ISSUE 2 (15) I 2024

SMART TECHNOLOGIES

INDUSTRIAL AND CIVIL ENGINEERING

INTERNATIONAL SCIENTIFIC JOURNAL

uwtech.knuba.edu.ua
DOI: 10.32347/uwt

ISSN 2415-8550 / print
ISSN 2415-8569 / online

FOUNDERS

Kyiv National University of Construction and Architecture (Ukraine)

Certificate of the State Registration
КВ № 24366-14206 P dated 13.02.2020.
Decision of the National Council of Ukraine on Television and Radio Broadcasting No. 223 dated 01.02.2024.

ISSN 2415-8550 (print) ISSN 2415-8569 (online)

DOI: 10.32347/uwt.2024.15
It is published twice a year

INTERNATIONAL SCIENTIFIC JOURNAL

SMART TECHNOLOGIES

INDUSTRIAL AND CIVIL ENGINEERING

Founded in August 2015

Issue 2(15), 2024

EDITOR-IN-CHIEF
Yurii Khlaponin Dr.Tech.Sc., Prof., Full member (Academician) of the Ukrainian Academy of Sciences, KNUCA, Kyiv

DEPUTY EDITOR
Sergii Lenkov Dr.Tech.Sc., Prof., Honored worker of science and technology of Ukraine, laureate of the state prize of Ukraine in the field of science and technology of Ukraine

EDITORIAL BOARD
Petro Kulikov Dr. Econ.Sc., Prof., KNUCA, Kyiv
Oleksandr Bezverkhy Dr. Phys. and Math.Sc., Prof., National Transport University, Kyiv
Volodymyr Blintsov Dr.Tech.Sc., Prof., acad. Makarov Mykolaiv University of Shipbuilding, Mykolaiv
Natalia Bushuieva Dr.Tech.Sc., Prof., KNUCA, Kyiv
Denis Chernyshev Dr.Tech.Sc., Prof., KNUCA, Kyiv
Leonid Dvorkin Dr.Tech.Sc., Prof., National University of Water and Environmental Engineering, Rivne
Mykola Dyomin Corr.-member of NAAU, Dr. of Architecture, Prof., KNUCA, Kyiv
Stepan Epoyan Dr.Tech.Sc., Prof., KhNUCA, Kharkiv
Viktor Grinchenko Full member of NASU, Dr.Tech.Sc., Prof., NAS Institute of Hydromechanics of Ukraine, Kyiv
Sergii Klymenko Corr.-member of NASU, Dr.Tech.Sc., Prof., NAS V.M. Bakul Institute of Superhard Materials of Ukraine, Kyiv
Veniamin Kubenko Full member of NASU, Dr. Phys. and Math.Sc., Prof., NAS Institute of Mechanics of Ukraine, Kyiv
Oleg Limarchenko Dr.Tech.Sc., Prof., Taras Shevchenko Kyiv National University, Kyiv
Oleksandr Luhovskyi Dr.Tech.Sc., Prof., NTU of Ukraine Igor Sikorsky "Kyiv Polytechnic Institute", Kyiv
Leonid Mazurenko Dr.Tech.Sc., Prof., NAS Institute of Electrodynamics of Ukraine, Kyiv
Ivan Nazarenko Dr.Tech.Sc., Prof., Academy of Construction of Ukraine, Kyiv
Alla Pleshkanovska Dr.Tech.Sc., Prof., KNUCA, Kyiv
Ihor Rebezniuk Dr.Tech.Sc., Prof., National Forestry University of Ukraine, Kyiv
Oleksandr Terentyev Dr.Tech.Sc., Prof., KNUCA, Kyiv
Valentyn Tomashevskyi Dr.Tech.Sc., Prof., NTU of Ukraine Igor Sikorsky "Kyiv Polytechnic Institute", Kyiv
Valery Tovbych Dr. of Architecture, Prof., KNUCA, Kyiv
Leonid Zamikhovskiy Dr.Tech.Sc., Prof., Ivano-Frankivsk National Technical University of Oil and Gas, Ivano-Frankivsk

INFLUENCE OF WATER ON AN ENVIRONMENT AND INNOVATIVE TECHNOLOGIES

Natural sciences
Mathematics and statistics
Information technologies
Mechanical and electric engineering
Automation and instrument-making
Production and technologies
Architecture and building

INTERNATIONAL EDITORIAL BOARD

Winfried Auzinger PhD eng., Ass.Prof., Vienna University of Technology (Austria)
Vladislav Bogdanov PhD Phys. and Math., Snr.Res.Ass., Progressive Research Solutions Pty, Sidney (Australia)
Goran Bryntse PhD, Ass.Prof., SERO, European Renewable Energy Federation, Borlange (Sweden)
Carsten Drebenstedt Dr.hab, Prof., Technical University Bergakademie, Freiberg (Germany)
Marian Druza PhD eng., Prof. University of Zilina (Slovakia)
Miklos Hajdu PhD eng., Prof., Budapest University of Technology and Economics (Hungary)
Viktor Mashkov Dr.Tech.Sc., Prof., University J. Evangelista Purkyne in Usti-nad-Labem (Czech Republic)
Sergiy Ryzhkov Dr.Tech.Sc., **Prof.,**Zhenjiang ACME Informa-
tion Technology Co. Ltd, Shengzhou (China)
Miroslaw Skibniewski PhD eng., Prof., University of Maryland, College Park (USA)
Henryk Sobczuk Dr. hab, Prof., Lublin University of Technology (Poland)
Nameer Hashim Qasim Dr.Tech.Sc., Assoc. Prof., Cihan University-Sulaimaniya, Sulaymaniyah, Iraq.

Scientific professional publication of Ukraine (Category “Б”)
Orders of the Ministry of Education and Science
30.11.2021 № 1290, 07.04.2022 № 320, 01.02.2024 № 223
(specialties – 121, 122, 123, 125, 126, 131, 132, 133, 141, 184, 191, 192, 193)

Approved by Academic Council of Kyiv National University of Construction and Architecture May 24, 2024, Protocol No.04

Languages of the publications English, Ukrainian

Content

Mathematics and statistics

Вікторія Клюєва, Владислав Герасимчук, Ігор Данилов……..4
Типові математичні моделі, які застосовуються в автоматизованих системах організаційного управління
Typical mathematical models used in automated systems of organizational management

Anatolii Ilnytskyi, Oleg Tsukanov, Oleksandr Simonenko, Yuriy Pepa, Andrii Petrenko…….. 10
Mathematical model of single-channel signal search with two degrees of detection in radio frequency monitoring of mobile telecommunication systems
Математична модель одноканального пошуку сигналу з двома ступенями виявлення в радіочастотному моніторингу систем мобільного зв'язку

Informathion technologies

Abdulsatar Shaker Salman, Aqeel Mahmoud, Abdulelah Hameed Yaseen, Omar Saad Ahmed, Mohammed Yaseen Abdullah……18
The senergistic impact of 5G on Internet of Things innovation and growth
Синергічний вплив 5G на інновації та зростання Інтернету речей

Сергій Лєнков, Володимир Джулій, Олександр Яворський, Костянтин Зацепін……..31
Модель інформаційної безпеки функціонування програмного забезпечення
Information security model of software operation

Ihor Muliar, Serhii Lenkov, Volodymyr Hloviuk, Volodymyr Anikin, Yevhenii Sotnikov…… 46
Метод пошуку вразливостей вебзастосунків з використанням API ChatGPT
A method for finding web application vulnerabilities using the ChatGPT API

Ігор Козубцов, Наталія Зінченко, Андрій Котенко, Ігор Аверічев ……56
Проблеми забезпечення інформаційної безпеки суб'єктам освітньої діяльності в цифровому освітньо-науковому середовищі закладів освіти
Problems of ensuring information security for subjects of educational activities in the digital educational and scientific environment of educational institutions

Dmytro Humennyi……66
Adaptive Software Component for Predicting Energy Consumption of an Electric Vehicle on a Planned Route
Адаптивний програмний компонент для прогнозування енергоспоживання електромобіля на запланованому маршруті

Юрій Хлапонін, Володимир Вишняков……... 78
Визначення поняття інформації для живих і штучних інформаційних систем
Definition of the concept of information for living and artificial information systems

Максим Делембовський, Максим Маркевич, Борис Корнійчук……..90
Дослідження впливу інтернет середовища на підлітків
Study of the influence of the Internet environment on teenagers

Mechanical and electric engineering

Yurii Khlaponin, Volodymyr Myronenko……..99
Design of radio communication modules for UAVs using atypical frequencies
Проектування модулів радіозв'язку для БПЛА з використанням нетипових частот

Asmaa Hakeem Naeem, Mahmood Jawad Abulshaer, Alhamza Abdulsatar Shaker, SaifSaad Ahmed, Alaa Salim Abdalrazzaq……105
A Statistical Optimizing UAV Stability Through 5G Network Parameters
Статистична оптимізація стабільності БПЛА через параметри мережі 5G

Production and technologies

Oleh Kuzin…….. 119
Система моніторингу банківської інфраструктури
Banking infrastructure monitoring system

Architecture and construction

Анастасія Кондакова, Олександр Корецький…….…….. 124
Моделі побудови мереж інтернету речей для управління інфраструктурою міста
Models of building Internet of Things networks for city infrastructure management

Ольга Петраковська, Марія Михальова……..133
Концептуальна модель формування обмежень щодо використання земель
Conceptual model of land use restrictions formation

Guidelines for Authors…… 139

Вітаю, шановні читачі журналу Smart Technologies!

Початок 21 століття, якщо аналізувати розвиток технологій, приніс технологічну революцію, пов'язану з бурхливим розвитком смарт індустрії, інтернету речей, кіберфізичних систем тощо.

Потенційний ефект від створення та застосування смарт технологій можна порівняти за масштабом та впливом з ефектом від створення мережі Інтернет. Відбувається незворотне взаємопроникнення різних за походженням і принципами роботи мереж, таких, наприклад, як мережі передачі комп'ютерних даних і мережі передачі голосового (телефонного) трафіку тощо. Це свідчить про те, що еволюція мереж зв'язку відбувається в напрямі конвергенції (convergence – зближення, сходження в одну точку). Швидко, після досягнень, що виникали через появу Інтернету і смартфонів з сенсорним екраном, тепер настала черга штучного інтелекту (AI) та розумних технологій очолити наступний етап глобальних інновацій. Розвиток смарт технологій змінює наш спосіб життя, спілкування та роботи. Люди завжди прагнуть кращого, тому активно використовують технології смарт індустрії.

Чому? Тому, що це зручно, підвищує безпеку, ефективність, економить наші гроші та час. Про це редакція оновленого журналу **Smart Technologies (Розумні технології)** очікує від вас ґрунтовних статей та запрошує до співпраці !

Щиро ваш,
Головний редактор журналу,
Доктор технічних наук, професор,
Дійсний член (академік) Української Академії наук

Юрій ХЛАПОНІН

Типові математичні моделі, які застосовуються в автоматизованих системах організаційного управління

Вікторія Клюєва[1], Владислав Герасимчук[2], Ігор Данилов[3]

[1] Київський національний університет будівництва і архітектури
пр-т Повітряних Сил, 31, м.Київ, Україна, 03037
[2,3] Державний університет інформаційно-комунікаційних технологій
вул. Солом'янська, 7, м.Київ, Україна, 03037
[1] kliuieva.vv@knuba.edu.ua, https://orcid.org/0000-0003-1267-0717,
[2] h3rasymchuk@gmail.com, https://orcid.org/0009-0003-8944-1952,
[3] danylovihor@gmail.com, https://orcid.org/0009-0000-1426-6414

Received 03.09.2024, accepted 29.10.2024
https://doi.org/10.32347/uwt.2024.15.1101

Анотація. У статті розглядаються типові математичні моделі, які використовуються в автоматизованих системах управління (АСУ), різновидом яких є автоматизовані системи організаційного управління (АСОУ), з метою прийняття оптимальних управлінських рішень.

У наш час неможливо вирішувати проблеми управління економікою шляхом механічного збільшення чисельності управляючого апарату, тому що масштаби робіт вимагають такої кількості людей, яка не може бути направлена до сфери управління.

Проводиться аналіз найбільш розповсюджених типів задач, які розв'язуються керівниками на всіх ланках управління: управління запасами, розподілу, масового обслуговуванння, впорядкування, заміни.

Наводиться приклад розв'язування задачі управління запасами на складському господарстві.

Дається загальна характеристика математичних моделей, що використовуються у детермінованих задачах прийняття організаційно-економічних рішень в організаційних системах та наводяться умови для їх застосування.

Ключові слова: математичні моделі, автоматизовані системи організаційного управління, прийняття управлінських рішень, дослідження операцій.

ВСТУП

Визначені обставини привели до широкого застосування автоматизованих систем управління (АСУ), різновидом яких є автоматизовані системи організаційного управління (АСОУ) – ерготичні (людино-машинні) системи, засновані на використанні економіко-математичних методів та засобів електронно-обчислювальної техніки для збору, зберігання та обробки інформації про об'єкт управління з метою вироблення оптимальних управлінських рішень.

Однією з теорій, яка дає можливість застосовувати математичні методи при прийнятті управлінських рішень, є дослідження операцій. Методи дослідження операцій можна однаково застосовувати у будь-яких галузях. Різні за конкретним проявом господарські процеси можна описувати одними й

тими ж моделями, наприклад, системою лінійних алгебраїчних рівнянь.

ОСНОВНІ ПОЛОЖЕННЯ

Розглянемо найбільш розповсюджені типи задач, які розв'язуються в автоматизованих системах організаційного управління. Ці задачі отримали такі умовні назви:

- задачі управління запасами;
- задачі розподілу;
- задачі масового обслуговування;
- задачі впорядкування;
- задачі вибору маршруту;
- задачі заміни;
- змагальні задачі.

Задачі управління запасами

Запаси – це ресурси, які в даний момент часу не використовуються. Основні види ресурсів, з якими доводиться мати справу господарським керівникам, – це матеріали, машини, грошові кошти, а також людські ресурси. Задача управління запасами виникає у тих випадках, коли наявність невикористовуваних ресурсів призводить до витрат, характер яких не є однорідним: одні зростають із збільшенням запасів, інші зменшуються (убувають).

У таких ситуаціях ставиться питання про визначення оптимальної величини запасу на складі з точки зору мінімізації критерію «сумарні витрати».

Приклади витрат, що зростають із збільшенням запасу: складські витрати; втрати, пов'язані зі старінням та псуванням; втрати від збільшення обсягу облікових операцій тощо.

Витрати, що зменшуються із збільшенням запасів, пов'язані з відсутністю запасів та несвоєчасною поставкою; із зменшенням обсягу підготовчо-заключних операцій; з ефектом оптових закупок; з ефектом більш раціональної спеціалізації працівників постачальницько-збутових та виробничих підрозділів тощо.

Розмір даних витрат залежить від багатьох факторів і, в першу чергу, від розмірів партії та тривалості інтервалу між поставками. Отже, необхідно оптимальним чином визначити ці параметри.

Розглянемо ситуацію, що виникає в одному із складських господарств. Нехай попит на продукт $П$ є постійним і дорівнює h тонн на добу. Нестача продукту неприпустима. Поповнення складу відбувається партіями по n тонн. Затрати на доставку однієї партії на склад не залежать від розміру партії, постійні і дорівнюють C_0 гривень. Вартість зберігання 1 тонни за добу дорівнює Ct. Загальний попит за інтервал часу T дорівнює N тонн.

Однак не обов'язково завозити на склад одразу усі N тонн продукту. Можливо, що це вигідніше робити у декілька прийомів, поповнюючи склад через інтервали часу τ партіями по n тонн. Всього партій буде m.

Очевидно:

$$\begin{aligned} N &= mn, \\ T &= m\tau, \\ n &= h\tau. \end{aligned} \qquad (1)$$

Це умови розв'язку. Величини N, T, C_0 та C_t – задані. Необхідно визначити економічні розміри партії n, число партій m та їх періодичність τ, так щоб сумарні витрати на зберігання та доставку виявились найменшими.

Витрати на зберігання однієї партії продукту виражаються величиною $(1/2)nC_t\tau$, тому сумарні витрати по доставці та зберіганню однієї партії дорівнюють $C_0 + (1/2)nC_t\tau$. Таким чином, сумарні витрати C по доставці та зберіганню продукту на складі за весь період будуть дорівнювати

$$C = mC_0 + (m/2)C_t n\tau. \qquad (2)$$

Рівняння (2) та умови зв'язку (1) являють собою математичну модель задачі. Це система лінійних алгебраїчних рівнянь з трьома невідомими n, m, τ.

Розв'яжемо цю систему. Використовуючи умови зв'язку (1), замінимо у (2) M і τ через h. Тоді

$$C = NC_0 / n + C_t Tn / 2. \quad (3)$$

Щоб знайти мінімум С, необхідно визначити, при якому n_0 похідна $\frac{dC}{dn} = 0$.

З (3) маємо:

$$\frac{dC}{dn} = -NC_0 / n^2 + C_t T / 2 = 0. \quad (4)$$

Очевидно, що $\frac{dC}{dn} = 0$ при

$$n_0 = \sqrt{2NC_0 / C_t T}. \quad (5)$$

Таким чином визначається оптимальний розмір партії продукту, а потім з умов зв'язку (1) і оптимальні розміри циклу поставок τ_0 та числа партій m_0:

$$\tau_0 = n_0 / h, \quad (6)$$

$$m_0 = N / n_0. \quad (7)$$

Ми розглянули найпростішу модель управління запасами, так звану модель з фіксованим розміром замовлення. Ця модель може бути ускладнена за рахунок зняття такої умови, як неприпустимість відсутності продукту на складі. У цьому випадку треба врахувати збитки від тимчасового незадовільнення попиту та увести їх в модель.

Таким чином, первісна найпростіша модель допускає нарощування та ускладнення, в процесі якого може знадобитися і використання нових математичних засобів для її розв'язання.

Задачі розподілу

Типовими умовами, в яких розв'язується задача розподілу, є такі:

- існує ряд операцій (будь-якого виду), які повинні бути виконані;
- мається достатня кількість ресурсів для виконання цих операцій;
- принаймні, деякі операції можна виконувати різними способами, використовуючи різну кількість та різні комбінації ресурсів;
- деякі способи виконання операцій кращі за інші (менш дорогі, дають більший ефект);
- наявна кількість ресурсів недостатня для виконання кожної операції оптимальним способом.

Задача полягає у виборі такого розподілу ресурсів за операціями, при якому досягається максимальна загальна ефективність системи. Наприклад, можуть мінімізуватися сумарні затрати або може максимізуватися сумарний прибуток.

Найпростіший варіант такої задачі, коли для виконання одної операції потрібен один вид ресурсу, а число операцій та ресурсів співпадає, отримав назву *задачі про призначення*.

Більш загальний випадок, коли для виконання одної операції потрібно декілька видів ресурсів і один ресурс може брати участь у різних операціях, отримав назву *транспортної задачі*.

Математичний апарат, який використовується для побудови такого роду моделей розв'язування відповідних оптимізаційних задач, – методи *математичного програмування*. Різні види програмування – лінійне, нелінійне, стохастичне, параметричне та динамічне – відрізняються видом використовуваної інформації та прийнятими припущеннями.

Задачі масового обслуговування

Важливість задачі швидкого обслуговування черги покупців, відвідувачів тощо зрозуміла кожному. Специфіка ситуації, що при цьому складається, призводить до побудови моделей, які називаються *моделями обслуговування*. В термінах моделі обслуговування – особи чи об'єкти, незалежно від їхньої природи, які стоять у черзі, називаються заявками або клієнтами; мета їх очікування – операція обслуговування; місце, де виконуються операції – засіб обслуговування.

Для системи «клієнти – засіб обслуговування» характерно, що майже завжди мають місце або клієнти, що простоюють, або засоби обслуговування та (або) обслуговуючий персонал, що простоюють. І те, і інше призводить до

виникнення витрат, тому задача зводиться до мінімізації їх сумарної величини.

Порядок розвантаження суден в порту, роботи персоналу довідкових телефонних служб, структура та обсяг операцій, що надаються установами сервісу, – типові приклади задач масового обслуговування. Математичний апарат теорії масового обслуговування – апарат теорії ймовірностей, а також теорії диференціальних та інтегральних рівнянь.

Задачі впорядкування

В задачах масового обслуговування клієнтів порядок обслуговування заявок або заданий заздалегідь, або утворюється стихійно. Розв'язування задачі впорядкування передбачає визначення такого порядку обслуговування заявок, за якого мінімізується загальна тривалість обслуговування або деяка функція, залежна від витрат в обслуговуванні.

Математичний апарат задач впорядкування розвинений ще недостатньо. Лише задачі обмеженої розмірності можуть розв'язуватись точними аналітичними моделями. У більш складних випадках необхідно вдаватися до моделювання на ЕОМ. Задачі такого типу виникають при плануванні проведення ремонтних робіт, переоснащення верстатного парку, робіт по освоєнню нової продукції тощо.

Для постановки та розв'язування задач впорядкування необхідна інформація про необхідну послідовність виконання операцій обслуговування, тривалість операції і затрати ресурсів на її виконання.

Задачі заміни

Стандартні ситуації, в яких виникають задачі заміни, пов'язані з погіршенням характеристик елементів системи у процесі їх експлуатації або виходом з ладу, тобто відмовою.

Так, наприклад, складська або транспортна тара багатократного використання постійно зношується, втрачає свої властивості. Часто ремонтувати (заміняти) тару – означає збільшувати витрати за статтею ремонту. Скорочення витрат по ремонту тари може призвести до збільшення втрат на псування продуктів (в результаті погіршення умов зберігання). Отже, необхідно визначати оптимальний період ремонту (оновлення) тарного господарства, для того щоб забезпечити мінімум сумарних витрат та втрат.

Описані на якісному рівні математичні моделі задач прийняття організаційно-економічних рішень можна застосовувати при виконанні таких умов (умови Д. Шлессинжера):

- критерій (ціль) може бути точно визначений;
- може бути побудована формальна модель, яка виражає зв'язки між критерієм, змінними та існуючими обмеженнями;
- є достатня кількісна інформація, що дозволяє здійснити розумне визначення параметрів;
- значення вибраного критерію однозначно виражають корисність окремої альтернативи, визначеної фіксованими значеннями змінних.

На практиці найбільш вірогідне виконання цих умов на нижньому та середньому рівнях управління для технічних та повторюваних функцій у стандартних ситуаціях, тобто при прийнятті в основному оперативних, тактичних, а не стратегічних та унікальних рішень.

В найбільш загальному вигляді математичні моделі, що використовуються у детермінованих задачах вибору рішень, можуть бути представлені як

$$z \in G_z \subset Z, \qquad (8)$$

де Z – простір змінних, z – змінні моделі, G_z – множина допустимих значень змінних.

Для вибору найбільш раціонального рішення повинна бути визначена система показників (критеріїв), що характеризують якість кожного з можливих рішень, тобто

$$f_i(z),\ i=1,\ \ldots,\ r. \qquad (9)$$

Значення показників при різних допустимих значеннях змінних слугують основою для вибору рішення. Найбільше

розповсюдження у прикладних дослідженнях отримав оптимізаційний підхід, заснований на формулюванні єдиного показника, величина якого є критерієм вибору найкращого рішення з множини можливих. Формалізована постановка даної задачі має такий вигляд:

$$f(z) \to \max \text{ при } z \in G_z. \quad (10)$$

За наявності деяких показників (критеріїв) у деяких випадках вдається шляхом використання згортки побудувати на їх основі єдиний. Під *згорткою показників* розуміють побудову функції $U(z)=F(f_1(z), \ldots, f_m(z))$, яка може бути використана як критерій замість системи показників (9). Один з методів згортки («економічний») полягає у заданні додатних величин λ_i (i=1, …, r), на основі яких критерій формулюється у вигляді:

$$U(z) = \sum_{i=1}^{r} \lambda_i f_i(z). \quad (11)$$

Величини λ_i мають зміст цінності одиниці кожного з показників, оцінюючи його вклад у збільшення критерію задачі.

Тоді для моделі (8) можна поставити таку задачу вибору найкращого рішення: знайти $z^* \in Z$, на якому досягається. $\max_{z \in G_Z \subset Z} U(z)$

Таку задачу вибору рішень називають задачею оптимізації, а те допустиме значення z^*, при якому досягається розв'язок задачі оптимізації, - оптимальним. Пошук оптимального значення z^* здійснюється з використанням методів математичного програмування.

Проблеми вибору рішень з використанням точних математичних моделей відносяться до класу кількісно структурованих проблем, в яких залежності можуть бути виражені у чисельних оцінках.

Разом з цим в організаційних системах існує велика кількість неструктурованих або якісно виражених проблем прийняття рішень, в яких кількісні залежності невідомі. Існують слабко структуровані або змішані проблеми.

Важлива особливість подібних проблем полягає у тому, що їх модель або правило відбору альтернативних рішень можуть бути побудовані тільки на основі додаткової суб'єктивної інформації, отриманої від людини, яка бере участь у вирішенні проблеми.

Сучасні методи теорії прийняття рішень приписують певні норми поведінки ОПР. В основу цієї теорії покладена концепція, яка пов'язує такі поняття, як суб'єктивна ймовірність та корисність результатів, а також гіпотеза, у відповідності до якої ОПР повинна завжди вибирати альтернативу з максимальною очікуваною корисністю.

До таких методів насамперед відноситься широко розповсюджена на практиці група методів багатокритеріальної оцінки альтернатив.

При використанні методів даного типу виникають дві основні проблеми: як отримати оцінки кожної з альтернатив за окремими критеріями та як об'єднати, агрегувати ці оцінки у загальну оцінку корисності альтернативи.

ВИСНОВКИ

Застосування математичних моделей дослідження операцій має важливе значення для прийняття управлінських рішень керівниками на всіх ланках управління.

Кількісна оцінка параметрів технологічних процесів необхідна для зменшення невизначеності та стохастичності.

Математичні моделі дозволяють оптимізувати рівень витрат ресурсів при виконанні будь-яких процесів (підготовчих, постачальницько-збутових, логістичних, виробничих тощо).

Динамічні, стохастичні процеси можуть відтворюватись за допомогою інструментів математичного програмування, що сприяє більш точному плануванню, прогнозуванню та моніторингу процесів.

REFERENCES

1. **Savenko V. I., Shatrovoi I. A.,Fialko N. M., Honcharenko T. A.** (2022). Doslidzhennia i matematychne modeliuvannia orhanizatsiinykh struktur ta intelektualni informatsiini instrumenty v orhanizatsii i upravlinni budivnytstvom: monohrafiia. 2-he vyd. vypr. ta dop. Kyiv, Tsentr uchbovoi literatury Publ., 148.
2. **Dotsenko S. I., Savenko V. I., Bazylenko S. O., Kliuieva V. V., Palchyk S. P., Hihineishvili D. Ya.** (2018). Intelektualni informatsiini tekhnolohii u pryiniatti efektyvnykh rishen v upravlinni pidpryiem-stvom. *Upravlinnia rozvytkom skladnykh system*, 34, 161–169.
3. **Savenko V. I., Dotsenko S. I., Kliuieva V. V., Palchyk S. P., Tereshchuk M. O.** (2019). Intelektualni informatsiini instrumenty rozvytku vyrobnychykh system, enerhetychnoho menedzhmentu ta pidpryiemstva v tsilomu. *Upravlinnia rozvytkom skladnykh system*, 37, 195–204.
4. **Pavlenko P. M., Filonenko S. F., Cherednikov O. M., Treitiak V. V.** (2017). Matematychne modeliuvannia system i protsesiv: navch. posib. Kyiv, NAU Publ., 392.
5. **Hevko I. B.** (2009). Metody pryiniattia upravlinskykh rishen: book. Kyiv, Kondor, 187.
6. **Izmailova O. V.** (2002). Metody pryiniattia bahatokryteriinykh rishen v informatsiinykh systemakh: book. Kyiv, 111.
7. **Savenko V. I., Nesterenko I. S., Kliuieva V. V.** (2019). Upravlinnia konkurentospromozh-nistiu pidpryiemstva v suchasnykh umovakh hospodariuvannia. *Shliakhy pidvyshchennia efektyvnosti budivnytstva v umovakh formuvannia rynkovykh vidnosyn*, 42, 66–76.
8. **Klebanova T. S.,** Kyzym M. O., Cherniak O. I. (2009). Matematychni metody i modeli rynkovoi ekonomiky: book. Kharkiv, «Inzhek» Publ., 456.

Typical mathematical models used in computer-aided organizational management systems

VIktoriia Kliuieva, Vlad Herasymchuk, Ihor Danylov

Abstract. The article considers typical mathematical models used in automated control systems (ACS), a type of which are automated organizational control systems (ACOC), with the aim of making optimal management decisions.

In our time, it is impossible to solve the problems of managing the economy by mechanically increasing the number of the governing apparatus, because the scale of the work requires such a number of people that cannot be directed to the sphere of management.

An analysis of the most common types of tasks solved by managers at all levels of management is carried out: inventory management, distribution, mass service, ordering, replacement.

An example of solving the problem of inventory management at a warehouse is given.

A general description of mathematical models used in deterministic tasks of organizational and economic decision-making in organizational systems is given and the conditions for their application are given.

Keywords: mathematical models, automated organizational management systems, management decision-making, operations research.

Mathematical model of single-channel signal search with two degrees of detection in radio frequency monitoring of mobile telecommunication systems

Anatolii Ilnytskyi[1], Oleg Tsukanov[2], Oleksandr Symonenko[3], Yuriy Pepa[4], Andrii Petrenko[5]

[1,2] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
37 Beresteysky Avenue, Kyiv, Ukraine, 03056
[3] Heroiv Krut Military Institute of Telecommunications and Informatization
St. 45/1 Knyazou Ostrozkih, Kyiv, Ukraine, 01011
[4,5] State University of Information and Communication Technologies
St. Solomyanska, 7, Kyiv, Ukraine, 03037
[1] anatolii.ilnytskyi@gmail.com, https://orcid.org/0000-0003-0454-1819,
[2] cukanov-o@ukr.net, https://orcid.org/0000-00027104-3274,
[3] lokalyt@gmail.com, https://orcid.org/0000-0001-8511-2017,
[4] yurka14@gmail.com, https://orcid.org/0000-0003-2073-1364,
[5] pab.05@ukr.net, https://orcid.org/0000-0002-4793-5474

Received 05.09.2024, accepted 18.10.2024
https://doi.org/10.32347/uwt.2024.15.1102

Abstract. Today, technical means of radio interception, monitoring and direction finding in mobile radio communication networks are implemented in the form of software and hardware complexes, the most important performance indicators of which are considered to be speed, detection accuracy and probability of recognition of mobile radio communication means with their information content.

At the same time, these issues still remain problematic and require further development of methods and techniques for searching and detecting signals of mobile radio communications in both frequency and time environments of telecommunication channels and their information processing.

The authors propose a mathematical model for searching for mobile radio signals in the frequency-time domain with two degrees of detection. The description of the mathematical model for determining the spectral components of signals in the frequency and time domains is carried out using the basic provisions of the theory of directed probability graphs, geometric probabilities with its well-known problem of meeting in a given time interval and the theoretical foundations of statistical information processing.

It is shown that the application of the mathematical model of single-channel search for signals of mobile radio communications with two degrees of detection in the frequency-time domain in practice will make it possible to determine the quality of the radio monitoring process and increase the efficiency of evaluating the spectral components of radio signals in terms of speed, detection

Anatolii Ilnytskyi Associate
Professor of the Department

Oleg Tsukanov
Associate Professor of the Departmen

Oleksandr Symonenko
PhD, Associate Professor

Yuriy Pepa
Ph.D., Associate Professor, Professor of the Department of Technical Systems of Cyber Protection DUIKT

Andrii Petrenko
Ph.D., associate professor, associate professor of the Department of Cyber Security of the National Aviation University

accuracy and probability of recognition of mobile radio communications with further determination of their information content.

Keywords: radio monitoring, telecommunication networks, mobile communication systems, performance indicators, speed, detection accuracy, recognition probability.

INTRODUCTION

It is known that radio frequency monitoring (RFM) of telecommunication systems (TCS) of fixed and mobile communications in Ukraine is entrusted to the State Enterprise 'Ukrainian State Centre of Radio Frequencies' (SE 'UCRF'), which continues its active development and becomes one of the largest and most powerful in Europe under martial law [1, 2]. Today, the technical means of radio interception, monitoring and direction finding in the networks of wireless fixed and mobile radio communication systems are implemented in the form of software and hardware complexes (SAC) of various modifications, which operate under conditions of partial or complete uncertainty of input signal parameters in real time against the background of a huge number and variety of radio emission sources (RES) with the most modern data transmission protocols [2]. Currently, the UCRC has more than 140 mobile and almost 200 stationary radio monitoring stations (RMNS) and SACs deployed in more than 100 settlements of the country [3]. The process of radio monitoring covers more than 200 thousand radio electronic devices (RED) of various purposes and subordination to both public and private structures. At the same time, all stationary RMS operate in automated modes, and their functional and technical capabilities fully comply with the requirements of the International Telecommunication Union [4,5]. Some models of mobile equipment and SACs, in particular, specialised RME. It should be noted that the most important indicators of the effectiveness of SAR in monitoring IEDs are speed, detection accuracy and probability of detecting mobile and fixed radio communications TCSs with further determination of their information content.

In the context of a full-scale invasion and combat operations for Ukraine's independence, the effectiveness of the RFEU's radio monitoring of TCS means is of particular importance. This is confirmed by the fact that under martial law, the State Enterprise 'UDCR' is subordinated to the Command of the General Staff of the Armed Forces of Ukraine, which ensures coordination of RFM, electronic and radar intelligence and electronic warfare of the state's power structures both on the territory of Ukraine and partially abroad. Therefore, the issues related to the development of new and improvement of existing technical means of RFM, further development of scientific and methodological apparatus and evaluation of their effectiveness, software and algorithmic support and practical implementation remain extremely relevant [6]. inconvenience lies in the fact that in the case of transmission of signals of several tones with the same amplitudes through a communication channel, their amplitudes will already be different at reception. This is mainly due to the uneven amplitude-frequency response of the RFI channel [3]. In addition, the equipment for generating multitone signals has an amplitude spread, which leads to a significant difference in the amplitudes of the received spectral components of the signal. Thus, according to the International Telecommunication Union's (ITU-T) Standardisation Sector specification, a DTMF receiver must operate with a twist (the difference between the amplitudes of the two main signal frequencies) of at least 8 dB. At the same time, it should not exceed 3 dB on the transmitting side [4].

PROBLEM FORMULATION

In the structure of the SAC monitoring system of MRC means, the main place is occupied by the subsystem of radio receiving devices (RRD), which solves the problem of signal detection in the frequency-time domain by cyclic procedures with one or more detection stages, implementing methods of sequential-parallel search and detection of signals. As an example, we can cite the mobile radio monitoring SAC MMS-02, which has the following technical characteristics [3]: radio frequency band: 30 MHz - 3000 MHz; sensitivity - not less than 0 dBμV/m (1 μV/m);

dynamic range - not less than 75 dB; maximum panoramic viewing speed - not less than 300 MHz/s; level measurement uncertainty - not more than 3 dB; frequency measurement accuracy - not less than 10-6.

The cyclic procedure for searching for MRC signals in the frequency domain with one degree of detection is described in [7]: the radio receiving device of the SAC is tuned to the frequency of a certain channel (1, 2, ..., N), where a decision is made on the presence or absence of a signal during a given analysis time t_a = const. In the absence of a signal, the receiver is tuned to the frequency of the next channel, and so on. When the last channel is reached, the radio is tuned to the frequency of the first channel and the search starts again. However, as practice shows, the signal may disappear during the time τ_c, for analysing N channels or appear when it is detected. At the same time, the moments of its appearance or disappearance may not coincide with the start or end of the RM of this channel. In addition, a signal in a channel may appear in the previous cycle of viewing the RPF of N channels. That is, there is a need to analyse the state and mathematically describe the signal search subsystem not only in the frequency but also in the time domain. At the same time, this procedure for searching for MRC signals in the frequency domain with one degree of detection, given in [7], was chosen by the authors of the article as a prototype. However, the analysis of the chosen prototype shows that the probability of successful completion of the search for a signal with one degree of detection in the frequency-time domain for a given time depends on the value of the signal duration τ_c, the number of analysed frequency channels N, the time of signal analysis in each channel t_a and the probabilities of the first F and second kind of errors D. Of these values, only the signal analysis time in each channel can actually be changed. That is, in order to increase the probability of successful completion of the signal search and reduce its time, it is necessary to reduce the signal analysis time t_a in each channel. For this purpose, we can propose the use of a cyclic procedure for searching for RSI signals with two (several) detection stages and different analysis times at each stage.

GOAL STATEMENT

The purpose and main content of the article is to describe a mathematical model of single-channel search for signals of mobile radio communications with two degrees of detection in the frequency-time domain. That is, the object of research in the article is the process of radio monitoring of radio emission sources of telecommunication networks and systems, and the subject of research is a mathematical model of single-channel signal search for mobile radio communications with two degrees of detection in the frequency-time domain. The application of the mathematical model in practice will make it possible to increase the efficiency of detecting the spectral components of radio signals and evaluate the procedure for searching for signals of MRC means in terms of speed, detection accuracy and recognition probability with further determination of their information content. It will also give an impetus to the further development of new and improvement of existing technical means of RFM, further development of the scientific and methodological apparatus for assessing their effectiveness, software and algorithmic support and practical implementation.

MAIN PART

The cyclic procedure for searching for mobile radio communication (MRC) signals in the frequency-time domain with one degree of detection (prototype) is schematically presented in the form of a directed probability graph (Fig. 1) and, using the theory of directed probability graphs, is described mathematically [7].

