent Pekdağ, Serüven Publishing, June 2023, pp. 147-162.

6. Dmitry Lande and Leonard Strashnoy, Concept Networking Methods Based on ChatGPT & Gephi (April 17, 2023). Available at SSRN: https://ssrn.com/abstract=4420452 or http://dx.doi.org/10.2139/ssrn.4420452
7. Циганок В.В., Андрійчук О.В. Експериментальне дослідження методу визначення змістової подібності об'єктів баз знань систем підтримки прийняття рішень / Реєстрація, зберігання і обробка даних. – 2014, - Т.16, №4 – С.65-76.

## SCIENTOMETRIC ANALYSIS OF PAPERS REGARDING UKRAINIAN HERITAGE (HISTORY, CULTURE, AND NATURE)

Balagura Iryna[1,2], Kryuchun Andriy [1]
[1]Institute for Information Recording of National Academy of Sciences of Ukraine, 2, Mykoly Shpaka Street, Kyiv, 03113, Ukraine
[2]NottinghamUniversity Business School, Jubilee Campus, Nottingham, NG81BB, United Kingdom

### Introduction

Studying national heritage is essential for fostering cultural identity, preserving diversity, understanding history, and promoting social cohesion. It contributes to a sense of pride and appreciation of human culture, both on a national and global scale. The research regarding national heritage is of great importance for each country and plays a significant role in representing the country to the global community.

The aim of the research is to discover the main topics of research, place and meaning of Ukrainian heritage in scientific papers and on the Internet using complex network analysis of *Ukrainika naukova* abstract database, *Scopus* and *ChatGpt*.

### Methods

National heritage encompasses a wide range of tangible and intangible elements that collectively represent the cultural, historical, and natural identity of a nation. So, for the analysis of the topic such keywords as `history`, `culture` and `literature` were chosen.

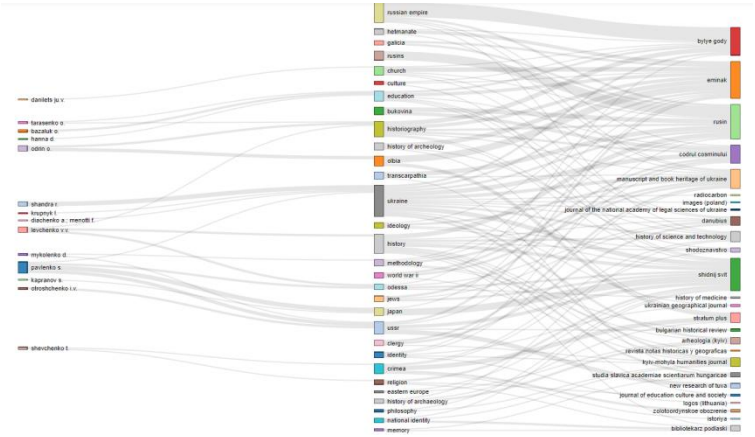



Fig. 1 Co-word-author-journal network for key-word ‘history’ in Scopus

The idea of the research is to indicate and compare the main keywords and corresponding co-word networks of Ukrainian national heritage in Ukrainian scientific papers, international journals and on the Internet. In order to form the data, the following prompts were used for search in *SCOPUS* and *Ukrainika naukova*: history, culture, and literature. Co-word-author-journal networks were formed for each keyword. According to the Times Series analysis of publication activity and main keywords, main research in this area gradually moved to the international space.

The investigation of the topic also included the analysis of keywords and co-word networks using ChatGpt 3.5 and the methodology proposed by Lande et al (Lande et al, 2023). In order to form the network of 500 nodes the prompt was used several times: `Give me another 50 main pairs of linked concepts correspondent with Ukrainian heritage: history, culture, and literature in the format "concept 1; concept 2"`. The most frequent terms in the network were Ukrainian easter tradition, Lviv, Ukrainian fashion, Vasyl Stus.

## Conclusions

Proposed methods and tools could be used for the identification and description of scientific groups and research topics, the most communicative researchers, and main principles of science communication;estimating the level of inter-scientist cooperation, detecting actual topics and priorities, and possible science

cooperation;determining associative relations as well as entry relations for subject field model formation.

## References

1. D. Lande, A. Feher, L Strashnoy. «Cybersecurity in AI-Driven Casual Network Formation". Theoretical and Applied Cybersecurity», Vol. 5. – Issue 2 (2023). – pp. 105-113. DOI: https://doi.org/10.20535/tacs.2664-29132023.2.287139

# ВИКОРИСТАННЯ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ В ПІДГОТОВЦІ КЕРІВНИКІВ ПІРОТЕХНІЧНИХ ПІДРОЗДІЛІВ ДСНС УКРАЇНИ

Є. О. Макаров, С. Д. Гассієв
Національний університет цивільного захисту України, м. Харків, Україна
makarov1993@ukr.net, serhiy.hassiev@gmail.com

Обґрунтовується необхідність використання віртуальної реальності (VR) в підготовці керівників піротехнічних підрозділів ДСНС України. Показано, що VR дозволяє відпрацьовувати навички та стратегії в безпечних умовах, імітуючи реальні ситуації. Використання VR в підготовці керівників піротехнічних підрозділів дозволить підвищити їхню професійну підготовку та ефективність роботи.
**Ключові слова:** віртуальна реальність, VR, підготовка керівників, піротехнічні підрозділи ДСНС України, розмінування, вибухонебезпечні предмети, військові тренажери.

## Вступ

Сучасна війна в Україні призвела до значного збільшення кількості вибухонебезпечних предметів на території країни. Це створює додаткові ризики для цивільного населення і вимагає від піротехнічних підрозділів ДСНС України підвищеної готовності до виконання завдань з розмінування. Сучасні боєприпаси часто містять в собі нові інноваційні технології, що ускладнюють процес розмінування. Це вимагає від піротехнічних підрозділів досконалих навичок, високого рівня професійності та розуміння новітніх методів та засобів виявлення та знищення

вибухонебезпечних предметів. Сучасний підхід до підготовки керівників піротехнічних підрозділів передбачає поєднання теоретичного навчання з практичними тренуваннями. Однак реалістичні практичні сценарії із застосуванням вибухонебезпечних матеріалів можуть бути надзвичайно небезпечними, та іноді навіть неможливими для практичної реалізації без небезпеки для життя та здоров'я. У цьому контексті, VR виступає як потужний інструмент для забезпечення безпеки та ефективності навчання. VR дозволить підготуватися до можливих ситуацій, створюючи симульовані сценарії без реальних загроз [1].

## Мета та завдання дослідження

Метою дослідження є обґрунтування необхідності використання VR в підготовці керівників піротехнічних підрозділів ДСНС України.

Завданнями дослідження є:

- ознайомитися з досвідом використання VR в підготовці військових у країнах НАТО;
- розглянути актуальність використання VR в підготовці керівників піротехнічних підрозділів ДСНС України.