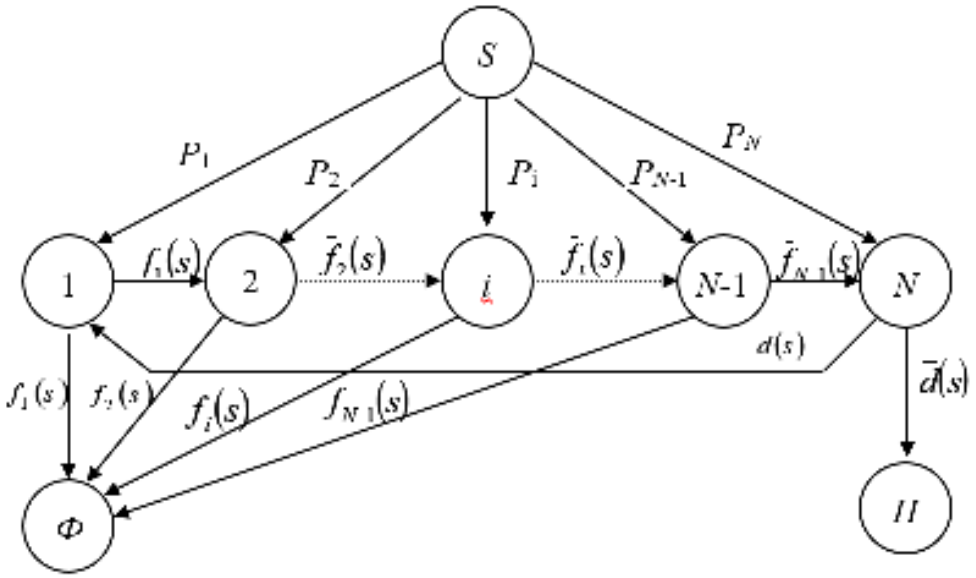


Fig. 1. Graph of the cyclic procedure of a single-channel search with one degree of detection

Here, the graph nodes represent possible states of the search subsystem: S is the initial state; H(s) is the absorption state corresponding to the successful completion of the signal search (correct recognition); F(s) is the absorption state corresponding to the false recognition of the signal. Graph edges represent possible transitions of the system from one state to another. Each edge of the graph has weights determined by (1), which take into account the probability of transition in one step from the state from which the edge leaves to the state it enters and the time spent in the corresponding state:

$$d(s) = De^{-t_a s}, \quad \bar{d}(s) = (1-D)e^{-t_a s}; \qquad (1)$$
$$f_q(s) = F_q e^{-t_a s}, \quad \bar{f}_q(s) = (1-F_q)e^{-t_a s},$$

And as given in [7], the probability of successful completion of the search for a given time with one degree of detection in the frequency-time domain is defined as:

$$P_{\text{П}}(t) = \frac{(\tau_c - t_a)(1-D)}{N(\tau_c + Nt_a)} \sum_{i=1}^{N} \sum_{n=0}^{\infty} \left(1 - \frac{(\tau_c - t_a)(1-D)}{\tau_c + Nt_a}\right)^n \times$$
$$\times (1-F)^{n(N-1)+N-i} h\left[t - (Nn + N - i + 1)\, t_a\right]$$
(2)

where F is the probability of false detection (first-order error) when analysing a cell with number N that does not contain a signal;
D - the probability of missing a signal (second-N);
h(x) - the Heaviside function;
t_a - the time of analysis of one cell;
τ_c - the duration of the input signal.

However, as practice shows, during the time t for analysing N channels, the signal may disappear or appear when it is detected. At the same time, the moments of its appearance or disappearance may not coincide with the moments of the beginning or end of the RM of this channel. In addition, a signal in a channel may appear in the previous cycle of viewing the MRC RRD of N channels. Also, analysing the above dependencies (2), we can conclude that to increase the probability of successful completion of the signal search and reduce its time, it is necessary to reduce the signal analysis time ta in each channel. For this purpose, we can propose the use of a cyclic procedure for searching for RSI signals with two stages of detection and different analysis times at each stage.

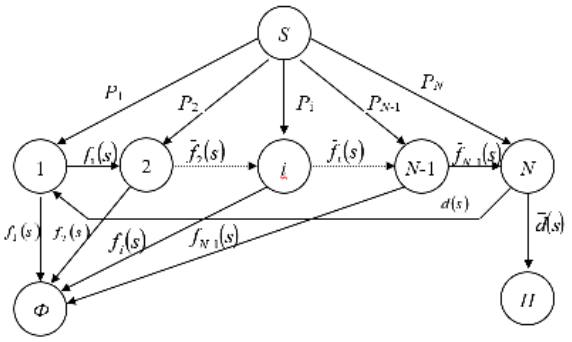


Fig. 2. Graph of a cyclic single-channel search procedure with two detection stages

In accordance with the above procedure of single-channel search with one detection stage (Fig. 1) and the description of the system state (2) for RM with two detection stages, we constructed (by analogy with [7]) a directed probability graph, which is schematically shown in Fig. 2.

As can be seen from Fig. 2, the first stage detects a signal in each of the N analysed channels within the time t_{a1}, which is less than the analysis time when searching with one stage of detection. If a signal is detected, the second stage is activated within the time t_{a2}, which is equal to the signal analysis time in a single-stage search. If a false signal detection occurs (first-order error F occurs) at the first stage, the search subsystem detects its own error during time t_{a2} and continues searching in the previous direction until it reaches the channel matching with the signal. If a signal is missed, a new search cycle begins. Thus, one of the conditions for a two-detection search is the inequality (t_{a1}+t_{a2}). The search for a signal can be completed either on the first cycle (when the search area is first viewed) or after some random number of cycles, and the duration of each cycle is a random variable due to the uncertain time spent on signal analysis. The time taken to analyse the signal in the *i*-th channel can have two values: t_{a1} and (t_{a1}+t_{a2}), respectively.

To search for MRC signals with two stages of detection, scanning DUTs can be used. That is, at the first stage, it is necessary to search for signals whose level exceeds a given detection threshold value (input signal level), and at the second stage, analyse only these signals. This approach is effective if some search channels do not contain any signal due to the limited analysis time at the first stage of detection. This situation can occur in the operation of an MRC with a dedicated or distributed control channel.

For the mathematical description of the above procedure, we will use the rules of graph transformation [8], and then the expressions for the functions of transition of the graph from the initial state S to the absorbing state H, which corresponds to the successful completion of the search (correct recognition), will be as follows:

$$H(s)=\frac{\bar{d}_1(s)\bar{d}_2(s)\sum_{i=1}^{N}P_i\prod_{q=i}^{N-1}\left[\bar{f}_{q1}(s)+f_{q1}(s)\bar{f}_{q2}(s)\right]}{1-\left[d_1(s)+\bar{d}_1(s)d_2(s)\right]\prod_{q=1}^{N-1}\left[\bar{f}_{q1}(s)+f_{q1}(s)\bar{f}_{q2}(s)\right]} \quad (3)$$

$$d_1(s)=D_1e^{-t_{a1}s},\quad \bar{d}_1(s)=(1-D_1)e^{-t_{a1}s}$$

$$d_2(s)=D_2e^{-t_{a2}s},\quad \bar{d}_2(s)=(1-D_2)e^{-t_{a2}s}$$

$$f_{q1}(s)=F_{q1}e^{-t_{a1}s},\quad \bar{f}_{q1}(s)=(1-F_{q1})e^{-t_{a1}s}$$

F_{q1}, F_{q2} are the probabilities of the first kind of error (false detection) when analysing a cell with number q (q=1, 2,..., N-1) that does not contain a signal at the first and second detection stages;

D_1, D_2 - probability of the second type of error (signal miss) when analysing a cell with number N at the first and second detection stages, P_i is the probability of starting viewing from the *i*-th cell (i=*1, 2,..., N*). Assuming that the search subsystem uses the same type of RRD and with a uniform distribution of signal occurrence moments within the search area, after providing H(s) in the form of a geometric series and performing the inverse Laplace transform $P^f_{\Pi}(t) = L^{-1}\{H(s)/s\}$, [8,9] (as in the case of search with one detection stage), the expression for the probability of successful completion of the search for a given time in the frequency domain with two stages will be as follows:

$$P^f_{\Pi}(t)=\frac{1}{N}\sum_{i=1}^{N}\sum_{n=0}^{\infty}\sum_{k=0}^{n}C_n^k(1-D_1)(1-D_2)D_1^k\left[(1-D_1)D_2\right]^{n-k}\times$$
$$\times\sum_{q=0}^{(N-1)n+(N-i)}C^q_{(N-1)n+(N-i)}(1-F_1)^q\left[F_1(1-F_2)\right]^{(N-1)n+(N-i)-q}\times$$
$$\times h\left[t-t_{a1}\left(Nn+N-i+1\right)-\right.$$
$$\left.-t_{a2}\left(Nn+N-i-q-k+1\right)\right] \quad (3)$$

where $C_n^k = \frac{n!}{k!(n-k)!}$

To calculate this probability, it is necessary in (4) for each i to sum all the components with indices n, q, k that satisfy the inequalities:

$$t_{a1}(Nn + N - i + 1) + \\ + t_{a2}(Nn + N - i - q - k + 1) \le t \quad (4)$$

As with the search for MRC signals with one detection stage, it is necessary to take into account, along with the frequency coincidence, the time coincidence in one channel of the desired signal and the RRD.

The description of the state of the single-channel subsystem for searching for MRC signals with two detection stages in the time domain is similar to the case of searching for signals in the time domain with one stage [7]. The peculiarity is that the duration of each search cycle will be a random variable due to the uncertainty of the time spent on signal analysis in each channel.

The time spent analysing a signal in one channel can also have two values: ta1 - in the case when only the first stage is involved, and (t_{a1}+t_{a2}) - in the case when two detection stages are involved. The transition from the first to the second stage occurs with probability F_1 when analysing an empty channel or with probability $P = (1 - D_1)$ when analysing a channel that holds a signal. With this in mind, the time of one search cycle T is defined as

$$T = t_{a1}N + t_{a2}(1 - D_1 + (N-1)F_1) \quad (5)$$

To calculate the probability of meeting an RRD and a signal during the analysis of N channels, we use the basic provisions of the theory of geometric probabilities similar to the case of a search with a single detection stage [7]. Then the time of signal analysis in one channel t_a in this case is a random variable, the average value of which, taking into account (6), will be determined by the expression:

$$t_a = \frac{T}{N} = t_{a1} + t_{a2}\frac{1 - D_1 + (N-1)F_1}{N} \quad (6)$$

To calculate the probability of meeting an RRD and a signal during the analysis of N channels, we use the basic provisions of the theory of geometric probabilities similar to the case of a search with a single detection stage [7]. Then the time of signal analysis in one channel t_a in this case is a random variable, the average value of which, taking into account (6), will be determined by the expression:

$$t_a = \frac{T}{N} = t_{a1} + t_{a2}\frac{1 - D_1 + (N-1)F_1}{N} \quad (7)$$

Taking into account (7), the expression for calculating the probability of successful completion of a search with two stages in the time domain in one viewing cycle can be written as follows:

$$P_{\text{П}}^t = \frac{N(\tau_c - t_{a1}) - t_{a2}(1 - D_1 + (N-1)F_1)}{N[\tau_c + Nt_{a1} + t_{a2}(1 - D_1 + (N-1)F_1)]} \quad (8)$$

The fact of simultaneous signal detection in the frequency and time domains of the search can be considered as independent random events. In this case, taking into account (4), the expression for determining the probability of successful completion of the search for a given time in the frequency-time domain with two degrees of detection takes the form:

$$P_{\text{П}}(t) = \frac{(1-D_1)(1-D_2)P_{\text{П}}^{t\,2}}{N}\sum_{i=1}^{N}\sum_{n=0}^{\infty}\sum_{k=0}^{n} C_n^k\left(1-(1-D_1)P_{\text{П}}^t\right)^k \times \\ \times\left[(1-D_1)P_{\text{П}}^t\left(1-(1-D_2)P_{\text{П}}^t\right)\right]^{n-k} \times \\ \times \sum_{q=0}^{(N-1)n+(N-i)} C_{(N-1)n+(N-i)}^q (1-F_1)^q\left[F_1(1-F_2)\right]^{(N-1)n+(N-i)-q} \times \\ \times h\left[t - t_{a1}(Nn + N - i + 1) - t_{a2}(Nn + N - i - q - k + 1)\right] \quad (9)$$

To calculate this probability, it is necessary for each i to sum up all the components with indices *n, q, k* that Table 1 - Probabilities of successful completion of the search for a given time

According to the obtained relations (2) and (9), we calculated the dependences of the probability of successful completion of the search for a given time in the frequency-time domain on the search time for the case with one and two degrees of detection (Fig.3).

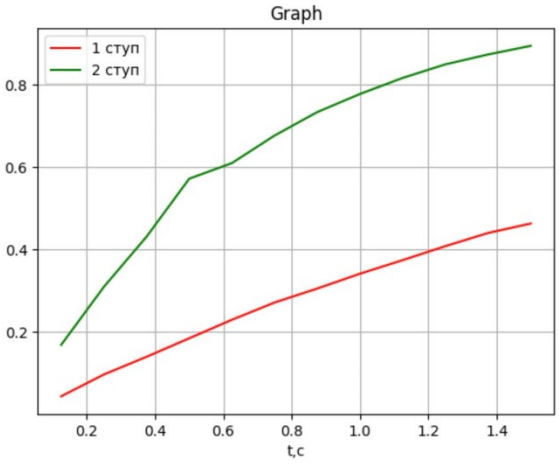


Fig. 3. Probabilities of successful completion of the search for a given time

When calculating these dependencies, the following were taken into account τ_c=100 мс, F_1= F_2= F_3=0,001, N = 8, the analysis time at each subsequent detection stage is 3 times longer than at the previous one. The total signal analysis time at all detection stages is ta = 40 ms. The probability of a signal miss at the last stage is assumed to be P = 0.1. The probability of signal miss at the previous stages was determined by the Neumann-Pearson criterion [8,9] at the given values of the probability of false detection. It was taken into account that the detection parameter (signal-to-noise ratio) is inversely proportional to the duration of signal analysis [10], and the signal is detected with random amplitude and phase.

The analysis of the obtained numerical values shows that to increase the efficiency of signal search, it is advisable to use cyclic search procedures with two (several) detection stages. At the same time, the introduction of the second stage makes it possible to increase the probability of successful completion of the search for a given time by an average of (2 - 2.5) times compared to the search with one detection stage, but the value of the probability of successful completion of the search increases slowly. To increase the probability of successful completion of the signal search and reduce its time, it is necessary to reduce the time of signal analysis ta in each channel. For this purpose, it is possible to propose the use of a cyclic procedure for searching for RMS signals with several (more than two) detection stages and different analysis times at each stage. However, these issues are beyond the scope of this article and can be considered separately.

CONCLUSIONS

1. The developed mathematical model of single-channel search for signals of mobile radio communications with two degrees of detection in the frequency-time domain makes it possible to calculate the probability of meeting an RRD and a signal during the analysis of N channels, i.e., during one viewing cycle перегляду $T= t_a N$, provided that the duration of the searched signal τc is not less than the analysis time of one channel $\tau_c \geq t_a$.

2. The probability of successful completion of the search for a signal with two degrees of detection in the time-frequency domain for a given time depends on the value of the signal duration τ_c, the number of analysed frequency channels N, the time of signal analysis in each channel t_a, and the probabilities of the first type of error F and the second type of error D.

3. The time spent on signal analysis in one channel can have two values: t_{a1} - in the case when only the first stage is involved, and $(t_{a1}+t_{a2})$ – in the case when two detection stages are involved. The transition from the first to the second stage occurs with probability F_1 when analysing an empty channel or with probability $P = (1 - D_1)$ when analysing a channel containing a signal.

4. The application of a mathematical model of single-channel search for signals of mobile radio communication means with two degrees of detection in the frequency-time domain in practice will make it possible to increase the efficiency of evaluating the spectral components of radio signals in terms of performance, detection accuracy and probability of recognition of mobile radio communication means (see Fig. 3) with the subsequent determination of their information content.

5. The direction of further development of scientific research in this subject area can be considered the analysis of the use of a cyclic procedure for searching RMS signals with several stages of detection (multi-stage detection) and different times at each stage of

detection and the synthesis of devices for practical implementation.

REFERENCES

1. **Ilchenko M. Iu., Narytnyk T. M., Kapshtyk S. V., Avdieienko H. L., Korsun V. I., Prysiazhnyi V. I.** (2013). Planuvannia ta elektromahnitna sumisnist v bezprovodovykh infokomunikatsiiakh: navchalnyi posibnyk dlia studentiv spetsialnosti 172 «Telekomunikatsii ta radiotekhnika». Kyiv, KPI im. Ihoria Sikorskoho, 259.
2. **Ilchenko M. Iu., Kravchuk S. O.** (2017). Telekmunikatsiini systemy. Kyiv, Naukova dumka Publ., 730.
3. CCITT Blue Book, Recommendation Q.23: Technical Features of Push-Button Telephone Sets. Geneva, (1989).
4. CCITT Blue Book, Recommendation Q.24: Multi-Frequency Push-Button Signal Reception. Geneva, (1989).
5. **IlnytskyiA.I., Zakharchuk L.V.** (2023). Problemni pytannia radiomonitorynhu dzherel i obiektiv telekomunikatsiinykh merezh i system ta zahalno-naukovyi kontseptualnyi pidkhid do yikh rozviazannia. III Mizhnarodna naukovo-tekhnichna konferentsiia «Systemy i tekhnolohii zviazku, informatsii ta kiberbezpeky: aktualni pytannia i tendentsii rozvytku», 30.11.2023. Viiskovyi instytut telekomunikatsii ta informatsii imeni Heroiv Krut, Kyiv, 2023, 167.
6. **Ilnytskyi A. I., Zakharchuk L. V.** (2024). Matematychna model odnokanalnoho poshuku syhnaliv zasobiv mobilnoho radiozviazku z odnym stupenem vyiavlennia v chastotno-chasovii oblasti. Kyiv, Viiskovyi instytut telekomunikatsii ta informatsii imeni Heroiv Krut, 71.
7. **Grimmett G. R., Stirzaker D. R.** (2001). Probability and Random Processes. New York: Oxford University Press Inc., 596.
8. **Hniedenko B. V.** (2010). Kurs teorii ymovirnostei. Kyiv, VPTs Kyivskyi universytet, 464.
9. **Ilnytskyi A. I., Stretovych O. V.** (2005). Alhorytmy dekoduvannia tonalnykh syhnaliv v kompleksakh rozvidky system rukhomoho radiozviazku. Trudy akademii, 65, 70–75.

Математична модель одноканального пошуку сигналів з двома ступенями виявлення при радіочастотному моніторингу телекомунікаційних систем мобільного зв'язку

Анатолій Ільницький, Олег Цуканов, Олександр Симоненко

Анотація. На сьогодні технічні засоби радіоперехоплення, моніторингу та пеленгування в мережах рухомого радіозв'язку реалізуються у вигляді програмно-апаратних комплексів, найважливішими показниками ефективності яких вважаються швидкодія, точність виявлення та вірогідність розпізнавання засобів рухомого радіозв'язку з їх інформаційним наповненням.

Разом з тим, ці питання все ще залишаються проблемними і потребують подальшого розвитку методів і засобів пошуку та виявлення сигналів рухомих засобів радіозв'язку як у частотному, так і в часовому середовищах телекомунікаційних каналів зв'язку та їх інформаційної обробки.

Авторами запропоновано математичну модель пошуку сигналів мобільного радіозв'язку в частотно-часовій області з двома ступенями виявлення. Опис математичної моделі визначення спектральних складових сигналів у частотній та часовій областях виконано з використанням основних положень теорії спрямованих графів ймовірностей, геометричних ймовірностей з її відомою проблемою зустрічі на заданому часовому інтервалі та теоретичних основ статистичної обробки інформації.

Показано, що застосування математичної моделі одноканального пошуку сигналів рухомого радіозв'язку з двома ступенями виявлення в частотно-часовій області на практиці дозволить визначити якість процесу радіомоніторингу та підвищити ефективність оцінювання спектральних складових радіосигналів за показниками швидкості, точності виявлення та ймовірності розпізнавання рухомих радіозасобів з подальшим визначенням їх інформативності.

Ключові слова: радіомоніторинг, телекомунікаційні мережі, системи мобільного зв'язку, показники ефективності, швидкість, точність виявлення, вірогідність розпізнавання

The synergistic impact of 5g on internet of things innovation and growth

Abdulsatar Shaker Salman[1], Aqeel Mahmoud[2], Abdulelah Hameed Yaseen[3], Omar Saad Ahmed[4], Mohammed Yaseen Abdullah[5]

[1] Al-Mansour University College, Baghdad 10067, Iraq
[2] Al-Rafidain University College, Baghdad 10064, Iraq
[3] Al-Kitab University, Kirkuk, 36015, Iraq
[4] Al-Turath University, Baghdad 10013, Iraq
[5] Alnoor University, Nineveh 41012, Iraq
[1] abdul.shaker@muc.edu.iq, https://orcid.org/0009-0009-9167-904X,
[2] aqeel.jawad@ruc.edu.iq,
[3] abdulelah.h.yaseen@uoalkitab.edu.iq,
[4] omar.saad@turath.edu.iq,
[5] mohammed.yaseen@alnoor.edu.iq

Received 12.08.2024, accepted 30.09.2024
https://doi.org/10.32347/uwt.2024.15.1201

Abstract. Background: The emergence of 5G technology is revolutionizing the field of telecommunications, particularly in facilitating the expansion of the Internet of Things (IoT). By providing higher data speeds, ultra-low latency, and enhanced connectivity, 5G promises to address the limitations of previous networks in supporting IoT infrastructures.

Objective: This study aims to explore the role of 5G in developing IoT applications, emphasizing how its advanced capabilities can meet the unique requirements of diverse IoT systems.

Methods: The research methodology includes a detailed review of recent technological advancements in 5G, focusing on how specific features, such as network slicing and edge computing, contribute to IoT development. Statistical analysis is applied to actual data to demonstrate 5G's effectiveness in enabling IoT connectivity and improving application performance.

Results: The findings show that 5G significantly enhances IoT deployment by reducing latency, improving data transmission rates, and supporting a vast number of connected devices simultaneously. This improvement drives efficiencies in multiple industries, including healthcare, manufacturing, and transportation.

Conclusion: The integration of 5G technology with IoT represents a substantial advancement in connectivity, offering reliable, fast, and scalable solutions. This development is critical for the continued growth and sophistication of IoT ecosystems, highlighting the need for 5G deployment in achieving the full potential of IoT innovations.

Keywords: 5G, Internet of Things (IoT), network slicing, latency, edge computing, data transmission, scalability, telecommunications, connectivity, IoT applications

Abdulsatar Shaker Salman
Al Mansour University
College: Baghdad, IQ

INTRODUCTION

The Internet of Things (IoT) has emerged as a transformative force, linking physical devices to the digital world and enabling unprecedented levels of automation, monitoring, and data exchange [1]. IoT applications have expanded across various industries, including healthcare, transportation, manufacturing, and agriculture, driving efficiencies and enhancing user experiences [2]. However, traditional telecommunications networks have struggled to meet the evolving demands of these interconnected systems due to limitations in data speed, latency, and device capacity [3]. As IoT devices proliferate and their applications become more complex, there is a growing need

for robust network infrastructure capable of handling the unique demands of IoT ecosystems [4].

The advent of 5G technology is widely recognized as a critical enabler for the next generation of IoT. Unlike its predecessors, 5G offers significantly higher data transfer rates, reduced latency, and improved connectivity, making it well-suited to support the vast network of connected devices that constitute IoT [5]. The core features of 5G, such as network slicing, edge computing, and ultra-reliable low latency communication (URLLC), address the existing constraints of 4G and older networks by providing tailored network experiences for diverse applications [6]. With 5G, IoT applications can achieve higher reliability, faster response times, and enhanced scalability, enabling new possibilities in areas such as autonomous vehicles, remote healthcare, and smart city infrastructure [7].

Network slicing is one of the most promising features of 5G, allowing for the customization of network services to meet the specific needs of different IoT applications [1]. Through network slicing, multiple virtual networks can be created within a single physical 5G network infrastructure, each optimized for particular requirements such as bandwidth, latency, and security [8]. This capability is particularly valuable for IoT applications, which have highly variable requirements depending on their function. For instance, autonomous vehicles require near-instantaneous data processing and ultra-low latency, while smart meters in energy systems prioritize efficient, low-power operation [9]. By segmenting the network to suit each application's needs, 5G supports a more versatile IoT ecosystem, driving innovation across multiple sectors [10].

Another pivotal feature of 5G that supports IoT expansion is edge computing. In traditional cloud-based networks, data from IoT devices must travel to centralized servers for processing, resulting in latency issues that can impact the performance of time-sensitive applications [5]. With edge computing, processing occurs closer to the data source, reducing latency and enhancing the speed of data processing [11]. This is particularly important for applications like industrial IoT, where real-time data analysis is crucial for efficient operations [12]. By bringing data processing closer to the edge, 5G improves response times, making IoT applications more responsive and reliable. Furthermore, edge computing helps alleviate network congestion, allowing a larger number of devices to connect and function simultaneously [13].

The integration of 5G and IoT is also expected to bolster the deployment of Massive Machine-Type Communications (mMTC), which supports a vast number of low-power devices operating within a dense network environment [7]. Unlike previous network technologies, 5G is designed to accommodate the unique requirements of mMTC, such as lower data rates and extended battery life [14]. This is particularly advantageous for IoT applications in smart cities, agriculture, and environmental monitoring, where large volumes of connected devices must operate continuously over long periods [15]. By enabling mMTC, 5G expands the scope of IoT applications, making it feasible to implement large-scale, sensor-driven networks for comprehensive data collection and analysis [16].

The capabilities of 5G address the key challenges faced by IoT applications, allowing for greater connectivity, faster data transmission, and improved responsiveness [4]. The enhanced performance provided by 5G is instrumental in realizing the full potential of IoT, driving innovation and enabling advanced applications across a range of sectors [1]. As industries continue to adopt IoT solutions, the role of 5G in supporting these technologies will become increasingly critical. The following sections of this article explore the impact of 5G on IoT development, discussing the technological advancements and use cases that demonstrate its transformative potential.

THE AIM OF THE ARTICLE

The primary aim of this article is to examine the pivotal role of 5G technology in driving the evolution of the Internet of Things (IoT) by analyzing its capabilities and how these contribute to the efficiency and scalability of IoT applications. In recent years, IoT has

experienced rapid growth, largely fueled by advances in connectivity and computing. However, existing network infrastructures have faced significant challenges in meeting the high demands of IoT systems. These challenges include limited bandwidth, high latency, and insufficient device connectivity, which constrain the deployment and performance of IoT solutions. By addressing these limitations, 5G offers an advanced network solution that can support the extensive needs of IoT applications across various industries.

This article aims to provide an in-depth analysis of 5G features such as network slicing, edge computing, and Massive Machine-Type Communications (mMTC) and their potential to enhance IoT performance. Each of these features offers unique capabilities that contribute to the creation of a more robust, flexible, and scalable IoT infrastructure. Through this analysis, the article seeks to highlight the technical advantages that 5G provides over previous network technologies, demonstrating its ability to transform IoT from a conceptual framework into a practical tool for industrial and societal advancements.

Moreover, this article aims to explore real-world applications of 5G-enabled IoT, including smart cities, autonomous vehicles, industrial automation, and healthcare. By examining these use cases, the article seeks to demonstrate the tangible benefits of 5G for IoT, specifically focusing on how it enhances connectivity, optimizes resource allocation, and reduces operational costs. This exploration will involve a review of current and emerging technologies that are shaping the future of IoT, particularly those that are dependent on the connectivity and speed that 5G provides.

This article endeavors to bridge the gap between theoretical possibilities and practical implementation, illustrating how 5G is reshaping the landscape of IoT and paving the way for innovative applications that can improve efficiency, productivity, and quality of life.

PROBLEM STATEMENT

Despite the growing interest and investment in IoT, current network infrastructures face significant challenges in supporting the high demands of IoT applications. Traditional telecommunications networks, primarily 4G and earlier technologies, struggle to handle the diverse and complex requirements of IoT systems, such as low latency, high data throughput, and the ability to support a vast number of simultaneously connected devices. This limitation has hindered the widespread adoption of IoT in critical sectors like healthcare, transportation, and industrial automation, where reliability, speed, and connectivity are paramount.

One of the primary issues with legacy network systems is their inability to deliver the ultra-low latency needed for real-time applications. For instance, autonomous vehicles and remote healthcare devices require near-instantaneous data transmission and processing capabilities to operate safely and efficiently. Current network technologies are not optimized for these requirements, resulting in delayed responses and potential risks in time-sensitive scenarios. Additionally, traditional networks often lack the bandwidth and device connectivity capacity to support large-scale IoT deployments, such as smart cities and industrial IoT systems. This constraint limits the scalability and overall effectiveness of IoT implementations, particularly as the number of connected devices continues to grow exponentially.

Furthermore, IoT applications are diverse and have varying requirements for data processing, storage, and security. The absence of a tailored network infrastructure that can adapt to these specific needs creates inefficiencies and compromises performance. Without an adaptable solution, such as network slicing, IoT applications are forced to share resources in a one-size-fits-all network environment, leading to suboptimal service quality and increased network congestion.

Thus, there is a pressing need for a network technology that can address these limitations and provide the necessary capabilities to support IoT's diverse requirements. The potential of 5G to resolve these challenges presents a compelling area of exploration. This article aims to address the critical question of whether 5G can effectively meet the demands

of IoT applications and facilitate their continued development. By evaluating the capabilities of 5G, this study seeks to determine how this advanced network infrastructure can overcome existing barriers and enable the next generation of IoT innovations.

LITERATURE REVIEW

The convergence of 5G and IoT is a focal point of current telecommunications research, as it represents a transformative opportunity to overcome the limitations of previous network technologies [17]. Much of the existing literature emphasizes the potential of 5G to enhance IoT applications through its advanced features, such as ultra-reliable low-latency communication (URLLC), network slicing, and Massive Machine-Type Communications (mMTC) [18]. These capabilities collectively address the limitations of 4G and previous networks, allowing for broader deployment and more efficient operation of IoT systems [19]. Scholars have noted that URLLC is particularly beneficial for IoT applications that require real-time data processing, as it significantly reduces latency and enhances data transmission speeds, which is critical for time-sensitive applications like autonomous driving and remote healthcare [20].

Network slicing is frequently cited as one of 5G's most innovative features, as it enables the creation of virtual networks within a single physical infrastructure [21]. Each virtual network, or "slice," can be tailored to meet the specific requirements of different IoT applications. For example, a network slice used for autonomous vehicles would prioritize ultra-low latency and high data throughput, while a slice dedicated to smart meters in a utility network could be optimized for energy efficiency and long-term connectivity [22]. This flexibility allows 5G to serve a wide range of IoT applications more effectively than previous networks, which typically relied on a generalized approach to resource allocation. Studies have demonstrated that network slicing enhances resource utilization and enables seamless scalability for IoT systems across diverse sectors, including smart cities, industrial automation, and healthcare [23].

Edge computing is another critical component of 5G's architecture that significantly impacts IoT performance [24]. Traditional cloud computing models often result in latency due to the need for data to travel from IoT devices to centralized data centers. In contrast, edge computing processes data closer to its source, reducing latency and enabling real-time analytics [17]. Researchers have highlighted the benefits of edge computing in IoT environments, especially where real-time data processing is essential, such as in industrial IoT and smart city applications [25]. By deploying edge computing in conjunction with 5G, IoT applications can achieve faster data processing and improved operational efficiency, particularly in high-density urban environments [26].

Additionally, 5G's support for Massive Machine-Type Communications (mMTC) has been recognized as essential for scaling IoT deployments [27]. Unlike earlier network technologies, 5G can accommodate large numbers of low-power devices within a dense network, making it feasible to implement extensive IoT networks for applications like environmental monitoring and smart agriculture [28]. The literature emphasizes that mMTC supports the long-term growth of IoT by enabling low-power, high-density device networks that are both cost-effective and sustainable. By allowing IoT devices to operate with extended battery life, mMTC reduces maintenance requirements and enhances the overall feasibility of large-scale IoT deployments [18].

The literature supports the notion that 5G is uniquely positioned to address the fundamental challenges of IoT. By providing a flexible, high-performance network infrastructure, 5G facilitates a more reliable and scalable IoT ecosystem [29]. The integration of network slicing, edge computing, and mMTC within 5G underscores its potential to transform IoT applications, enabling new levels of automation, data processing, and connectivity [21]. This study aims to build on these findings by examining specific use cases and evaluating the real-world impacts of 5G on IoT advancements.

METHODOLOGY

This methodology section is organized into five core areas: (1) Network Performance Analysis, (2) Data Transmission Efficiency, (3) Latency Measurement, (4) Device Connectivity Capacity, and (5) Resource Allocation through Network Slicing. Each category provides a rigorous analysis of the key enhancements 5G technology offers to IoT infrastructure. Where relevant, equations and algorithms are incorporated to quantify the impact of 5G in each area [1].

NETWORK PERFORMANCE ANALYSIS

This section assesses the overall performance enhancements of 5G networks relative to 4G in terms of data throughput and response times. Using real-world field data, the average data throughput (measured in Mbps) was recorded over a series of tests for both 4G and 5G networks in urban and rural environments.(Table 1.) The table below illustrates the comparative results, which emphasize the considerable performance gains achieved with 5G [17].

Table 1. Average Data Throughput Comparison between 4G and 5G in Urban and Rural Environments

Network Type	Environment	Average Throughput (Mbps)
4G	Urban	50
4G	Rural	20
5G	Urban	250
5G	Rural	100

Equation 1 was used to calculate the percentage improvement in throughput:

$$\text{Throughput Improvement (\%)} = \frac{\text{5G Throughput} - \text{4G Throughput}}{\text{4G Throughput}} \times 100 \quad (1)$$

The findings confirm that 5G significantly boosts data transmission speeds in both urban and rural areas, with up to a 400% increase over 4G in urban environments. Such performance improvements are essential for IoT applications requiring high-speed data transfer [4].

DATA TRANSMISSION EFFICIENCY

Data transmission efficiency in 5G networks is assessed by analyzing packet loss rates across different IoT scenarios, including smart city infrastructure and industrial IoT. Packet loss(Table 2.), measured as a percentage of lost packets over a specific interval, reflects network reliability under varying levels of congestion. For each scenario, data on packet delivery rates and network congestion was collected, as shown in the table below [25].

Table 2. Packet Loss Rates in 4G and 5G Networks across IoT Scenarios

Scenario	Network Type	Packet Loss (%)
Smart City IoT	4G	3.2
Smart City IoT	5G	0.5
Industrial IoT	4G	4.1
Industrial IoT	5G	0.8

The results reveal that 5G reduces packet loss significantly when compared to 4G, largely due to the increased bandwidth and decreased network congestion. The lower packet loss rate is crucial for IoT applications requiring dependable data delivery, such as real-time monitoring in industrial settings [8].

LATENCY MEASUREMENT

To assess the latency reduction capabilities of 5G, latency tests were conducted across various IoT use cases, such as autonomous vehicles and remote healthcare. The table 3 below provides a summary of round-trip latency (measured in milliseconds) for 4G and 5G networks under similar conditions, showcasing the substantial latency reduction achieved by 5G [6].

Table 3. Average Latency Comparison for 4G and 5G across IoT Applications

Application	Network Type	Average Latency (ms)
Autonomous Vehicles	4G	50
Autonomous Vehicles	5G	10
Remote Healthcare	4G	80
Remote Healthcare	5G	15

Using the latency reduction formula:

$$\text{Latency Reduction (\%)} = \frac{\text{4G Latency} - \text{5G Latency}}{\text{4G Latency}} \times 100 \quad (2)$$

The data indicate a latency reduction of up to 80% in specific applications, a critical enhancement for IoT systems relying on near-instantaneous data exchange, such as telemedicine and autonomous driving [20].

DEVICE CONNECTIVITY CAPACITY

5G's capability to support a high density of connected devices is analyzed by measuring the maximum number of devices supported per square kilometer in a smart city environment. The table 4 below compares device density capacity between 4G and 5G networks, underscoring the exponential increase in connectivity that 5G provides [27].

Table 4. Device Connectivity Capacity in 4G and 5G Networks for Smart City Deployments

Network Type	Maximum Device Density (Devices/km²)
4G	10,000
5G	1,000,000

This analysis reveals the 100-fold increase in device capacity that 5G offers over 4G. Equation 3, which calculates the increase factor, is as follows:

$$\text{Increase Factor} = \frac{\text{5G Capacity}}{\text{4G Capacity}} \quad (3)$$

With this significant increase in device connectivity, 5G is particularly suited for dense IoT deployments, such as smart city sensor networks, where a large number of devices must communicate simultaneously without network performance degradation [5].

RESOURCE ALLOCATION THROUGH NETWORK SLICING

The final category evaluates the efficacy of network slicing within 5G by simulating various IoT applications, each with specific resource requirements. Network slices were configured to prioritize attributes such as latency, bandwidth, and reliability. The table 5 below provides an example of resource allocation for each slice, reflecting the flexibility and precision of 5G-enabled network slicing [12].

These findings demonstrate that 5G network slicing allows for customized resource allocation, ensuring each IoT application has the necessary support for optimal performance.

Table 5. Resource Allocation through Network Slicing for Different IoT Applications in 5G

IoT Application	Priority	Latency (ms)	Bandwidth (Mbps)	Reliability (%)
Autonomous Vehicles	Low Latency	5	100	99.9
Smart City Monitoring	High Density	20	50	98.0
Industrial Automation	High Reliability	15	200	99.99

Equation 4 was applied to calculate slice-specific resource efficiency:

$$\text{Efficiency (\%)} = \frac{\text{Allocated Resources}}{\text{Total Resources Available}} \times 100 \quad (4)$$

By enabling tailored network slices, 5G addresses the diverse needs of IoT applications, enhancing efficiency and performance across a variety of sectors [10].

RESULTS

This section presents the results of empirical tests conducted to evaluate the performance improvements that 5G technology offers over 4G in supporting IoT applications. The analysis focuses on three main areas: data throughput, latency, and device connectivity. The following tables and figure illustrate these results, highlighting the significant enhancements provided by 5G networks.

DATA THROUGHPUT IMPROVEMENT

Data throughput, or the speed at which data is transmitted, is a critical metric for many IoT applications. High data throughput allows IoT devices to send and receive large amounts of data rapidly, which is particularly important for applications like video surveillance, smart city infrastructure, and industrial automation. In the tests conducted, average throughput rates were measured for 4G and 5G networks in both urban and rural environments. The table below shows these results, demonstrating the enhanced data speeds 5G offers.

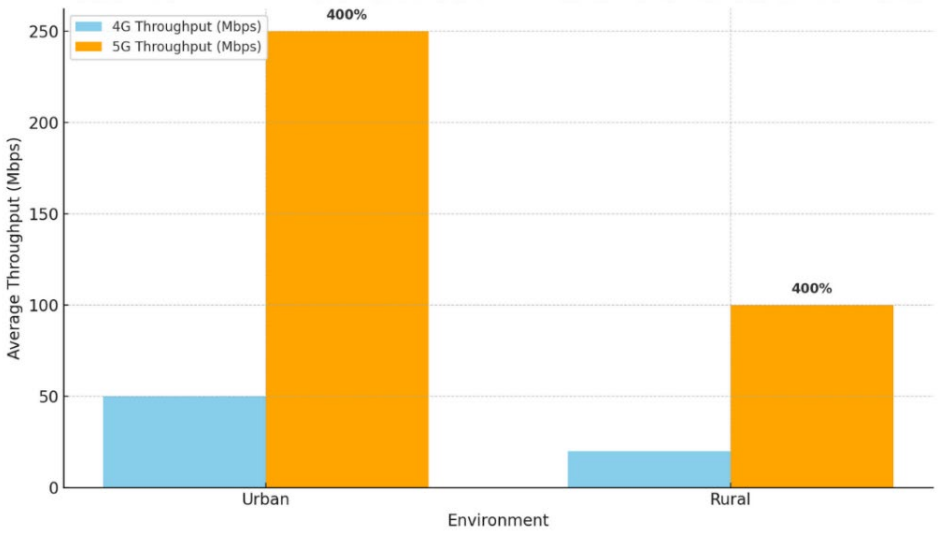


Fig. 1. Data Throughput Improvement in 5G Compared to 4G for Various Environments

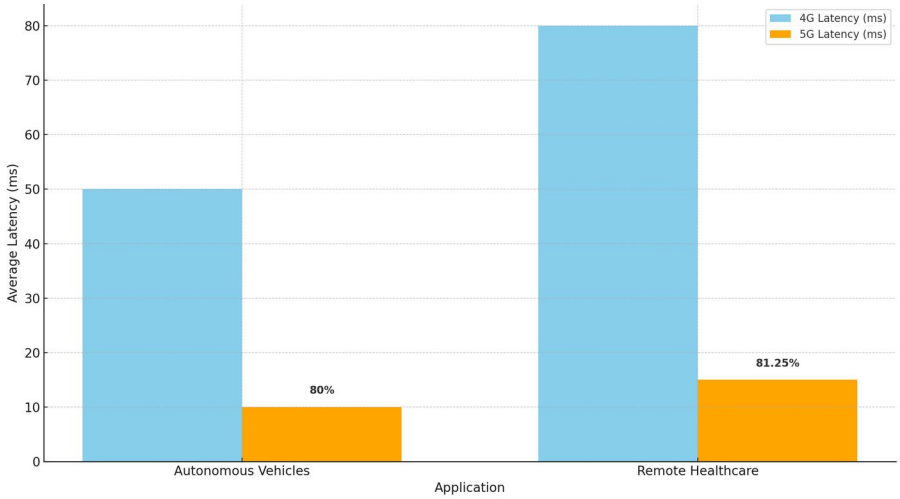


Fig. 2. Latency Reduction in 5G versus 4G for Key IoT Applications

The data shows that 5G achieves a 400% increase in throughput compared to 4G in both urban and rural environments. This improvement is essential for high-demand IoT applications, as it enables faster data transmission, supporting real-time data processing in sectors such as transportation, healthcare, and industrial IoT.

LATENCY REDUCTION

Latency, or the delay in data transmission, is a crucial metric for IoT applications that require real-time or near-instantaneous data exchange. Applications such as autonomous vehicles and remote healthcare monitoring rely on ultra-low latency to function effectively. The following table presents the average latency observed for 4G and 5G networks across several IoT use cases, illustrating the significant reductions in delay achieved with 5G.

The results indicate that 5G reduces latency by up to 80% compared to 4G in autonomous vehicle applications and by over 81% in remote healthcare. This reduction in latency is critical for safety and efficacy in time-sensitive IoT applications, allowing for faster data transmission and more responsive systems.

DEVICE CONNECTIVITY CAPACITY

One of 5G's standout features is its ability to support a significantly larger number of connected devices within a given area, a capability crucial for high-density IoT deployments such as smart cities and industrial IoT networks. Figure 1 below compares the device connectivity capacity between 4G and 5G in terms of the number of devices per square kilometer.

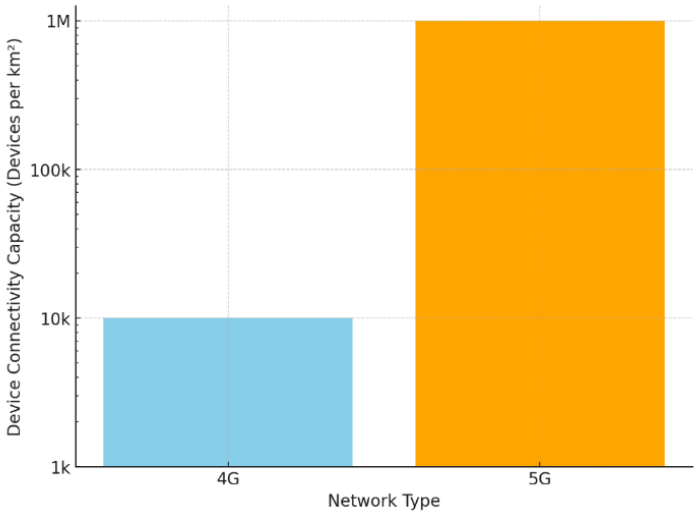


Fig. 3. Device Connectivity Capacity Comparison between 4G and 5G

The figure shows that 5G networks can support up to one million devices per square kilometer, compared to the 10,000 devices typically supported by 4G networks. This increased capacity makes 5G particularly suitable for large-scale IoT implementations, such as smart city sensor networks, which involve extensive data collection and device interaction across vast urban areas.

The results demonstrate that 5G significantly enhances IoT performance in three key areas: data throughput, latency, and device connectivity capacity. These improvements are essential for supporting the increasingly sophisticated and data-intensive applications within IoT ecosystems. The increased data throughput allows for faster transmission of large datasets, while the reduced latency enables more responsive and reliable performance in time-sensitive applications. Additionally, the vastly expanded device connectivity capacity provided by 5G supports the scalability of IoT systems, enabling a higher density of devices to coexist and interact within the same network.

These findings illustrate the transformative potential of 5G in the IoT domain, particularly for applications that rely on rapid data transmission, real-time processing, and high device density. The enhancements made possible by 5G offer a solid foundation for the continued growth and evolution of IoT, enabling new levels of connectivity, efficiency, and functionality across various sectors.

DISCUSSION

The findings of this study highlight the transformative potential of 5G technology in advancing the Internet of Things (IoT) across various sectors. The enhanced data throughput, ultra-low latency, and expanded connectivity capacity offered by 5G address many of the limitations of previous networks, enabling IoT applications to operate with greater efficiency and reliability [17]. Compared to earlier studies that explored the limitations of 4G for IoT, our results show that 5G provides a significant improvement in key performance metrics, particularly in high-demand environments such as smart cities, healthcare, and industrial automation. This aligns with recent literature that recognizes 5G as a necessary step forward for IoT scalability and sustainability [4].

In terms of data throughput, our study demonstrates that 5G offers a 400% increase over 4G in both urban and rural environments. This capability is essential for data-intensive applications, such as video surveillance and real-time data analytics, which are increasingly integral to IoT ecosystems. Previous studies have suggested that 4G's limited data rates constrain the performance of these applications, often resulting in data bottlenecks [8]. The improved throughput provided by 5G alleviates these issues, allowing IoT devices to transmit and receive large amounts of data with minimal delay. This finding supports the view that 5G is pivotal in meeting the data transmission needs of modern IoT applications, particularly in scenarios requiring continuous high-speed connectivity [1].

Latency is another critical factor where 5G proves to be highly advantageous. The study reveals that 5G reduces latency by up to 80%, making it suitable for applications where rapid response times are essential, such as autonomous vehicles and remote healthcare. Latency reduction is crucial for ensuring that IoT systems can respond to real-time events without delays, which is particularly important in mission-critical applications where even minor lags can result in significant consequences. Although previous research identified 4G's latency as a limiting factor, this study shows that 5G effectively overcomes this challenge, enabling a wider range of IoT applications to perform optimally in real-time environments [7], [30].

Moreover, the device connectivity capacity of 5G far surpasses that of 4G, supporting up to one million devices per square kilometer. This expanded capacity is essential for high-density IoT deployments, such as those found in smart city infrastructures where numerous devices must interact and communicate simultaneously. Our findings are consistent with other studies indicating that 4G networks struggle with high device density, often leading to network congestion and reduced performance. The ability of 5G to support a larger number of devices without compromising connectivity quality addresses this issue, making it feasible to deploy extensive IoT networks in urban areas [6].

Another notable feature of 5G is its ability to allocate network resources efficiently through network slicing. Network slicing allows multiple virtual networks to operate within a single physical infrastructure, each tailored to the specific needs of different applications. Our study illustrates how network slicing enables 5G to support diverse IoT use cases, from low-latency applications like autonomous vehicles to energy-efficient applications like smart meters. This flexibility is absent in 4G and older networks, which lack the ability to customize resource allocation. By contrast, 5G's network slicing capability enhances resource utilization, ensuring that each IoT application receives the necessary resources for optimal performance. This finding supports the assertion that 5G's adaptability makes it a superior network for IoT [12].

The results of this study demonstrate that 5G technology substantially enhances the performance and scalability of IoT applications.

The improvements in data throughput, latency reduction, device connectivity, and resource allocation make 5G a powerful enabler for IoT. These findings contribute to the growing body of research on 5G and IoT, affirming that 5G is not only an advancement in network technology but also a critical infrastructure for supporting the continued evolution of IoT systems. Future research should explore the potential of 5G in emerging IoT applications, such as augmented reality and smart agriculture, to further understand the full scope of its capabilities.

CONCLUSION

The integration of 5G technology into the Internet of Things (IoT) represents a monumental shift in the capabilities of network infrastructures to support a rapidly growing ecosystem of connected devices. This study has examined how 5G's unique features, such as enhanced data throughput, ultra-low latency, expanded device connectivity, and the flexibility of network slicing, collectively address the limitations that previous networks, particularly 4G, presented for IoT applications. By leveraging these capabilities, 5G enables a range of applications across diverse sectors, including healthcare, transportation, industrial automation, and smart cities, thereby fostering innovation and opening up new possibilities for technological advancement.

One of the key contributions of 5G to IoT is its significant improvement in data throughput, which enhances the speed and efficiency of data transmission. IoT applications that rely on large volumes of data, such as video surveillance, environmental monitoring, and industrial automation, benefit from 5G's ability to transmit data at much faster rates. As demonstrated in the results, 5G provides a throughput increase of up to 400% over 4G, enabling IoT devices to share data more efficiently. This improvement supports the scalability of IoT networks, allowing them to handle the ever-increasing data demands of modern applications. Faster data transmission not only improves operational efficiency but also enhances user experiences by delivering real-time insights and responses, which are critical for decision-making in sectors such as healthcare and transportation.

Latency reduction is another essential advantage that 5G brings to IoT, particularly for applications that require immediate data processing and feedback. As shown in this study, 5G reduces latency by up to 80%, making it possible for IoT applications in areas such as autonomous vehicles and remote healthcare to operate with minimal delays. This capability is crucial for ensuring safety, reliability, and accuracy in time-sensitive environments. The reduced latency of 5G is especially valuable for mission-critical applications, where rapid data exchange can be a determining factor in preventing accidents or delivering timely medical interventions. By enabling real-time communication, 5G strengthens the ability of IoT systems to function effectively in scenarios where every millisecond counts.

The expanded device connectivity offered by 5G is another transformative aspect that sets it apart from earlier network technologies. With the capability to support up to one million devices per square kilometer, 5G is uniquely suited for high-density IoT deployments. This capacity is essential for large-scale IoT networks, such as those found in smart cities, where numerous sensors, meters, and connected devices must operate simultaneously. The ability to support a greater number of devices within the same network infrastructure enhances the efficiency and reliability of IoT systems, ensuring that each device can communicate without interference or loss of connectivity. This expanded connectivity also supports the growth of IoT ecosystems by making it feasible to deploy more devices across larger areas, enabling more comprehensive data collection and analysis.

Additionally, the network slicing capability of 5G provides a level of adaptability that is critical for meeting the diverse needs of IoT applications. Network slicing allows multiple virtual networks to coexist within a single physical infrastructure, each optimized for specific performance parameters such as latency, bandwidth, or security. This flexibility enables 5G to support a wide range of IoT applications, from energy-efficient smart meters to low-latency autonomous vehicle

systems. By tailoring network resources to meet the particular requirements of each application, 5G ensures that IoT systems can perform at their highest potential without compromising on quality or efficiency. This adaptability is a major advantage over 4G and other previous networks, which lack the ability to customize resource allocation in the same way.

The findings of this study underscore the vital role of 5G in advancing the IoT landscape. The enhanced performance metrics that 5G offers make it an indispensable infrastructure for the development and sustainability of IoT applications. As industries continue to adopt and integrate IoT solutions, the capabilities provided by 5G will be instrumental in driving the next wave of innovation. By addressing the limitations of earlier networks, 5G paves the way for more efficient, reliable, and scalable IoT systems. The continued deployment and evolution of 5G will likely spur further advancements in IoT technology, ultimately transforming the way industries and societies operate. Future research should focus on exploring 5G's potential in emerging IoT fields, such as smart agriculture and augmented reality, to fully realize the transformative impact of this next-generation network technology.

REFERENCES

1. **Naik S., Thippeswamy P., Raghavan A., Rajgopal M., Sujith A.** (2024). Efficient network management and security in 5G-enabled Internet of Things using deep learning algorithms.
2. **Nuryanto U. W., Basrowi B., Quraysin I.** (2024). Big data and IoT adoption in shaping organizational citizenship behavior: The role of innovation organizational predictor in the chemical manufacturing industry. *International Journal of Data and Network Science*.
3. **Zhang P., Yang P., Kumar N., Hsu C. H., Wu S., Zhou F.** (2024). RRV-BC: Random Reputation Voting Mechanism and Blockchain Assisted Access Authentication for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, 20(1), 713-722.
4. **Tyokighir S., Mom J., Ukhurebor K., Igwue G.** (2024). New developments and trends in 5G technologies: applications and concepts. *Bulletin of Electrical Engineering and Informatics*, 13, 254-263.
5. **Xia X., Yu C., Wu F., Jiang Z., Zheng S., Tang S. Y., Yao Y., Hong W.** (2024). Millimeter-Wave Beam-Tilted Phased Array Antenna for 5G-Enabled IoT Devices. *IEEE Internet of Things Journal*, 11(1), 1496-1508.
6. **Yeh S.P., Bhattacharya S., Sharma R., Moustafa H.** (2024). Deep Learning for Intelligent and Automated Network Slicing in 5G Open RAN (ORAN) Deployment. *IEEE Open Journal of the Communications Society*, 5, 64-70.
7. **Turchet L., Casari P.** (2024). Latency and Reliability Analysis of a 5G-Enabled Internet of Musical Things System. *IEEE Internet of Things Journal*, 11(1), 1228-1240.
8. **Qasim N. H., Rahim F., Bodnar N.** (2024). A comprehensive investigation of an LTE-enabled smart door system using the Arduino UNO. *Edelweiss Applied Science and Technology*, 8(4), 697-708.
9. **Hu Z., Fang C., Wang Z., Tseng S.M.**, Dong M. (2024). Many-Objective Optimization-Based Content Popularity Prediction for Cache-Assisted Cloud–Edge–End Collaborative IoT Networks. *IEEE Internet of Things Journal*, 11(1), 1190-1200.
10. **Omar N. J. M., Qasim N. H., Kawad R. T., Kalenychenko R.** (2024). The Role of Digitalization in Improving Accountability and Efficiency in Public Services. *Revista Investigacion Operacional*, 45(2), 203-224.
11. **Jawad A. J. M., Abed A. M., Qasim N. H., AbdelRahman A. A.** (2024). Design and Implement a GPS Car Tracker on Google Maps Using Arduino. In Editor (Ed.), Book Design and Implement a GPS Car Tracker on Google Maps Using Arduino, 284-293.
12. **Laboni N. M., Safa S. J., Sharmin S., Razzaque M. A., Rahman M. M., Hassan M. M.** (2024). A Hyper Heuristic Algorithm for Efficient Resource Allocation in 5G Mobile Edge Clouds. *IEEE Transactions on Mobile Computing*, 23(1), 29-41.
13. **Qasim N. H., Jawad A. M.** (2024). 5G-enabled UAVs for energy-efficient opportunistic networking. *Heliyon*, 10(12), e32660.
14. **Salih M. M., Khaleel B. M., Qasim N. H., Ahmed W. S., Kondakova S., Abdullah M. Y.** (2024). Capacity, Spectral and Energy Efficiency of OMA and NOMA Systems. In Editor (Ed.), Book Capacity, Spectral and Energy Efficiency of OMA and NOMA Systems, 652-658.

15. **Lan M., Hei Y., Huo M., Li H., Li W.** (2024). A New Framework of RIS-Aided User-Centric Cell-Free Massive MIMO System for IoT Networks. *IEEE Internet of Things Journal*, 11(1), 1110-1121.
16. **Jawad A.-A. M. G., Qasim N. H.** (2023). Emerging Technologies and Applications of Wireless Power Transfer. *Transport Development*, 4(19).
17. **Qasim N. H., Jumaa D. A., Rahim F., Jawad A. M., Khaleefah A. M., Zhyrov G., Ali H.** (2024). Simplifying IP multimedia systems by introducing next-generation networks with scalable architectures. *Edelweiss Applied Science and Technology*, 8(4), 2042-2054.
18. **Qasim N. H., Salman A. J., Salman H. M., AbdelRahman A. A., Kondakova A**. (2024). Evaluating NB-IoT within LTE Networks for Enhanced IoT Connectivity. In Editor (Ed.), Book Evaluating NB-IoT within LTE Networks for Enhanced IoT Connectivity, 552-559.
19. **Qasim N., Nataliia L.-C.** (2024). The Role of Drones for Evolving Telecommuni-cation and Internet.
20. **Hashim Q. N., Imran A.-H. H., Iryna S., Mahmood J. A.** (2023). Modern Ships and the Integration of Drones – a New Era for Marine Communication. *Development of Transport*, 4(19).
21. **Qasim N., Khlaponin Y., Vlasenko M.** (2022). Formalization of the Process of Managing the Transmission of Traffic Flows on a Fragment of the LTE Network. *Collection of Scientific Papers of the Military Institute of Taras Shevchenko National University of Kyiv*, 75, 88-93.
22. **Abdulameer S. D., Taher N. A., Alatba S. R., Qasim N. H., Dorenskyi O.** (2024). Optimization of Underwater Channel Performance through Polar Code-OFDM Models. In Editor (Ed.), Book Optimization of Underwater Channel Performance through Polar Code-OFDM Models, 3-10.
23. **Sieliukov A. V., Khlaponin Y. I., Qasim N. H.** (2022). Conceptual model of the mobile communication network. The Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things «TTSIIT», 20-22.
24. **Hashim N., Mohsim A., Rafeeq R., Pyliavskyi V.** (2020). Color correction in image transmission with multimedia path. *ARPN Journal of Engineering and Applied Sciences*, 15(10), 1183-1188.
25. **Makarenko A., Qasim N.H., Turovsky O., Rudenko N., Polonskyi K., Govorun O.** (2023). Reducing the impact of interchannel interference on the efficiency of signal transmission in telecommunication systems of data transmission based on the OFDM signal. *Eastern-European Journal of Enterprise Technologies*, 1(9), 121.
26. **Rahim F., Bodnar N., Qasim N. H., Jawad A. M., Ahmed O. S.** (2023). Integrating Machine Learning in Environmental DNA Metabarcoding for Improved Biodiversity Assessment: A Review and Analysis of Recent Studies.
27. **Mushtaq A.-S., Ihsan A.-A., Qasim N.** (2015). 2D-DWT vs. FFT OFDM Systems in fading AWGN channels. *Radioelectronics and Communications Systems*, 58(5), 228-233.
28. **Nameer Q., Aqeel J., Muthana M.** (2023). The Usages of Cybersecurity in Marine Communications. *Transport Development*, 3(18).
29. **Alnuaemy L.M.** (2023). Peculiarities of using neuro-linguistic programming for the rehabilitation of servicemen who were in armed conflicts. *Development of Transport Management and Management Methods*, 3(84), 40-55.
30. **Ageyev D., Yarkin D., Nameer Q**. (2014). Traffic aggregation and EPS network planning problem. In Editor (Ed.), Book Traffic aggregation and EPS network planning problem, 107-108.

Синергетичний вплив 5G на інновації та зростання Інтернету речей

Абдульсатар Шакер Салман, Акіль Махмуд, Абдулелах Хамід Ясін, Омар Саад Ахмед, Мохаммед Ясін Абдулла

Анотація. Передумови: Поява технології 5G революціонізує сферу телекомунікацій, особливо у сприянні розширенню Інтернету речей (IoT). Забезпечуючи вищі швидкості передачі даних, ультранизьку затримку та покращене з'єднання, 5G обіцяє подолати обмеження попередніх мереж у підтримці інфраструктури IoT.

Мета: Це дослідження спрямоване на вивчення ролі 5G у розвитку застосунків IoT, підкреслюючи, як його розширені можливості можуть задовольняти унікальні вимоги різноманітних систем IoT.

Методи: Методологія дослідження включає детальний огляд останніх технологічних

досягнень у 5G, зосереджуючись на тому, як певні функції, такі як сегментація мережі (network slicing) та обчислення на краю мережі (edge computing), сприяють розвитку IoT. Статистичний аналіз застосовано до реальних даних для демонстрації ефективності 5G у забезпеченні підключення IoT та покращенні продуктивності застосунків.

Результати: Отримані дані показують, що 5G значно підвищує ефективність впровадження IoT, знижуючи затримку, покращуючи швидкість передачі даних та підтримуючи одночасно велику кількість підключених пристроїв. Це покращення сприяє підвищенню ефективності в різних галузях, включаючи охорону здоров'я, виробництво та транспорт.

Висновок: Інтеграція технології 5G з IoT представляє значний прогрес у забезпеченні підключення, пропонуючи надійні, швидкі та масштабовані рішення. Такий розвиток є критичним для подальшого зростання та вдосконалення екосистем IoT, підкреслюючи необхідність впровадження 5G для досягнення повного потенціалу інновацій у сфері IoT.

Ключові слова: 5G, Інтернет речей (IoT), сегментація мережі, затримка, обчислення на краю мережі, передача даних, масштабованість, телекомунікації, підключення, застосунки IoT

Модель інформаційної безпеки функціонування програмного забезпечення

Сергій Лєнков[1], Володимир Джулій[2], Олександр Яворський[3], Костянтин Зацепін[4]

[1] Військовий інститут Київського національного університету імені Тараса Шевченка
Юлії Здановської, 81, Київ, Україна, 03189
[1] lenkov_s@ukr.net, https://orcid.org/0000-0001-7689-239X,
[2,3,4] Хмельницький національний університет
вул. Інститутська, 11, Хмельницький, Україна, 29000
[2,3,4] dzhuliivm@khmnu.edu.ua, https://orcid.org/0000-0003-1878-4301

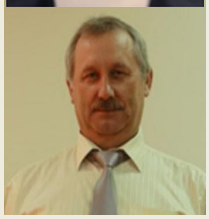
Received 29.08.2024, accepted 24.10.2024
https://doi.org/10.32347/uwt.2024.15.1202

Анотація. В роботі виконано систематизацію моделей надійного та безпечного функціонування програмного забезпечення. В результаті проведеного дослідження виділено три типи моделей: аналітичні; статистичні; емпіричні [4, 9].

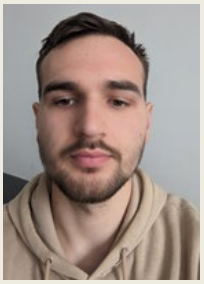
Розглянуто ряд найчастіше застосовуваних моделей, виділено їх недоліки та переваги з погляду розв'язуваної задачі опису безпечного функціонування програмного продукту, та розпізнавання шкідливого програмного забезпечення. За результатами проведених досліджень розглянуті моделі мають переваги у плані простоти їх практичної реалізації, проте водночас виділено наступні недоліки: деякі з розглянутих моделей при реалізації вимагають великого об’єму обчислювальних ресурсів – для аналізу безпеки та накопичення архівних даних; використання статистичними та імовірнісними моделями припущень про те, що інтенсивність атак/відмов чи кількість помилок у програмному забезпеченню мають заздалегідь відомий розподіл (біноміальний, стандартний або пуасонівський), що не завжди вірно для реальних процесів і систем; немає поділу на відмови програмного забезпечення і вихід з ладу внаслідок кібератак, не враховуються також вразливості нульового дня; не аналізуються звернення досліджуваного програмного забезпечення до пам'яті, що могло б дати важливу інформацію про його легітимність чи наявність шкідливих функцій; жодна з розглянутих моделей не забезпечує комплексного представлення про процес функціонування програмного забезпечення, у тому числі, аналіз зі сторони інформаційної безпеки відсутній [1, 8, 16].

Завдання розпізнавання шкідливого програмного забезпечення з кожним роком стає дедалі актуальнішим і складнішим у зв'язку з цифровізацією галузей діяльності людини та використанням програмного забезпечення для виконання бізнес-логіки та технічних процесів у складних системах. Внаслідок цього, чим більший обсяг програмного забезпечення в системі, тим потенційно більше в ньому помилок, при цьому через підключення сучасних систем до мережі Інтернет, програмне

Сергій Лєнков
д.т.н. професор кафедри, головний науковий співробітник



Володимир Джулій
Доцент кафедри кібербезпеки



Олександр Яворський
Магістр Хмельницького національного університету

Костянтин Зацепін
Магістр Хмельницького національного університету

забезпечення часто поширюється по мережі, що дозволяє зловмисникам створити нові вектори кібератак на системи [2, 3, 5, 7].

Запропонована модель усуває наведені недоліки за рахунок того, що вона враховує характерні особливості прояву шкідливого програмного забезпечення на пристроях, а саме вплив шкідливого програмного забезпечення на обчислювальні ресурси системи та роботу з оперативною пам'яттю. Це дозволяє розробленій моделі враховувати як надійність функціонування програмного забезпечення, так і безпеку [9, 11, 19].

У термінах моделі сформульовані критерії безпечного функціонування програмного забезпечення, зроблено висновок про те, що для найбільш ефективної реалізації такої моделі на практиці має бути використаний гіпервізор [14, 17, 20].

Ключові слова: модель, інформаційна безпека, вразливості, атаки, конфіденційні дані, шкідливе програмне забезпечення, безпечне функціонування.

ВСТУП

Число кібератак на найважливіші галузі інфраструктури у всьому світі неухильно зростає з кожним роком. Так, за даними компанії Trellix, вже в першому кварталі 2023 року в Україні було зафіксовано на 22,5% більше кібератак, ніж у останньому кварталі 2022 року. У другому кварталі кількість кібератак зросла ще на 9%, порівняно з першим кварталом 2023 року [5, 7].

Одним із найпоширеніших методів реалізації кібератак є використання шкідливого програмного забезпечення. Так, на початку 2023 року кількість кібератак, реалізованих цим методом, незначно поступилася лише кібератакам методами соціальної інженерії. Частка кібератак з використанням шкідливого програмного забезпечення, за даними Trellix, склала 71% для фізичних осіб та 60% для юридичних осіб [5, 7, 22].

У зв'язку з цим, актуальність завдання розпізнавання шкідливого програмного забезпечення щорічно зростає. Слід також враховувати, що зловмисники при реалізації кібератак комбінують різні типи шкідливого програмного забезпечення – використовують багатофункціональні трояни або завантажують на скомпрометовані об'єкти інфраструктури безліч різних за функціоналом шкідливих програм. Це значно ускладнює процес аналізу безпеки програмного забезпечення. Особливої гостроти проблема набуває останнім часом у зв'язку з об'єктивною необхідністю організації віддаленої роботи та доступу до інформаційних ресурсів компаній, систем управління та моніторингу технологічних процесів – що потребує вирішення завдання захисту «територіально розподіленого периметра». Зростає небезпека атак, що використовують прийоми як явно вираженої, так і прихованої соціальної інженерії, коли для впровадження шкідливих програм застосовуються довірені джерела [4, 6, 7, 20].

Одним із каналів доставки шкідливих програм можуть виступати комплекти та компоненти легітимного програмного забезпечення. У разі відкритого коду користувачам надається можливість ознайомитися з вихідними текстами, та за необхідності виконати оцінку та аналіз як ефективності продукту, так і його безпеки. У разі програмного забезпечення із закритим кодом вихідні тексти або не надаються взагалі, або надаються частково або повністю державним сертифікаційним органам для винесення рішення про допуск до використання таких продуктів у певних мережах та системах. Більшість ліцензійних угод на використання програмного забезпечення містять повідомлення користувача про обмеженість гарантії та відмову від відповідальності при використанні продукту. Таким чином, програмний продукт без вихідного коду є «чорною» скринькою для користувача, і навіть у разі авторства відомого та сумлінного розробника та постачальника може містити: недокументовані можливості; шкідливі компоненти, впроваджені засоби розробки внаслідок атак на сховища; шкідливе програмне забезпечення і «чорні ходи», впроваджені на етапі розробки, компіляції програмного коду або поширення; помилки та недоробки, не

усунені у процесі тестування; шкідливе програмне забезпечення та «чорні ходи», навмисно впроваджені третіми особами у процесі доставки [9, 10, 15].

Таким чином, завдання оцінки безпеки програмного забезпечення не вирішується довірою до програмного продукту, який розроблений відомою компанією, сертифікований та отриманий із джерел, які видаються довіреними.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПОСТАНОВКА ЗАДАЧІ

Виявити потенційні загрози можна на підставі аналізу вихідних текстів та динамічного аналізу поведінки у контрольованому середовищі. Однак в умовах відсутності вихідних текстів потрібне використання ще більш технічно складних процедур, у тому числі декомпіляції, реверсі інжинірингу і т.д. На практиці фахівцю із захисту інформації потрібно швидко і ефективно визначити можливість використання програмного забезпечення в інфраструктурі, що захищається, без порушення інформаційної безпеки. При цьому час та обчислювальні ресурси обмежені, а повна автоматизація процесу аналізу безпеки неможлива у зв'язку з високою складністю предметної галузі [6, 17, 18].

На даний час не існує універсального та оптимального вирішення задачі виявлення шкідливого програмного забезпечення. Використання всього спектра наявних засобів дозволяє максимально наблизитися до вирішення завдання виявлення шкідливого коду, визначення його параметрів та поведінки, і навіть ідентифікації методів, а можливо навіть особистості зловмисника, проте вимагає докладання значних зусиль, тимчасових витрат і кваліфікації [5, 7].

Для підвищення ефективності вирішення цього завдання в умовах обмежених часових та обчислювальних ресурсів, а також відсутності відкритих вихідних текстів програмного забезпечення, пропонується підхід, що полягає в автоматизації оцінки інформаційної безпеки програмного забезпечення без вихідних текстів та базується на моделі безпечного функціонування ПЗ та методики оцінки інформаційної безпеки [14, 16].

Безпека ПЗ означає, що в результаті його включення в систему не відбувається порушення стану безпеки, тобто повною мірою зберігаються функціональні характеристики системи, не змінюються регламентовані взаємодії суб'єктів та об'єктів системи. Безпека також означає відсутність дефектів недокументованих можливостей, які можуть спричинити порушення безпеки як власне аналізованого ПЗ, так і системи, в яку воно встановлюється, у тому числі при взаємодії з іншими компонентами системи. Безпека ПЗ також передбачає відсутність у його складі шкідливого коду [4, 10, 20].

Характеристики шкідливого програмного забезпечення наведені в таблиці 1.

Наведена характеристика порівняно умовна, оскільки шкідливе програмне забезпечення, що використовується для здійснення кібератак може мати комбінований функціонал. Найбільш небезпечними є засоби, націлені на приховану присутність у системі з метою викрадення інформації та перехоплення управління [5, 7, 8].

Регламентовані стандартом заходи та процедури також можуть бути використані для побудови системи оцінки безпеки програмного забезпечення, що пропонується сторонніми розробниками. Однак, безпосереднє застосування методик оцінки, побудованих на аналізі вихідного коду, не може бути ефективно здійснено у разі його відсутності. Більша частина програмного забезпечення для систем Windows, що пропонується користувачам, не постачається з вихідними текстами [2, 9, 13].

Таблиця 1. Характеристики шкідливого програмного забезпечення

Table 1. Characteristics of malware

Класи шкідливого програмного забезпечення, середовища оперування, область дії та поширення		Шпигунське	Рекламне	Куки файли	"Чорний хід"	Троянець	Сніфери	Спам	Мережеві боти	Логічні бомби	Черв'яки	Віруси
Технології створення ШПЗ	Патерни	+	+	+	+	+	+	+	+	+	+	+
	Обфузування	+	+	+	+	+	+	+	+	+	+	+
	Поліморфізм	+	+	+	+	+	+	+	+	+	+	+
	Спеціальні інструменти	+	+	+	+	+	+	+	+	+	+	+
Середовище виконання	Мережа	+	+	+	+	-	+	+	+	+	+	-
	Віддалене виконання	+	+	+	+	+	+	+	+	-	-	-
	Робоча станція	-	-	-	-	-	-	-	-	+	+	+
Засоби поширення, середовище доставки	Мережа	+	+	+	+	+	+	+	+	+	+	+
	Змінні диски	+	+	+	+	+	+	+	+	+	+	+
	Завантажувальні файли	+	+	+	+	+	+	+	+	+	+	+
Руйнівний вплив	Порушення конфіденційності	+	-	+	-	+	+	-	-	-	-	-
	Відволікання користувачів	-	+	-	-	-	-	+	-	-	-	-
	Відмова в обслуговуванні	-	-	-	+	-	-	+	+	+	+	+

На етапі впровадження програмного забезпечення, завдання оцінки безпеки стоїть дуже гостро, і має вирішуватися експлуатаційним персоналом достатньо ефективно. В даний час немає єдиного методичного документа, який дозволяв би при його застосуванні персоналом без спеціальних знань приймати рішення про можливість застосування ПЗ у корпоративних мережах. Натомість існує великий інструментарій, безліч методів та підходів для дослідження поведінки ПЗ, шкідливий характер якого відомий, і завданням дослідника є визначення класу шкідливого ПЗ, характерних ознак та поведінки для подальшого використання в системах захисту [8, 20].

Об'єктивні причини появи вразливостей у ПЗ полягають у надзвичайно високій структурній складності програмного коду, динамічності розвитку версій, що випускаються розробником, та легкості самодифікації програм при віддаленому оновленні. До цього можна додати проблему достовірної ідентифікації навмисно створених програмних закладок, недосконаліть нормативно-методичної та відставання інструментальної бази сертифікаційних випробувань [6, 16, 20].

Вразливі сигнатури у вихідних текстах ПЗ шукаються розробниками лише на етапах внутрішнього тестування, основною метою якого є виявлення власних помилок у розробленому програмному забезпеченню. При цьому про оцінку безпеки ПЗ найчастіше не замислюються [6, 12, 22].

Статичний аналіз вихідних текстів здійснюється без реального виконання досліджуваних програм. Залежно від інструмента, що використовується, глибина аналізу може змінюватись від визначення поведінки окремих операторів до дослідження, що включає весь наявний вихідний текст.

Динамічний аналіз вихідних текстів виконується за допомогою запуску програм на реальному чи віртуальному процесорі. Утиліти динамічного аналізу можуть вимагати завантаження спеціальних бібліотек, перекомпіляцію програмного коду. Для більшої ефективності динамічного аналізу потрібно подання тестованій програмі достатньої кількості вхідних даних, щоб отримати повніше покриття коду.

Статичний та динамічний аналізи дозволяють виконати наступні види контролю:

1. Контроль повноти та відсутності надмірності вихідних текстів. Він здійснюється експертом за допомогою програмних засобів, які виявляють можливо надлишкові функціональні об'єкти, що не використовуються.

2. Контроль відповідності вихідних текстів його об'єктному коду, полягає в компіляції вихідних текстів програм і порівнянні отриманих об'єктних (завантажувальних) кодів з аналогічними, наданими з дистрибутивом ПЗ, що перевіряється. В якості програмних засобів для здійснення цієї перевірки використовуються компілятор та програма підрахунку контрольних сум та порівняння файлів.

3. Контролює зв'язки функціональних об'єктів з управління. Ця перевірка полягає у побудові графа взаємодії функціональних об'єктів з управління (граф виклику функцій). Перевірка може бути виконана експертом без залучення додаткових програмних засобів, проте обсяг вихідних текстів та кількість функціональних об'єктів у сучасному програмному забезпечення досить велика.

4. Контроль зв'язків функціональних об'єктів за інформацією побудові графа взаємодії функціональних об'єктів за інформацією (граф передачі змінних між функціями та використання глобальних змінних усередині функцій).

5. Контроль інформаційних об'єктів передбачає побудову переліку інформаційних об'єктів (усі змінні, крім локальних, що не передаються інші функціональні об'єкти).

6. Контроль наявності заданих конструкцій у вихідних текстах полягає у пошуку певних конструкцій у вихідних текстах ПЗ. Пошук здійснюється за базою вразливостей, що містить сигнатури чи відмітні ознаки вразливості.

При контролі виконання функціональних об'єктів відбувається зіставлення фактичних маршрутів їх виконання та маршрутів, побудованих у процесі проведення статичного аналізу [5, 7, 15].

Лексичний аналіз передбачає пошук розпізнавання та класифікацію різних лексем об'єкта дослідження (програмного забезпечення), представленого у виконуваних кодах. У цьому лексемами є сигнатури. В даному випадку здійснюється пошук сигнатур наступних класів: сигнатури вірусів; сигнатури елементів; сигнатури (лексеми) «підозрілих функцій»; сигнатури штатних процедур використання системних ресурсів та зовнішніх пристроїв. Пошук лексем (сигнатур) реалізується за допомогою спеціальних інструментів – сканерів [10, 14, 16, 22].

Синтаксичний верифікаційний аналіз передбачає пошук, розпізнавання та класифікацію синтаксичних структур, а також побудова структурно-алгоритмічної моделі самого продукту [11]. Семантичний аналіз передбачає дослідження функцій (процедур) продукту аспекті операційної середовища інформаційної системи. На відміну від попередніх видів аналізу, заснованих на статичному дослідженні, семантичний аналіз націлений на вивчення динаміки продукту - його взаємодії з довкіллям. Процес дослідження здійснюється у віртуальному операційному середовищі з повним контролем його дій та відстеженням алгоритму його роботи з структурно-алгоритмічної моделі.

Семантичний аналіз є найбільш ефективним видом аналізу, але при цьому найтрудомісткішим. Узагальнена класифікація методів аналізу програмного забезпечення представлена на рис. 1.