## Застосування віртуальної реальності в підготовці військових

Військові сили країн-членів НАТО активно впроваджують VR у навчальні програми, тренування та військові вправи. Ця технологія дозволяє військовослужбовцям набувати навички та виконувати завдання у віртуальних умовах, що максимально наближені до реальних бойових ситуацій. Завдяки цьому, вони можуть відпрацьовувати стратегії, координацію дій та реакцію на небезпеку [2-3].

Ось деякі приклади використання VR у підготовці військових: відпрацювання навичок стрільби та бойової стрільби в різних умовах, включаючи міські забудови, лісові масиви, підземні та водні об’єкти; відпрацювання навичок ведення бойових дій у містах, та гірській місцевості де існує високий ризик для цивільного населення.

## Впровадження віртуальної реальності в підготовку саперів

Війна в Україні призвела до значного збільшення кількості вибухонебезпечних предметів на території країни. За даними Державної служби з надзвичайних ситуацій України, станом на 15 січня 2023 року на території України виявлено та знешкоджено понад 500 тисяч вибухонебезпечних предметів. Серед ключових викликів, які стоять перед піротехнічними підрозділами, можна виділити складність виявлення сучасних інженерних мін. Окупаційні війська мінують велику площу території використовуючи нестандартні способи встановлення для ускладнення їх виявлення [4].

В Україні також розпочато впровадження VR в підготовку піротехнічних підрозділів. Кафедрою піротехнічної та спеціальної підготовки в межах меморандуму про співпрацю між Благодійною організацією «Фонд свобода 4.5.0» та Національним університетом цивільного захисту України розпочато процес впровадження в навчання VR. Завдяки цьому майбутні фахівці отримали змогу відпрацьовувати набуті теоретичні знання на практиці, фото їх навчання наведено на рис. 1.

Рис. 1 - Відпрацювання навичок з пошуку вибухонебезпечних предметів

Використання VR в підготовці керівників піротехнічних підрозділів ДСНС України включає такі сценарії: 1) Навчання виявленню предметів в різних умовах, таких як міські, лісові, підземні та водні; 2) Відпрацювання навичок знешкодження та знищення різних типів вибухонебезпечних предметів, таких як інженерні міни, артилерійські снаряди та мінометні міни; 3) Використання VR-тренажерів для відпрацювання навичок командування роботами з розмінування, які використовуються для виявлення та знешкодження вибухонебезпечних предметів у важкодоступних місцях.

Ці сценарії допомагають підготовці майбутніх піротехніків, забезпечуючи їхню ефективність у реальних ситуаціях та підвищуючи безпеку робіт з розмінування.

## Висновок

Використання VR в підготовці керівників піротехнічних підрозділів ДСНС України є ефективним способом підвищити їхню професійну підготовку та ефективність роботи. VR дозволяє відпрацьовувати навички та стратегії в безпечних умовах, імітуючи реальні ситуації. Це сприятиме підвищенню рівня безпеки та зменшенню ризиків для цивільного населення під час розмінування території України.

## Перелік посилань


1. Ушакова І.О. Вплив комп'ютерних ділових ігор на формування компетенцій у майбутніх фахівців. Системи обробки інформації. 2017. № 2 (148). С. 206– 210.
2. Jack, D., Boian, R., Merians, A., Tremaine, M., Burdea, G., Adamovich, S. & Poizner H. (2001). Virtual Reality-Enhanced Stroke Rehabilitation. IEEE transactions on neural systems and rehabilitation engineering, vol. 9, 3. DOI: 10.1109/7333.948460
3. «Virtual Reality: State of Military Research and Applications in Member Countries» Report of the RTO Human Factors and Medicine Panel (HFM). ISBN 92-837-0030-9.
4. Краус Н. М. Інституціоналізація інноваційної економіки: глобальні та національні тенденції: автореф. дис. на здобуття наук. ступеня докт. економ. наук: спец. 08.00.01 «Економічна теорія та історія економічної думки» / Н. М. Краус. – К.: Знання, 2017. – 40 с.

# ПІДХІД ДО ПІДВИЩЕННЯ НАДІЙНОСТІ ТА БЕЗПЕКИ ПЕРЕДАЧІ В МОРСЬКИХ БЕЗПІЛОТНИХ СИСТЕМАХ

В.І. Слюсар[1], Н. С. Бігун[2]
[1,2] Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, м. Київ, Україна
swadim@ukr.net, bigun0714@ukr.net

Ця стаття представляє інноваційний підхід до покращення передачі даних на морських безпілотних платформах. Він зосереджується на інтеграції передових моделей автокодерів, зокрема з використанням архітектури U-Net, для підвищення ефективності та надійності каналу управління. У статті висвітлюється новий метод кодування високорозмірних даних зображень у низькорозмірний латентний простір, що значно зменшує розмір даних для передачі, зберігаючи при цьому важливу інформацію. Ключовим аспектом дослідження є акцент на підвищенні завадостійкості каналу управління та безпечній передачі даних.

**Ключові слова:** морські безпілотні платформи, архітектура U-Net, автоенкодер, передача даних, шифрування.

## Вступ

Галузь морських технологій, що стрімко розвивається, постійно прагне подолати виклики передачі даних у водному середовищі [1]. Традиційні методи, хоча й ефективні в певних сценаріях, часто не відповідають специфічним потребам морських безпілотних платформ, особливо з точки зору розміру даних, завадостійкості та безпечної передачі даних. Ця стаття представляє новий підхід до вирішення цих проблем, використовуючи потенціал сучасних автокодерів з акцентом на архітектуру U-Net [2]. Запропонований метод змінює спосіб обробки та передачі даних високорозмірних зображень у морських безпілотних системах.

Суть нашого підходу полягає в ефективному стисненні зображень у компактне латентне представлення, значно знижуючи обсяг даних, необхідний для передачі, не втрачаючи

при цьому критичної інформації. Це стиснення має велике значення для безпілотних платформ, де пропускна спроможність та потужність обмежені. Крім того, ми вирішуємо проблему шуму в комунікаційних каналах, використовуючи новаторську стратегію кодування. Поділяючи закодовані дані на косинусні та синусоїдальні компоненти, підвищується стійкість системи до шумів, забезпечуючи надійну передачу даних навіть у присутності значного зовнішнього шуму.

Традиційні методи, такі як стиснення JPEG і акустичні модеми (наприклад, стандарт JANUS), мають обмеження по пропускній здатності, затримці та якості зображення в специфічних морських умовах [3]. На відміну від них, запропонований метод пропонує інтегроване рішення, пристосоване до багатогранних потреб морських технологій, від покращення якості зображення до ефективності передачі даних.