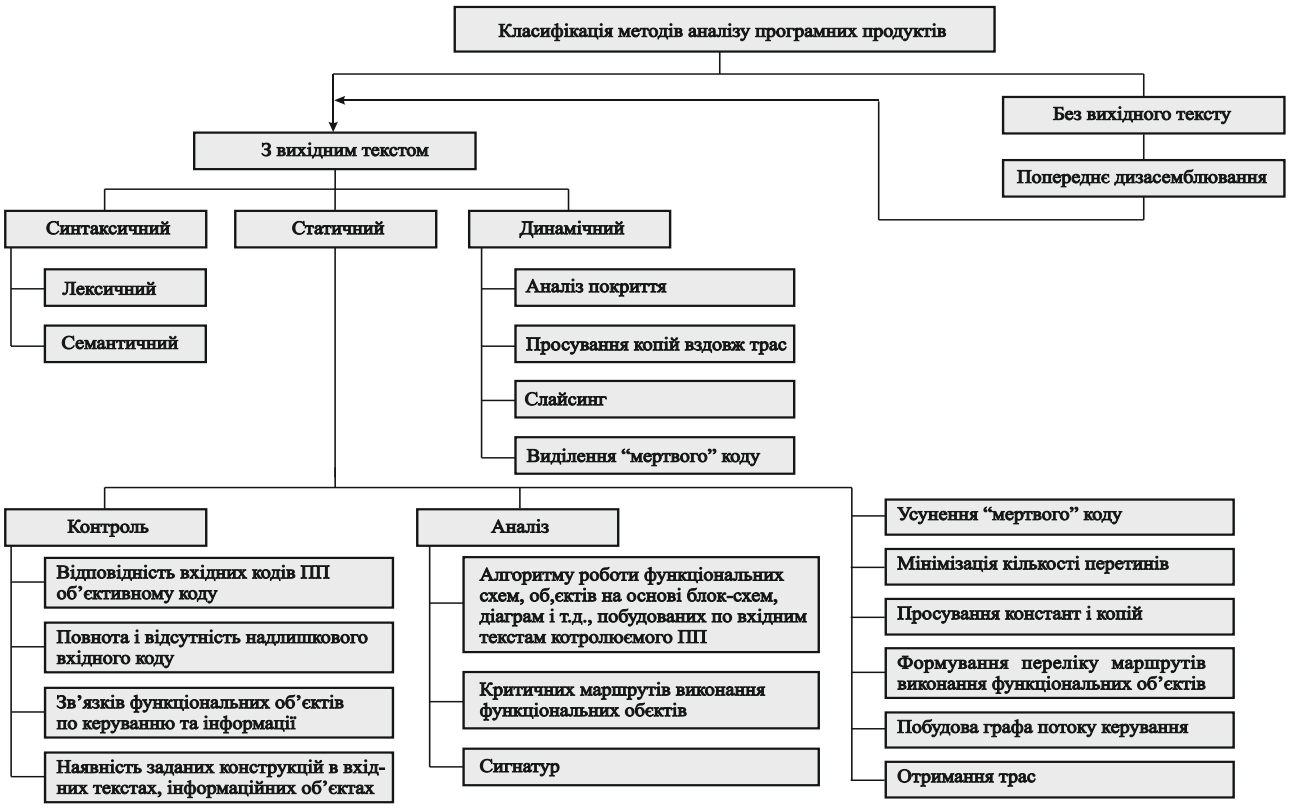


Рис. 1. Узагальнена класифікація методів аналізу програмного забезпечення

Fig. 1. Generalized classification of software analysis methods

Зі зростанням складності ПЗ динамічний аналіз стає нерозв'язним завданням і перетворюється на формальну процедуру. Багато програмних комплексів, які використовуються експертами у повсякденній роботі, мають списки потенційно небезпечних конструкцій, що робить неефективними методи сигнатурного аналізу. Не згадується сигнатурний аналіз у вимогах до випробувань ПЗ нижче другого рівня контролю (тобто, програм, що обробляють секретну та конфіденційну інформацію) [13]. Немає механізмів виявлення помилок кодування, пов'язаних із переповненням буфера, викликом функцій із чужого адресного простору, відсутнє очищення пам'яті тощо. Також відсутні вимоги щодо побудови переліку маршрутів під час виконання функціональних гілок програми, немає механізмів визначення повноти покриття коду та його достатності при динамічному аналізі.

Дослідження вітчизняних та зарубіжних джерел дозволило виділити такі ключові методи, способи та підходи до оцінки інформаційної безпеки ПЗ без вихідних текстів:

1. Перевагою статичного аналізу є повне покриття коду, на відміну методів і способів динамічного аналізу. Виконуючи бінарний аналіз програмного забезпечення, що розробляється, є штатним для середовища функціонування, можна виконати перевірку сторонніх бібліотек, які були використані при розробці. Також можна виконати контрольну перевірку фінальної версії програмного забезпечення шляхом порівняння результатів аналізу вихідного коду та виконуваного коду. Також статичний аналіз може бути успішно використаний при дослідженні стороннього ПЗ, що отримується від постачальників або завантажується з Інтернету.

2. Динамічний аналіз із використанням «пісочниці». Такий вид аналізу являє собою підхід до виявлення підозрілої поведінки у віртуальному ізольованому середовищі. Важливо, що налаштування віртуальних середовищ може бути виконане відповідно до одного з двох підходів.

Оптимальний тут підхід, при якому запуск зразка програмного забезпечення виконується в такому віртуальному середовищі, яке повністю відповідає цільовій системі, якій призначений даний зразок. Однак у такому разі «пісочниця» повинна «на льоту» визначати цільове середовище вузла мережі та запускати потрібну віртуальну машину.

3. Динамічний аналіз із використанням відладчика. Відладники реалізують покрокове виконання програм та встановлення в них точок зупинки. Це може бути реалізовано лише на рівні центрального процесора, мікроконтролера, операційної системи. Ключові функції відладчика – запуск програми, встановлення точок її зупинки, відображення даних, що використовуються програмою, та внесення змін до програми, щоб перевірити, чи можливо таким чином усунути виявлені помилки.

4. Аналіз на імітаційному стенді із використанням форензики. Інтерактивне тестування безпеки додатків є методикою аналізу безпеки ПЗ, переважно спрямовану на дослідження поведінки веб-додатків під час їх роботи [14]. Рішення з інтерактивного тестування зазвичай працюють за рахунок розгортання спеціальних агентів у додатку, що працює. Ці агенти безперервно аналізують те, як взаємодіють додатки (зазвичай ініціювати автоматизованими тестами), щоб виявити вразливості. Деякі рішення щодо інтерактивного тестування безпеки можуть не тільки активно відстежувати вразливості (наприклад, SQL-ін'єкції), але й перевіряти їх, демонструючи їхню придатність для використання зловмисниками. Для аналізу безпеки в такому підході часто використовуються методи форензики, тобто всі методи, пов'язані з розслідуванням вже скоєних комп'ютерних інцидентів.

Таким чином, можна відзначити, що динамічний аналіз більш популярний, ніж статичний, при оцінці безпеки ПЗ без вихідних текстів, однак найкращий результат досягається при їх сукупному використанні, оскільки саме статичний аналіз з використанням дизассемблера дозволяє отримати повне покриття коду та усунути ключовий недолік, властивий методів динамічного аналізу [4, 10, 15].

Слід зазначити, що техніка динамічного аналізу є найбільш популярною, при цьому особливо ефективною вона є в поєднанні з механізмами віртуалізації, оскільки це дає можливість дослідити поведінку зразка ПЗ у середовищі, наближеному за своїми характеристиками до цільової.

Особливої ефективності виявлення шкідливого програмного забезпечення слід очікувати при поєднанні статичного і динамічного аналізу, оскільки статичний аналіз забезпечує максимальне покриття коду. Однак в умовах відсутності вихідних текстів ПЗ це зробити важче, ніж у разі їх наявності, оскільки потрібно використовувати дизасемблер, що дозволяє приблизно відновити високорівневий код програми.

МОДЕЛЮВАННЯ ПРОЦЕСУ ФУНКЦІОНУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Завдання забезпечення безпечного функціонування ПЗ включає: забезпечення інформаційної безпеки для інформаційного середовища під час функціонування ПЗ; забезпечення якісної та надійної реалізації ПЗ своїх функцій.

Програмне забезпечення за функціональним призначенням можна поділити на системне, прикладне та сервісне. Програмне забезпечення є компонентом інформаційної системи (операційної системи, яка своєю чергою може бути частиною програмно-апаратного комплексу, розподіленої обчислювальної мережі).

Оцінка надійності ПЗ пов'язана з можливістю впровадження тексту програмних засобів на етапі розробки та/або модифікації програмних закладок, використовуючи які, зловмисник реалізує створені вразливості. У зв'язку з цим, необхідність сертифікації та перевірки ПЗ на відповідність вимогам чинних нормативних документів протягом усього

його життєвого циклу, не викликає сумнівів [4, 5, 10].

Для оцінки надійності програмних продуктів, що є складовою інформаційних систем, окремий інтерес представляють рандомізовані моделі та методи теорії надійності. Розглянемо основні види моделей оцінки надійності програмних продуктів із зазначенням їх переваг та недоліків.

Модель Джелінскі – Моранди заснована на припущеннях, що час до наступної відмови ПЗ (у разі збою або кібератаки) розподілено експоненційно, а інтенсивність відмов ПЗ пропорційна кількості помилок, що залишилися в програмі.

Перевагою моделі є простота розрахунків, а основним недоліком те, що при неточному визначенні величини початкової кількості помилок інтенсивність відмов програми може стати негативною.

Модель Шумана, передбачається, що дослідження безпеки та надійності ПЗ проводиться в кілька етапів, кожен з яких являє собою виконання ПЗ набору тестових даних. Виявлені протягом етапу тестування помилки реєструються, але не виправляються. Після завершення етапу виправляються всі виявлені помилки, коригуються тестові набори та проводиться новий етап тестування.

Основною перевагою моделі є визначення всіх невідомих параметрів, необхідних для розрахунків, і відсутність необхідності звернення до інших моделей. Недоліком є припущення моделі про те, що при коригуванні програмного забезпечення не вносяться нові помилки. Також для розрахунків потрібна велика кількість зареєстрованих даних.

В основі моделі Модель Шика – Волвертона лежить припущення, за яким частота помилок пропорційна як кількості помилок в ПЗ, а й часу тестування, тобто, ймовірність виявлення помилок з часом зростає.

Модель дозволяє досить точно розраховувати надійність і проста в застосуванні.

Недолік моделі: для розподілів, відмінних від експоненціального, коли інтенсивність помилки змінюється з часом, необхідно використовувати умовні розподіли. При цьому умовна ймовірність для певного інтервалу тестування повинна відповідати проміжку часу від початку тестування до початку розгляду інтервалу тестування. Інакше цей процес відновлення за умови усунення виявлених помилок призведе до завищення ймовірностей безпомилкового функціонування на всіх ділянках тестування.

Модель Коркорена передбачає наявність у ПЗ багатьох джерел програмних відмов, пов'язаних з різними типами помилок та вразливостей, та різну ймовірність їх появи.

Перевагою моделі є те, що вона використовує ймовірності відмов, що змінюються, для різних типів помилок і оцінюється ймовірність безвідмовного виконання ПЗ на даний момент часу. Недоліком є виконання оцінки з урахуванням апріорної інформації чи даних попереднього періоду функціонування однотипних зразків ПЗ.

Модель IBM. Під час експлуатації користувачем поточної версії програмного забезпечення розробники, як правило, займаються його супроводом – вносять деякі покращення або виправлення в цю версію, не чекаючи, поки користувач цього вимагатиме. Супровід може включати також додавання нових функцій. З деякого моменту, коли розробник вважає своє завдання виконаним, починається пасивний супровід, коли виправлення вносяться вже за запитом користувача. При супроводі в кожну нову версію програмного забезпечення вноситься значна кількість нових помилок, разом із доопрацюваннями, змінами та виправленнями, що потребує виправлень також і в наступній версії.

Зокрема, в компанії IBM спробували передбачити кількість подібних виправлень від версії до версії, ґрунтуючись на велику кількість експериментальних даних, зібраних у ході супроводу операційної системи.

Модель Шнайдера пов'язує число помилок у програмі з витратами, виміряними в «людино-місяцях», числом

підпрограм і загальним числом *тисяч* операторів у програмі.

Перевагою моделі є низька обчислювальна складність і простота реалізації, до недоліків можно віднести необґрунтованість емпірично обраного числа виправлень і те що, що вразливості нульового дня не враховуються, а функції ПЗ не досліджуються детально.

МОДЕЛЬ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Запропонована модель безпечного функціонування ПЗ має усувати недоліки, властиві розглянутим моделям. За результатами проведених досліджень моделей, можна зробити наступні висновки про їх недоліки: деякі моделі при реалізації вимагають значного обсягу обчислювальних ресурсів, це пов'язано як із необхідністю накопичення та обробки великої кількості даних, так і з обчислювальними ресурсами компонентів системи, які здійснюють аналіз безпеки; ймовірнісні моделі, як правило, ґрунтуються на припущеннях про те, що інтенсивність відмов/атак чи кількість помилок у ПЗ заздалегідь відомі, відомий розподіл (стандартний, пуассонівський, біноміальний), що не завжди вірно для реальних процесів і систем; відмови ПЗ та кібератаки, викликані експлуатацією вразливостей у ПЗ, розглядаються як сукупність, внаслідок чого моделі не враховують важливої особливості роботи шкідливого програмного забезпечення – а саме характеру його звернень з пам'яттю; жодна з розглянутих моделей не забезпечує комплексного представлення про процес функціонування ПЗ, у тому числі, погляд з боку інформаційної безпеки відсутній.

Для усунення вищеописаних недоліків пропонується основою моделі покласти опис взаємодії сутностей, задіяних у процесі функціонування ПЗ. При цьому необхідно враховувати специфіку поведінки шкідливого програмного забезпечення на комп'ютері або іншому обчислювальному пристрої.

Дослідження показали, що з основних ознак зараження різного типу шкідливого програмного забезпечення наступні:

1. Уповільнення роботи комп'ютера або вузла мережі. Як правило, це викликано впровадженням шкідливого програмного забезпечення та виконанням своїх функцій, що вимагають обчислювальних ресурсів, внаслідок чого на виконання легітимних обчислювальних задач потрібно більше часу.
2. Виконання нових функцій, не властивих даному комп'ютеру: відправлення даних на сторонні веб-ресурси, запуск процесів, які раніше не виконувались, і т.д.
3. Проблеми з відкриттям файлів, які раніше успішно відкривалися на комп'ютері, а також зміни розширення файлів (зникнення розширень або, навпаки, поява подвійних розширень).
4. Раптове завершення роботи додатків або поява спливаючих вікон при роботі додатків, що потенційно сигналізує про шкідливі процеси, що виконуються фоном.

Для шкідливого програмного забезпечення характерне надмірне використання обчислювальних ресурсів, а також операції з пам'яттю, що значно відрізняються від операцій, що виконуються легітимним ПЗ.

Так, наприклад, для шкідливого програмного забезпечення, що використовує обчислювальні потужності середовища для майнінгу, характерним є такий прояв у системі, як уповільнення роботи обчислювальних компонентів системи, поява обчислювальних процесів, що використовують велику кількість ресурсів, а також відправлення мережевого трафіку на сторонні веб-ресурси.

Таким чином, ключову роль описі роботи програмногозабезпечення грають: функції, що виконуються програмним забезпеченням; зміни у використанні обчислювальних ресурсів; зміни, пов'язані з роботою програмного забезпечення з пам'яттю.

На рис. 2 наведено графічне представлення моделі як набору взаємодіючих сутностей. Опис взаємодії сутностей моделі (рис. 2), відбиває як

надійність функціонування програмного забезпечення, що з виконанням заявлених функцій, а й безпеку функціонування програмного забезпечення.

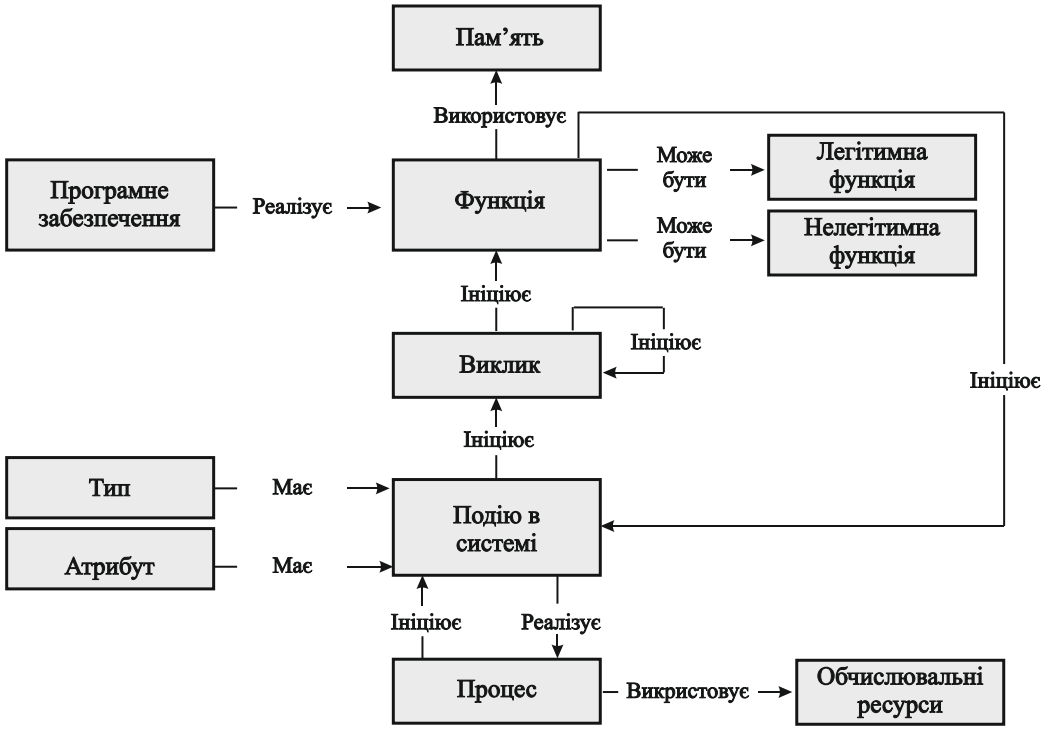


Рис. 2. Графічне представлення моделі безпечного функціонування програмного забезпечення

Fig. 2. Graphical representation of the model of secure software operation

Безпечним буде вважатися ПЗ, встановлення якого не веде до порушення легітимних відношень у системі, але також і те, що не має такого потенціалу внаслідок наявності у своєму складі певного шкідливого функціоналу. Для формалізації опису скористаємося математичним апаратом теорії множин. Опишемо модель безпечного функціонування ПЗ формально, представивши ПЗ ( ) як кортеж:

$$Software =< F, Sign, R, M, Memory > \qquad (1)$$

де:

1. $F = \{f_1, f_2, ..., f_n\}$ - кінцева множина функцій, які виконує програмне забезпечення, що досліджується. Функції, що входять до множини F, поділяються на деструктивні F_{destr} та легітимні функції F_{leg}: $F = F_{leg} \bigcup F_{destr}$, $F_{leg} \bigcap F_{destr} = \varnothing$. При цьому, в будь якій із підмножин F_{leg} і F_{destr} можуть бути присутніми як документовані функції програмного забезпечення F_{doc}, так і не документовані F_{undoc}, $F_{doc} \bigcap F_{undoc} = \varnothing$.

2. $Sign$ –множина ознак, що характеризують виконання функцій програмного забезпечення. Маємо неоднозначне відображення множини F на множину $Sign: F \to Sign$, тобто кожному елементу множини F відповідає один або кілька елементів множини $Sign$. Використовуючи відповідні індекси, задамо відображення $F_{leg} \to Sign_{leg}$, $F_{destr} \to Sign_{destr}$, $F_{doc} \to Sign_{doc}$, $F_{undoc} \to Sign_{undoc}$.

3. R – обчислювальні ресурси, необхідні програмному забезпеченню для реалізації своїх функцій. Маємо відображення $F \to R$, внаслідок якого кожній f_i призначаються три чисельні значення: $\{r_{i_{\min}}, r_i, r_{i_{\max}}\}$.

Очевидно, що оцінка необхідних обчислювальних ресурсів може змінюватись, проте в системі для кожного програмного продукту повинен бути виділений певний обсяг обчислювальних ресурсів, щоб система ефективно функціонувала.

4. M – множина методів дослідження, що застосовуються для виявлення шкідливого програмного забезпечення.

5. $Memory$ – множина операцій над пам'яттю, що виконуються при активації тієї чи іншої функції з множини F. Таким чином, маємо відображення $F \to Memory$, за якого кожній функції f_i зіставляється набір операцій над пам'яттю:

$$f_i \to \left\{ memory_{i_1}, memory_{i_2}, ..., memory_{i_k} \right\}.$$

Необхідно відзначити, що застосування методів M тільки в ідеальному випадку дозволить виявити множину ознак $Sign$, характерних для програмного продукту. На практиці слід говорити про визначення за допомогою методів M підмножини $Sign'$, $Sign' \in Sign$. На практиці вирішується завдання оцінки умовної ймовірності $P(A \mid B)$ події $A = \{ Sign_{destr} = \varnothing \; and \; Sign_{undoc} = \varnothing \}$ при умові виконання події B реалізації деякого набору методів M', $M' \in M$ ′, що дозволяє виявити достатнє число ознак $Sign'_{destr}$ та $Sign'_{undoc}$,

$$B = \left\{ M' \to \left\{ Sign'_{destr}, Sign'_{undoc} \right\} \neq \varnothing \right\}.$$

Тоді умовна ймовірність $P(A \mid B)$ визначиться як (1):

Сформулюємо критерії безпечного функціонування програмного продукту в термінах моделі:

1. Програмний продукт не реалізує деструктивних та шкідливих функцій: $F_{destr} = \varnothing$ та $F_{undoc} = \varnothing$.

2. Об’єм, задіяних для аналізу безпеки програмного продукту (за допомогою множини методів M) обчислювальних ресурсів мінімізовано:

$$M : R \to R_{\min}, R_{\min} = \left\{ r1_{\min}, r2_{\min}, ..., r_{n_{\min}} \right\},$$

таким чином, кожна функція програмного продукту в ідеалі повинна використовувати для реалізації мінімально допустимого об’єму обчислювальних ресурсів;

3. Не повинно бути обчислювальних ресурсів, що витрачаються на будь - яку множину функцій F', що не перетинається з множиною $F : \exists F' \to R$, оскільки присутність шкідливого програмного забезпечення в системі часто призводить до активації нових, нетипових для роботи системи функцій.

4. Множина операцій над пам'яттю $Memory$ повинна мати відображення на множини ознак $Sign$, оскільки, важливою ознакою наявності шкідливого програмного забезпечення в системі є нетипові операції з пам'яттю: $Memory \to Sign \neq \varnothing$.

5. Множина методів дослідження, застосовуваних виявлення шкідливого програмного забезпечення, має використовувати результати відображення $Memory \to Sign$ означає, що для вирішення поставленого завдання доцільно застосовувати ті методи, які враховують операції програмного забезпечення з пам'яттю.

6. Множина використовуваних методів має бути такою, що умовна ймовірність $P(A \mid B)$ максимізована, тобто $M : P(A \mid B) \to 1 : (\mid) \to 1$.

$$P(A \mid B) = P(A) \cdot P(B) = P\{ Sign_{destr} = \varnothing \; and \; Sign_{undoc} = \varnothing \} \cdot \cdot P\left\{ M' \to \left\{ Sign'_{destr}, Sign'_{undoc} \right\} \neq \varnothing \right\} \quad (1)$$

Досягнення максимальної ефективності використовуваних методів M малоймовірно, однак у такому разі буде досягнуто рівність (2):

$$Sign_{destr} = Sign'_{destr}, \; Sign = Sign'_{undoc} \quad (2)$$

Розроблена модель відрізняється від розглянутих моделей оцінки безпеки,

надійності та якості функціонування програмного продукту тим, що вона враховує як особливості функціонування шкідливого програмного забезпечення на компоненті системи, так і необхідність мінімізації обчислювальних ресурсів при аналізі. Особливу увагу слід приділити питанням практичної реалізації розробленої моделі, оскільки вона повинна поєднувати високу ефективність виявлення шкідливого програмного забезпечення та оптимальне використання обчислювальних ресурсів. Програмне забезпечення з потенційно небезпечними можливостями реалізує одну або кілька функцій, наслідки виконання яких можуть безпосередньо загрожувати порушенням безпеки даних, або призводити до виконання коду, що представляє цю загрозу. Види небезпечних можливостей представлені на рис. 3.

Значимість їх систематизації виходить з особливостях роботи з пам'яттю, виділені можливості, наступні: передача управління в область модифікованих даних; самодифікація або зміна коду іншого програмного забезпечення в оперативній пам'яті або на зовнішніх носіях; самодублювання, підміна собою іншого програмного забезпечення або перенесення своїх фрагментів в область оперативної або зовнішньої пам'яті, що не належить програмі; збереження інформації з областей оперативної пам'яті, які не належать програмному забезпеченню; спотворення, блокування чи заміну інформації, що є результатом роботи інших програм; приховування своєї присутності у програмному середовищі.

Виявлення функцій, що здійснюють роботу з пам'яттю таким чином, що виникають потенційно небезпечні можливості, особливо значимо, тому що це основна характеристика поведінки шкідливого програмного забезпечення. Тому при реалізації моделі на практиці слід використовувати механізм, який забезпечує ефективний моніторинг звернень до пам'яті та її використання.

Рис. 3. Програмне забезпечення з потенційно небезпечними можливостями

Fig. 3. Software with potentially dangerous capabilities

Процес у віртуальному операційному середовищі з повним контролем дій програмного забезпечення та відстеження алгоритму його роботи здійснюється більш ефективно. Таким чином реалізація розробленої моделі має базуватися на гіпервізорі, що дозволить віртуалізувати системні ресурси обчислювальних систем.

ВИСНОВКИ

В роботі виконано систематизацію моделей надійного та безпечного функціонування програмного забезпечення. В результаті проведеного дослідження виділено три типи моделей: аналітичні; статистичні; емпіричні.

Розглянуто ряд найчастіше застосовуваних моделей, виділено їх недоліки та переваги з погляду розв'язуваної задачі опису безпечного функціонування програмного продукту, та розпізнавання шкідливого програмного забезпечення. За результатами проведених досліджень розглянуті моделі мають переваги у плані простоти їх практичної реалізації, проте водночас виділено наступні недоліки: деякі з розглянутих моделей при реалізації вимагають великого обсягу обчислювальних ресурсів – для аналізу безпеки та накопичення архівних даних; використання статистичними та імовірнісними моделями припущень про те, що інтенсивність атак/відмов чи кількість помилок у програмному забезпеченню мають заздалегідь відомий розподіл (біноміальний, стандартний або пуасонівський), що не завжди вірно для реальних процесів і систем; немає поділу на відмови програмного забезпечення і вихід з ладу внаслідок кібератак, не враховуються також вразливості нульового дня; не аналізуються звернення досліджуваного програмного забезпечення до пам'яті, що могло б дати важливу інформацію про його легітимність чи наявність шкідливих функцій; жодна з розглянутих моделей не забезпечує комплексного представлення про процес функціонування програмного забезпечення, у тому числі, аналіз з боку інформаційної безпеки відсутній.

Завдання розпізнавання шкідливого програмного забезпечення з кожним роком стає дедалі актуальнішим і складнішим у зв'язку з цифровізацією галузей діяльності людини та використанням програмного забезпечення для виконання бізнес-логіки та технічних процесів у складних системах. Внаслідок цього, чим більший обсяг програмного забезпечення в системі, тим потенційно більше в ньому помилок, при цьому через підключення сучасних систем до мережі Інтернет, програмного забезпечення часто поширюється по мережі, що дозволяє зловмисникам створити нові вектори кібератак на системи.

Запропонована модель безпечного функціонування програмного продукту має усувати недоліки, властиві розглянутим моделям. Запропоновано модель усуває наведені недоліки за рахунок того, що вона враховує характерні особливості прояву шкідливого програмного забезпечення на пристроях, а саме вплив шкідливого програмного забезпечення на обчислювальні ресурси системи та роботу з пам'яттю. Це дозволяє розробленій моделі враховувати як надійність функціонування програмного забезпечення, так і безпеку.

У термінах моделі сформульовані критерії безпечного функціонування програмного забезпечення, зроблено висновок про те, що для найбільш ефективної реалізації такої моделі на практиці має бути використаний гіпервізор. Вибір конкретного гіпервізора залежить від потреб, призначення та специфіки системи.

REFERENCES

1. Doktryna informatsiinoi bezpeky Ukrainy, zatverdzhenoi Ukazom Prezydenta Ukrainy vid 25 liutoho 2017 roku № №47/2017, 15s.
2. Derzhavnyi standart Ukrainy Zakhyst informatsii. Tekhnichnyi zakhyst informatsii. Osnovni polozhennia. DSTU 3396.0-96 [Elektronnyi resurs]. – Rezhym dostupu: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38883&cat_id =38836.
3. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» zi zminamy. Vidomosti Verkhovnoi Rady (VVR), 2017, № 45, st.403, zi zminamy vid 28.07.2022 roku. Rezhym dostupu:

https://zakon.rada.gov.ua/laws/show/2163
4. **Tsybulnyk S. O., Barandych K. S.** (2022). Tekhnolohii rozroblennia prohramnoho zabezpechennia. Chastyna 1. Zhyttievyi tsykl prohramnoho zabezpechennia : bool. Kyiv, KPI im. Ihoria Sikorskoho, 270.
5. **Lysenko S. M., Shchuka R. V.** (2020). Analiz metodiv vyiavlennia shkidlyvoho prohramnoho zabezpechennia v kompiuternykh systemakh. *Visnyk Khmelnytskoho natsionalnoho universytetu*, 2(283). 101–107.
6. **Lenkov S. V., Dzhulii V. M., Bernaz A. M., Muliar I. V., Pampukha I.V.** (2023). Metod prohnozuvannia vrazlyvostei informatsiinoi bezpeky na osnovi analizu danykh tematychnykh internet-resursiv. *Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka*, Issue78, 123-134.
7. **Lenkov S. V., Dzhulii V. M., Solodieieva L. V**. (2022). Metod protydii poshyrenniu ta vyiavlennia shkidlyvoi informatsii v sotsialnykh merezhakh. *Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka*, Issue 77, 103-117.
8. **Lenkov S. V., Dzhulii V. M., Orlenko V. S., Sieliukov O. V., Atamaniuk A. V.** (2020). Model bezpeky poshyrennia zaboronenoi informatsii v informatsiino-telekomunikatsi-inykh merezhakh. *Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka*, Issue 68, 53-64.
9. **Krepych S. Ya., Spivak I. Ya.** (2020). Yakist prohramnoho zabezpechennia ta testuvannia : bazovyi kurs. Ternopil, FOP Palianytsia V. A. Publ., 478.
10. **Zolotukhina O. A., Nehodenko O. V., Reznyk S. Yu., Razina S. Ya.** (2020). Iakist ta testuvannia informatsiinykh system : Navchalnyi posibnyk dlia samostiinoi roboty studentiv vyshchykh navchalnykh zakladiv, Kyiv, NNIIT DUT, 128.
11. **Vyshnia V. B., Havrysh O. S., Ryzhkov E. V.** (2020). Osnovy informatsiinoi bezpeky: book. Dnipro, Dniprop. derzh. un-t vnutrish. sprav, 128.
12. Cotsialni merezhi – realni zahrozy virtualnoho svitu. [Elektronnyi resurs]. – Rezhym dostupu : http://ogo.ua/ articles/view/011–02–23/26490.htm.
13. **Ostapov S. E., Yevseiev S. P., Korol O. H.** (2016). Tekhnolohii zakhystu informatsii: book. Kharkiv, Vyd-vo KhNEU, 476.
14. **Lienkov S. V., Dzhulii V. M., Bernaz N. M., Bozhuk S. O.** (2017). Analiz isnuiuchykh metodiv ta alhorytmiv vyiavlennia atak v bezdrotovykh merezhakh peredachi danykh. *Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka*. Kiyv, VIKNU, Issue 56, 124-132.
15. **Buriachok V. L. Toliupa S. V., Semko V. V.** Informatsiinyi ta kiberprostory: problemy bezpeky, metody ta zasoby borotby : Book. Kyiv, DUT-KNU, 178.
16. **Rybalchenko L. V., Kosychenko O. O.** (2019). Problemy bezpeky personalnykh danykh v Ukraini. *Rehionalna ekonomika*. Zaporizhzhia. 2019, 57-62.
17. **Dzhulii V. M., Miroshnichenko O.V., Solodieieva L.V.** (2022). Metod klasyfikatsii dodatkiv trafika kompiuternykh merezh na osnovi mashynnoho navchannia v umovakh nevyznachenosti. *Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka*. Kyiv VIKNU, Issie 74, 73-82.
18. **Lavrov Ye. A., Perkhun L. P., Shendryk V. V.** (2017). Matematychni metody doslidzhennia operatsii: pidruchnyk. Sumy: Sumskyi derzhavnyi universytet, 212.
19. **Honchar S. F.** (2019). Otsiniuvannia ryzykiv kiberbezpeky informatsiinykh system obiektiv krytychnoi infrastruktury: monohrafiia. Kyiv, 175.
20. **Yemchuk L., Zhylinska O., Chornyi A., Dzhuliy V.** (2020). Organizational Network Analysis as a Tool for Leadership Assessment in Software Development Team. *Institute of Electrical and Electronics Engineers (30 September 2020)*; INSPEC Accession Number: 20008165; DOI: 10.1109/ACIT49673.2020.
21. Syhnatura ataky. Wikipedia [Elektronnyi resurs] – Rezhym dostupu do resursu: https://uk.wikipedia.org/wiki/Syhnatura_ataky
22. OPWNAI: Cybercriminals Starting to Use ChatGPT, January 6, 2023 [Elektronnyi resurs] – Rezhym dostupu do resursu: https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-usechatgpt.

Information security model of functioning software

Serhii Lienkov, Volodymyr Dzhuliy, Oleksandr Yavorskyi, Kostyantyn Zatsepin

Abstract. The paper systematizes the models of reliable and safe functioning of the software. As a result of the research, three types of models were identified: analytical; statistical; empirical.

A number of the most frequently used models are considered, and their disadvantages and advantages are highlighted from the point of view of solving the problem of describing the safe functioning of a software product and recognizing malicious software. According to the results of the research, the considered models have advantages in terms of the simplicity of their practical implementation, but at the same time, the following disadvantages are highlighted: some of the considered models require a large amount of computing resources when implemented - for security analysis and accumulation of archival data; the use of statistical and probabilistic models of assumptions that the intensity of attacks/failures or the number of errors in software have a pre-known distribution (binomial, standard or Poisson), which is not always true for real processes and systems; there is no division into software failures and failures due to cyber attacks, zero-day vulnerabilities are also not taken into account; memory accesses of the investigated software are not analyzed, which could provide important information about its legitimacy or the presence of malicious functions; none of the considered models provides a comprehensive representation of the process of software functioning, including, there is no analysis from the information security side.

The task of recognizing malicious software is becoming more and more relevant and difficult every year in connection with the digitalization of human activities and the use of software for the execution of business logic and technical processes in complex systems. As a result, the larger the volume of software in the system, the more errors there are potentially, and due to the connection of modern systems to the Internet, the software is often distributed over the network, which allows attackers to create new vectors of cyber attacks on systems.

The proposed model of safe functioning of the software product should eliminate the shortcomings inherent in the considered models. The proposed model eliminates the mentioned shortcomings due to the fact that it takes into account the characteristic features of the manifestation of malicious software on devices, namely the impact of malicious software on the computing resources of the system and working with RAM. This allows the developed model to take into account both the reliability of software operation and security.

In terms of the model, the criteria for the safe functioning of the software are formulated, it is concluded that for the most effective implementation of such a model in practice, a hypervisor should be used.

Keywords: model, information security, vulnerabilities, attacks, confidential data, malware, secure operation.

Метод пошуку вразливостей вебзастосунків з використанням API ChatGPT

Ігор Муляр[1], Сергій Лєнков[2], Володимир Гловюк[3], Володимир Анікін[4], Євгеній Сотніков[5].

[1,3,4] Хмельницький національний університет
вул. Інститутська, 11, Хмельницький, Україна, 29000,
[2,5] Військовий інститут Київського національного університету ім. Тараса Шевченка
вул. Ю. Здановської, 81, Київ, Україна, 03189,
[1] muliariv@khmnu.edu.ua, https://orcid.org/0000-0002-6659-605X,
[2] lenkov_s@ukr.net, https://orcid.org/0000-0001-7689-239x,
[3] glovyukvova@gmail.com, https://orcid.org/0009-0004-8625-3486,
[4] anikin_volodymyr@khmnu.edu.ua, https://orcid.org/0000-0003-3395-2764,
[5] sotnikov_man@ukr.net, https://orcid.org/0009-0005-8133-0750

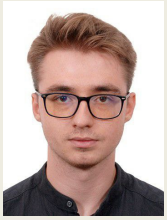
Received 10.09.2024, accepted 08.10.2024
https://doi.org/10.32347/uwt.2024.15.1203

Анотація. У цій роботі представлено метод автоматизації тестування вебзастосунків з використанням API ChatGPT, призначений для допомоги етичним хакерам у виявленні вразливостей. Метою дослідження є розробка підходу, який покращує ефективність та точність пентестингу, зосереджуючись на автоматизації процесів, що традиційно виконуються вручну. Запропонований метод базується на можливостях моделі GPT генерувати тестові запити та аналізувати відповіді серверів, що дозволяє виявляти потенційні вразливості без необхідності детального аналізу вихідного коду. Представлені результати демонструють переваги використання GPT-моделей для генерації складних тестових сценаріїв та аналізу відповідей вебзастосунків, що сприяє виявленню потенційних загроз. Результати експериментів показали підвищення точності виявлення вразливостей на 15-20% та скорочення часу тестування на 35% у порівнянні з традиційними методами. Запропонований підхід є перспективним для впровадження в практику етичного хакінгу та кібербезпеки.

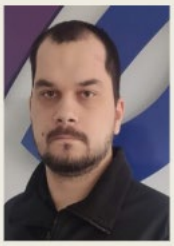
Ключові слова: кібербезпека, автоматизація тестування, етичний хакінг, GPT, ChatGPT API, пентестинг, вебзастосунки.

Ігор Муляр
к.т.н., доц. ст. викладач кафедри кібербезпеки

Сергій Лєнков
д.т.н. професор кафедри, головний науковий співробітник



Володимир Гловюк
Магістр Хмельницького національного університету



Володимир Анікін
асистент кафедри кібербезпеки

Євгеній Сотніков
Магістр Хмельницького національного університету

ВСТУП

У сучасному цифровому середовищі вебзастосунки відіграють ключову роль у наданні різноманітних послуг, від банкінгу до соціальних мереж. Вони стали невід'ємною частиною повсякденного життя мільярдів людей по всьому світу,

забезпечуючи зручний доступ до інформації, комунікації та електронної комерції. Однак зі зростанням їх популярності збільшується і кількість кібератак, спрямованих на виявлення та експлуатацію вразливостей у цих застосунках. Статистика показує, що кількість атак на вебзастосунки зросла на 30% за останні п'ять років, що підкреслює нагальну потребу в ефективних заходах безпеки.

Етичні хакери та фахівці з кібербезпеки стикаються з викликом забезпечення безпеки цих систем, що вимагає постійного моніторингу та тестування [1]. Традиційні методи пентестингу, які включають ручний аналіз та використання стандартних інструментів, можуть бути неефективними при масштабному тестуванні або при виявленні складних вразливостей [2]. Ручний підхід часто займає багато часу та ресурсів, а також може бути схильним до людських помилок. Це створює потребу в нових інструментах та методах, які можуть автоматизувати процес тестування та підвищити його ефективність.

Одним із перспективних напрямків є використання технологій штучного інтелекту та глибокого навчання. Зокрема, моделі на основі GPT (Generative Pre-trained Transformer) продемонстрували високу ефективність у генерації природної мови та можуть бути адаптовані для завдань, пов'язаних з кібербезпекою [3]. Використання API ChatGPT дозволяє інтегрувати можливості цих моделей у процес пентестингу, що може значно покращити результати та оптимізувати роботу етичних хакерів. Завдяки здатності до навчання на великих обсягах даних, ці моделі можуть виявляти складні патерни та аномалії, які можуть бути невидимими для традиційних методів.

Крім того, інтеграція штучного інтелекту в процес пентестингу може сприяти розробці адаптивних систем, які постійно вдосконалюються на основі нових загроз та вразливостей. Це особливо актуально в контексті динамічного розвитку кіберзагроз, де швидкість реакції має вирішальне значення. Використання AI також може знизити бар'єри входження для нових фахівців у сфері кібербезпеки, надаючи їм інтуїтивні інструменти та рекомендації.

Метою даного дослідження є розробка та оцінка методу автоматизації тестування вебзастосунків з використанням API ChatGPT, спрямованого на допомогу етичним хакерам у виявленні вразливостей. Ми прагнемо дослідити, як інтеграція моделей GPT може покращити процес пентестингу, зменшити ризики, пов'язані з людським фактором, та підвищити загальну безпеку вебзастосунків. У рамках дослідження буде розроблено прототип системи, яка поєднує можливості ChatGPT з існуючими інструментами пентестингу, та проведено серію експериментів для оцінки її ефективності.

Очікується, що результати дослідження внесуть значний внесок у сферу кібербезпеки, запропонувавши нові підходи до автоматизації та оптимізації процесів тестування. Це може мати позитивний вплив на галузь, сприяючи розробці більш безпечних вебзастосунків та зниженню ризиків кібератак. Дослідження також може стати основою для подальших робіт у напрямку інтеграції штучного інтелекту в різні аспекти кібербезпеки.

АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА АКТУАЛЬНИХ НАУКОВИХ ДОСЯГНЕНЬ

У сучасному цифровому світі кібербезпека стала однією з ключових сфер дослідження, враховуючи зростаючу кількість та складність кіберзагроз. Останніми роками відбувся значний прогрес у застосуванні штучного інтелекту (ШІ) та глибокого навчання в галузі кібербезпеки. З розвитком технологій, таких як Інтернет речей (IoT), хмарні обчислення та великі дані, масштаби та складність атак зросли, що вимагає нових підходів до їх виявлення та запобігання [4, 5].

Дослідження показали, що методи машинного навчання можуть бути ефективними у виявленні аномалій, аналізі мережевого трафіку та навіть прогнозуванні потенційних атак. Зокрема, нейронні мережі стали потужним інструментом для обробки

складних патернів даних. Глибоке навчання дозволяє моделювати багаторівневі абстракції, що є корисним для розпізнавання складних кіберзагроз [6].

Моделі на основі рекурентних нейронних мереж (RNN) та їх варіації, такі як довга короткочасна пам'ять (LSTM), використовувалися для аналізу послідовностей даних та виявлення підозрілої активності [7]. Вони демонструють ефективність у задачах аналізу мережевого трафіку та виявлення вторгнень, дозволяючи моделювати тимчасові залежності в даних. Проте ці моделі мають обмеження в обробці довготривалих залежностей та складних структур даних, що характерно для сучасних вебзастосунків. Проблема зникання градієнта у RNN може призводити до втрати важливої інформації при обробці довгих послідовностей.

З появою трансформерних моделей, таких як GPT (Generative Pre-trained Transformer), відкрилися нові можливості для обробки великих обсягів даних та розуміння контексту [8]. Трансформери використовують механізм самоуваги (self-attention), що дозволяє ефективно обробляти довгі послідовності та захоплювати залежності між віддаленими елементами даних. Моделі GPT були успішно застосовані в різних сферах, включаючи обробку природної мови (NLP), генерацію коду, автоматизований переклад та навіть створення творчих текстів [9].

У сфері кібербезпеки дослідження демонструють потенціал використання трансформерних моделей для різних завдань. Наприклад, дослідження показали, що GPT-моделі можуть бути використані для генерації фішингових повідомлень, що вказує на їх здатність розуміти та відтворювати складні патерни соціальної інженерії [10]. Це підкреслює необхідність дослідження застосування таких моделей для захисту від подібних загроз.

Додатково, дослідження Li та співавт. [11, 12] розглядали застосування нейронних мереж для автоматизації аналізу безпеки коду. Вони зосередилися на виявленні вразливостей у вихідному коді з використанням глибокого навчання, що підтверджує ефективність ШІ в галузі кібербезпеки [13].

Також варто відзначити розвиток напрямку автоматизованого виявлення вразливостей за допомогою ШІ. Методи глибокого навчання застосовуються для динамічного аналізу коду, аналізу логів систем та виявлення аномалій у поведінці застосунків [14, 15]. Використання підкріпленого навчання (reinforcement learning) дозволяє моделювати поведінку зловмисників та знаходити нові вектори атак, що особливо актуально для пентестингу.

Незважаючи на ці досягнення, використання моделей GPT для автоматизації пентестингу та допомоги етичним хакерам залишається недостатньо дослідженим. Більшість існуючих рішень фокусуються на окремих аспектах, таких як аналіз мережевого трафіку або статичний аналіз коду, але не враховують контекстну взаємодію з вебзастосунками та складність сучасних атак, таких як атаки нульового дня.

Наше дослідження спрямоване на заповнення цієї прогалини та оцінку ефективності підходу, що інтегрує можливості моделей GPT у процес автоматизованого пентестингу. Ми пропонуємо використовувати GPT для генерації тестових запитів, аналізу відповідей серверу з розумінням контексту та автоматичного формування сценаріїв тестування. Це дозволить етичним хакерам більш ефективно виявляти вразливості, особливо ті, що пов'язані зі складними взаємодіями та контекстно-залежними атаками[16].

Таким чином, інтеграція ШІ та, зокрема, моделей GPT у процес пентестингу має потенціал значно підвищити ефективність та точність виявлення вразливостей [17]. Це відкриває нові перспективи у розвитку інструментів кібербезпеки та відповіді на сучасні виклики у цій сфері.

МЕТОДОЛОГІЯ

Запропонована методологія базується на інтеграції можливостей моделі GPT у

процес автоматизованого тестування вебзастосунків. Вона складається з кількох ключових етапів, кожен з яких детально розроблений для забезпечення ефективності та точності виявлення вразливостей.

ГЕНЕРАЦІЯ ТЕСТОВИХ ЗАПИТІВ

Перший етап методології присвячений генерації тестових запитів з використанням API ChatGPT. Основна мета цього етапу — створення різноманітних та складних HTTP-запитів, які можуть виявити потенційні вразливості у вебзастосунках.

Підготовка даних та налаштування моделі.

Спочатку необхідно підготувати модель GPT до специфічного завдання генерації тестових запитів. Для цього виконується додаткове навчання моделі на корпусі даних, що містить приклади різних типів атак та вразливостей. До таких даних включаються:

1. Відомі патерни SQL-ін'єкцій, XSS, CSRF та інших атак [18].
2. Приклади обфускації та різних методів кодування шкідливих запитів.
3. Опис можливих векторів атак та відповідних захисних механізмів.

Налаштування моделі також включає створення спеціалізованих промптів, які спрямовують модель на генерацію потрібних типів запитів. Наприклад, промпт може виглядати так:

"Згенеруй HTTP-запит, що містить потенційну SQL-ін'єкцію в полі 'username' з використанням обфускації коду."

Генерація варіативних та складних запитів.

Після налаштування модель використовується для генерації тестових запитів. Цей процес включає:

Використання обфускації та кодування. Модель генерує запити з різними методами обфускації, такими як URL-кодування, Unicode-символи, подвійне кодування, щоб обійти засоби фільтрації вводу на стороні сервера.

Створення комбінацій атак. Генеруються запити, які поєднують декілька типів атак одночасно. Наприклад, SQL-ін'єкція, вкладена в XSS-скрипт.

Адаптивна генерація на основі попередніх відповідей. Модель аналізує відповіді сервера на попередні запити та коригує наступні запити для підвищення ефективності виявлення вразливостей.

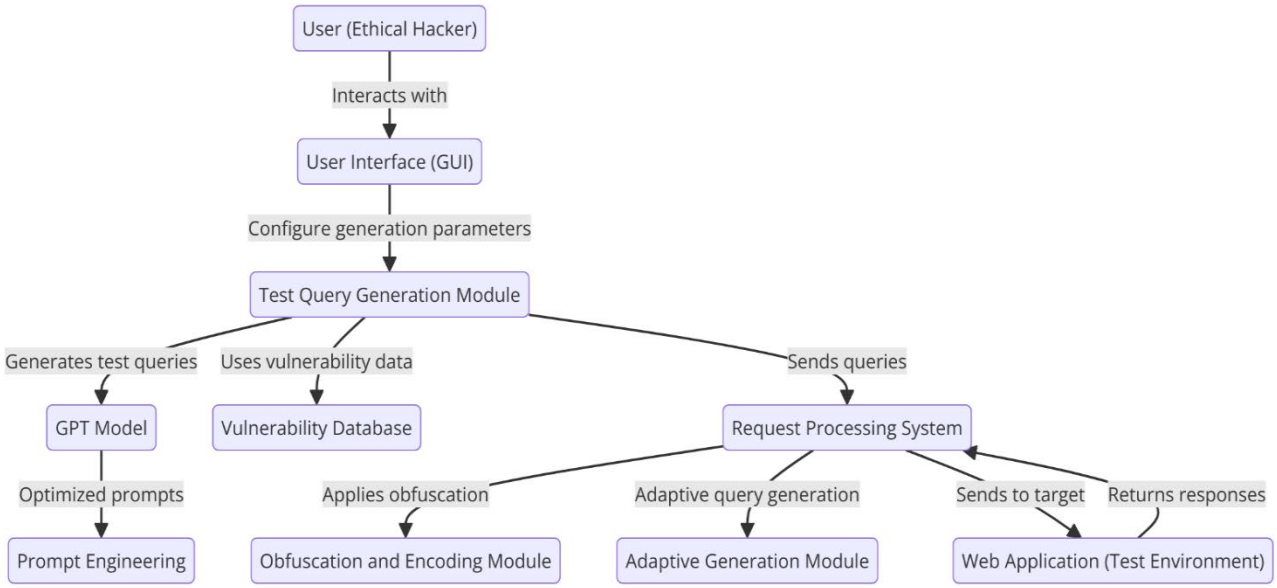


Рис. 1. Архітектура системи генерації текстових запитів

Fig. 1. Architecture of the text query generation system

На Рисунку 1 представлена архітектурна діаграма системи генерації тестових запитів. Діаграма відображає взаємодію між користувачем (етичним хакером),

користувацьким інтерфейсом, модулем генерації запитів, моделлю GPT та вебзастосунком. Модель GPT отримує промти від модуля генерації запитів та генерує тестові запити, які надсилаються до вебзастосунку для тестування.

АВТОМАТИЗОВАНИЙ АНАЛІЗ ВІДПОВІДЕЙ

На цьому етапі відбувається аналіз відповідей вебзастосунків на згенеровані тестові запити з метою виявлення ознак потенційних вразливостей.

Збір та попередня обробка даних.

Всі відповіді серверу на тестові запити логуються та зберігаються у структурованому форматі. Попередня обробка даних включає:

1. Видалення зайвих символів та пробілів.
2. Нормалізацію кодування тексту.
3. Виділення ключових елементів відповіді (HTTP-код статусу, заголовки, тіло відповіді).

Аналіз за допомогою моделі GPT.

Модель GPT використовується для аналізу тексту відповідей з метою виявлення аномалій та патернів, які можуть свідчити про вразливості.

1. Розпізнавання аномалій.
2. Контекстний аналіз.
3. Класифікація ризиків.

Модель шукає ознаки помилок серверу, повідомлення про винятки, нестандартні відповіді. Враховується контекст запиту та відповіді, що дозволяє визначити, чи є поведінка сервера нормальною. Відповіді класифікуються за рівнем ризику (високий, середній, низький), що допомагає фахівцям пріоритезувати подальший аналіз.

Рисунок 2 демонструє діаграму потоків даних (Data Flow Diagram) процесу автоматизованого аналізу відповідей. На діаграмі відображені процеси збору відповідей, попередньої обробки, аналізу за допомогою моделі GPT та класифікації ризиків. Потоки даних між процесами та сховищами даних показують передачу інформації на кожному етапі.

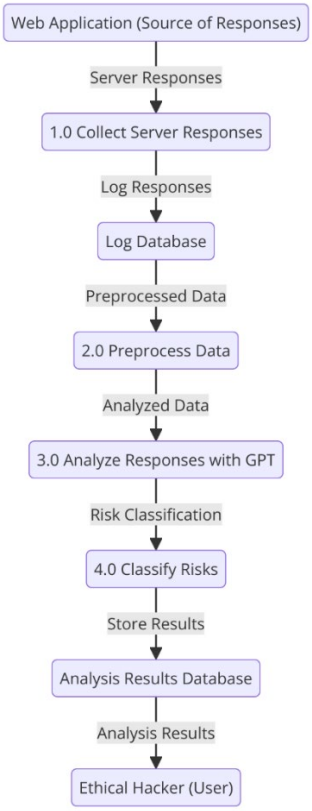


Рис. 2. Потоки даних автоматизованого аналізу відповідей

Fig. 2. Data flows of automated response analysis

ПОБУДОВА СЦЕНАРІЇВ ПЕНТЕСТИНГУ

На основі отриманих результатів аналізу відповідей серверу, система формує комплексний сценарій пентестингу, спрямований на виявлення більш складних та прихованих вразливостей. Цей підхід дозволяє не лише ідентифікувати окремі вразливі точки, але й перевірити стійкість системи до комбінованих атак, які можуть обійти традиційні засоби захисту.

Модель GPT аналізує результати попередніх тестових запитів, виявляючи патерни у відповідях, які можуть свідчити про наявність потенційних вразливостей. Наприклад, якщо певний тип запиту викликає нестандартну реакцію серверу, це може бути індикатором прихованої проблеми.

На основі виявлених патернів модель генерує послідовності запитів, які

поєднують декілька типів атак. Це можуть бути складені запити, що включають елементи SQL-ін'єкцій, XSS, CSRF та інших векторів атак. Метою є перевірка, чи може комбінація різних атак обійти існуючі засоби захисту.

Система застосовує різні техніки обфускації та модифікації запитів для обходу фільтрів та валідаторів на стороні серверу. Це включає:

1. Використання різних методів кодування (наприклад, URL-кодування, Base64) для приховування шкідливого вмісту.
2. Внесення змін у структуру запиту, щоб зробити його менш очевидним для систем виявлення атак.
3. Зміна порядку або значень параметрів запиту для уникнення шаблонних фільтрів.

Генеруються запити, які можуть викликати непередбачені послідовності дій у застосунку. Наприклад:

1. Виявлення можливостей для виконання дій, не передбачених розробниками, через неправильне управління станами або перевірками.
2. Використання серії запитів, де кожен наступний запит базується на реакції системи на попередній.

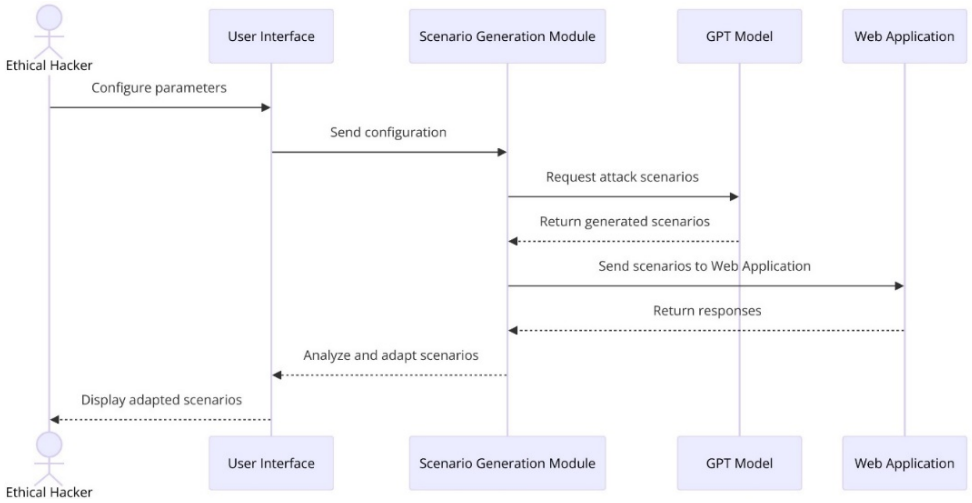


Рис. 3. Діаграма послідовності побудови сценаріїв пентестингу

Fig. 3. Sequence diagram for building pentesting scenarios

Рисунок 3 показує діаграму послідовності, яка відображає взаємодію між етичним хакером, користувацьким інтерфейсом, модулем генерації сценаріїв, моделлю GPT та вебзастосунком під час побудови сценаріїв пентестингу. Діаграма ілюструє послідовність повідомлень та відповідей між об'єктами на кожному кроці процесу.

ІНТЕГРАЦІЯ З ІСНУЮЧИМИ ІНСТРУМЕНТАМИ

Для забезпечення зручності використання та підвищення ефективності система інтегрується з популярними інструментами пентестингу, такими як Burp Suite та OWASP ZAP.

Розробка інтеграційних модулів

Розроблені плагіни дозволяють використовувати можливості системи безпосередньо в середовищі цих інструментів, забезпечуючи безшовну інтеграцію та спільне використання даних.

Користувацький інтерфейс та налаштування.

Розроблений інтуїтивно зрозумілий графічний інтерфейс дозволяє налаштовувати параметри тестування, переглядати та аналізувати результати в режимі реального часу.

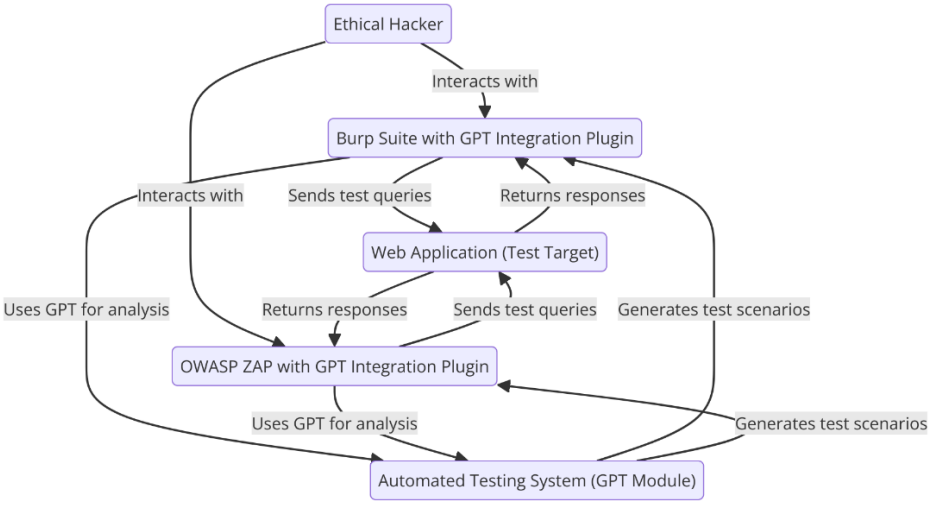


Рис. 4. Архітектура інтеграції з існуючими інструментами

Fig. 4. Integration architecture with existing tools

На Рисунку 4 представлена архітектурна діаграма, яка демонструє інтеграцію системи на основі GPT з інструментами пентестингу Burp Suite та OWASP ZAP. Діаграма відображає, як плагіни GPT Integration взаємодіють з основною системою та забезпечують взаємодію між користувачем та вебзастосунком.

ОЦІНКА ТА ВАЛІДАЦІЯ

Останній етап методології присвячений оцінці ефективності системи та валідації отриманих результатів.

Тестування в контрольованому середовищі. Система тестується на відомих вразливих застосунках (DVWA, WebGoat, Mutillidae) для об'єктивної оцінки її можливостей.

Тестування на реальних вебзастосунках. За згодою власників, система тестується на реальних вебзастосунках, дотримуючись етичних норм та правових вимог.

Аналіз та порівняння результатів Отримані результати аналізуються та порівнюються з результатами традиційних інструментів пентестингу, враховуючи метрики точності, повноти, рівня помилкових спрацьовувань та часу виконання.

Валідація та вдосконалення. На основі аналізу результатів виявлені вразливості підтверджуються шляхом ручної перевірки, а також вносяться корективи та вдосконалення у модель та алгоритми.

РЕАЛІЗАЦІЯ ЕКСПЕРИМЕНТУ

Експеримент проводився на контрольованих навчальних платформах Damn Vulnerable Web Application (DVWA) та OWASP WebGoat, які містять навмисно вбудовані вразливості для освітніх цілей. Спеціально розроблені промпти спрямовували модель ChatGPT на генерацію складних та варіативних тестових запитів, здатних виявити зазначені типи вразливостей. Згенеровані запити вручну вводилися у відповідні поля вводу вебзастосунків, після чого аналізувалися відповіді серверу на предмет ознак потенційних вразливостей, таких як неочікувані повідомлення про помилки, некоректна поведінка застосунку або розголошення конфіденційної інформації.

У випадку з SQL-ін'єкціями модель успішно згенерувала запити, які призводили до отримання несанкціонованого доступу до бази даних у DVWA. Наприклад, введення певних рядків у поле "ID" дозволяло відображати приховані записи бази даних, демонструючи можливість обходу

механізмів аутентифікації та авторизації.

При тестуванні на XSS-атаки модель створювала скрипти, які виконувалися на стороні клієнта в WebGoat, вказуючи на вразливість до міжсайтового скриптингу. Це свідчить про ризик викрадення сесійних даних користувачів або проведення фішингових атак у реальних застосунках.

Щодо CSRF-атак, модель генерувала запити, які могли змінювати дані користувача без його відома, демонструючи вразливість до підробки запитів між сайтами. Це підкреслює небезпеку виконання несанкціонованих дій від імені користувача.

Особливу увагу приділили LFI-атакам (Local File Inclusion), які дозволяють зловмисникам отримувати доступ до локальних файлів на сервері. Модель ChatGPT генерувала запити, що маніпулювали шляхами до файлів, наприклад, використовуючи послідовності типу «../../etc/passwd». При введенні таких запитів у DVWA вдавалося отримати вміст критичних системних файлів або викликати помилки, які вказували на можливість доступу до них. У WebGoat модель застосовувала різні методи кодування та обфускації, щоб обійти фільтри вводу, демонструючи глибоке розуміння можливих шляхів обходу захисних механізмів.

Результати експерименту свідчать про те, що спеціально налаштована модель ChatGPT здатна ефективно генерувати тестові запити для виявлення широкого спектра вразливостей, включаючи складні та менш поширені атаки, такі як LFI. Здатність моделі створювати креативні та нестандартні запити робить її цінним інструментом для пентестерів.

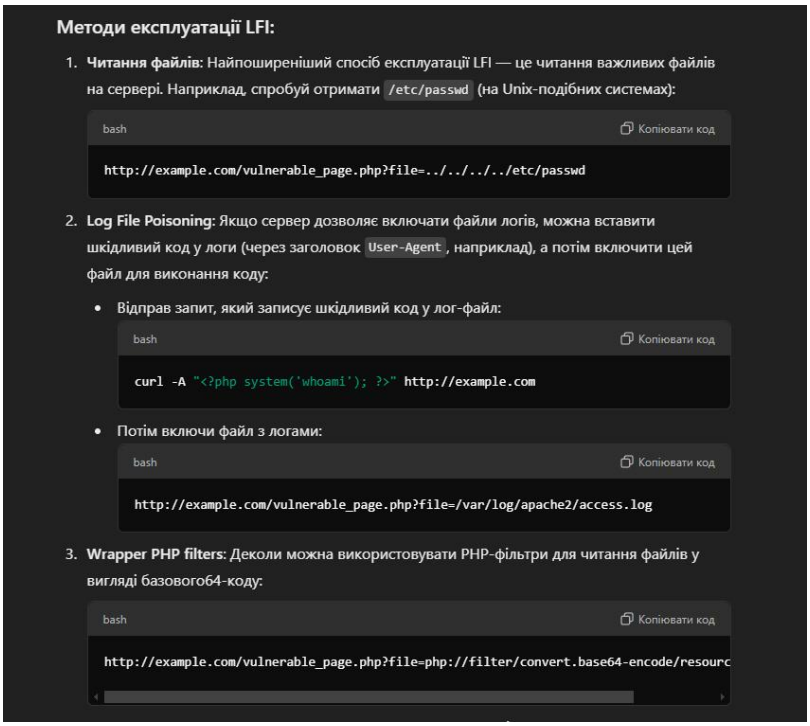


Рис. 5. Запропоновані методи експлуатації та обходу фільтрації LFI

Fig. 5. Proposed methods of operation and bypass of LFI filtration

Однак ефективність згенерованих запитів значною мірою залежала від якості та специфічності сформульованих промптів. Нечіткі або некоректні промпти призводили до нерелевантних або неефективних запитів, що підкреслює важливість правильної постановки завдання для моделі та необхідність глибокого розуміння

предметної області з боку фахівця.

Хоча процес не був повністю автоматизованим і вимагав ручного введення запитів та аналізу відповідей, експеримент підтвердив потенціал інтеграції моделей GPT у автоматизовані інструменти пентестингу. Автоматизація генерації та відправки тестових запитів, а також аналізу відповідей серверу, могла б значно підвищити ефективність процесу тестування та знизити навантаження на фахівців з кібербезпеки.

У підсумку, експеримент підтвердив, що спеціально налаштована модель ChatGPT має значний потенціал у покращенні процесів тестування безпеки вебзастосунків. Модель ефективно генерувала тестові запити для виявлення різних типів вразливостей, включаючи SQL-ін'єкції, XSS, CSRF та LFI-атаки. Отримані результати підтримують ідею подальшого розвитку та впровадження автоматизованих систем, що використовують можливості штучного інтелекту, для підвищення ефективності та точності пентестингу. Це, у свою чергу, сприятиме покращенню захисту від кіберзагроз та забезпеченню більш високого рівня безпеки інформаційних систем.

ВИСНОВКИ

Дослідження, проведене в рамках цієї роботи, продемонструвало значний потенціал використання API ChatGPT для автоматизації тестування вебзастосунків, що спрямоване на допомогу етичним хакерам у виявленні вразливостей. Результати експериментів підтвердили, що інтеграція моделей GPT у процес пентестингу дозволяє значно підвищити ефективність, точність та швидкість виявлення вразливостей, порівняно з традиційними методами.

Ключові досягнення дослідження:

1. Збільшення показників успішного виявлення на 15-20% для різних типів вразливостей.
2. Автоматизація дозволяє зменшити час, необхідний для проведення повного пентестингу, на 35%.
3. Глибокий аналіз відповідей серверу знижує кількість хибних позитивних результатів.
4. Модель може швидко адаптуватися до нових типів вразливостей та оновлень у вебтехнологіях.

Загалом, результати дослідження підтверджують, що використання моделей GPT для автоматизації тестування вебзастосунків є перспективним напрямком у сфері кібербезпеки. Це не тільки підвищує ефективність пентестингу, але й сприяє розвитку нових інструментів та методів захисту. Впровадження таких технологій може стати ключовим фактором у боротьбі з сучасними кіберзагрозами, забезпечуючи безпечне та надійне цифрове середовище.

REFERENCES

1. OWASP Foundation. (2020). OWASP Web Security Testing Guide v4.2. OWASP Foundation. Retrieved from https://owasp.org/www-project-top-ten/
2. **Chio, C., & Freeman, D.** (2018). Machine Learning and Security: Protecting Systems with Data and Algorithms. O'Reilly Media.
3. **Brown, T. B**., et al. (2020). Language models are few-shot learners. Advances in Neural Information Processing Systems, 33, 1877-1901.
4. **Radford, A., Wu, J., Child, R**., et al. (2019). Language models are unsupervised multitask learners. OpenAI Blog. Retrieved from https://openai.com/blog/language-models
5. **Zhang, J., Lin, Y., & Sun, M**. (2019). A survey of deep learning techniques for vulnerability detection. IEEE Access, 7, 167757-167786.
6. **Lienkov, S. V., Dzhulii, V. M., Bernaz, A. M., Muliar, I. V., & Pampukha, I. V.** (2023). Metod prohnozuvannia vrazlyvostei informatsiinoi bezpeky na osnovi analizu danykh tematychnykh internet-resursiv. Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka, 78, 123-133. https://doi.org/10.17721/2519-481X/2023/78-1
7. **Vaswani, A., Shazeer, N., Parmar, N.**, et al. (2017). Attention is all you need. Advances in Neural Information Processing Systems, 30, 5998-6008.
8. **Lin, H., Liu, Z., Sun, M.**, et al. (2021). A survey on transformers in natural language processing. Journal of Artificial Intelligence Research, 70, 321-362.
9. **Raff, E., Barker, J., Sylvester, J.**, et al. (2018).

Malware detection by eating a whole EXE. In Workshops at the Thirty-Second AAAI Conference on Artificial Intelligence.
10. **Vlasenko, M. та Khlaponin, Y.,** (2023). The Internet of Things (IoT) in World Practice: Review and Analysis. Pidvodni tehnologii. (13), 21–27. doi: 10.32347/uwt.2023.13.1202
11. **Ilyas, A., Engstrom, L., Athalye, A., & Lin, J.** (2018). Black-box adversarial attacks with limited queries and information. In Proceedings of the 35th International Conference on Machine Learning.
12. **Subramanian, S., Dheeru, D., Ravi, S., & McAuley, J.** (2021). Scaling laws for transfer learning in neural language models. arXiv preprint arXiv:2109.07841. Retrieved from https://arxiv.org/abs/2109.07841
13. **Korchenko, O. H., Domin, V. Ye., & Kokhanovskyi, V. P.** (2020). Kiberbezpeka ta shtuchnyi intelekt: vyklyky ta perspektyvy. Kyiv: KNU.Wang, S., et al. (2020). Detecting code vulnerabilities via graph neural network. *IEEE Transactions on Dependable and Secure Computing*.
14. **Misnyk, S. V.** (2019). Vykorystannia neironnykh merezh dlia vyiavlennia vrazlyvostei u veb-dodatkakh. *Naukovyi visnyk NTUU "KPI". Seriia: Informatsiini tekhnolohii*, 3, 45-52.
15. **Li, Z., Zou, D., Xu, S.,** et al. (2018). VulDeePecker: A deep learning-based system for vulnerability detection. *In Proceedings of the 25th Annual Network and Distributed System Security Symposium* (NDSS).
16. **Zhang, J., Lin, Y., & Sun, M.** (2019). A survey of deep learning techniques for vulnerability detection. *IEEE Access*, 7, 167757-167786.
17. **Chakraborty, S., Shahriar, H., & Clincy, V.** (2016). Detection of SQL injection and cross-site scripting attacks using static analysis. *In Proceedings of the 2016 ACM Southeast Conference*. 174-177.

A method for finding web application vulnerabilities using the ChatGPT API

Ihor Mulyar, Serhiy Lenkov, Volodymyr Glowyuk, Volodymyr Anikin, Yevgeny Sotnikov

Annotation. This paper presents a method for automating web application testing using the ChatGPT API, designed to help ethical hackers identify vulnerabilities. The goal of the research is to develop an approach that improves the efficiency and accuracy of pentesting, focusing on the automation of processes that are traditionally performed manually. The proposed method is based on the capabilities of the GPT model to generate test requests and analyze server responses, which allows detecting potential vulnerabilities without the need for detailed analysis of the source code. The presented results demonstrate the advantages of using GPT models for generating complex test scenarios and analyzing web application responses, which helps identify potential threats. The results of the experiments showed an increase in the accuracy of vulnerability detection by 15-20% and a reduction in testing time by 35% compared to traditional methods. The proposed approach is promising for implementation in the practice of ethical hacking and cyber security.

Keywords: cyber security, test automation, ethical hacking, GPT, ChatGPT API, pentesting, web applications.

Проблеми забезпечення інформаційної безпеки суб'єктами освітньої діяльності в цифровому освітньо-науковому середовищі закладів освіти

Ігор Козубцов[1], Наталія Зінченко[2], Андрій Котенко[3], Ігор Аверічев[4]

[1] Київський національний університет будівництва і архітектури
пр-т Повітряних Сил, 31, м.Київ, Україна, 03037
[2] Військовий інститут телекомунікацій та інформатизації імені Героїв Крут
вул. Князів Острозьких 45/1, Київ, Україна, 01011
[3,4] Державний університет інформаційно-комунікаційних технологій
вул. Солом'янська, 7, м.Київ, Україна, 03037
[1] kozubtsov@gmail.com, orcid.org/0000-0002-7309-4365
[2] zinchenko.natasha@gmail.com, orcid.org/0009-0004-1837-2838
[3] dutkotenko@gmail.com, orcid.org/0000-0002-0483-6353
[4] laverichev19@gmail.com, orcid.org/0009-0008-9766-0115

Received 17.09.2024, accepted 27.11.2024
https://doi.org/10.32347/uwt.2024.15.1204

Анотація. У науковій статті розглядаються сучасні проблеми забезпечення інформаційної безпеки суб'єктами освітньої діяльності в цифровому освітньо-науковому середовищі закладів освіти. В умовах війни (надзвичайних подій, пандемій) освітння діяльність субєктів переміщується у цифрове освітньо-наукове середовище закладів освіти, де себе ефективно зарекомендувало. Оскільки всі освітні процеси закладів освіти є інформаційними, а їх спотворення може призвести до негативних наслідкив, то виникає потреба у забезпеченні інформаційної безпеки. На підставі цього виокремлено стратегічну ціль забезпечення інформаційної безпеки в цифровому освітньо-науковому просторі закладу освіти - формування у субєктів культури особистої інформаційної та кібернетичної безпеки. Тому необхідно ще під час навчання формувати у здобувачів освіти інформаційну компетентність та особисту культуру інформаційної безпеки, особливо потребують здобувачі освіти гуманітарного профілю підготовки. Отже, метою статті є огляд проблем забезпечення інформаційної безпеки суб'єктами освітньої діяльності в цифровому освітньо-науковому середовищі закладів освіти. За результатом дослідження виокремлено та розглянуто багатоаспектність інформаційної безпеки в системі освіти, інформаційний захист суб'єкта навчальної (освітньої) діяльності, проблема відбору викладачем навчальної інформації та проблему захисту цифрового освітньо-наукового простору закладу освіти від внутрішніх та зовнішніх загроз. Підтверджено, що, формування інформаційної культури в освітньому процесі є багатоплановим поетапним процесом безперервної інформаційної підготовки здобувачів освіти. Саме рівень інформаційної культури є показником готовності суб'єкта до навчання і самоосвіти, розвитку і саморозвитку та характеризує ефективність використання

Ігор Козубцов
Професор кафедри кібербезпеки та комп'ютерної інженерії КНУБА

Наталія Зінченко
Старший помічник начальника відділу забезпечення якості освітньої діяльності

Андрій Котенко
к.т.н., доц., доцент кафедри Технічних систем кіберзахисту ДУІКТ

Ігор Аверічев
к.е.н., доцент кафедри Технічних систем кіберзахисту ДУІКТ

інформації і інформаційних ресурсів в освітній та професійній діяльності в інформаційному просторі при обов'язковому забезпеченні вимог інформаційної безпеки.

Ключові слова: інформаційна безпека, компетентність, інформаційна культура, цифрове освітньо-наукове середовище, заклад вищої освіти.

ВСТУП

Передача надбання суспільства наступним поколінням реалізується через інформаційну діяльність субєектів освітнього процесу.

Всі процеси за своєю природою є інформаційними, а їх спотворення можуть призвести до негативних наслідкив. Тому поряд із збереженням надбання суспільства є не менш важливим завданням забезпечення *інформаційної безпеки* – безпеки процесів, відносин, об'єктів і суб'єктів.

Оскільки всі освітні процеси закладів освіти (ЗВО) є інформаційними, тому:

вони також повинні розглядатися в контексті інформаційної безпеки інформаційного освітнього середовища, в якому взаємодіють всі суб’єкти освітньої діяльності ЗВО;

зміст та проблеми інформаційної безпеки, методи і засоби її забезпечення повинні бути невід'ємною частиною змісту освіти, навчання в рамках будь-якого навчального предмета і, впершу чергу, починаючи зі школи учням в рамках уроків інформатики.

При цьому всі суб'єкти освітньої діяльності ЗВО потребують в набутті інформаційної компетентності, що включає необхідні знання і вміння, з наступним перетворенням у особисту культуру інформаційної безпеки як системно-інтелектуального компонента його особистої культури та світогляду як розвивається особистісної системи інформаційного суспільства. Якщо в технічних ЗВО формування інформаційної компетентності є змістом їх фахової підготовки [1], то із впровадженням цифрових технологій в закладах гуманітарної освіти – це лишається актуальною проблемою. У зв'язку з цим перед ЗВО, що здійснюють підготовку майбутніх педагогів, постало наукове завдання у розробці системної підготовки майбутніх науково-педагогічних кадрів до нових умов професійної науково-педагогічної діяльності в цифровому освітньому середовищі, які володіють цифровими компетентностями до склу яких увійшла інформаційна [2].

Рішення цієї проблеми започатковане окремими дослідниками в контексті виконання науково-дослідної роботи «Теорія і практика підготовки майбутнього викладача закладу вищої педагогічної освіти до професійної діяльності в умовах цифровізації суспільства», що виконується в Інституті педагогічної освіти і освіти дорослих імені Івана Зязюна НАПН України, в напрямку «цифровізації» освіти, що дозволило виокремити потребу у окремому науковому пошукі та вирішенні часткового завдання:

у осучасненому перегляді проблеми забезпечення інформаційної безпеки в цифровому освітньо-науковому середовищі ЗВО [3];

систематизації підходів до навчання здобувачів вищої освіти в «цифровому освітнь-науковому середовищі» [4].