## Шифрування та відновлення даних у морській комунікації

Метод використовує розділену модель автокодера, де сегменти кодера і декодера навчаються як одна модель, але розгортаються окремо [4]. Сегмент кодера, розташований на морській безпілотній платформі, відповідає за первинну обробку, він дозволяє ефективно стиснути дані, зменшуючи їх розмір для передачі, при цьому зберігаючи важливу інформацію. Процес стиснення також допомагає у виключенні зайвої інформації, що може бути використано для декодування зображення несанкціонованими особами.

Після стиснення, дані зображення в латентному просторі додатково шифруються за допомогою поділу на косинусні та синусоїдальні компоненти. Цей процес не тільки підвищує стійкість до шумів у комунікаційному каналі, але й забезпечує додатковий рівень безпеки, ускладнюючи несанкціоноване відновлення даних. Шифровані дані передаються у двох окремих потоках - косинусному та синусоїдальному. Це ефективно подвоює обсяг даних, що передаються у тому ж частотному діапазоні, підвищуючи пропускну спроможність без потреби в додаткових частотних ресурсах [5].

На приймальній станції (декодері) приймаються два потоки закодованих даних - косинусний та синусоїдальний. Ці потоки, які представляють відповідно "реальну" та "уявну" частини закодованих даних, комбінуються для відновлення оригінальної

інформації. Використання ортогональності косинусних і синусоїдальних функцій забезпечує точне та чітке відновлення даних, навіть у присутності значного рівня шумів. Ця методика значно підвищує надійність та точність передачі даних у складних умовах морського середовища.

## Висновки

У цьому дослідженні представлено новий підхід до підвищення надійності та безпеки передачі даних у морських безпілотних системах. Розроблений метод енкодування даних у латентному просторі, з використанням ортогональних косинусних та синусоїдальних компонент, є ключовим у покращенні якості та безпеки комунікацій у складних умовах морського середовища. Оскільки, застосування автоенкодерів з архітектурою U-Net для стиснення та шифрування даних не тільки ефективно зменшує обсяг передаваних даних, але й забезпечує додатковий рівень безпеки через складність відновлення оригінального зображення. Поділ закодованих даних на окремі потоки подвоює пропускну спроможність і збільшує стійкість системи до шумів.

Цей підхід відкриває нові перспективи для розширення можливостей морських безпілотних систем, особливо у сферах, де високі вимоги до безпеки та конфіденційності даних. У майбутньому, поєднання цього підходу з іншими передовими технологіями обіцяє ще більше покращити ефективність та безпеку морських безпілотних платформ.

## Перелік посилань


1. K.M. Awan, P.A. Shah, K. Iqbal, S. Gillani, W. Ahmad, Y. Nam. “Underwater wireless sensor networks: A review of recent issues and challenges”. Wirel. Commun. Mob. Comput. 2019, 2019, 6470359. doi:10.1155/2019/6470359
2. E. Bourtsoulatze, D. Burth Kurka, D. Gündüz, Deep Joint Source-Channel Coding for Wireless Image Transmission, in: Proceedings of the IEEE Transactions on Cognitive Communications and Networking, 5(3), 2019, pp. 567-579. doi: 10.1109/TCCN.2019.2919300
3. J. Potter, J. Alves, D. Green, G. Zappa, I. Nissen and K. McCoy, The JANUS underwater communications standard, 2014 Underwater Communications and Networking

(UComms), Sestri Levante, Italy, 2014, pp. 1-4. doi: 10.1109/UComms.2014.7017134
4. V. Badrinarayanan, A. Kendall, R. Cipolla, SegNet: A Deep Convolutional Encoder-Decoder Architecture for Image Segmentation, in: Proceedings of the IEEE Transactions on Pattern Analysis and Machine Intelligence, 39(12), 1 Dec. 2017, pp. 2481-2495. doi: 10.1109/TPAMI.2016.2644615
5. V. Slyusar, N. Bihun, "The Method of Increasing the Immunity of Data Transmission in Communication Channels," 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 2022, pp. 301-305. doi: 10.1109/PICST57299.2022.10238546

# ЕКСПЕРТНИЙ АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ІНТЕНСИВНОГО РОЗВИТКУ ШТУЧНОГО ІНТЕЛЕКТУ

В.В. Циганок[1], В.В. Голота[2], О. В. Григоренко[2], С.Л. Бурукін[3]
[1]Інститут проблем реєстрації інформації НАН України, Київ, Україна
[2]Воєнна академія імені Євгенія Березняка, Київ, Україна
[3]Customertimes Corp., Нью-Йорк, США
vitaliy.tsyganok@gmail.com, v.holota@ukr.net, gregorenko@ukr.net, s.burukin@i.ua

Останнім часом у міжнародному середовищі намітився активний пошук консенсусу щодо необхідності вжиття колективних скоординованих заходів для виявлення, моніторингу, вимірювання та мінімізації ризиків від розвитку штучного інтелекту (ШІ) як на глобальному, так і національному рівнях. В основу даного дослідження покладено аналіз потенційних загроз інтенсивного розвитку ШІ, який проведено колективом експертів із застосуванням програмної системи розподіленого збору експертної інформації «Консенсус-2». Як результат групового експертного оцінювання, складено перелік найвпливовіших загроз та визначено їх відносні вагомості.

**Ключові слова:** засоби штучного інтелекту, експертне оцінювання загроз, колективна експертиза

## Вступ

Останнім часом у міжнародному середовищі намітився активний пошук консенсусу щодо необхідності вжиття колективних скоординованих заходів для ***виявлення, моніторингу, вимірювання*** та ***мінімізації ризиків*** від розвитку штучного інтелекту (ШІ) як на глобальному, так і національному рівнях.

У жовтні 2023 р. створено ***Консультативну групу ООН з питань ШІ*** (UN Artificial Intelligence Advisory Body), яка має розробити загальні рекомендації стосовно оцінки ризиків, можливостей та механізмів міжнародного управління технологіями ШІ. Зазначені рекомендації мають бути оприлюднені напередодні ***"Саміту майбутнього"*** (вересень 2024 р.), а також лягти в основу ***Глобальної цифрової угоди*** (Global Digital Compact) [1].

У листопаді 2023 р. у Блечлі-Парк (Велика Британія) відбувся перший в історії Саміт з безпеки ШІ. У заході взяли участь високопосадовці урядів Великої Британії, США, Китаю, Японії, Франції, ФРН, Канади, Італії, Іспанії, Індії, Ізраїлю, Південної Кореї, Сінгапуру, Швейцарії, України, Туреччини, ОАК, Саудівської Аравії, Кенії, Руанди та Нігерії, а також керівники провідних компаній-розробників сервісів ШІ, серед яких OpenAI, Google, Meta, Microsoft та інші [2].

Аналіз підсумкового комюніке та коментарів учасників саміту зводиться до того, що ***міжнародна спільнота реально занепокоєна потенційною загрозою виходу ШІ з-під контролю людини***. Іншими ризиками визнано: формування упередженого ставлення ШІ до тих чи інших речей; зловживання спроможностями ШІ у сферах кібербезпеки, біотехнологій та дезінформації.

Учасники заходу підписали ***підсумкове комюніке,*** в якому йдеться про необхідність зосередження спільних зусиль на таких основних напрямах:

ідентифікація спільних ризиків для безпеки ШІ, їх наукове осмислення та обґрунтування на основі зібраної доказової бази;

розробка відповідної політики країнами-підписантами, яка забезпечила зниження цих ризиків, визнаючи можливу наявність відмінностей у підходах та необхідність залучення компаній-розробників до вирішення цього завдання. Основними питаннями

є розробка методик оцінки ризиків та інструментів для тестування безпечності технологій ШІ [3].

Від нашої держави у саміті взяв участь заступник очільника Міністерства цифрової трансформації України Г. Дубинський [4].

Заслуговує на увагу той факт, що учасники саміту, насамперед керівники компаній-розробників, ***погодилися з необхідністю делегувати урядам країн повноваження з контролю за безпечним розвитком ШІ***. Одна з основних проблем, яка, на думку учасників саміту, потребує негайного вирішення – ***розробка стандартів для виявлення, моніторингу та вимірювання ризиків, пов'язаних зі ШІ***.

Під час саміту прем'єр-міністр Великої Британії Р. Сунак оголосив про створення ***Інституту з безпеки ШІ***, який перевірятиме та надаватиме дозвіл на використання нових сервісів ШІ перед їх виходом на ринок. Аналогічний заклад створюється в США. За словами Р. Сунака ***у наступному році очікується завершення роботи над новими проривними технологіями ШІ***. Саме тому на 2024 р. заплановано проведення аж двох міжнародних самітів з безпеки ШІ – в Республіці Корея та Франції [5].

## Дослідження

Першим етапом цього процесу має стати **комплексне осмислення** проблеми потенційних загроз, які можуть виникнути в результаті бурхливого розвитку штучного інтелекту. З метою виявлення та формування переліку можливих загроз, спричинених розвитком ШІ, було проведено колективну експертизу із залученням дев'ять експертів зі складу ІПРІ НАН України, Міністерства оборони України, Воєнної академії імені Євгенія Березняка та одного з лідерів вітчизняного ринку – компанії "Інфозахист".

Експертиза проводилась у дистанційному режимі із застосуванням Системи розподіленого збору експертної інформації «Консенсус-2» [6]. У цьому дослідженні у більшій мірі розглядались потенційні загрози від неконтрольованого використання людиною засобів ШІ, які наразі бурхливо розвиваються та у меншій мірі – загрози від наслідків можливого виходу ШІ «з-під контролю людини» та самостійного прийняття ним рішень.

Відповідно до технології проведення групової декомпозиції, реалізованої в системі «Консенсус 2», колективна експертиза

включала декілька етапів. Ці етапи об'єднали в собі, по суті, процес декомпозиції (виділення складових) проблеми «Загрози, спричинені розвитком засобів ШІ» з подальшим оцінюванням відносної важливості цих загроз.

На початковому етапі після формування експертної групи, кожен експерт, оперуючи дистанційно, через веб-інтерфейс системи, особисто, мав сформувати перелік загроз, які на його думку є найбільш впливовими в проблемній ситуації, що розглядається. За результатами даного етапу експертами було сформульовано 46 загроз (5-7 загроз кожним із експертів було незалежно ідентифіковано).

Наступним етапом стало групування формулювань, однакових за змістом, оскільки при автономній роботі є велика ймовірність формулювання однієї, і тієї ж загрози різними експертами у різний спосіб. На даному етапі знеособлені формулювання (без вказування їх авторства) були об'єднані у групи однакових за змістом довкола таких проблем: втрата людиною креативності; зниження рівня зайнятості людей; порушення права на приватність життя людини; проведення небезпечних експериментів; (не)навмисна маніпуляція даними; надання ШІ права приймати рішення про позбавлення життя людини; прийняття ШІ хибних рішень про позбавлення життя людини.

У подальшому експерти, що надавали формулювання загроз, були долучені до голосування щодо вибору кращого формулювання у кожній групі однакових за змістом. Рішення приймалось за більшістю голосів при умові, що усі експерти вважались рівнокомпетентними (відносна компетентність експерта у групі в питаннях, що розглядались, не враховувалась). При голосуванні за краще формулювання загрози в групі однакових за змістом, окрім опціонального вибору формулювання пропонувався вибір «жодне з перелічених» формулювань. У разі вибору більшістю експертів цієї опції, жодне з формулювань загрози із даної групи не включається у результуючий перелік загроз, тобто, у такому разі, колектив експертів вважає, що дана загроза не має значного впливу поряд з іншими сформульованими або ж не є загрозою взагалі. У результаті експертизи було обрано вісім формулювань загроз, спричинених розвитком засобів ШІ.

Заключним етапом було визначення відносної важливості впливу загроз із отриманого переліку. Групове експертне

оцінювання проводилось у 7-ми бальній шкалі і результатом став чисельний ***рейтинг загроз:***

| Порядковий рейтинг | З а г р о з а | Балів | Чисельний рейтинг |
|---|---|---|---|
| 1 | Надання ШІ права (правила) на прийняття рішень щодо позбавлення життя людини (і військова, і цивільна сфери); | 47 | 0,1526 |
| 2 | Дезинформація людей через фейкові новини, діпфейки та фейкові джерела інформації; | 45 | 0,1461 |
| 3 | Надмірна залежність від технології штучного інтелекту може призвести до втрати людського творчого потенціалу; | 42 | 0,1364 |
| 4 | Проблеми зі занятістю населення; | 38 | 0,1234 |
| 5 | Зростання рівня загроз для свободи людини через спрощену її ідентифікацію; | 36 | 0,1169 |
| 6 | За допомогою ШІ будь-хто зможе проводити небезпечні експерименти (у сфері біохімії, генетики, когнітивної психології, ядерної фізики тощо); | 35 | 0,1136 |
| 7 | Впровадження ШІ в СППР, може призвести до помилки в прогназуванні та відповідно в прийнятті рішення експертом; | 34 | 0,1104 |
| 8 | Зміна військового та промислового лідерства між країнами, які можуть навчити провідний ШІ (наприклад, для виявлення цілей у складному середовищі), і яки цього зробити не зможуть по причині недоступності апаратних засобів чи недостатніх даних для навчання; | 31 | 0,1006 |

Водночас у рамках експерименту до цього процесу було долучено засоби ШІ, а саме ChatGPT 3.5. Ця генеративна лінгвістична модель ШІ може бути корисною при вдалому

формулюванні запиту на виконання задачі групування ідентичних за змістом формулювань. Саме тому, ми використали цей чат-бот для отримання відповіді на запитання про загрози, які би могли витікати з розвитку штучного інтелекту. На це запитання ***ChatGPT 3.5 згенерував відповідь про потенційні загрози в галузі ШІ, а саме*** (наводимо згенерований чат-ботом контент без правок):