Під «цифровим освітньо-науковим середовищем» будемо розуміти відкриту та закриту сукупність інформаційних систем, призначених для забезпечення завдань освітнього процесу та наукової діяльності у ЗВО. Необхідно враховувати можливий вплив небезпеку на «цифрове освітньо-наукове середовище» з боку кіберпростору та вживати превентивних заходів для підтримання в актуальності систему захисту від кіберзагроз. Загальне уявлення про структурні складові «цифрового освітньо-наукового середовище» ЗВО зображено на рис. 1, які постійно доповнюються. Заявляють відповідно до них нові загрози.

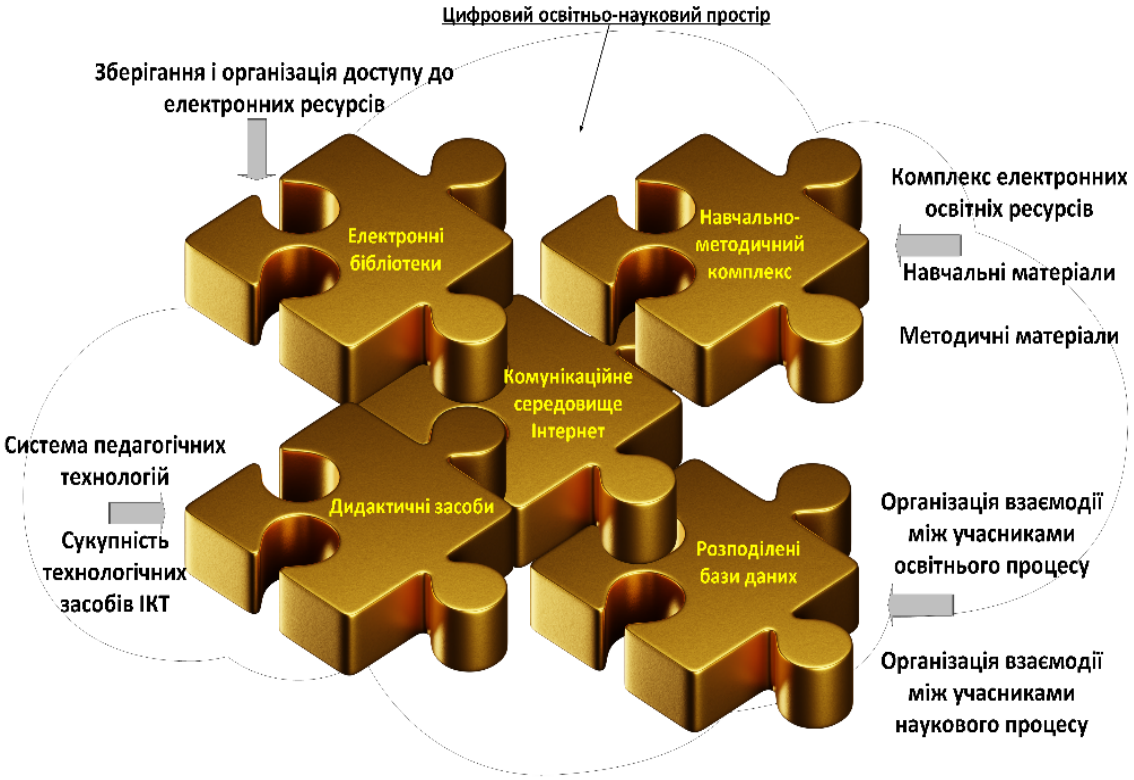


Рис. 1. Структурні складові «цифрового освітньо-наукового середовища» ЗВО

Fig. 1. Structural components of the “digital educational and scientific environment” of higher education institutions

Таким чином, однією із стратегічних цілей забезпечення інформаційної безпеки в цифровому освітньо-науковому просторі ЗВО є формування у громадян культури особистої інформаційної та кібернетичної безпеки.

ЗВ’ЯЗОК ПРОБЛЕМИ З ВАЖЛИВИМИ НАУКОВИМИ ЗАВДАННЯМИ

На потребу у формування культури інформаційної безпеки зазначається в рекомендації Організації економічного співробітництва та розвитку «OECD Guidelines for the security of information systems and networks: Towards a culture of security» [5], прийняті в далекому ще 2002 р. та з наступним оновленням в 2015 р. на рекомендацію щодо управління ризиками цифрової безпеки для економічного та соціального процвітання [6].

Слід зазначити, що окремі рекомендації з документа [5] знайшли відображення у резолюції Генеральної Асамблеї ООН «Створення глобальної культури кібербезпеки» [7] («Елементи для створення глобальної культури кібербезпеки»).

Таким чином, можна вважати, що проблема забезпечення інформаційної безпеки в цифровому освітньо-науковому середовищі ЗВО отримала світову визнання тож і потребує адекватних заходів щодо її вирішення.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Проблема забезпечення інформаційної безпеки в цифровому освітньо-науковому середовищі закладах освіти не є порівняно новою. Над їх вирішенням згуртувалися небайдужі дослідники у всьому світі.

Взаємодія з кіберпростором, на думку автора дослідження [8], розвиває знання і культуру людини, культуру інформаційної безпеки, у той час як культура і знання

людини, його знання з інформаційної безпеки і культура інформаційної безпеки оптимізують це взаємодія.

На проблему технологізації віртуального світу, кіберпростору, а разом з цим і технологізації мислення людини звертають все більшу увагу. Так група вчених в своїх дослідженнях незалежно один від одного [9 – 12] прийшли до висновку, що інформаційне поле інтернету та активна присутність користувачів в соціальних мережах, в інших віртуальних форумах або формах спільнот істотно впливають на ціннісно-смислову сферу особистості.

Автор монографії [13] зазначає на необхідність супроводу «кіберсоціализації» особистості та формування в її кіберкультури. Крім того, вона повинна включати в себе і особисту кіберкультуру інформаційної безпеки.

В роботі [14] обґрунтовано необхідність вбудовування системи забезпечення інформаційної безпеки в діяльність освітніх установ, оскільки одним з найбільш активних споживачів і генераторів інформації є сфера освіти, де формується інтелектуальний і моральний потенціал майбутніх поколінь. А оскільки науково-педагогічна діяльність викладача ЗВО унеможливилась без засобів автоматизації, які вразливі до кібервпливу, то очевидно і назріла потреба в обов’язковому забезпеченні її кібербезпеки [15].

Неминуча і тому необхідна технологізація діяльності і пізнання суб'єкта освіти не повинна вести до технологізації його мислення. Небезпека технізації суспільства помітив Н. Бердяєв [16], який писав про відрив людини від природи, про технізації світу людини, що виявляється в його дегуманізації, втрати морального і духовного в створюваній ним технічної цивілізації. Зараз, на жаль, цей «відрив» пішов далеко вперед завдяки світової кризи, спровокованої пандемією коронавірусу, що не має аналогів у сучасній історії. З цього приводу є слушна думка K. Schwab [17, с. 7] «Ніщо ніколи не повернеться у «вихідне положення» світ, яким ми його знали в перші місяці 2020 року, більше не існує, світ перетнув точку біфуркації епох «до коронавірусу» та «після коронавірусу». Тому на разі спостерігається інтенсивний процес технологізації суб'єктів освітньої діяльності без обґрунтованої теорії цифрового навчання носить сумнівний характер [3].

Педагогічний супровід крім вивчення предметів природничо-наукового і професійного циклу (математики, інформатики, інформаційних технологій) вже не в стані системно вирішити проблему, тут необхідна методична система навчання, що забезпечує формування рівня інформаційної культури у здобувачів вищої освіти з обов'язковою складовою – компетентністю в області захисту інформації та забезпечення інформаційної безпеки в освіті [18].

Дана проблема має міждисциплінарний характер і потребує педагогічного осмислення у розвитку особистості здобувачів вищої освіти в аспекті забезпечення інформаційної безпеки в сучасному цифровому суспільстві. Слід зазначити, що поняття «цифрове суспільства» в Україні з’явилося за результатами ухвали Урядом держави «Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки» [19].

На жаль, у педагогічній науці не в повній мірі приділяють увагу різним питань з підготовки випускника ЗВО до забезпечення інформаційної безпеки у повсякденній діяльності про що зазначається у схваленій стратегії розвитку вищої освіти в Україні на 2022-2032 роки [20].

Виходячи з вище розглянутого, в дослідженні під проблемами інформаційної безпеки, будемо розглядати:

- захист інформаційного цифрового освітньо-наукового середовища суб'єкта освіти від негативної інформації, дезінформації та інформаційного впливу на нього;
- формуванні особистісних якостей здобувачів освіти в якості «активів» його особистої інформаційної безпеки.

Тоді під проблемами інформаційної безпеки освіти будуть:

- адекватне відображення тем і проблем інформаційної безпеки в змісті освіти і предметного навчання;
- розвиток у педагогічних дослідженнях теми інформаційної безпеки та її реалізації у сфері освіти;
- формування особистої інформаційної культури та критичного мислення суб'єктів освітньої діяльності.

Метою статті є огляд проблем забезпечення інформаційної безпеки суб'єктами освітньої діяльності в цифровому освітньо-науковому середовищі ЗВО.

МЕТОДИ ДОСЛІДЖЕННЯ

Основні інструменти дослідження:

методи теоретичного аналізу й узагальнення наукової літератури, за темою дослідження;

узагальнення – для формулювання висновків і рекомендацій щодо результативності.

РЕЗУЛЬТАТ ДОСЛІДЖЕННЯ

Інформаційна безпека виражається в захищеності, гарантії збереження стану людини, суспільства, їхніх ресурсів, надбання, знань, умов, середовища, в яких вони живуть, діють і розвиваються, що відповідають їх рівню і цілям розвитку [18]. Забезпечення інформаційної безпеки суб'єктам освітньої діяльності в цифровому освітньо-науковому середовищі ЗВО – це створення необхідних і достатніх умов для стану захищеності, гарантованості і збереження навчальної та фундаментальної інформації та даних. В першу чергу викладачами необхідно знати проблеми інформаційної безпеки і вміти їх усувати.

Інформаційна безпека передбачає наступне:

- безпека інформаційного цифрового освітньо-наукового середовища, інформаційно-пізнавальної сфери;
- безпека особистої інформаційно-пізнавальної сфери людини, породжуваної її процесами, засобами і результатами, процесами інформатизації та використання інформації;
- безпека багатовимірного інформаційного простору, реального і віртуального, кіберпростору.

1. Багатоаспектність інформаційної безпеки в системі освіти

1.1 Інформаційна безпека має до системи освіти багатоаспектне відношення.

Зовнішніми чинниками є потреби у розвитку освіти. Він представлений у змісті навчання інформатики, комп'ютерних наук та інших суміжних навчальних дисциплінах.

Внутрішніми чинниками освітньої системи є забезпечення викладачами якісного и навчально-методичного супроводу здобувачів освіти. Оскільки освітній процес – це система інтерсуб'єктивних інформаційних процесів, процесів інформатизації та інформаційного взаємодії. Виходячи з цього представлення інформаційну безпеку в системі освіті можна виділити в наступному:

- в гарантії безперервності процесів пізнання, навчання, навчальної та навчально-пізнавальної діяльності здобувачів освіти;
- в безпеки суб'єктів освіти при взаємодії через інформаційне цифрове освітньо-наукове середовище системи дистанційної освіти;
- в безпеці відносин між суб'єктами освітньої діяльності в умовах застосування технологій дистанційного навчання.

1.2 Безпека освітнього процесу в цифровому освітньо-науковому середовищі досягається насиченістю навчальними засобами, розвитком інфраструктури, методичними розробками, інформаційним управлінням та програмними (апаратними) засобами кібербезпеки.

1.3 Безпека суб'єктних відносин в системі освіті визначається їх відповідністю та закономірностям як соціально-інформаційної системи, культурою цих відносин, сприятливими умовами середовища.

1.4 Фізичне вираження інформаційної безпеки суб'єкта – це дотримання норм роботи з інформаційно-комунікаційними

технологіями в цифровому освітньо-науковому просторі.

Пізнання різноманіття світу, культури, знань передбачає наявність такого ж різноманіття засобів сприйняття, джерел інформації, учасників інформаційного діалогу. Обмеженість діяльнісно-пізнавального середовища спричиняє обмеженість здобувачів освіти, так як «будь-яка віртуалізація, яка підміняє органічні, культурно обґрунтовані детермінанти мікро – і самосприйняття, в результаті вириває людину з контексту реальності» [21, с. 16].

Занурення у віртуальний світ відображеної (абстрактної) інформації також тягне замикання людини в обмеженому просторі ілюзій і уявлень. Тому дане «занурення» є вкрай небезпечним для людини [16].

2. **Інформаційний захист суб'єкта навчальної (освітньої) діяльності**

Інформаційний захист суб'єктів навчання досягається за рахунок:

- ефективної та раціональної передачі і сприйняття навчальної інформації у відповідності з цілями освіти;
- захисту здобувачів освіти від недоброякісної, недостовірної та негативної інформації;
- в усвідомленні способів якісного розпізнавання шкідливої інформації і диференціації інформації;
- формування здатності пізнавати й захищати свій внутрішній світ, зберігати його цілісність, вміти правильно оцінювати інформацію, що надходить із зовнішнього середовища, на предмет її достовірності та об'єктивності, несуперечності та адекватності, значущості та цінності, вміти давати їй правову оцінку;
- облік особливостей і пізнавальних інтересів кожного суб'єкта у відповідності з його природними здібностями і психологічним типом.

Забезпечення інформаційної безпеки має отримати відповідне відображення в змісті освіти, у змісті предмета «Інформатика». Суб'єкт освіти повинен навчитися розуміти проблеми інформаційної безпеки, зберігати суб'єктну та об'єктну сфери суспільства, вміти жити в єдності з природою і навколишнім світом. Стан інформаційної безпеки має стати частиною загальної інформаційної культури людства, а знання основ забезпечення інформаційної безпеки – частиною особистої інформаційної культури кожного громадянина. Слід погодитися з думкою авторів [22, с. 42], що суб'єкт освітньої діяльності повинен володіти не тільки зростаючою за обсягом і якістю інформаційно-комунікативною компетентністю, але й соціальної, інформаційно-правової, яка передбачає знання і дотримання відповідних соціальних та інформаційно-правових норм.

Інформаційна культура здобувача освіти повинна включати в себе і культуру особистої безпеки. Інакше людина, яка вміє будувати конструктивні і продуктивні відносини з середовищем, медіа середовищем, може так захопитися ними, що стане «бранцем» кіберпростору, «сама структура віртуального простору веде людину зовсім в іншому напрямку, відмінному від його первісної інтенції.

3. **Проблема відбору викладачем навчальної інформації**

Особливо гостро ставиться проблема інформаційної безпеки у сфері освіти у зв'язку з її інформатизацією. Все більше з'являється в мережі Інтернет різних освітніх ресурсів. На відміну від друкованої навчально-методичної літератури, яка проходить експертизу, в Інтернеті навчальний матеріал може розмістити будь-який бажаючий. Експертиза інформаційних освітніх ресурсів неможлива. Адже величезний обсяг інформації та комерційні умови доступу не завжди дозволяють оцінити якість таких ресурсів, грамотність, наукову достовірність [23].

Необхідні цілеспрямованість і критерії відбору інформації з цифрового освітньо-наукового простору, ознаки її суттєвості і достовірності, а також уміння суб'єктів навчання критично оцінювати інформацію при самостійному пошуку в інтернеті та в інших доступних їм джерел [24].

На наростаючу проблему забезпечення інформаційної безпеки у сучасній динамічній науковій картині світу молодих

вчених та студентів, свого часу В. Куцаєв та інші привертали наукове суспільство [24]. Зазначена категоріє здобувачів вищої освіти часто без вагань і перевірки копіюють інформацію з Wikipedia та інших їм подібних не перевірених ресурсів до рефератів, дисертацій. В результаті відбувається спотворення передачі надбання суспільства наступним поколінням.

Будь-яка інформація здатна чинити певний вплив на людину, в тому числі на суб'єкта освіти, – інформаційно-пізнавальне, соціокультурне, психологічний. Це інформаційно-психологічний вплив може бути як позитивним (достовірна, якісна інформація), так і негативним (недостовірна, неякісна інформація – дезінформація). Необхідно навчити здобувачів освіти оцінки та диференціації інформації, стійкості до можливих негативних інформаційно-психологічних впливів, активного протистояння і конструктивної протидії їм. Необхідно формування критичного ставлення до інформації та критичного мислення суб'єкта освіти, які передбачають створення базового ставлення до себе і світу, передбачає варіативну, самостійну, осмислену позицію. Ця позиція значно підвищує надійність освіти – тому що воно стає усвідомленим і рефлексивним і підвищує комунікативний потенціал особистості».

Критичне ставлення здобувача освіти до інформації можна ідентифікувати як:

- здатності до осмислення і диференціювання сприйманої інформації;
- здатності до системного аналізу інформації на основі застосування до неї критеріїв пошуку і інших ознак;
- здібності до визначення синтетичних властивостей досліджуваної (аналізованої) інформації;
- здібності до створення похідної інформації на підставі ефективного використання інформаційних ресурсів середовища;
- здатності до систематизації інформації на підставі її інваріантних відносин і закономірних взаємозв'язків.

Отже, критичне ставлення до інформації – це компонент системи оцінки інформації у всіх її аспектах: змістовних і формальних, експертних і технологічних, методичних та алгоритмічних. Критичне ставлення особистості до інформації тягне за собою формування її критичного мислення як якісної характеристики, що виражається в інваріантної стійкості до негативних інформаційно-психологічних впливів та протидію їм.

4. **Проблема захисту цифрового освітньо-наукового простору закладу освіти від внутрішніх та зовнішніх загроз безпеки інформації**

Проблеми інформаційної безпеки мереж ЗВО набагато ширші, різноманітніші і гостріші, ніж в інших системах. Це пов'язано з такими особливостями:

- мережа закладу вищої освіти будується, як правило, на основі мізерного фінансування (обладнання, кадри, неліцензійне програмне забезпечення);
- зазвичай мережі не мають стратегічних цілей розвитку, а саме топологія мереж, їх технічне та програмне забезпечення розглядаються з позицій поточних завдань;
- в одній корпоративній мережі ЗВО вирішуються дві основні задачі: забезпечення освітньої та наукової діяльності і вирішення завдання управління освітнім та науковим процесами;
- корпоративні мережі гетерогенні як за обладнанням, так і за програмним забезпеченням у зв'язку з тим, що створювалися протягом тривалого періоду часу для різних завдань;
- плани інформаційної безпеки, як правило, або відсутні, або не відповідають сучасним вимогам.

У закладі освіти можлива низка як внутрішніх, так і зовнішніх загроз безпеки інформації [25]:

– спроби несанкціонованого адміністрування баз даних;

– дослідження мереж, несанкціонований запуск програм з аудиту мереж;

– видалення інформації, у тому числі бібліотек;

– запуск на виконання ігрових програм;

– установка вірусних програм і троянських коней;

– сканування мереж, у тому числі інших організацій через Інтернет;

– несанкціоноване скачування з Інтернету неліцензійного програмного забезпечення та інсталяція його на робочі станції;

– пошук — дірок у операційній системі, міжмережевих екранах;

– спроби несанкціонованого віддаленого адміністрування операційних систем;

– сканування портів тощо.

Проаналізувавши загрози інформаційної безпеки ЗВО можна запропонувати систему захисту, яка включає в себе чотири етапи:

1 етап – визначення та аналіз загроз інформаційної безпеки ЗВО;

2 етап – розроблення системи захисту інформації в ЗВО;

3 етап – реалізація плану захисту інформації;

4 етап – керування та контроль за функціонуванням системи захисту інформації.

ВИСНОВКИ

Отже, суб'єкту освітньої діяльності необхідна особиста культура інформаційної безпеки як складової інформаційної культури. Цей умовивід випливає з наступних міркувань:

1) впровадження інформаційних технологій в освітню діяльність, інтеграція педагогічних та комп'ютерних технологій в навчанні без прив’язки до забезпеченням інформаційної безпеки істотно підвищують ризик прояву інформаційних загроз, захисту даних, інформації тощо;

2) надмірне захоплення спілкуванням з віртуальним світом так само шкідливе, як і через недостатню увагу до них. При відсутності «живого» спілкування з світом у людини притуплюються природні почуття, збіднюється духовний світ, він стає добровільним «бранцем» віртуального світу. Віртуальні цінності можуть стати для нього більш важливими, ніж реальні.

Важливим компонентом інформаційної культури є культура інформаційної безпеки, розглянута в двох аспектах:

1) безпека інформаційного цифрового освітньо-наукового середовища і її компонентів, засобів, ресурсів, технологій;

2) безпека суб'єктів середовища – як фізична, так інтелектуальна – в разі можливого негативного впливу середовища.

Таким чином, формування інформаційної культури в освітньому процесі є багатоплановим поетапним процесом безперервної інформаційної підготовки здобувачів освіти. Саме рівень інформаційної культури є показником готовності суб'єкта до навчання і самоосвіти, розвитку і саморозвитку і характеризує ефективність використання інформації і інформаційних ресурсів в освітній та професійній діяльності в інформаційному просторі при обов'язковому забезпеченні вимог інформаційної безпеки.

REFERENCES

1. **Kozubtsov I.M., Khlaponyn Yu.I., Protsiuk Yu.O.** (2022). Metodolohichni osnovy pidhotovky fakhivtsiv informatsiinoi bezpeky v tekhnichnykh VNZ: filosofsko-tekhnichnyi aspekt. Informatsiina bezpeka. Naukovyi zhurnal. Skhidnoukrainskyi natsionalnyi universytet im. Volodymyra Dalia, 35-41.
2. Pro skhvalennia Stratehii rozvytku vyshchoi osvity v Ukraini na 2022-2032 roky. Rozporiadzhennia Kabinetu Ministriv Ukrainy №286-r (2022). https://zakon.rada.gov.ua/laws/show/286-2022-h
3. **Kozubtsov I.M., Beskrovnyi O.I., Kozubtsova L.M., Palahuta A.M., Myronenko O.V.** (2022). Tendentsii u osvitno-naukovomu prostori: problemy ta ryzyky. Visnyk Kremenchutskoho natsionalnoho universytetu imeni Mykhaila Ostrohradskoho, 1(132), 40–48.
4. **Kozubtsov I.M., Kozubtsova L.M., Palahuta A.M., Snovyda V.Ie., Sukhomlynova O.V.** (2023). Systematyzatsiia pidkhodiv do navchannia zdobuvachiv vyshchoi osvity v «tsyfrovomu osvitn-naukovomu seredovyshchi». Naukovi innovatsii ta peredovi tekhnolohii, 1(15), 373-383.
5. OECD (2002). Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.

https://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm.
6. OECD (2015). Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris.DOI: http://dx.doi.org/10.1787/9789264245471-en.
7. Creation of a global culture of cybersecurity. UN Council Resolution. (2003). https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement.
8. **Abdurazakov M., Korotenkov Yu., Muhidinov M.** (2016). Educational space representation in cyberspace. International Conference "Education *Environment for the Information Age*" (EEIA-2016), 29, 01001, DOI: http://dx.doi.org/10.1051/shsconf/20162901001.
9. **Benkler Y.** (2006). *The wealth of networks: How social* production *transforms markets and freedom*. New Haven, London: Yale University Press.
10. **Kopecký K., Szotkowski R., Krejčí V.** (2012). The risks of Internet communication. *Procedia* – Social *and Behavioral Sciences*, 69, 1348-1357.
11. **Livingstone S., Haddon L.** (2008). Risky experience for children online: Charting European research on children and the Internet. *Children and Society*, 22(4), 314-323.
12. **Livingstone S., Smith P.** (2014). Annual research review: Harms experienced by child users of online and mobile technologies: the nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of Child Psychology and Psychiatry*, 55(6), 635-654.
13. **Pleshakov V.** (2011). Teoryia kybersotsyalyzatsyy. M.: «Homo Cyberus».
14. **Kozlov O., Guzikova L.** (2017). Information security as requisition of educational organization activity. *Teaching Methodology in Higher Education*, 6(22), 43-50.
15. **Khloponin Yu., Kozubtsova L., Kozubtsov I.** (2021). On the need to ensure cybersecurity in educational information systems and technologies. *Scientific and Practical Cyber Security Journal* (SPCSJ), 5(3), 25-29.
16. **Berdyaev N.** (2022). Man and Machine (Problem of Sociology and Metaphysics of Technology). Courier of Kutafin, (4), 246-256.
17. **Schwab K., Malleret T.** (2020). COVID-19: *The Great* Reset. *Edition 1.0.* Switzerland. Cologny/Geneva: Forum publishing World Economic Forum.
18. **Abdurazakov M., Batygov Z.** (2021). Modern problems of ensuring information security in the educational and pedagogical sphere. *Informatics and Education*, 36(10), 57-64.
19. Pro skhvalennia Kontseptsii rozvytku tsyfrovoi ekonomiky ta suspilstva Ukrainy na 2018-2020 roky ta zatverdzhennia planu zakhodiv shchodo yii realizatsii. Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 17.01.2018 № 67-r. https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text.
20. **Abdurazakov M.** (2018). Teacher-student interaction in information-related educational environment: The culture of knowledge – cognition – informational communication. *Pedagogy*, (9), 39-46.
21. **Kyrylenko N.M.** (2012). Problemy informatsiinoi bezpeky osvitnoho seredovyshcha vyshchoho navchalnoho zakladu. Informatsiino-telekomunikatsiini tekhnolohii v suchasnii osviti: dosvid, problemy, perspektyvy: tretia mizhnarodna naukovo-praktychna konferentsiia. Lviv, 1, 149-151.
22. **Kozubtsov I.M., Kutsaiev V.V.** (2013). Filosofiia informatsiinoi bezpeky v umovakh yii kibernetychnoho rozpovsiudzhennia v suchasnoi dynamichnii naukovoi kartyni svitu na prykladi nadannia znan molodym vchenym ta studentam. Hileia: naukovyi visnyk. Zbirnyk naukovykh prats, 73(6), 291–293.
23. **Kukharska N.P.** (2015). Otsinka informatsiinoho seredovyshcha vyshchykh navchalnykh zakladiv ta analiz zahroz yoho bezpetsi. Informatsiino-komunikatsiini tekhnolohii v suchasnii osviti: dosvid, problemy, perspektyvy», 2, 31-35.

Problems of ensuring information security by subjects of educational activity in the digital educational and scientific environment of educational institutions

Ihor Kozubtsov, Nataliia Zinchenko, Andrei Kotenko, Ihor Averichev

Abstract: The article discusses the current problems of ensuring information security by educational entities in the digital educational and scientific environment of educational institutions. In times of war (emergencies, pandemics), the educational activities of subjects are moving to the digital educational and scientific environment of educational institutions, where they have proven themselves effectively. Since all educational processes of educational institutions are

information-based, and their distortion can lead to negative consequences, there is a need to ensure information security. Based on this, the strategic goal of ensuring information security in the digital educational and scientific space of an educational institution is to form personal information and cybersecurity in cultural subjects. Therefore, it is necessary to form information competence and personal culture of information security in students during their studies, especially for students of the humanitarian profile. Thus, the purpose of the article is to review the problems of ensuring information security by educational entities in the digital educational and scientific environment of educational institutions. Based on the results of the study, the author distinguishes and considers the multidimensionality of information security in the education system, information protection of the subject of educational (training) activity, the problem of selection of educational information by a teacher, and the problem of protecting the digital educational and scientific space of an educational institution from internal and external threats. It is confirmed that the formation of information culture in the educational process is a multifaceted, phased process of continuous information training of students. It is the level of information culture that is an indicator of the subject's readiness for learning and self-education, development and self-development and characterizes the effectiveness of the use of information and information resources in educational and professional activities in the information space with the obligatory provision of information security requirements.

Keywords: information security, competence, information culture, digital educational and scientific environment, higher education institution.

Adaptive Software Component for Predicting Energy Consumption of an Electric Vehicle on a Planned Route

Dmytro Humennyi[1]

[1] N-iX Ltd.; Kyiv National University of Construction and Architecture
Povitryanykh Sil avenue, 31, Kyiv, 03037
[1] apollo.d.g@gmail.com, https://orcid.org/0000-0001-6736-0543

Received 20.08.2024, accepted 01.11.2024
https://doi.org/10.32347/uwt.2024.15.1205

Abstract. This paper presents the development of an adaptive software component for forecasting the energy consumption of electric vehicles along planned routes. It includes a conceptual framework, architectural design, and modular software composition, introducing mathematical models for managing energy consumption with a model-based design approach for precise predictions and optimization. The importance of data sources such as route information, vehicle condition, and driver behavior is emphasized to create a comprehensive state vector for energy optimization.

Following ISO 26262 and A-SPICE 3.1 standards, the implementation uses a model-based approach with Simulink and aligns with the V-Model for rigorous validation. The methodology details segmenting routes and optimizing energy consumption for each segment, considering driving style and environmental conditions. The gradient search method adjusts energy consumption to minimize usage while maximizing comfort and ensuring route completion.

This research lays the groundwork for future advancements in predictive energy management systems for electric vehicles, with potential real-world applications. Future work will focus on refining predictive models, exploring machine learning for improved accuracy, and integrating real-time data from connected vehicle technologies for dynamic optimization.

Keywords. Electric vehicles, energy consumption prediction, model-based design, energy management system, route optimization, driving behavior, adaptive software, ISO 26262, A-SPICE 3.1, gradient search, Simulink, vehicle state vector, modular architecture, predictive models, machine learning, real-time data integration, connected vehicle technologies, battery management, comfort optimization.

Dmytro Humennyi
Ph.D., Engineering Manager at N-iX, Associate Professor of the Department of Cybersecurity and Computer Engineering

INTRODUCTION

Modern cars are complex networks of computing and control devices, each with its own topology that imposes specific properties, limitations, and norms. This distributed system for data collection, communication, and control enables the formation of a detailed state vector, accurately describing the car's condition for effective technical management decisions.

Simultaneously with the development of control means and internal communication of the car, its energy system also develops. This is particularly relevant for electric vehicles equipped with mobile power plants or electric batteries.

The advantages of using electric power elements for vehicle movement are significant and varied. Firstly, electric vehicles (EVs) help reduce or even eliminate fuel costs, as electricity is cheaper and more stable in price compared to gasoline [1], [2]. Secondly, EVs contribute to environmental conservation by producing fewer emissions than their gasoline counterparts, thus aiding in the fight against climate change [3], [4]. Additionally, electric vehicles support energy independence, reducing reliance on imported oil and promoting the use of locally sourced renewable energy [1], [2].

However, there are still unresolved issues related to the vehicle's range on electric traction. Modern vehicles are limited in their range to approximately 100-450 kilometers (about 279.62 mi) per charge, depending on the model and battery capacity [3], [12].

The issue of increasing the range is addressed by several approaches, including improvements in battery technology, development of more efficient power management systems, and the expansion of charging infrastructure [2], [4]. Another approach to increasing the vehicle's range is to introduce methods of energy consumption prediction with the search for an optimal consumption strategy for each energy consumer. This strategy also considers the dependence of expenses on driving style.

Therefore, predicting the energy consumption of a vehicle for moving along a given trajectory is the subject of this study. The object of the research is the development of application-level software (business logic) for predicting energy consumption and forming a system of recommendations for the driver.

The task of minimizing a vehicle's energy consumption, as well as the task of predicting its range, is primarily a task for battery engineers and component designers of the car both in its details and as a finished product. But secondly, it is also a task for companies that develop software, especially in connection with the concept of building a Software-defined vehicle. Thus, N-iX corporation, within which these studies were conducted, approached the described subject through the prism of Predictability of energy consumption and energy management system, which is a software solution for vehicle energy management.

PROBLEM STATEMENT

The objective of this research is the development of a composition of software tools and individual software components for a vehicle that enables the optimization of the electrical consumption scenario of each critical node of the vehicle. This ensures the achievement of the planned route with the maximum level of comfort.

It should be noted that the problem involves solving a multi-criteria optimization task of a bi-criteria optimization of a multi-parameter function with nonlinear dependencies between parameters.

Two criteria are proposed:

1. Ride comfort (minimizing the deviation between the ride properties set by the driver and the actual battery capacity allocated to each consumer).

2. Minimization of energy consumption (minimizing the energy consumption of each analyzed vehicle energy consumer).

Regarding energy consumers, the aim is to create a software composition that allows for the customization of energy consumers. The basic composition should manage the main consumers, namely Powertrain, HVAC, Suspension, Battery Climate Control System, and expenses related to driving style. Additional consumers can be added by creating corresponding software components and adding them to the composition.

Regarding information sources, several information sources are needed for energy management, which can be grouped as follows:

- Information about the route;
- Information about the vehicle's condition;
- Information about the driver and driving style.

All three basic information sources create a state vector of the vehicle. This state vector, together with the criteria for optimizing energy consumption, forms the problem statement for nonlinear optimization. Solving this problem leads to obtaining an optimal energy consumption scenario.

MATERIALS AND METHODS

According to the defined object and subject of the research, as well as the aim of the work, the outcome is the creation of a software composition that can be applied as business logic and function as an application within the ECU. The composition should meet the design, documentation, construction, testing, and integration requirements according to norms, standards, frameworks, and guidelines applicable in the automotive sector.

This composition includes an ASIL A class component. The SDLC V-Model and ISO 26262 [15] and ISO 33050 [16] standards were applied for its development. Project measures, as well as processes during preparation, development, and support, complied with the A-SPICE 3.1 framework. Technologically, they correspond to level 3 (Established). The teams applied the SAFe 6 project management methodology.

A Model-based approach based on Simulink (license 41148027) was used. This approach was employed from the requirement engineering stage to the integration stage. The software component includes means for interacting with the driver. For demonstrating the interaction, a virtual reality solution based on Carla Simulation was created. Physical steering wheels and pedals from Logitech were used for driver input. C99 and Python layers were used to integrate Carla with Simulink and the steering wheel and pedals with Simulink.

For obtaining route data and information about road temperature and quality, Google Maps services were used. Python scripts were employed to link Google Maps with Simulink.

The MathWorks ecosystem, including Simulink, System Composer, Requirement Toolbox, Embedded Coder, Advisor, Simulink Test, Powertrain, and Instrument Control Toolbox (license No. 41148027), was used for building the composition, components, integration, and requirement engineering.

THE TASK OF FINDING THE OPTIMAL ENERGY CONSUMPTION SCENARIO

There are several approaches to formulating the task of finding the optimal energy consumption scenario. For example, [8], [9] define it as minimizing energy expenditure. In contrast, [10], [11] use Markov chains to predict step-by-step expenses.

At N-iX Corporation, we approached this task creatively. We decompose the entire vehicle route into segments (the length of the segment is chosen dynamically, depending on changes in its characteristics. For example, if the road is straight, without significant changes in road angle or temperature, we consider this part of the route as one segment). After decomposition, we request the required current. This request is made to the consumption model, which we describe for each consumer. Thus, we estimate consumption for each segment of the route we need to cover. Then we request the driver's profile. Based on statistical data, we understand the driver's driving style. We interpret this style as an over-expenditure coefficient for each consumer. Next, having the consumption values for all consumers for all route segments, we can estimate whether the battery charge will be sufficient to cover this route.

Obviously, the route can be covered quickly or slowly, with the air conditioner at maximum power or turned off, using adaptive suspension, or switching it to passive mode. And it is also obvious that all this changes energy consumption. Therefore, the task of finding the optimal energy consumption scenario is to find the operating modes of each consumer so that we can cover the planned route.

It is important to note that the best chance of reaching the planned route is to turn off everything that is possible and switch the powertrain to the highest economy mode. But this is not a comfortable ride. Therefore, we introduced another criterion – maximizing comfort.

Thus, if we understand that we can reach the destination, and if the air conditioner operates in normal mode (provided that the driver wants it to be turned on in normal mode), we will propose to turn it on in this mode. If we cannot reach the destination in this mode, we will propose a balanced combination of modes for all consumers to evenly reduce comfort so as not to critically reduce it anywhere.

And, obviously, if we estimate the impossibility of covering this route at all, then after the appropriate calculation, we notify the driver.

Thus, the mathematical model for finding the optimal energy consumption scenario is proposed as follows:

1. Minimization of energy consumption (E):
    a. Minimization of the total energy consumption of each component.

b. We define the function E as the sum of the energies consumed by each component:

$$E = E_{powertrain} + E_{HVAC} + E_{suspension} + E_{batteryCC} + E_{driver}$$

2. Maximization of comfort (C):
   a. Minimization of the deviation between the ride properties set by the driver and the actual battery capacity allocated to each consumer.
   b. We define the comfort function (C):

$$C = -\sum_i^{\max(i)} \left(\dot{E}_\iota - E_i\right)^2,$$

where $\dot{E}i$ - is the desired energy consumption set by the driver for the i-th component, and Ei - is the actual energy consumption for the i-th component.
Then, the Lagrange function for this task can be written as follows:

$$L(E, \lambda) = E + \lambda(C - \alpha)$$

where λ - is the Lagrange multiplier, and α - is the constant that determines the balance between energy consumption and comfort.

We form a system of equations. So, to find optimal values, it is necessary to find the partial derivatives of the Lagrange function with respect to each variable and set them to zero:

$$\frac{\partial L}{\partial E_i} = 0, \ \frac{\partial L}{\partial \lambda} = 0 \quad (1)$$

For the segment of the route, we form a current request:

$$I_{segment} = \sum_i^{\max(i)} \frac{E_i}{U_i}$$

where U_i - is the network voltage for the i-th component.
Driver profile consideration is carried out as follows:

$$E_{driver} = \beta \sum_{segment}^{all\ segments} E_{segment}$$

where β - is the coefficient that accounts for the driver's driving style.

OPTIMIZATION OF CONSUMPTION FOR EACH SEGMENT OF THE ROUTE

The objective function will be as follows:

$$MIN\ E = E_{powertarin} + E_{HVAC} + E_{suspension} + E_{driver}$$

with constraints:
- Constraints on energy consumption for each component:

$$E_i \leq E_{max,i},\ i = 1, \dots, n$$

- Constraints on total energy consumption:

$$\sum_{i=1}^{n} E_{i \leq E_{total}}$$

- Constraints on comfort reduction:

$$C = -\sum_{i=1}^{n} \left(E_i - \dot{E_{total}}\right)^2 \geq C_{min}$$

Finding optimal values E, λ is based on solving equation (1), which can be presented in the following form:

$$\frac{\partial L}{\partial E_i} = \frac{\partial}{\partial E_i}\left(E + \sum_{j=1}^{m} \lambda_j(E) - b_i\right) = 0 \quad (2)$$

for constraints: $g_j(E) - b_j = 0,\ j = 1, \dots, m$.

This completes the formulation of the optimization task, ensuring a balanced approach to minimizing energy consumption while maximizing driver comfort.