***"втрата робочих місць*:** розвиток автоматизації та автономних систем може призвести до втрати робочих місць в тих галузях, де люди виконують повторювані завдання;

***приватність і безпека даних:*** збільшена здатність аналізу та обробки інформації ШІ може призвести до проблем з приватністю та забезпеченням безпеки даних, якщо не буде встановлено відповідні заходи захисту;

***зброя ШІ:*** використання штучного інтелекту в області військових технологій може породжувати етичні питання та збільшувати ризик неконтрольованих військових дій;

**етичні аспекти:** розробка і використання ШІ також породжує ряд етичних питань, включаючи визначення відповідальності за дії ШІ, прозорість систем, та питання справедливого та багатокультурного використання;

***залежність від технології:*** з розвитком ШІ може збільшуватися залежність суспільства від цих технологій, що може мати негативні соціальні та економічні наслідки;

***неспроможність контролю:*** ШІ може розвиватися настільки швидко, що суспільство може бути неспроможним адекватно контролювати його розширення та застосування".

Додатковий коментар ChatGPT 3.5: "важливо підкреслити, що багато з цих питань може бути вирішено з правильним регулюванням, розробкою етичних стандартів та включенням різних груп зацікавлених сторін у процес прийняття рішень. ШІ має великий потенціал для розвитку і покращення життя, але його розвиток також потребує уважної уваги до можливих негативних наслідків".

Нажаль, ***сьогодні пересічні українці вкрай легковажно ставляться до питання ШІ загалом та загрози з його боку зокрема.*** У червні 2023 р. Центр Разумкова на замовлення газети "Дзеркало тижня" провів опитування стосовно ставлення українців до ШІ. Згідно з отриманими результатами, близько 60% опитаних або не знають, або не вважають за необхідне вводити обмеження щодо застосування чат-ботів зі ШІ. Слід

зауважити, що на початку опитування 34% учасників відповіли, що взагалі не знають, що таке ШІ [7].

Отже, проблема ШІ потребує популяризації в Україні насамперед з метою підвищення "цифрової" грамотності нашого населення, яке на даний час має вкрай низький рівень обізнаності з цим питанням. Це створює сприятливі умови для маніпуляцій громадською думкою за допомогою ***фейків, дезінформації*** та ***маніпуляції даними***. За даними проекту NewsGuard, у червні 2023 р. було зафіксовано 217 сайтів, що публікують сумнівні новинні сюжети, згенеровані виключно ШІ (Unreliable Artificial Intelligence-Generated News websites). І тут питання в їх продуктивності – кожен з цих сайтів продукує в середньому 1200 новин щодоби [8].

Ці матеріали підхоплюються найпотужнішими пошуковими системами, такими як Google Ads, що автоматично створює величезний попит на ринку реклами та стимулює бурхливе неконтрольоване поширення випадків застосування ШІ для генерування дешевого і сумнівного контенту. Поряд з економічною рекламо, ШІ має великий потенціал і в сенсі політичної реклами, що може бути використано під час виборів та інших форм плебісциту.

***Для України це не лише політична та економічна проблема, це також і проблема національної безпеки***. Наприклад, усі пам’ятають, про діпфейки з Головнокомандувачем ЗС України генералом В. Залужним, які поширювалися через російські Telegram-канали у листопаді цього року [9].

## Висновки

У ході проведення колективної експертизи з допомогою системи розподіленого збору експертної інформації «Консенсус-2» проаналізовано потенційні загрози інтенсивного розвитку штучного інтелекту. Складено перелік найвпливовіших загроз та у результаті групового експертного оцінювання визначено їх відносну вагомість.

Проведене дослідження засвідчило існування потенційних загроз від інтенсивного розвитку ШІ таких як втрата людиною креативності; зниження рівня зайнятості людей; порушення права на приватність життя людини; проведення небезпечних експериментів; (не)навмисна маніпуляція даними; надання ШІ права приймати

рішення про позбавлення життя людини; прийняття ШІ хибних рішень про позбавлення життя людини.

Дослідження та реагування на потенційні загрози з боку ШІ потребує активізації зусиль і держави, і громадянського суспільства. Для того, щоб більш системно та якісно підійти до вирішення цієї проблеми необхідно:

брати активну участь у ключових міжнародних заходах з наведеної проблематики, таких як саміти (конференції) з безпеки ШІ, ініційовані провідними країнами світу та ООН;

підвищувати рівень "цифрової" грамотності населення. Важливого значення набуває реалізація Дорожньої карти з регулювання ШІ в Україні , яка має, серед іншого, допомогти пересічним громадянам навчитися захищатися від ризиків ШІ;

інституалізувати дослідження зазначеної проблеми шляхом створення нових державних установ (на кшталт Інститутів безпеки ШІ, які вже створені

у США та Великій Британії) із залученням експертів приватного сектору, які будуть опікуватися питанням безпеки ШІ на національному рівні;

розробляти імовірні сценарії реалізації потенційних загроз від розвитку ШІ з відповідними індикаторами та заходами з мінімізації виявлених загроз.

Подальші дослідження у цій галузі планується продовжити із залученням ширшого кола експертів та використовуючи відповідну інтелектуальну технологію, згенерувати ймовірні сценарії реалізації потенційних загроз від розвитку ШІ.

## Перелік посилань


1. New UN Advisory Body aims to harness AI for the common good. https://news.un.org/en/story/2023/10/1142867.
2. The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023. https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023.
3. Там же.
4. Україна підписала міжнародну декларацію щодо безпеки використання ШІ. https://www.epravda.com.ua/news/2023/11/2/706166/.

5. Prime Minister's speech at the AI Safety Summit: 2 November 2023. https://www.gov.uk/government/speeches/prime-ministers-speech-at-the-ai-safety-summit-2-november-2023.
6. «Консенсус-2» – система розподіленого збору експертної інформації. Свідоцтво про реєстрацію авторського права на твір № 75023 від 17/11/2017. https://dss-lab.org.ua/ua/applications/konsensus-2.
7. Ставлення українців до штучного інтелекту на диво легковажне. Дарма. https://zn.ua/ukr/TECHNOLOGIES/stavlennja-ukrajintsiv-do-shtuchnoho-intelektu-na-divo-lehkovazhne-darma.html.
8. Funding the Next Generation of Content Farms: Some of the World's Largest Blue Chip Brands Unintentionally Support the Spread of Unreliable AI-Generated News Websites. https://www.newsguardtech.com/misinformation-monitor/june-2023/.
9. «Залужний заявив про держпереворот і пригрозив Зеленському». ЩО? Та звісно, ні! Просто росіяни запустили два діпфейки з головкомом, а ми їх розібрали. Штучний і власний інтелект у поміч. https://babel.ua/texts/100408-zaluzhniy-zayaviv-pro-derzhperevorot-i-prigroziv-zelenskomu-shcho-ta-zvisno-ni-prosto-rosiyani-zapustili-dva-dipfeyki-z-golovkomom-a-mi-jih-rozibrali-shtuchniy-i-vlasniy-intelekt-nam-u-pomich.

## A METHOD FOR REDUCING THE UNCERTAINTY CAUSED BY A POWER OUTAGE DURING A CYBER INCIDENT RESPONSE

Vitalii Zubok, Roman Draguntsov
G.E.Pukhov Institute for Modelling In Electric Energy, Kyiv, Ukraine
vitaly.zubok@gmail.com, draguntsow@yahoo.com

Well-known that modern war strategies widely include cyber attacs along with kinetic strikes. There are investigations reporting Russian aggressors use systematic cyber attacks on Ukrainian power energy sector to increase negative consequences of air strikes. And vice versa, blackouts cased by air strikes make it difficult to respond to a cyber attack.

Responding to and investigating any cyber incident in the midst of blackouts is notably complicated by an additional layer of uncertainty. To address the challenges inherent in the decision-making process, a decision making system simplification algorithm becomes necessary. This paper represents overview of impacts for cybersecurity caused by massive power outages, Specific challenges for cyber incident response, and some practical approach to loss of observability problem mitigation.

**Keywords:** preparatory cyber attacks, synchronous cyber attacks, power outages, cyber incident uncertainty, cyber incident response, cyber security, cyber resilience.

## Introduction

During the Russo-Ukrainian war, the russian armed forces executed a multi-phased operation with the objective of dismantling the Ukrainian power supply infrastructure and capabilities. Utilizing high-range missiles and Unmanned Aerial Vehicles (UAVs), the attacks resulted in extensive devastation to the national energy system, inflicting severe economic losses on Ukraine through widespread power outages. In response to these attacks, international allies and donors have prioritized the provision of critical components to repair damaged energy infrastructure and provide generators and fuel supply to protect the operation of essential facilities and services. NATO also provides additional weapons for defense of critical energy infrastructure badly damaged by massive Russian missile and drone strikes. Nevertheless, these attacks have left up to 40 percent of the power system damaged, with around 30 percent of the country's power stations destroyed. This has substantially eroded the power grid's resilience and operational integrity.

The tense situation remains in digital domain. Digital resilience often referred as a new KPI for digital transformation. And the most prioritized event which stresses digital domain is cascading effect of widespread power outages. Regular and unpredictable power outages exerted a considerable impact on the functionality of Information Technology (IT) systems within Ukraine. The primary impact vectors were identified as losses in system availability, while certain aspects related to cybersecurity extended into the observability domain, tightly linked with the aforementioned availability of information systems.

The blackouts presented challenges in monitoring the state of IT systems, impeding effective log management, and compromising the integrity of cybersecurity controls coverage. In such adverse conditions, managing a cyber incident — a process inherently characterized by a high degree of uncertainty — becomes a formidable challenge for Computer Security Incident Response Team (CSIRT) commands. The complexity is further compounded by an additional layer of uncertainty arising from the loss of observability. The efficacy of the decision-making process in cyber incident response hinges upon a lucid comprehension of activities detectable within infrastructural components and a reliance on the veracity of the data retrieved from them. These requisites encounter substantial complexity due to observability losses resulting from extensive power outages. To streamline the decision-making task within cyber incident response, an algorithm for system decomposition and simplification can be applied, involving the sequential isolation and examination of components. This paper delves into the intricacies of applying this algorithm to the cyber incident response process, aiming to enhance the support provided for decision-making processes within Computer Security Incident Response Team (CSIRT) commands.

## Overview of impacts for cybersecurity caused by massive power outages

A military operation resulted in widespread power outages, as well as other reasons for a state-wide, massive energy crisis imposes diverse impact vectors (see Table 1) on the cybersecurity of information systems and their capacity to effectively respond to a cyber incident. While certain impact vectors, such as losses in system availability, are evident, others are less apparent and bear a closer relationship to the cyber incident response process.

Table 1 – Impact vectors of cyber attacks

| **Impact vector** | **Description** |
|---|---|
| System availability [1] | The occurrence of a power outage in information systems facilities leads to disruptions in regular operations and influences information availability. This represents the most evident impact vector, serving as the root cause for subsequent |

| | |
|---|---|
| | effects. |
| System integrity [2] | While certain system components may experience downtime during power outage, others may persist online. In the case of protective systems situated independently from the safeguarded entity, the integrity of the defense architecture may be compromised. Integrity impacts can also arise from power outages that momentarily disrupt data flow, with shortly restoration after a brief timeout. Instances of data transmission gaps, challenges in system state synchronization, and interruptions in ongoing operations susceptible to failure may constitute integrity risks for a system suffering from power outages. |
| System observability [3] | Ability to get a clear view into a system functionality flow and it's history is a crucial part of a system's security architecture. When an information system's component goes offline, it stops sending logging information to the central console. But this behavior may be caused by at least three reasons: power outage of the component, power outage of some part of data transmission channel and a threat agent's activity aimed to break the visibility of a component. Power outage poses a danger to system's observability not only with a direct logging information shortage, but also with an additional uncertainty level of needing to separate a threat-caused observability loss from a natural one. |
| Response capability [4] | An ability to respond for a cyber incident is heavily dependent on a system's main parameters, impacted by power outage and |

| | |
|---|---|
| | mentioned before. But some other factors heavily complicate the process of incident response – broken communication channels caused by the power outage bring havoc into a normal communication between CSIRT command members that may work in a power-shortened component of a system. That may also impact an ability to use several security systems and controls that may also go offline. |

As evident from the table presented above, the cyber incident response process within an environment affected by extensive power outages faces multiple levels of uncertainty. Specifically, the primary challenge in responding to and investigating a cyber incident under such conditions lies in the ability to differentiate between system components that have experienced a breach and those that have not. This is compounded by circumstances where trust in the logging data of components is compromised, and the logging data itself may be incomplete [5].

**Specific challenges for cyber incident response during the power outage**

Let's examine the nature of a system undergoing a breach in the context of extensive power outages. Consider a hypothetical system model, for instance, a geographically dispersed multi-component information system primarily situated in a country suffering from an energy crisis. The components within such a system can be conceptualized as the fundamental building blocks, encompassing data centers, networks, IP ranges, VLANs, and similar entities [6].

The initial imperative for a component is to exhibit some form of isolation from other components. While the boundaries between components may be virtual, the presence of attributes that fortify access restrictions from one component to another is essential. If such restrictions prove valuable during the incident response process, these components should be regarded as distinct entities. The second criterion involves recognizing that the impact of a power outage on a given component may differ for various reasons compared to surrounding components. If the component of an information system

possesses a distinct reserve power source or exhibits a varying susceptibility to power outage impacts compared to its surroundings, it warrants consideration as a separate component. The final criterion for defining a component lies in business functionality. If a specific part of an information system supports a clearly defined business function that is not shared with other parts, that particular section should be acknowledged as a distinct component.