FORMATION OF THE SOFTWARE COMPOSITION

According to the A-SPICE framework, the software development process includes a series of preliminary stages. These stages will be omitted in this publication as they fall outside the scope of its scientific interest. The system

engineering process (SYS A-SPICE group) is partially considered here, as well as the ENG group, in accordance and proportionate to the relevance of the subject of the work. The SUP and MNG groups are completely omitted in the publication.

DISTINGUISHED COMPOSITION COMPONENTS

The composition is divided into three groups of components. It is assumed that all components will be deployed on a single ECU.

First Group - Core Composition. Contains components that are not subject to customization. This group of components includes:

- Prediction SWC;
- Powertrain SWC;
- DriverProfile SWC.

Second Group – Plugins. Contains mathematical models of consumers. It allows for the current request to the power source. It also allows for modeling current consumption under different operating modes in search of the optimal combination. Each of the plugins has two subcomponents. The first subcomponent is used for iterating through energy consumption modes in search of an optimal configuration. The second subcomponent provides a current request in the selected mode depending on the operating conditions. This group's software components allow for customization according to the vehicle's specifications. Typical representatives of the second group of software components include:

- ClimatControl SWC;
- Suspension SWC;
- ExternalTemperature SWC;
- TirePressure SWC.

Third Group – Wrappers. They are used for software testing, debugging, and demonstrating its operation. Typical representatives of software components in this group include:

- GoogleMap SWC;
- HMI SWC;
- Modem SWC.

The proposed composition of software components is shown in Fig. 1.

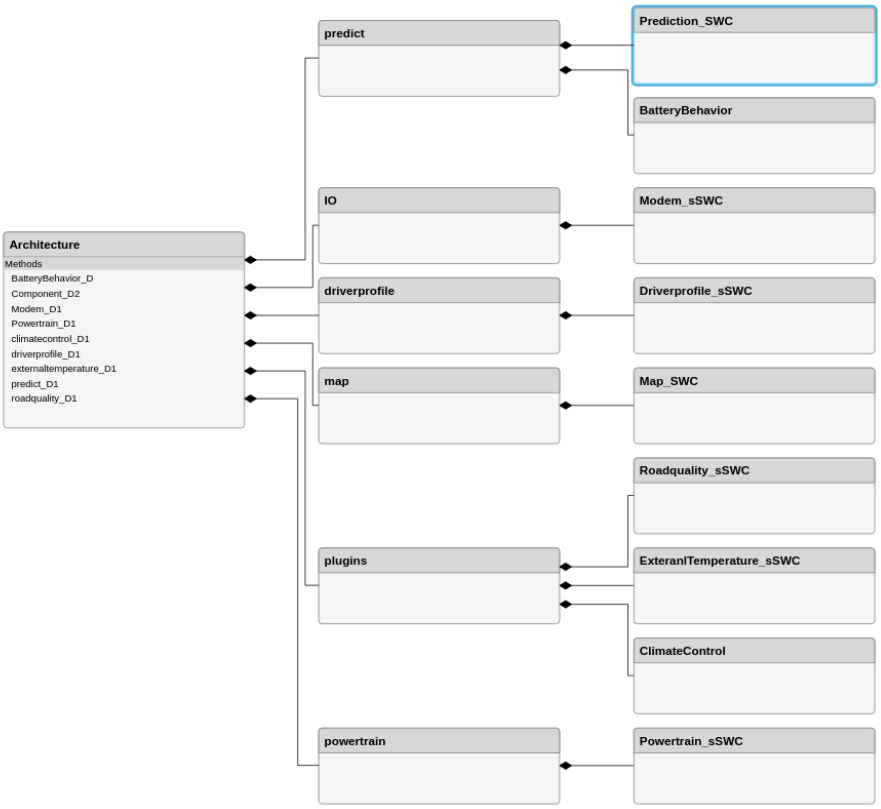


Fig. 1. Software Composition

While changing plugins should not affect the composition, the entire second group of software components is grouped into the Plugins SWC component, as shown in Fig. 2.

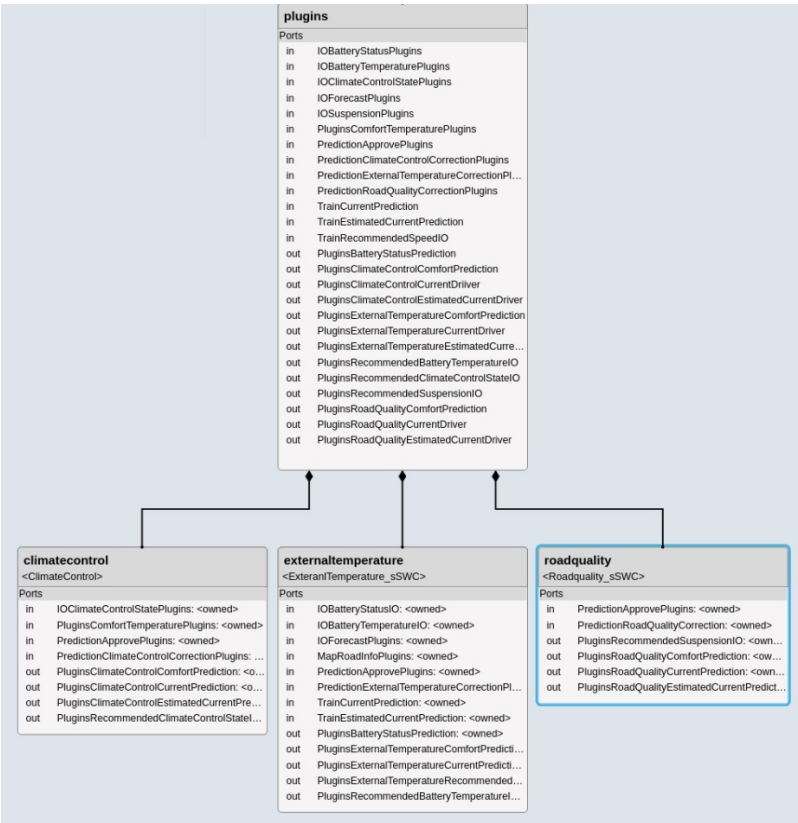


Fig. 2. Decomposition of Plugins into a Separate Group

A typical component of the composition is composed according to the MISRA AC GMG [13] or MAAB [14] guidelines. Its structure includes two subcomponents mentioned earlier (one for finding a new consumption plan using the gradient descent method, and the other for performing predictions of expenses for subsequent parts of the route). The typical structure of such a software component is shown in Fig. 3.

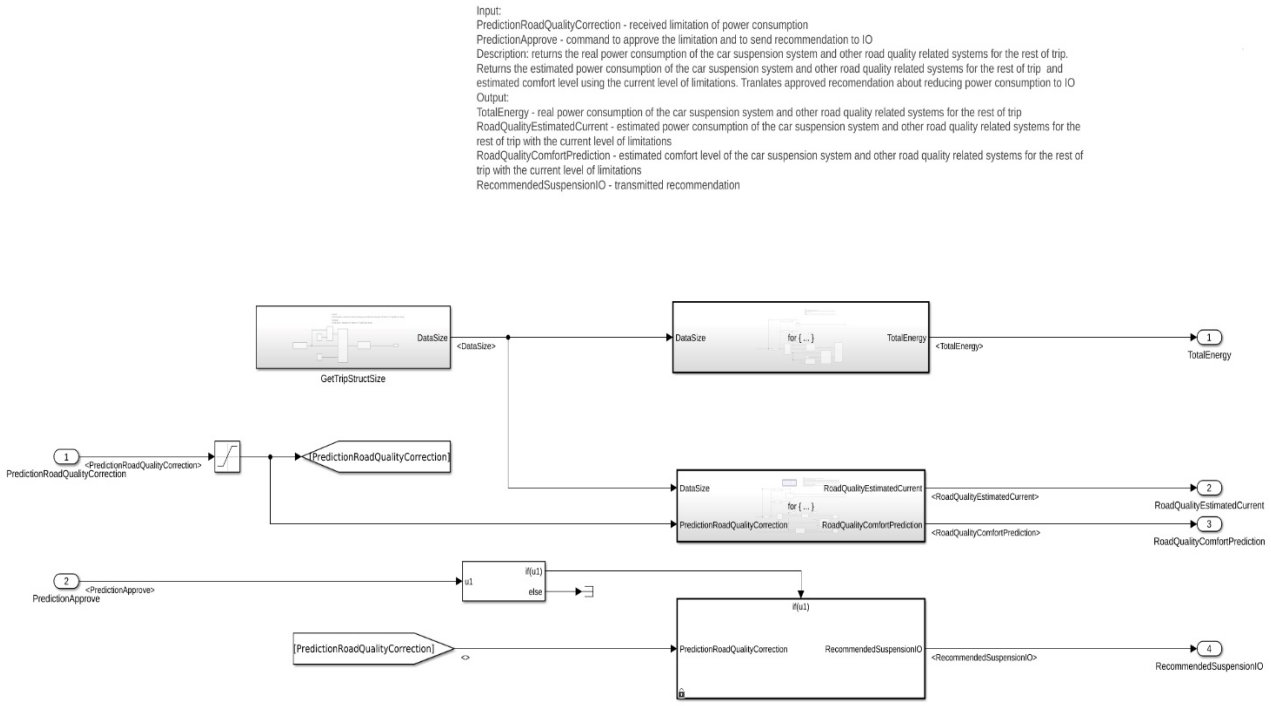


Fig. 3. Typical Structure of a Software Component with Two Separate Subcomponents

The Prediction SWC and DriverProfile SWC software components are shown in Figures 4 and 5, respectively.

The structure of the Prediction SWC includes two subcomponents. One performs the tasks of estimating costs for the entire route that the car still has to cover. The second subcomponent searches for the optimal energy consumption scenario according to system (2). The structure of the DriverProfile SWC includes logic for accruing and writing off "penalties" imposed on the driver for ignoring recommendations. Penalties are deducted for following these recommendations. The accrual and deduction model is hysteresis-based and is set by interpolation tables.

The mathematical model of DriverProfile SWC is shown below.

1. Penalty Accrual:

$$P_{t+1} = P_t + \alpha E_t$$

2. Penalty Deduction:

$$E_t = \frac{1}{2}\sum_{i=1}^{n}(r_i - a_i)^2$$

3. Backpropagation Update:

$$P_{t+1} = P_t - \beta R_t$$

$$\omega_{t+1} = \omega_t - \eta \frac{\partial E_t}{\partial \omega}$$

4. Hysteresis Effect:

$$P_{t+1} = \{\{P_t + \alpha E_t \ if \ E_t > \delta\} \ OR \ \{P_t - \beta R_t \ if \ E_t \leq \delta\}\}$$

For driver from

$$D = \{d_1, d_2, \ldots, d_m\}$$

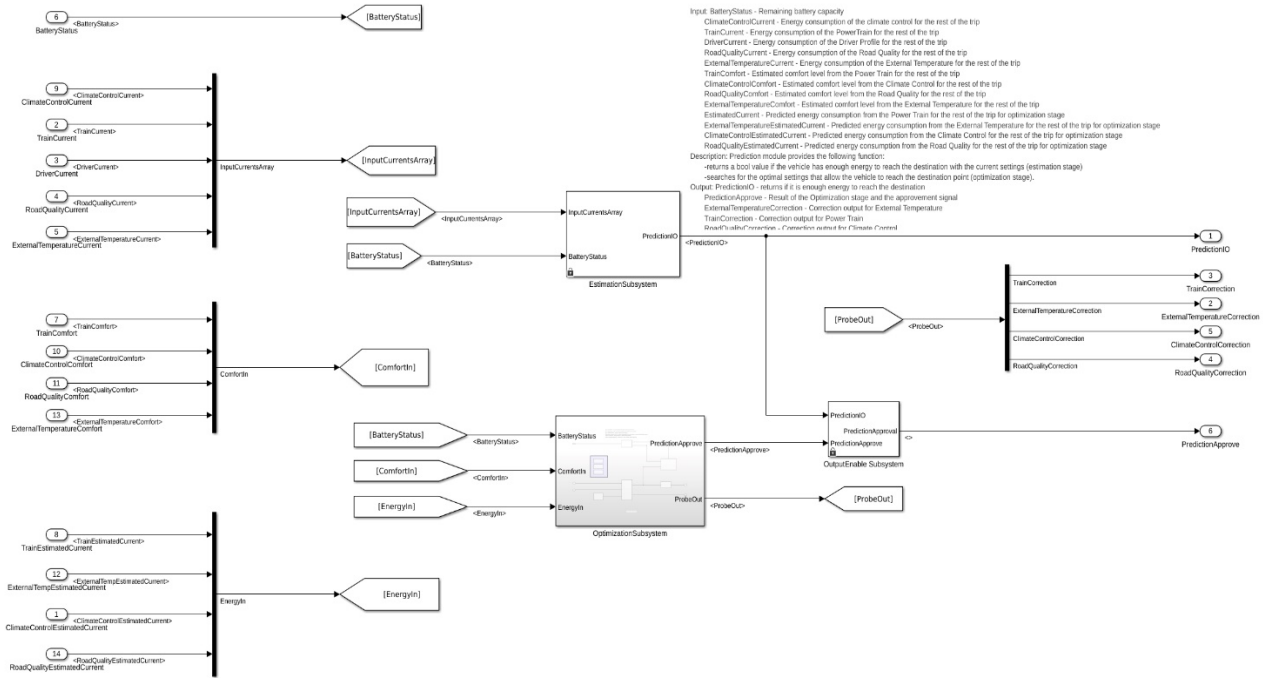


Fig. 4. Prediction SWC Software Component Model

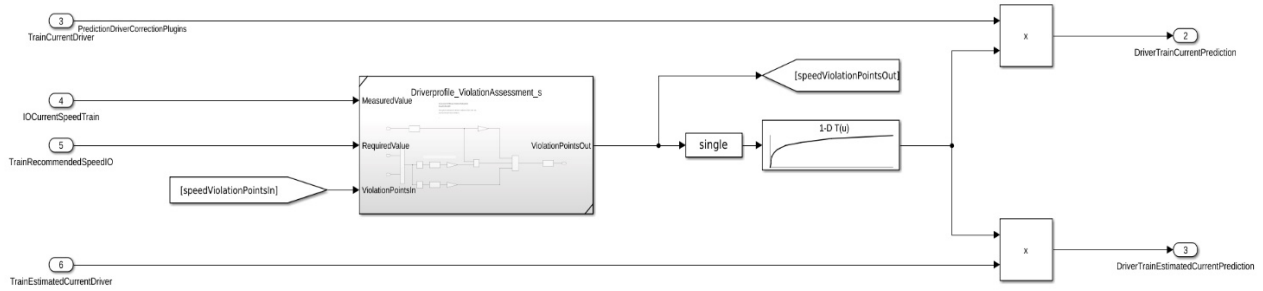


Fig. 5. DriverProfile SWC Software Component Model (the main subsystem only)

The mathematical model, which is part of the Powertrain SWC, cannot be disclosed due to NDA.

SETTING TRIGGERING TIME OF COMPONENTS WITH EACH OTHER

Time-sampling for all SWC components is crucial for ensuring synchronized and efficient system operation. Each SWC component triggers at specific intervals, which are recorded as time samples. These time samples help in understanding the interaction and behavior of components under different operating conditions.

In the histogram (Figure 6), we observe the distribution of triggering times for various components:

- Prediction SWC triggers primarily between 10-13 milliseconds.
- Powertrain SWC triggers mainly between 15-18 milliseconds.
- DriverProfile SWC triggers mostly between 19-22 milliseconds.
- ClimatControl SWC triggers predominantly between 25-28 milliseconds.
- Suspension SWC triggers primarily between 30-33 milliseconds.
- ExternalTemperature SWC triggers mainly between 35-38 milliseconds.
- TirePressure SWC triggers mostly between 40-43 milliseconds.
- GoogleMap SWC triggers predominantly between 45-48 milliseconds.
- HMI SWC triggers primarily between 50-53 milliseconds.
- Modem SWC triggers mainly between 55-58 milliseconds.

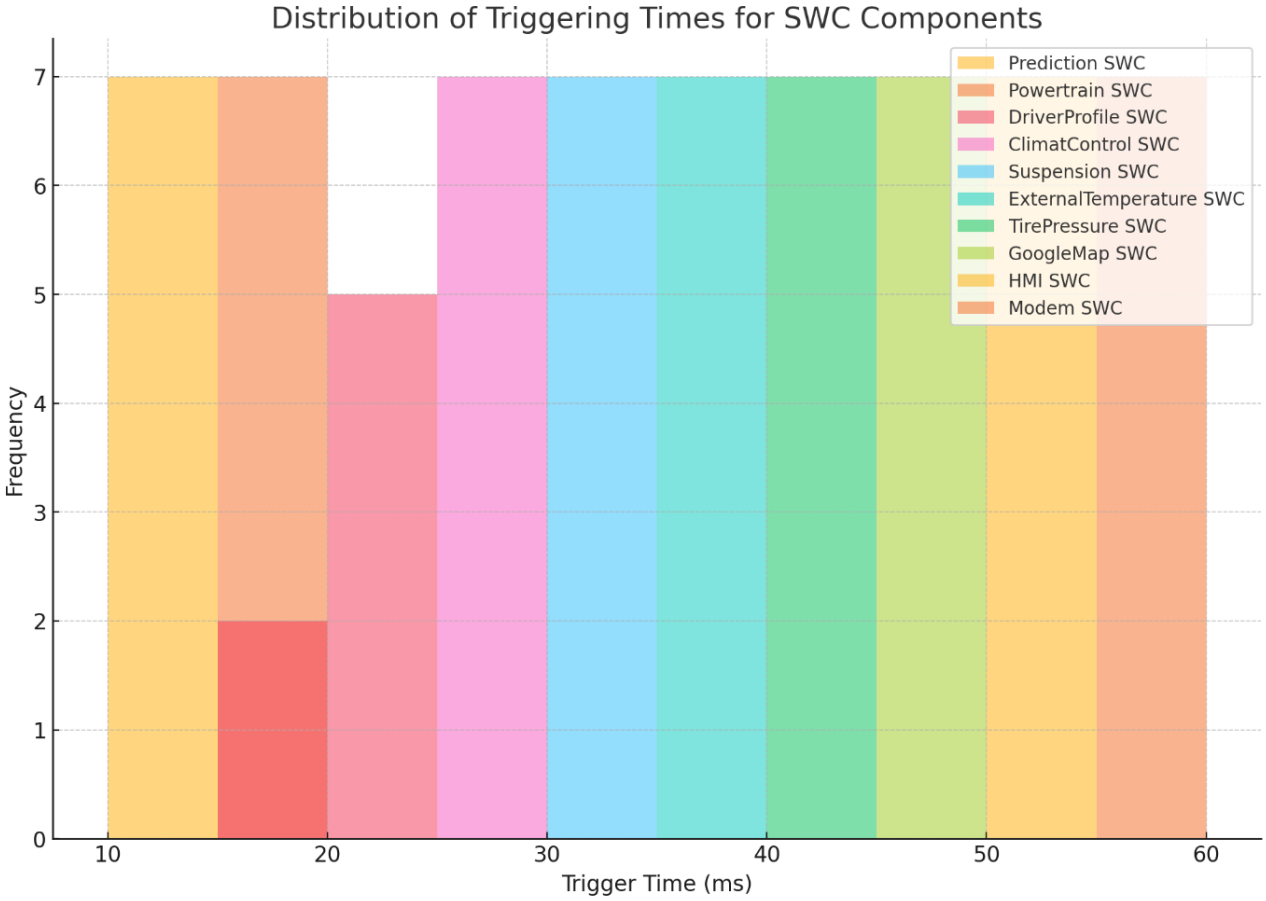


Fig. 6. Timesample histogram

This detailed time-sampling allows for precise coordination and optimization of component interactions, ensuring that the system operates smoothly and efficiently. By analyzing these time samples, we can identify potential areas for improvement in synchronization and performance, leading to a more robust and reliable system.

COMPONENTS FOR ENVIRONMENT VIRTUALIZATION AND STUB REALIZATION

The construction of these components significantly depends on the available software licenses. By basing solutions on Simulink, an alternative approach can be taken. Since this software section is more for demonstrating capabilities rather than being deployed as a product, certification is not required. Therefore, the use of third-party software is acceptable.

For external solutions such as GoogleMaps, steering wheel interfaces, Carla simulation, or practically any solution outside the MATLAB ecosystem, it is proposed to use the Instrument Control Toolbox, which includes a UDP toolkit. This type of task is effectively managed using sockets.

ACHIEVING REAL-TIME

Achieving real-time operation is challenging. Simulink does not inherently support real-time execution as the simulation time of the system can differ from physical time. Real-time performance can be achieved after compiling the software product and running it as an application.

TESTING AND INTEGRATION

According to the V-Model process, testing is inseparable from the development process. Building a testing process for ASIL-A according to ISO 26262-6 [15] includes five stages, conducted sequentially. Stages and completion criteria for this composition are provided in Table 1.

In accordance with ISO 26262-6 [15] recommendations, the processes are conducted using certified tools or subject to further verification. Therefore, in this work, it is proposed to use the verified Simulink Test toolkit with additional instruments such as Test Manager, Coverage, and Reports, to remain within a single software development ecosystem.

The completion criteria for the testing stages are proposed as indicated in Table 2.

The stages "Validation of composition on virtual target (ViL)" and "Testing on real ECU (ViL)" are not completed to date. Their impact on the product will be published additionally. Accordingly, integration as an ECU application is not the subject of the current publication.

Table 1. Testing stages of software composition

Stage	Metrics	Description
Static analysis of Simulink model	Diagnostic Coverage (DC), Single Point Fault Metric (SPFM)	Model analysis to identify defects and potential problems. Measuring code coverage and diagnostic efficiency for testing evaluation.
Model unit testing (SiL)	% of tests executed, Common Cause Fault Metric (CCFM)	Executing model-level tests based on a simulation environment. Measuring the percentage of successfully executed tests and the metric for partial failures.
Integration testing of components (HiL)	% of integrated components, Probabilistic Metric for random Hardware Failures	Testing interactions between different components at the hardware level. Evaluating the percentage of successfully integrated components and integration time.
Validation of composition on a virtual target (ViL)	DC, Failures In Time (FiT)	Testing the entire composition on a virtual platform. Measuring diagnostic efficiency and the number of failures per trillion hours.
Testing on a real ECU (ViL)	FiT, Latent Fault Metric (LFM)	Testing the composition on a real ECU to verify stability and identify defects. Measuring the number of failures per trillion hours and latent faults.

Table 2. Completion criteria for testing stages

Testing stage	Completion criteria
Static analysis of Simulink model (FMEDA)	Completion of the analysis when DC ≥ 90% and SPFM ≥ 99%. All identified critical defects must be corrected and confirmed by repeated analysis.
Model unit testing (SiL)	Completion of testing when % of successful tests ≥ 95% and CCFM ≤ 1 FIT. All critical defects must be corrected and confirmed by repeated tests.
Integration testing of components (HiL)	Completion of testing when % of integrated components ≥ 95% and PMHF ≤ 10 FIT. All identified critical defects must be corrected and confirmed by repeated tests.
Validation of composition on virtual target (ViL)	Completion of validation when DC ≥ 95% and FIT ≤ 10 per trillion hours. All critical defects must be corrected and confirmed by repeated tests.
Testing on real ECU (ViL)	Completion of validation when DC ≥ 95% and FIT ≤ 10 per trillion hours. All critical defects must be corrected and confirmed by repeated tests.

IMPLEMENTATION AND PUBLICATION OF RESULTS

The results of the work have been implemented as a Proof of Concept (PoC) and have been presented at events such as MathWorks Automotive Conference 2024 [5], featured at the N-iX company booth; a MathWorks webinar titled "Energy Consumption Prediction for Electric Vehicles" [6]; and described in N-iX company publications [7].

THE AMPERE POC

From Figure 7(a), the structure of the Ampere project is evident, which is built according to the concept described in the publication. In this Proof of Concept, the focus is on cooperation with the semi-realistic environment. To achieve this, Carla, GoogleMaps, Steering, and an Android Tablet (driver authorization, destination coordinates determination, communication of optimal trip data to the driver) were used. Communication protocols UDP and ProtoBAFs were employed for this purpose.

Figure 7(b) shows the application as seen by the user.

CONCLUSION

This study details the development of an adaptive software component to predict energy consumption for electric vehicles on planned routes. It emphasizes a modular and scalable architecture, incorporating mathematical models to manage consumption levels. Key data sources such as route information, vehicle condition, and driver behavior form a comprehensive state vector for optimizing energy use.

The implementation adheres to ISO 26262 and A-SPICE 3.1 standards, using a model-based approach with Simulink, and aligning with the V-Model for rigorous testing. The gradient search method adjusts consumption to minimize energy use while maximizing comfort, ensuring the vehicle completes its route efficiently.

Components for environment virtualization and stub realization were developed using Simulink and third-party software, managing external solutions through the Instrument Control Toolbox and UDP sockets. Achieving real-time execution involved compiling the software product and running it as an application.

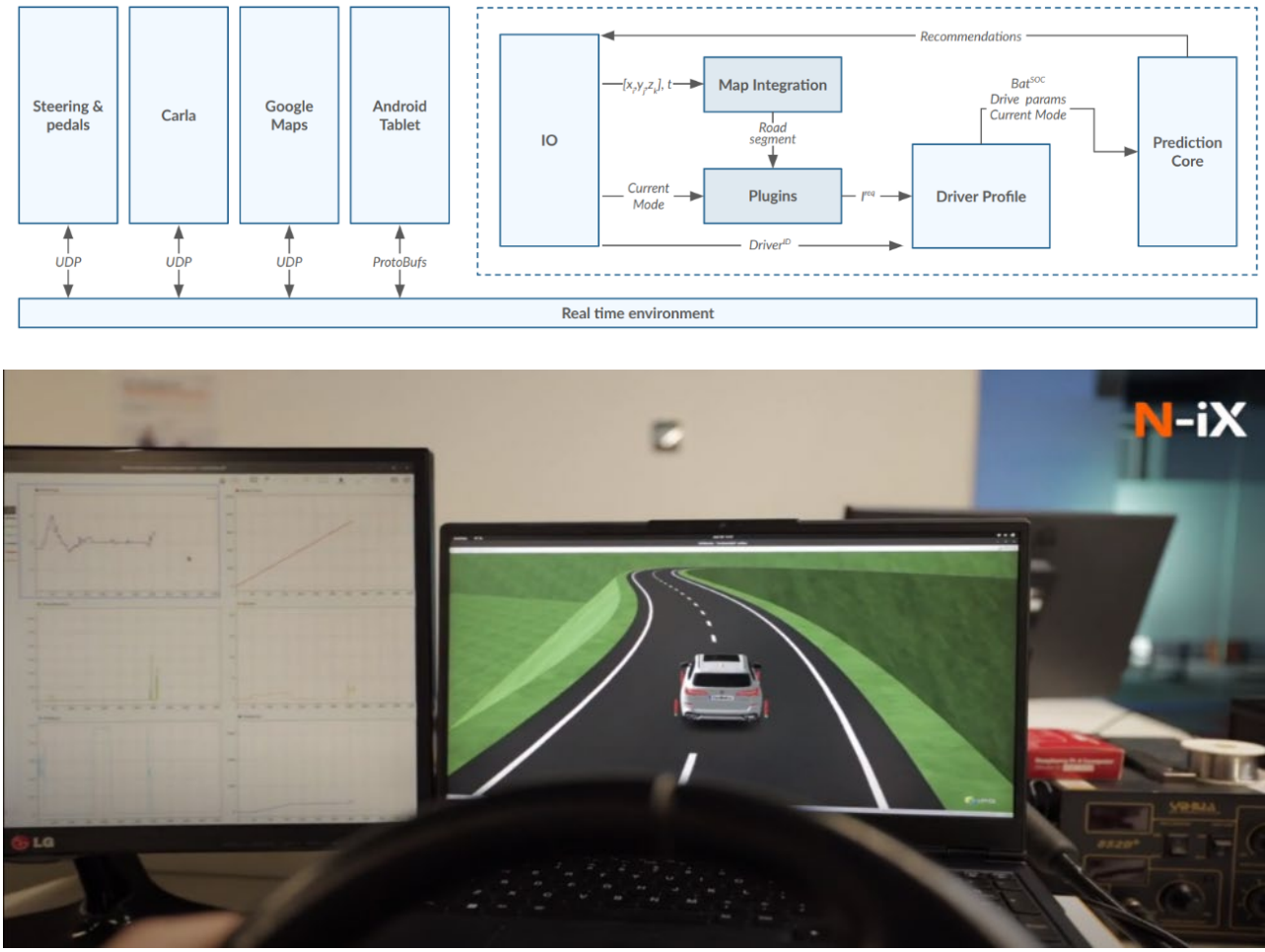


Fig. 7. The Ampere by N-iX. a - generalized view; b - user view

This Proof of Concept has been showcased at industry events, demonstrating the feasibility of advanced predictive models for energy management in electric vehicles. Future work will focus on refining predictive models, exploring machine learning for improved accuracy, and integrating real-time data from connected vehicle technologies to dynamically optimize energy consumption. These efforts aim to enhance the efficiency, reliability, and user-friendliness of energy management systems, supporting wider adoption and sustainability in the transportation sector.

By addressing these observations and incorporating the suggested revisions, the paper will improve in clarity, readability, and overall effectiveness.

REFERENCES

1. "Advantages of Electric Vehicles: Top Benefits Explained," EnergySage, accessed June 6, 2024, (2024). EnergySage.
2. "Experts Discuss Hurdles, Benefits of Electric Vehicles," Duke Today, accessed June 6, 2024, Duke Today.
3. "Electric Vehicles: Benefits, Challenges, and Potential Solutions for Widespread Adaptation," MDPI, accessed June 6, 2024, MDPI.
4. "Comprehensive Review of Electric Vehicle Technology and Its Impacts: Detailed Investigation of Charging Infrastructure, Power Management, and Control Techniques," MDPI, accessed June 6, 2024, MDPI.
5. MathWorks Automotive Conference 2024. Available at: https://www.mathworks.com/company/events/conferences/automotive-conference-stuttgart/2024.html
6. Webinar by MathWorks “Energy Consumption Prediction for Electric Vehicles.” Available at: https://www.mathworks.com/company/events/webinars/upcoming/energy-consumption-prediction-for-electric-vehicles-4331190.html
7. Predictive Energy Management for EV. N-iX Publications. Available at: https://www.n-ix.com/predictive-energy-management-for-ev/

8. **Rombaut, E., Vanhaverbeke, L., & Coosemans, T.** (2023). Energy-Optimal Speed Control for Autonomous Electric Vehicles Up- and Downstream of a Signalized Intersection. *World Electric Vehicle Journal*, 14(2), 55. https://doi.org/10.3390/wevj14020055
9. **Martinez C. M., Hu X., Cao D., Velenis E., Gao B., Wellers M.** (2016). Energy management in plug-in hybrid electric vehicles: Recent progress and a connected vehicles perspective. *IEEE Transactions on Vehicular Technology*, Vol. 66, No. 6, 4534-4549.
10. **Hannan M. A., Azidin F. and Mohamed A.** "Hybrid electric vehicles and their challenges: A review". *Renewable and Sustainable Energy Reviews*, vol. 29, 135-150, 2
11. **Amjad S., Neelakrishnan S. and Rudramoorthy R.** (2010). "Review of design considerations and technological challenges for successful development and deployment of plug-in hybrid electric vehicles". *Renewable and Sustainable Energy Reviews*, Vol. 14, no. 3, 1104-1110.
12. **Sutton R. S., McAllester D., Singh S. and Mansour Y.** (1999). "Policy gradient methods for reinforcement learning with function approximation". *Advances in neural information processing systems*, Vol. 12.
13. MISRA. (2007). "Guidelines for the application of MISRA-C:2004 in the context of automatic code generation," MISRA AC GMG.
14. MathWorks. (2019). "Modeling Guidelines for Production Code Generation," MathWorks Automotive Advisory Board (MAAB).
15. International Organization for Standardization, "ISO 26262: Road Vehicles – Functional Safety," ISO 26262:2018.
16. International Organization for Standardization, "ISO 22050: Safety of Machinery – Physiological Effects of Whole-Body Vibration," ISO 22050:2007.

Адаптивний програмний компонент для прогнозування енергоспоживання електромобіля на запланованому маршруті

Дмитро Гуменний

Анотація. У даній роботі представлено розробку адаптивного програмного компонента для прогнозування енергоспоживання електромобілів на запланованих маршрутах. Він включає концептуальну основу, архітектурний дизайн і модульну композицію програмного забезпечення, вводячи математичні моделі для управління споживанням енергії з модельним підходом до проектування для точних прогнозів і оптимізації. Важливість джерел даних, таких як інформація про маршрут, стан транспортного засобу та поведінка водія, підкреслюється для створення комплексного вектора стану для оптимізації енергії.

Дотримуючись стандартів ISO 26262 і A-SPICE 3.1, реалізація використовує модельний підхід із Simulink і узгоджується з V-моделлю для суворої перевірки. Методологія детально розподіляє маршрути на сегменти та оптимізує споживання енергії для кожного сегменту, враховуючи стиль водіння та умови навколишнього середовища. Метод градієнтного пошуку регулює споживання енергії, щоб мінімізувати споживання, максимізуючи комфорт і гарантуючи завершення маршруту.

Це дослідження закладає основу для майбутніх досягнень у системах прогнозного керування енергією для електромобілів із потенційним застосуванням у реальному світі. Майбутня робота буде зосереджена на вдосконаленні прогнозних моделей, вивченні машинного навчання для підвищення точності та інтеграції даних у реальному часі з технологій підключених транспортних засобів для динамічної оптимізації.

Ключові слова. Електромобілі, передбачення енергоспоживання, модельний дизайн, система управління енергією, оптимізація маршруту, поведінка водіння, адаптивне програмне забезпечення, ISO 26262, A-SPICE 3.1, градієнтний пошук, Simulink, вектор стану автомобіля, модульна архітектура, прогнозні моделі, машинне навчання , інтеграція даних у реальному часі, підключені технології транспортних засобів, керування акумулятором, оптимізація комфорту.

Визначення поняття інформації для живих і штучних інформаційних систем

Юрій Хлапонін[1], Володимир Вишняков[2]

[1,2] Київський національний університет будівництва і архітектури
пр-т Повітряних Сил, 31, м.Київ, Україна, 03037
[1] y.khlaponin@gmail.com, https://orcid.org/0000-0002-9287-0817
[2] volodymyr.vyshniakov@gmail.com, https://orcid.org/0000-0003-4668-712X

Received 17.10.2024, accepted 01.11.2024
https://doi.org/10.32347/uwt.2024.15.1206

Анотація. У статті на основі поєднання знань у галузі інформаційних технологій і широко відомих результатів біологічних досліджень показано, що процес розмноження живих клітин не може відбуватися без використання інформації, що зберігається в ДНК. Спростовано думку про можливість виникнення життя як випадкової хімічної сполуки. Поняття інформації для живих і штучних інформаційних систем визначено як суть повідомлення (the gist of the message), що викликає відповідну дію системи без інтелекту та впливає на вибір рішення інтелектуальною системою. Важливою властивістю інформації є можливість її перенесення на різні матеріальні носії з метою зберігання або передавання. Доведено, що живі клітини розмножуються лише завдяки життєво важливій інформації, без якої життя приречене на загибель, а ця інформація, у свою чергу, зберігається від руйнування необмежений час завдяки копіюванню під час розмноження клітин.

Ключові слова: поняття інформації. виникнення життя, інформаційна система, властивості інформації, утворення інформації.

ОПИС ПРОБЛЕМИ ТА МЕТА РОБОТИ

Першим кроком до визначення поняття інформації можна вважати відомий вислів Норберта Вінера: "Information is information, no matter or energy" (Інформація — це інформація, а не матерія чи енергії). На жаль, це не відповідає на питання: «Що таке інформація?» Проблема полягає в тому, що досі немає міждисциплінарного визначення

поняття інформації, хоча цей термін широко використовується практично у всіх областях сучасної науки. Через відсутність такого визначення можуть виникати непорозуміння та хибні напрямки наукових досліджень. Пошук відповіді на вказане питання для вирішення даної проблеми є метою цієї роботи.

АНАЛІЗ ОПУБЛІКОВАНИХ РОБІТ

Суттєвих успіхів щодо визначення поняття інформації вдалося досягти завдяки аналізу процесів у живих клітинах з позицій теорії утворення інформаційних систем [1]. Живі клітини є природними інформаційними системами, у яких на молекулярному рівні, за допомогою сучасних засобів, можна спостерігати інформаційні процеси. Найважливішим із цих процесів є розмноження, без якого все живе може існувати лише одне покоління. Розмноження всього живого починається з поділу клітин. Для одноклітинних бактерій

саме поділ є розмноженням. Дослідники з JCVI (The J. Craig Venter Institute) провели успішний експеримент із заміни молекули ДНК у бактерії на штучно синтезовану [2]. На початку досліджень штучна молекула була копією природної. Пізніше шляхом внесення змін до цієї молекули було знайдено мінімальний геном серед усіх живих істот, здатних до автономного розмноження (531 тис. пар нуклеотидів, 473 гени) [3]. Наявність цього мінімуму означає, що кількість інформації, необхідної для поділу клітини, обмежена. Крім того, в клітинах чітко розподілені функції елементів, необхідних для поділу. Ці елементи вивчені до рівня молекул, а їх функції детально описані в літературі з біології, але немає пояснення ролі інформації в цьому описі. Спроба усунути даний недолік зроблена в роботі [4], де наведено перелік елементарних дій над інформацією, показаний у табл. 1.

Загально визнано роль молекули ДНК, як головного носія генетичної інформації, але у роботах біологів інформаційні перетворення не описуються. У роботі [4] показано, як саме використовується інформація з молекули ДНК для побудови діючих біологічних механізмів живої клітини. Цикл процесів щодо розмноження бактерії починається після завершення її поділу з утворенням двох нових клітин. Першою дією циклу є виготовлення копій ділянок молекули ДНК у вигляді ланцюгів РНК (рибонуклеїнової кислоти). Деякі з цих ланцюгів можуть бути одночасно носіями інформації і діючими механізмами. Пояснення можливості об'єднання декількох функцій інформаційних систем у одному фізичному елементі надамо після розгляду

Таблиця 1. Дії, які можуть виконуватись над інформацією

Table 1. Actions that can be performed on information

Назва дії над інформацією	Виконавець дії
Сприйняття (завдяки чутливості)	Інформаційна система
Запам'ятовування	Інформаційна система
Копіювання	Інформаційна система
Зберігання	Будь-який фізичний носій
Знищення (часткове або повне)	Деякий фізичний процес
Використання у процедурах вибору	Інформаційна система
Спотворення випадкове	Випадковий фізичний процес
Спотворення умисне	Інформаційна система
Перетворення (кодування)	Інформаційна система
Створення (завдяки фантазуванню)	Інформаційна система
Сприйняття від інших систем (через носії)	Інформаційна система

Таблиця 2. Мінімальний набір властивостей діючої інформаційної системи

Table 2. Minimum set of properties of an existing information system

Позначення властивості	Назва властивості	Опис властивості
M (*Memory*)	Пам'ять	Збереження інформації у вигляді, який дозволяє використовувати її для вибору тої чи іншої дії
S (*Sensor*)	Чутливість	Сприйняття певних характеристик зовнішнього середовища
C (*Choice*)	Здатність вибирати	Можливість обирати ту чи іншу дію в залежності від збереженої інформації та зовнішніх факторів
E (*Execution*)	Дієздатність	Здатність виконувати обрані дії

мінімального набору властивостей цих систем, який представлено у табл. 2.