The given above system decomposition methodology is largely simplified [7], but gives enough abilities to imagine a model for a system suffering from an incident and one that will be investigated. Let's assume, that an imaginary information system has two geographical facilities and one cloud-based resource. One of those facilities experienced considerable observability loss that may be linked to a cyber incident. But the traces of a cyber incident can be found in all of the system's facilities (Figure 1).

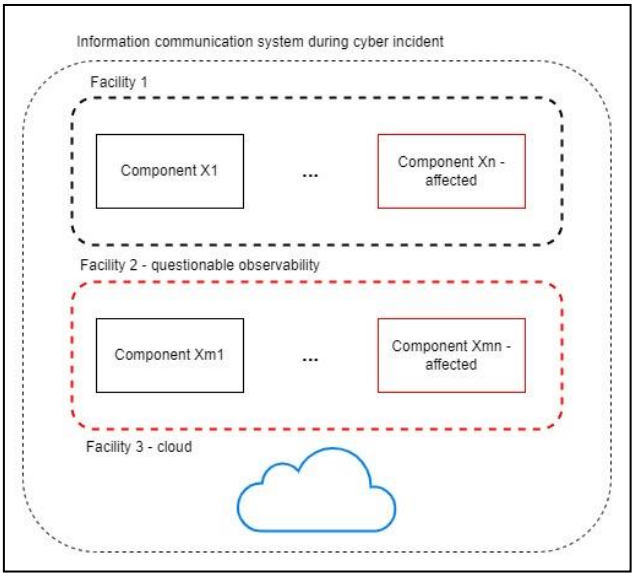



Figure 1 – Uncertaainity cased by observability loss

When a CSIRT command is aware of an incident occurred in infrastructure and possess all the information above, it faces some specific challenges:

- Was the reason for observability loss in Facility 2 caused by a power outage or by a threat agent?
- What logging information from Facility 2 was missing?
- Is observability of Facility 1 trusted or not?
- What components in Facility 2 were targeted by a threat agent and how that may be proven in low observability condition?

Analyzing the aforementioned questions, it is evident that they are interlinked, each prompting the other. Addressing these concerns can prove challenging and resource-intensive when examining the system as an entirety. However, dissecting each component in isolation from others may introduce significant risks. These risks encompass the potential escalation of threat agents from one non-investigated component to another or from an uninvestigated component to an already scrutinized one. This likelihood characterizes a direct, component-based analysis as perilous and ineffective, introducing the issue of a 'horizontal threat shift.' This term denotes the threat agent's capacity to traverse between system components in conditions of low observability.

**System simplification algorithm to defeat the challenge of observability loss.** The investigation and response process can be facilitated and rendered more comprehensive through the decomposition of the system into the aforementioned components [7], with each component subsequently undergoing individual investigation. However, this approach is susceptible to the previously mentioned issue of horizontal threat shift. A potential remedy for this problem involves isolating each component and investigating its activity in isolation. However, a significant challenge arises in that it is not feasible to isolate every component without inflicting a substantial business impact. The isolation of all system components would result in a complete enterprise shutdown, an outcome inappropriate during any investigation.

To address this challenge, we propose an algorithm for system simplification aimed at supporting the decision-making process during cyber incident response. This algorithm serves as a precursor to the standard incident response and investigation process, breaking down the entire information system into smaller parts (components). It facilitates the processes of isolation and investigation prioritization. The fundamental concept of the algorithm revolves around the isolation of any system components that can be separated without causing inappropriate impact. This isolation is performed prior to a comprehensive investigation when a substantial observability impact

has been incurred by the system due to an external factor, such as a massive power outage. For those components that cannot be isolated due to business requirements, they are designated as first-priority candidates for investigation.

The investigation process is designed to address whether an observability loss has transpired in the component and if it was instigated by the activity of a malicious actor. Additionally, it examines whether any traces of actor activity can be discerned within the component. Components confirmed to be impacted by a threat agent are unequivocally isolated and subsequently directed into the standard investigation flow. On the other hand, components for which there is no confirmation of threat agent activity, whether isolated or not, are unblocked and then channeled into the same investigation flow.

This algorithm represents a subtype of the decision tree algorithm specifically tailored for preprocessing incident investigations and responses under conditions of low observability. The graphical representation of the algorithm is illustrated in Figure 2.

The algorithm's core advantage lies in its capability to generate a sorted and prioritized list of components for investigation, facilitating more effective coordination of actions and optimizing the use of limited resources. This significantly enhances the decision-making process during incident response. The list can be conceptualized as a vector of objects, arranged by their criticality from least critical to most critical. Components are further categorized into two groups: isolated ones ($X1 \ldots Xn$) and unblocked ones ($Y1 \ldots Yn$). The investigation function iterates through the vector in reverse order, moving from $Y$n to $X$1. The graphical representation of the components vector and its application is depicted in Figure 3.

Assuming we have a set $S$ representing the information system, and $C$ representing the set of atomic components, the algorithm can be described as follows:

1) Define the information system as a set $S$ where $S=\{c1,c2,\ldots,cn\}$
2) Each $c_i$ is an atomic component of the information system.
3) Assign criticality values to each component using the function $f$: $f(ci)$ gives the criticality of component $c_i$.
4) Identify components with lower criticality values.
5) Isolate or remove components with criticality below a certain threshold of inappropriate business impact. Let $C_{important}$ be the set of remaining important components:

$$C\text{important} = \{ci \in C \mid f(ci) \geq threshold\}$$

6) Sort all components in $C$ by their criticality values in descending order to obtain a sorted list.
7) Define the function *investigation* : $C_{\text{sorted}} \rightarrow$*{"legit","illegal"}*, where *investigation*($c_i$) returns the status of the component $c_i$.
8) Apply the investigation function to each component in the sorted list from most critical to least critical.
9) Isolate components marked as "illegal" and pass them to the function *StandardIncidentResponse*.

## System simplification algorithm – practical implementation caveats

The upper-mentioned algorithm has some practical caveats applicable to several environments:

*High amount of non-isolatable components*. The component vector of a system, where the majority of components cannot be safely isolated without causing inappropriate business impact, is characterized by Xn significantly greater than Yn. This characteristic renders the algorithm less effective against horizontal threat shift, as a substantial portion of the components remains unblocked and unobservable during the initial investigation. This challenge can be addressed by either incorporating a less strict isolation procedure that avoids inappropriate business impact or implementing multiple, stricter, and trustworthy controls to monitor the activity between unblocked components.

*Significant scale of the components*. When the individual components of an information system exhibit significant scale, the basic investigation of each component will demand a substantial allocation of resources by the CSIRT. This can lead to an increased risk of horizontal threat shift and may amplify the repercussions of isolating the components that remain separated. To address this challenge, a CSIRT can implement more lenient requirements for the baseline investigation, focusing solely on checking for the reason behind the observability loss. This should suffice to ascertain whether a power outage has occurred and affected the system. Alternatively, another approach involves reducing the number of system components under investigation by segregating those components and facilities that have not been impacted by either a threat agent or a power outage with sufficient likelihood.

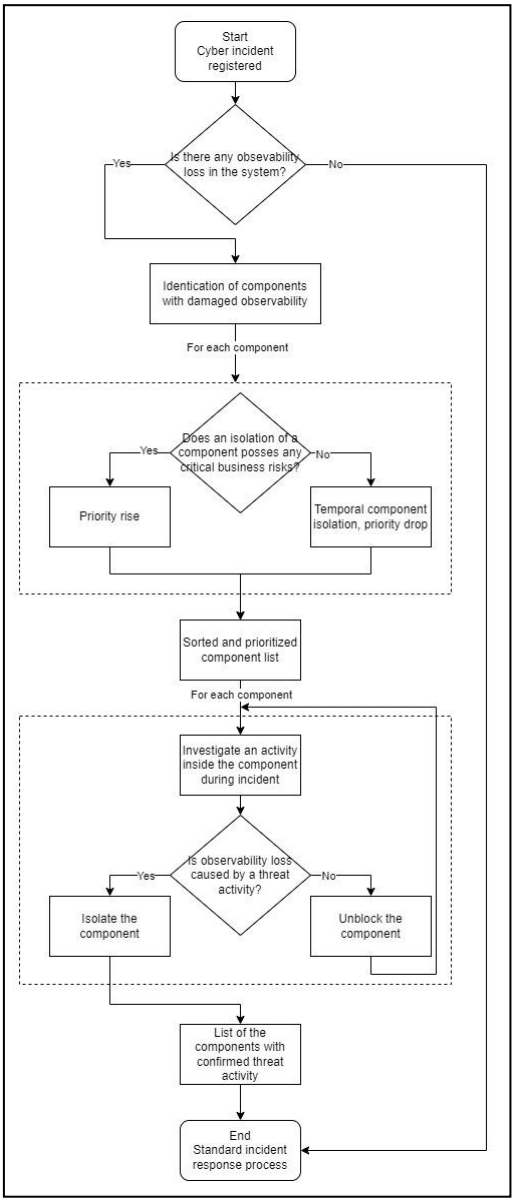



Figure 2 – Incident responce decision tree algorithm

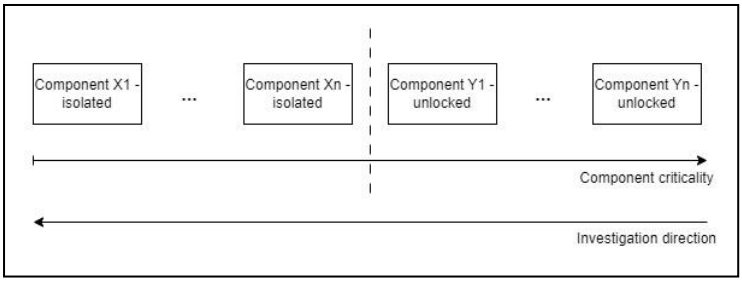



Figure 3 - The components vector and its application

*Inability to practically isolate a component.* Low observability conditions resulting from a power outage can lead to a substantial deterioration of active response capabilities, particularly the ability to isolate a component from others on various communication levels. This challenge may persist even when adequate security systems were not in place prior to the incident. As a rapid interim solution, compensatory monitoring-based controls can be contemplated for addressing this issue. By fixing and validating any communication between components, suitable capabilities can be deployed more swiftly compared to the implementation of comprehensive isolative measures.

While AI/ML methods and generative models usage is spreading in incident response and investigation [8], perhaps, in the future, investigation scenarios under conditions of uncertainty will be developed using generative models.

## Conclusions

Massive power outages pose at the state level a significant challenge to the cybersecurity of an enterprise. Responding to and investigating any cyber incident in the midst of such blackouts is notably complicated by an additional layer of uncertainty. To address the challenges inherent in the decision-making process, a decision making system simplification algorithm becomes necessary. The system simplification algorithm, based on component isolation, serves as a precursor to a standard investigation flow, breaking down the complex task and mitigating the layer of uncertainty induced by observability losses. Practical application of the algorithm entails

some noteworthy caveats, which can be mitigated by lowering isolation requirements and incorporating compensatory controls.

## References


1. E. Ahadu. The Effect of Electric Blackout on the Operation and Productivity of Small Manufacturing Enterprises IJRRIS. Vol. 6, Issue 3, pp: (11-21).
2. OSA Internal Audit Services. July 22, 2019 [online]. Available: https://osa.sc.gov/wp-content/uploads/2019/11/Gap-Analysis-Risk-Management-Final.pdf (accessed 11 Nov 2023).
3. Scarfone, K. (2023). Cybersecurity Log Management Planning Guide. *National Institute of Standards and Technology*. DOI:10.6028/nist.sp.800-92r1.ipd
4. Threat Report: Top Defense Evasion Techniques Used by Malware [online]. Available: https://www.forescout.com/resources/top-defense-evasion-techniques-used-by-malware/ (accessed 11 Nov 2023).
5. R. Drahuntsov, V. Zubok. Modeling Of Cyber Threats Related To Massive Power Outages And Summary Of Potential Countermeasures. *Elektronne modelyuvannya*, 2023, 45(3):116-128. DOI:10.15407/emodel.45.03.116
6. Network Visibility and Segmentation. *Cisco Public*. [online] Available: https://www.cisco.com/c/dam/en/us/products/se/2017/9/Collateral/cisco-securityservices-solutionoverview-013119.pdf (accessed 11 Nov 2023).
7. Maynard, P., McLaughlin, K., & Sezer, S. (2020). Decomposition and sequential-AND analysis of known cyberattacks on critical infrastructure control systems. *Journal of Cybersecurity*, 6(1). DOI:10.1093/cybsec/tyaa020
8. Lande, D, and Novikov, O., and Manko, D. The analysis of cybersecurity subject area terms based on the information diffusion model. *Theoretical and Applied Cybersecurity*, 2022, 4(1):55-60. DOI:10.20535/tacs.2664-29132022.1.274122

## ЗМІСТ

Національна академія наук України
Інститут проблем реєстрації інформації НАН України

# ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ І БЕЗПЕКА

## Матеріали XXIII Міжнародної науково-практичної конференції

Випуск 23

Підп. до друку 26.12.2023. Формат 60x84 1/16. Папір офс. Гарнітура Times.
Спосіб друку – ризографія. Ум. друк. арк. 10,5. Обл.-вид. арк. 24,36. Наклад 100 пр. Зам. № 15-200.

ТОВ "Інжиніринг"
ISBN 978-966-2344-96-7