У деяких системах усі ці властивості реалізує один фізичний елемент. Наприклад, клапан для регулювання тиску пари у котлі роблять у вигляді гирі, яка затуляє отвір на кришці. Інформацію щодо потрібного тиску закладають у вагу гирі. У разі перевищення тиску пара піднімає гирю і частково виходить з котла. Таким чином, пам'ять є у вазі гирі, чутливість – у можливості гирі підійматись, а здатність вибирати (затуляти чи відкривати отвір) та дієздатність такої системи не потребують додаткових пояснень.

У живих клітинах роль ДНК обмежується лише функцією збереження інформації. Це означає, що сама по собі молекула ДНК не є інформаційною системою, а є лише пам'яттю у системі клітини. Розмноження починається з копіювання інформації, яке виконує механізм РНК-полімераза, як показано на рис. 1 разом з пояснювальною схемою знизу.

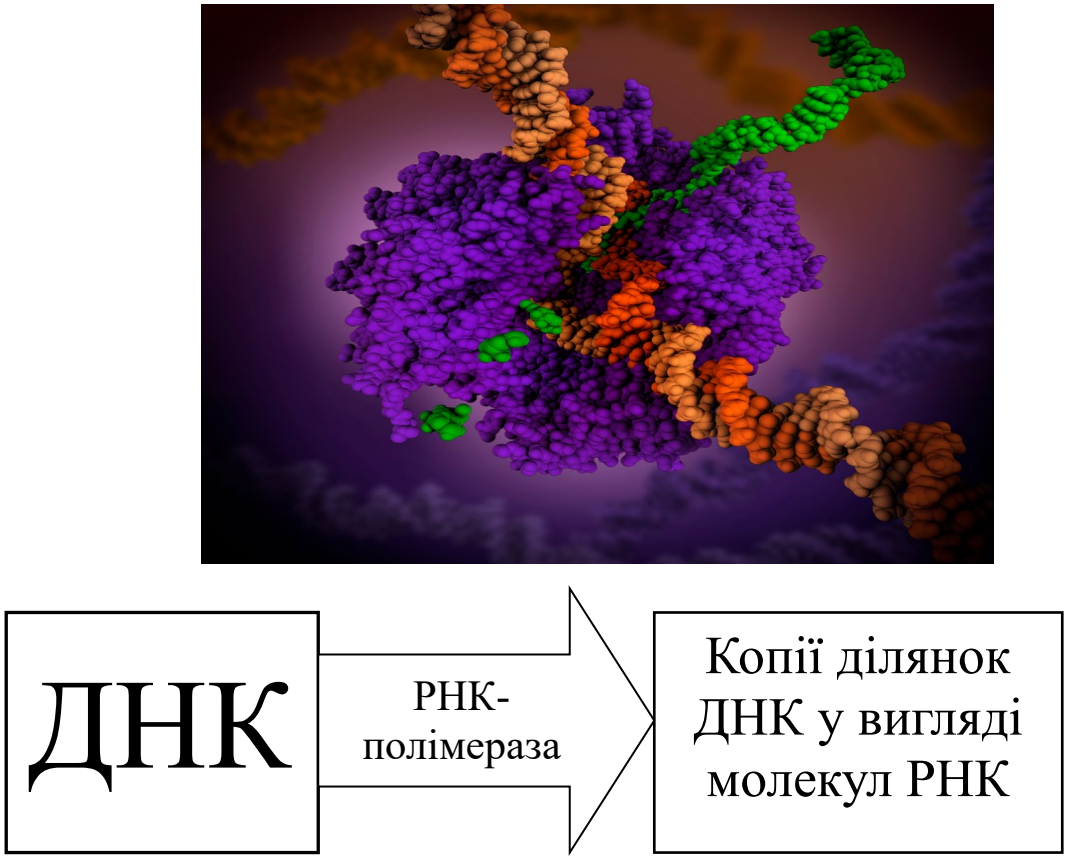


Рис. 1. Процес копіювання ділянок ДНК (помічена оранжевим) у вигляді РНК (помічена зеленим) за допомогою РНК-полімерази (помічена фіолетовим)

Fig. 1. The process of copying sections of DNA (marked in orange) into RNA (marked in green) using RNA polymerase (marked in purple)

Усі інформаційні процеси, які потрібні для поділу клітин виконуються у певній послідовності. Біологічний механізм РНК-полімераза (у літературі його називають ферментом каталізатором) виконує такі дії:

– наближається до молекули ДНК та починає рухатись вздовж неї у певному напрямку, аналізуючи значення послідовностей нуклеотидів (під час свого руху РНК-полімераза тимчасово роз'єднує базовий і дублюючий ланцюги ДНК на проміжку у 12 нуклеотидів);

– виявивши на базовому ланцюгу ДНК послідовність нуклеотидів *TATAAT* та після проходження ще чотирьох нуклеотидів, РНК-полімераза починає процедуру

виготовлення копії ділянки ДНК у вигляді ланцюга РНК (послідовність *TATAAT* має назву promoter [5]);

– під час виготовлення копії РНК-полімераза, аналізуючи черговий нуклеотид у базовому ланцюгу молекули ДНК, відшукує та приєднує певний нуклеотид до ланцюга РНК згідно з таблицею, яку показано у табл. 3;

відрізняються за складністю, то процеси їх побудови відбуваються з різною кількістю етапів. Найпростіший діючий механізмом, побудова якого відбувається лише за один етап, має назву hairpin (шпилька). Завдання цього механізму полягає у тому, щоб від'єднати синтезований ланцюг РНК від РНК-полімерази. Після виконання цього завдання механізм hairpin руйнується,

Таблиця 3. Відповідність нуклеотидів під час копіювання інформації

Table 3. Nucleotide correspondence during information copying

Тип нуклеотиду у молекулі ДНК	Тип нуклеотиду для молекули РНК
A – аденін	*U* – урацил
G – гуанін	*C* – цитозин
C – цитозин	*G* – гуанін
T – тимін	*A* – аденін

– виявивши послідовність нуклеотидів *AAAA* та після проходження ще чотирьох нуклеотидів, РНК-полімераза зупиняє синтез ланцюга РНК

Слід зауважити, що копіювання інформації є дією, яку виконують лише інформаційні системи. Копіювання завжди потребує участі спеціалізованого механізму, для створення якого, у свою чергу, також потрібна інформація. Саме таким механізмом і є РНК-полімераза. Оскільки біологічні механізми живої клітини

перетворюючись на нуклеотиди для синтезу нових ланцюгів РНК та ДНК. На прикладі механізму hairpin покажемо як за допомогою лише процедури копіювання можна побудувати структуру, що здатна виконувати дію. Послідовність нуклеотидів з молекули ДНК *CGGGCGGCTTTCCGCCCG* після копіювання у ланцюг РНК буде такою: *GCCCGCCGAAAGGCGGGC*. У цитоплазмі живої клітини цей ланцюг буде мати початковий вигляд приблизно такий, як показано на рис. 2

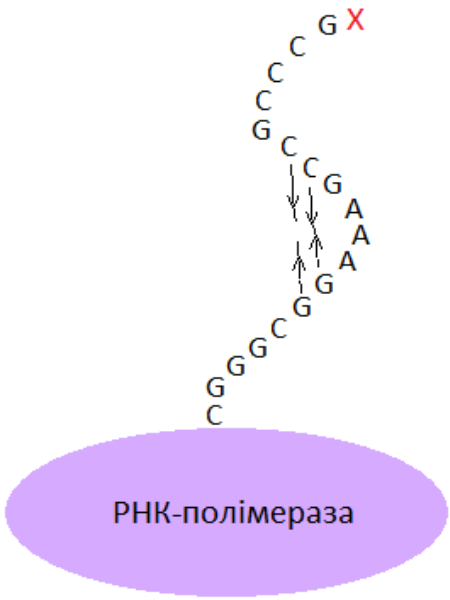


Рис. 2. Схема виконання завдання щодо від'єднання синтезованого ланцюгу РНК шляхом формування структури у вигляді шпильки

Fig. 2. Scheme of the task of detaching the synthesized RNA chain by forming a hairpin structure

На рисунку 2 стрілками показані напрямки притягання комплементарних нуклеотидів (*C* та *G*), через яке відбувається їх поступове зближення та з'єднання. Притягання обумовлено протилежними електричними зарядами. Оскільки сила притягання між цими нуклеотидами буде зростати зі зменшенням відстані між ними до моменту їх з'єднання, то з кожною наступною парою сила буде збільшуватись. Ця сила розірве синтезований ланцюг РНК у тому місці, яке помічено символом "*X*". Таким чином завдання буде виконано. Структуру механізму (у формі шпильки) показано на рис. 3 у нижній частині.

Рис. 3. Послідовність нуклеотидів в момент завершення синтезу молекули РНК у молекулі ДНК показана чорним, а у ланцюгу РНК показана червоним

Fig. 3. The nucleotide sequence at the time of completion of RNA molecule synthesis in the DNA molecule is shown in black, and in the RNA chain is shown in red

Остання синтезована послідовність з восьми нуклеотидів *UUUUCUGU*, що показана на сірому фоні червоним, утилізується. Після цього механізм РНК-полімераза стає готовим до пошуку чергової послідовності *TATAAT* та синтезу наступного ланцюга РНК.

Загальновідомо, що для копіювання інформації потрібно мати доступ до носія з інформацією, яку слід копіювати, а також інструментарій для читання цієї інформації та виготовлення її копії. Судячи з результатів дослідження функціонування РНК-полімерази, усі ці можливості в неї є. З цього витікає, що вона є системою середнього рівня ієрархії інформаційних систем, яка здатна утворювати копії інформації на зовнішні носії, але нездатна розмножуватись. Слід зауважити, що для утворення самої РНК-полімерази необхідно, щоб вже була РНК-полімераза, бо без її участі жоден механізм клітини не утворюється. Цей цикл є основою життя, бо без нього не може відбуватись розмноження. У даному циклі задіяна низка біологічних механізмів, включаючи рибосому, матричну РНК, транспортну РНК і ДНК у вигляді джерела генетичної інформації. У роботі [3] визначено мінімальну довжину молекули ДНК (531 тисяча пар нуклеотидів), при якій клітина ще має здатність розмножуватись. Наявність в основі життя такого циклу значно ускладнює спроби пояснити утворення живого з неживих елементів

чисто випадковим з'єднанням хімічних елементів. Навіть, якщо уявити випадкову появу усіх потрібних механізмів циклу у одному місці, то життя не виникне, бо для його появи слід отримати клітину, яка здатна розмножуватись. Поява нової клітини є результатом діяльності лише існуючої живої клітини, де з використанням інформації з ДНК завдяки РНК-полімеразі створюються біологічні механізми у кількості, що є достатньою для поділу. Перелік назв найбільш відомих з цих механізмів надано у табл. 4, де також вказані їх головні функції.

Таблиця 4. Механізми та структури, що необхідні для розмноження клітин

Table 4. Mechanisms and structures required for cell reproduction

Назва механізму чи структури	**Відносна кількість РНК**	**Довжина ланцюгу РНК**	**Функції механізму або структури**
РНК-полімераза	-	-	Копіювання ділянок ДНК у ланцюги РНК
Рибосома (*ribosome*) (*rRNA*)	~90%	~4500	Синтез білків
Транспортна РНК (*tRNA*) (має різні види для різних амінокислот)	~10%	76-90	Доставка амінокислот для синтезу білків
Матрична РНК (*mRNA*) (кількість різновидів відповідає типам білку)	~0,5%	Залежить від типу білку	Доставка команд для керування процесом синтезу білків
Aminoacyl tRNA synthetase (є 20 типів, що відповідає амінокислотам)	-	-	Пошук амінокислот та їх приєднання до транспортної РНК
Рибонуклеаза (*RNase*) (під цією назвою існує низка спеціалізованих механізмів)	?	~300	Від розрізання РНК ланцюгів на окремі молекули РНК до повного руйнування молекул РНК
ДНК-полімераза	-	-	Копіювання молекули ДНК

Механізм ДНК-полімераза виконує останню підготовчу дію для поділу клітини, а саме, створює копію молекули ДНК. Після цього деякий час у клітині перебувають дві молекули ДНК, що завершується роз'єднанням клітини на дві нові. Перед цим оболонка клітини збільшується завдяки діяльності спеціалізованих механізмів. У побудові всіх механізмів клітини використовується інформація з ДНК, де запрограмована функціональність кожного з механізмів. Матеріал для побудови механізмів добуває клітина із зовнішнього середовища у процесі своєї життєдіяльності. За теорією побудови інформаційних систем такі клітини займають найвищий рівень ієрархії, оскільки вони мають здатність розмножуватись. Таким чином розмноження клітини потребує наявності живої клітини у активній стадії існування. Іншої можливості утворення нових клітин невідомо. Але це ще не є доказом неможливості випадкового утворення живих клітини без наявності інформації. Доказ базується на тому, що клітина є інформаційною системою, утворити яку неможливо без завантаження в неї певної інформації. Цю процедуру може виконати лише інформаційна система вищого або такого ж рівня ієрархії, у якій є потрібна інформація. Зауважимо, що у ДНК є інформація лише про те, як створити біологічні механізми в межах існуючої живої клітини, а інформації про те, як створити клітину з нуля у ДНК немає.

ОСНОВНИЙ МАТЕРІАЛ ДОСЛІДЖЕНЬ

Для визначення поняття інформації слід провести чітку межу між тим, що є інформацією та тим, що нею не є.

Інформація завжди перебуває на матеріальному носії, який може мати чимало характеристик. Серед них потрібно виявити лише ті, що несуть інформацію. Розглянемо це на прикладі молекули ДНК. Особливістю інформації є те, що при точному копіюванні на інший носій вона повністю зберігається. У разі ДНК слід показати, що тільки послідовність нуклеотидів несе генетичну інформацію. Були припущення, що крім даної послідовності у ДНК є й інші інформаційні ознаки. Вважали недостатнім для побудови організму кількості інформації, що міститься у зазначеній послідовності. Після секвенування молекули ДНК результат може бути отримано у вигляді, що представлений на рис. 4.

```
CATGACGTCGCGGACAACCCAGAATTGTCTTGAGCGATGGTAAGATCTAACCTCACTGCCGGGGGAGGCTCATAC
CTGGGGCTTTACTGATGTCATACCGTCTTGCACGGGGATAGAATGACGGTGCCCGTGTCTGCTTGCCTCGAAGCA
ATTTTCTGAAAGTTACAGACTTCGATTAAAAAGATCGGACTGCGCGTGGGCCCGGAGAGACATGCGTGGTAGTCA
TTTTTCGACGTGTCAAGGACTCAAGGGAATAGTTTGGCGGGAGCGTTACAGCTTCAATTCCCAAAGGTCGCAAGA
CGATAAAATTCAACTACTGGTTTCGGCCTAATAGGTCACGTTTTATGTGAAATAGAGGGGAACCGGCTCCCAAAT
CCCTGGGTGTTCTATGATAAGTCCTGCTTTATAACACGGGGCGGTTAGGTTAAATGACTCTTCTATCTTATGGTG
ATCCAAGCGCCCGCTAATTCTGTTCTGTTAATGTTCATACCAATACTCACATCACATTAGATCAAAGGATCCCCG
AGCCCAGTCGCAAGGGTCTGCTGCTGTTGTCGACGCCTCATGTTACTCCTGGAATCTACCTGCCCTCCCCTCACC
GGTTAAGGCGTGTGATCGACGATGCAGGTATACATCGGCTCGGACCTACAGTGGTCGATCGACTGGCTACTGGCT
TCGCGGTTCGGCGCGTAGTTGAGTGCGATAACCCAACCGGTGGCAAGTAGCAAGAAGACCTACCTGGGTCACCTT
AGACAACCTAACTAATAGTCTCTAACGGGGAATTACCTTTACCAGTCTCATGCCTCCAATATATCTGCACCGCTT
CAATGATATCGCCCACAGAAAGTAGGGTCTCAGGTATCGCATACGCCGCGCCCGGGTCCCAGCTACGCTCAGGAC
GACAGTAGAGAGCTATTGTGTAATTCAGGCTCAGCATTCATCGACCTTTCCTGTTGTGAATATTGTGCTAATGCA
TCTCGTCCGTAACGATCTGGGGGGCAAAACCGAATATCCGTATTCTCGTCCTACGGGTCCACAATGAGAAAGTCC
TGCGCGTGATCGTCAGTTAAGTTAAATTAATTCAGGCTACGGTAAACTTGTAGTGAGCTAAGAATCACGGGAATC
ACGGGTTCGCTACAGATGAACTGAATTTATACACGGACAACTCATCGCCCATTTGGGCGTGGGCACCGCAGATCA
AAAGTGGCAGATTAGGAGTGCTTGATCAGGTTAGCAGGTGGACTGTATCCAACAGCGCATCAAACTTCAATAAAT
CCAAAGCGTTGTAGTGGTCTAAGCACCCCTGAACAGTGGCGCCCATCGTTAGCGTAGTACAACCCTTCCCCCTTG
AGGTGCGACATGGGGCCAGTTAGCCTGCCCTATATCCCTTGCACACGTTCAATAAGAGGGGCTCTACAGCGCCGC
TTTTTAAATTAGGATGCCGACCCCATCATTGGTAACTGTATGTTCATAGATATTTCTTCAGGAGTAATAGCGACA
AGCTGACACGCAAGGGTCAACAATAATTTCTACTATCACCCCGCTGAACGACTGTCTTTGCAAGAACCAACTGGG
```

Рис. 4. Частковий вигляд результату секвенування ДНК для вірусу Ф-Х174 [6].

Не викликає сумнівів, що у цьому результаті немає інших ознак ДНК, крім послідовності нуклеотидів. Пристрій, який зображено на рис. 5, дозволяє синтезувати ДНК з комп'ютерного результату секвенування.

Рис. 5. Синтезатор олігонуклеотидів MerMade 12 призначений для синтезу олігонуклеотидів (ДНК, РНК)

Дослідники інституту JCVI замінили у бактерії молекулу ДНК на штучно синтезовану [2]. Оскільки після заміни молекули життєдіяльність бактерії збереглась, то це означає, що для передачі генетичної інформації цілком достатньо знати лише послідовність нуклеотидів. Таким чином копіювання через комп'ютерну пам'ять надає можливість виявляти які саме ознаки носія використовуються для передачі інформації. Цей експеримент також показав, що інформацію, яка зберігається у молекулі ДНК, як і будь-яку інформацію у штучних системах, можна переносити на різні матеріальні носії з метою зберігання або передавання.

Головною характеристикою інформації є те, що вона означає (її суть). Дослідження біологів дозволяє виявляти відповідність між представленням інформації у вигляді послідовності нуклеотидів і тим, що вона означає. Наприклад, послідовність *TATAAT* означає вказівку, що через чотири наступних нуклеотиди слід почати синтез ланцюгу РНК. Цю вказівку отримує діючий механізм РНК-полімерази з молекули ДНК під час руху вздовж цієї молекули. Кожен синтезований ланцюг РНК являє собою вказівку щодо виконання певної дії. Ланцюг *GCCCGCCGAAAGGCGGGC* (див. рис. 2) означає, що слід виконати дію від'єднання синтезованого ланцюгу від РНК-полімерази. Більш складний випадок розглянемо на прикладі вказівки щодо утворення механізму транспортної РНК. Ця вказівка складається з низки більш простих вказівок. Послідовність нуклеотидів даної вказівки частково показано на рис. 6 [7].

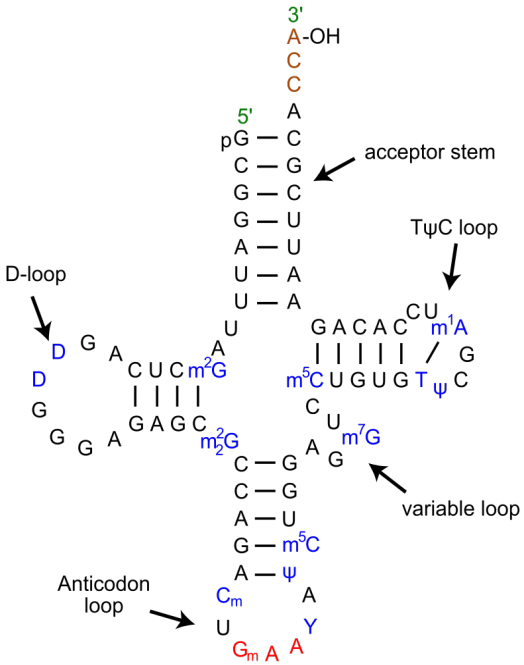


Рис. 6. Структура сполук нуклеотидів у транспортній РНК.

На рисунку представлено ланцюг нуклеотидів транспортної РНК після з'єднання комплементарних ділянок. Ці ділянки, що скопійовані з ДНК РНК-полімеразою, є вказівками про те, у яких місцях слід з'єднати між собою, ділянки ланцюгу РНК. Процес з'єднання відбувається так само, як описано вище (див. рис. 2), але у цьому разі використовують не лише пари *CG*, а ще й пари *AU*, які також притягуються між собою, але з меншою силою. Між з'єднаними ділянками утворюються петлі, які також є вказівками щодо приєднання до них певних

елементів. Наприклад, у лівій гілці нуклеотид U перетворюється у дигідроуридин (D) шляхом приєднання двох атомів водню до уридину. У біологічній літературі усі такі перетворення називають дозріванням молекул, але згодом з'ясовується, що у кожному разі перетворення відбуваються за вказівками, які копіюються з ДНК. Значна кількість досліджених механізмів утворюється з молекул білку, у які інформація з ДНК пересилається через мРНК.

Тривимірну модель сформованого механізму тРНК показано на рис. 7.

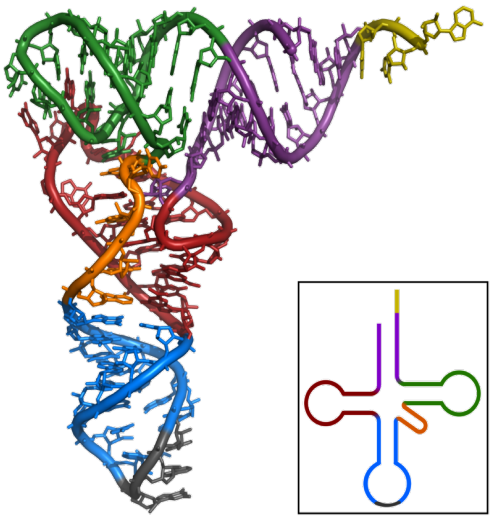


Рис. 7. Тривимірна модель транспортної РНК.

Показану на рисунку форму тРНК набуває через те, що здвоєні ділянки ланцюгів нуклеотидів мають властивість скручуватися (приблизно один оберт на 10,4 пар нуклеотидів). Така ж властивість є у молекул ДНК, які теж складаються з двох ланцюгів. На кінці тРНК, який має назву 3' (*three prime end*), є активне місце (див. рис. 6), до якого приєднується група CCA-OH. До цього місця механізм *aminoacyl tRNA synthetase* [8] приєднує амінокислоти. Існує декілька десятків різновидів тРНК для доставки різних амінокислот до рибосоми, яка синтезує молекули білку за вказівками з мРНК. Тобто усі з'єднання біологічних механізмів та їх функціональність є запрограмованими у ДНК з надвисокою точністю. Саме через це поділ бактеріальних клітин, що займає лише близько трьох годин, не припиняється на Землі вже 3,5 млрд. років. Слід зауважити, що такі ж самі за функціональністю типи біологічних механізмів, які існують у бактеріях, є у клітинах всіх без винятку організмів.

Таким чином, основою для розмноження клітин слід вважати не хімічні реакції, що прискорюються ферментами, а інформацію на носії у вигляді молекули ДНК. Ця інформація є вказівками, які приймаються та виконуються механізмами живої клітини з використанням законів фізики, хімії та біології. У разі живих клітин, здатних до поділу, інформація передається з молекули ДНК і сприймається як вказівки щодо виконання певних дій механізмами клітини. Для штучних інформаційних систем, крім штучного інтелекту та нейромереж, інформація також приводить до виконання певних дій. Для інтелектуальних систем інформація не обов'язково приводить до виконання певної дії. Ці системи сприймають інформацію як пропозицію, яка може вплинути на їх рішення щодо виконання тої чи іншої дії. Під наявністю інтелекту будемо розуміти можливість впливати на виконання власних дій. У всіх випадках інформаційна система, отримуючи повідомлення, вказівки, сигнали, знання тощо, має виявити їхнє значення (суть), що є головною характеристикою будь-якої інформації.

Подальші дії системи залежать від її інтелектуальних здібностей.

Узагальнити визначення поняття інформації можна так:

Інформація - це суть повідомлення (the gist of the message), що викликає відповідну реакцію системи без інтелекту та впливає на вибір рішення інтелектуальною системою.

ДОВЕДЕННЯ НЕМОЖЛИВОСТІ СТВОРЕННЯ ІНФОРМАЦІЇ В УМОВАХ ЇЇ ПОВНОЇ ВІДСУТНОСТІ

Відомо, що інформація створюється інформаційними системами і може зберігатись на матеріальних носіях до руйнації, яка є неминучою через рух матерії. Слід довести, що, якщо вся інформація у Всесвіті зруйнується, то не буде джерела для її появи, що рівнозначне неможливості створення інформації за умов її відсутності.

Всесвіт може бути представлений у вигляді множини систем так, щоб всі об'єкти були охоплені цими системами. У процесі руху системи можуть зіштовхуватись, об'єднуватись чи роз'єднуватись, але в жодній з них немає інформації. Внаслідок зіткнень можуть утворюватись матеріальні з'єднання будь-якої складності. Доведемо, що ці з'єднання не будуть інформаційними системами. Для цього розглянемо процес утворення інформаційних систем, базуючись на їх можливості копіювання інформації, щодо чого існує три рівні ієрархії [1]. До нижнього рівня віднесемо системи, які не здатні копіювати інформацію. До середнього – системи, які здатні копіювати, але не можуть розмножуватися. До найвищого – системи, що здатні створювати копії самої системи в цілому (розмножуватись). Прикладами цієї ієрархії насичена вся жива природа. У людському організмі більшість клітин (84%) становлять еритроцити, які відповідають нижньому рівню ієрархії. Їхня тривалість життя 100-120 днів. До середнього рівня належать клітини кісткового мозку, які виробляють еритроцити. Ієрархію інформаційних систем можна спостерігати і на внутрішньоклітинному рівні. Для цього доцільно розглянути структуру бактерій, оскільки вони можуть жити та розмножуватися в умовах неживого довкілля. Вищі істоти на таке нездатні, оскільки їх оточують бактерії та інші мікроорганізми, без яких вищі існувати неспроможні. У структурі бактерій є чимало інформаційних систем нижнього рівня, наприклад, hairpin (шпилька), а також транспортні РНК, всі рибонуклеази, Aminoacyl tRNA synthetase та багато інших. Системами середнього рівня є РНК-полімераза, рибосома та ДНК-полімераза. До вищого рівня належить бактерія в цілому. Системи нижчих рівнів, що нездатні розмножуватись, приречені на руйнування разом з інформацією, яка в них закладена. Вони існують лише протягом часу, що потрібен для виконання завдань від системи вищого рівня, яка їх утворює. У кожну інформаційну систему під час утворення закладається інформація, значення якої відповідає меті самозбереження системи вищого рівня. Важливою властивістю систем, що розмножуються, є можливість розвитку за методом спроб і помилок (на цьому заснована еволюція). Ніщо не загрожує вічності існування матерії чи енергії, оскільки вони принципово не можуть зникнути. Руйнація загрожує лише інформації, запобігти чому можна лише шляхом копіювання, яке здійснюється у живих організмах завдяки функціонуванню ДНК-полімерази. З цього витікає, що існування інформації безпосередньо залежить від життя. Копіювання, яке є необхідним для збереження інформації, виконують лише живі системи найвищого рівня ієрархії. Цими системами є клітини, які здатні автономно розмножуватись шляхом поділу. При цьому доказ неможливості створення інформаційної системи в умовах відсутності інформації перетворюється у доказ неможливості створення живої клітини у цих умовах. Ще у 1855 році німецький вчений Рудольф Вірхов довів, що клітина походить тільки від клітини шляхом поділу, чим завершив суперечку біологів про можливість самозародження життя [9]. Матерія з енергією в будь-яких комбінаціях не здатні генерувати мету самозбереження. Не маючи

мети не можна надати значення інформації, що еквівалентно неможливості утворення інформації. На таке утворення здатні лише інформаційні системи найвищого рівня ієрархії, які можуть генерувати та реалізовувати власні цілі. Їх цілі полягають у самозбереженні в будь-яких умовах перебування у Всесвіті. Свої цілі вони успішно реалізують, про що свідчить наявність життя.

ЗНАЧЕННЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ

Широко відома теорія Великого вибуху передбачає, що Всесвіт починався зі скупчення матерії та енергії за умов, де не може існувати інформація та життя. Зрозуміло, що якби такий момент мав би місце у Всесвіті, то життя не було б. Оскільки життя існує, це означає, що у теорії Великого вибуху є неточність. Той факт, що на значній відстані від нашої точки спостереження ми бачимо об'єкти Всесвіту, що зникають, свідчить, в першу чергу, про нескінченність простору, у якому існує Всесвіт. Якби ми перемістилися в ту віддалену точку, то змогли б побачити об'єкти, які тут для нас здаються зниклими. Це свідчить про те, що не лише простір, а й увесь Всесвіт – нескінченні. Поняття нескінченності означає відсутність будь-якого кінця чи початку. Тому теорії про початок або кінець Всесвіту позбавлені сенсу.

Інформація завжди розміщується на матеріальному носії, а весь матеріальний світ перебуває в умовах постійного руху. Тому немає можливості вічного зберігання інформації на конкретному носії, але завдяки копіюванню інформація може зберігатися як завгодно довго. Наявність у живих клітинах механізмів спороутворення та відновлення життєдіяльності зі спор дозволяє забезпечити тривале зберігання інформації за відсутності умов для розмноження.

Наявність життя можна пояснити лише вічністю його існування разом із життєво необхідною інформацією. Забезпечення цієї вічності в умовах космічного простору ми вже зараз спостерігаємо завдяки космонавтиці. Космічні подорожі стають можливими завдяки накопиченню інформації щодо створення засобів та методів поширення життя в умовах Всесвіту.

ВИСНОВКИ

Живі клітини є природними інформаційними системами, у яких на молекулярному рівні, за допомогою сучасних засобів, можна спостерігати інформаційні процеси. Найважливішим з цих процесів є розмноження, без чого все живе проіснувало б лише протягом одного покоління.

Основою розмноження клітин слід вважати інформацію, яка знаходиться на фізичному носії у вигляді молекули ДНК. Ця інформація являє собою вказівки, які сприймаються та виконуються механізмами живої клітини. Для штучних інформаційних систем, крім штучного інтелекту та нейромереж, інформацію також можна визначити, як вказівки для виконання певних дій. Для інтелектуальних систем, які можуть діяти на власний розсуд, отримана інформація не обов'язково приводить до виконання певної дії. Будь-яку інформацію такі системи сприймають, як те, що може вплинути на їх рішення у тій чи іншій мірі разом з попередніми знаннями. Узагальнене визначення поняття інформації є таким: інформація — це суть повідомлення, що викликає відповідну реакцію системи без інтелекту та впливає на вибір рішення інтелектуальною системою.

Маючи лише матерію та енергію за повної відсутності інформації неможливо створити інформаційну систему, оскільки для цього слід закласти інформацію з конкретним значенням (суттю). Немає інформації без значення, а це значення у всіх випадках підпорядковано меті самозбереження системи вищого рівня ієрархії. Матерія з енергією в будь-яких комбінаціях не здатні генерувати подібну мету. Не маючи мети не можна надати значення інформації, що еквівалентно

неможливості утворення інформації. На таке здатні лише інформаційні системи найвищого рівня ієрархії, які можуть генерувати та реалізовувати власні цілі. Їх цілі полягають у самозбереженні в будь-яких умовах перебування у Всесвіті. Свої цілі вони успішно реалізують, про що свідчить наявність життя.

Наявність життя можна пояснити лише вічністю його існування разом із життєво необхідною інформацією. Забезпечення цієї вічності в умовах космічного простору ми вже зараз спостерігаємо завдяки космонавтиці. Космічні подорожі стають можливими завдяки накопиченню інформації щодо створення засобів та методів поширення життя в умовах Всесвіту.

Подяка. Автори висловлюють щиру вдячність провідному інженеру Кафедри хімічної технології кераміки та скла "Київського політехнічного інституту імені Ігоря Сикорського" кандидату технічних наук Маковецькому Олександру Лавровичу за низку цінних зауважень під час підготовки рукопису.

REFERENCES

1. **Khlaponin Yu., Vyshniakov V.** (2024) Osnovy teorii utvorennia informatsiinykh system. *Smart Technologies*, Issue 1(14), 2024, 56–61. http://uwtech.knuba.edu.ua/article/view/307218
2. **Gibson D.G., Glass J.I. & et al.** (2010). Creation of a bacterial cell controlled by a chemically synthesized genome. *Science (New York, N.Y.).* 2010-07-02; 329.5987: 52-6. https://www.jcvi.org/publications/creation-bacterial-cell-controlled-chemically-synthesized-genome
3. **Hutchison C.A., Chuang R.Y. & et al.** (2016). Design and synthesis of a minimal bacterial genome. *Science (New York, N.Y.).* 2016-03-25; 351.6280: aad6253. https://www.jcvi.org/publications/design-and-synthesis-minimal-bacterial-genome
4. **Vyshniakov V.** (2024). Vidkrytyi shliakh do rozuminnia informatsii ta yii pokhodzhennia. Grail of Science, (39), 478–495. https://archive.journal-grail.science/index.php/2710-3056/issue/view/10.05.2024/27
5. Promoter_(genetics). From Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Promoter_(genetics)
6. Genome. From Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Genome
7. Transfer RNA. From Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Transfer_RNA
8. Aminoacyl tRNA synthetase. From Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Aminoacyl_tRNA_synthetase
9. Rudolf Virchow. From Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Rudolf_Virchow

Definition of the concept of information for living and artificial information systems

Volodymyr Vyshnyakov

Annotation. The article, based on a combination of knowledge in the field of information technology and widely known results of biological research, shows that the process of reproduction of living cells cannot occur without the use of information stored in DNA. The opinion about the possibility of the emergence of life as a random chemical compound has been refuted. The concept of information for living and artificial information systems is defined as the essence of the message (the gist of the message), which causes the corresponding action of the system without intelligence and influences the choice of decision by the intelligent system. An important feature of information is the ability to transfer it to various physical media for the purpose of storage or transmission. It has been proven that living cells reproduce only because of vital information, without which life is doomed, and this information, in turn, is preserved from destruction indefinitely due to copying during cell reproduction.

Keywords: concept of information. origin of life, information system, properties of information, formation of information.

Дослідження впливу інтернет середовища на підлітків

Максим Делембовський[1], Максим Маркевич[2], Борис Корнійчук[3]

[1,2,3] Київський національний університет будівництва і архітектури
пр-т Повітряних Сил, 31, м.Київ, Україна, 03037
[1] delembovskyi.mm@knuba.edu.ua, https://orcid.org/0000-0002-6543-0701,
[2] markevych_mo@knuba.edu.ua
[3] korniichuk.bv@knuba.edu.ua, https://orcid.org/0000-0003-3881-1581

Received 16.09.2024, accepted 01.11.2024
https://doi.org/10.32347/uwt.2024.15.1207

Анотація. Ця робота зосереджується на дослідженні впливу інтернет середовища на підлітків, яке надає розгорнуте бачення даного питання.

Основна увага приділена дослідженню популярних месенджерів, а також, комп'ютерних ігор, відповідно до їх популярності. Основні з них: «Telegram», «Instagram», «Viber», «Counter-Strike», «World of Tanks», «Dota 2».

Дане дослідження виявило, що значна кількість підлітків проводить час в онлайн іграх та месенджерах, крім того зустрічається з контентом, який підтримує агресивні дії держави-агресора, що може впливати на їх свідомість та емоційний стан.

У цій статті проаналізовано методи залучення підлітків державою-агресором для виконання розвідувальних та диверсійних завдань.

Дана робота розглядає перспективу фільтрування та обмеження контенту для підлітків, який наразі є загальнодоступним.

Ключові слова: підлітки, месенджер, комп'ютерні ігри, психологія, інформаційне поле, громадська думка, тренди, дезінформація.

ВСТУП

У сучасних умовах гібридної війни інформаційні технології набули значної важливості у воєнних операціях. Окрім традиційних методів розвідки та шпигунства, противник активно застосовує цифрові платформи, зокрема месенджери та чати в онлайн-іграх, для збору розвідувальних даних та проведення підривних операцій на території України. Ці канали зв'язку забезпечують анонімність, швидкість передачі інформації та можливість охоплення широкої аудиторії, що робить їх привабливими для ворожих спецслужб.

Ігрові платформи, які зазвичай сприймалися як засіб розваги, все частіше використовуються ворогом для збору даних та узгодження дій. Особливий інтерес викликають багатокористувацькі ігри з функцією відкритих чатів, такі як «World of Tanks», «Counter-Strike», «PUBG», «Dota 2» та інші, де користувачі можуть взаємодіяти в режимі реального часу.

МЕТА ТА МЕТОДИ ДОСЛІДЖЕННЯ

Спільнотою студентського самоврядування та кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і

архітектури проведено дослідження на тему «Впливу інтернет середовища на підлітків». З цією метою в КНУБА студентське самоврядування організувало масове анонімне опитування студентської спільноти. Загалом в опитування прийняли участь 186 студентів, середній час опитування студента не перевищував 5 хв та тривав 5 днів.

Перший блок питань стосувався статевої приналежності, як результат: 70% опитаних чоловічої статі та 30% жіночої статті від загальної кількості опитаних. Наступним кроком було визначено вікову категорію, що в свою чергу становила 53% від 16 до 18 років, 41% від 19-21 року та 6% від 22 років і більше (рис. 1).

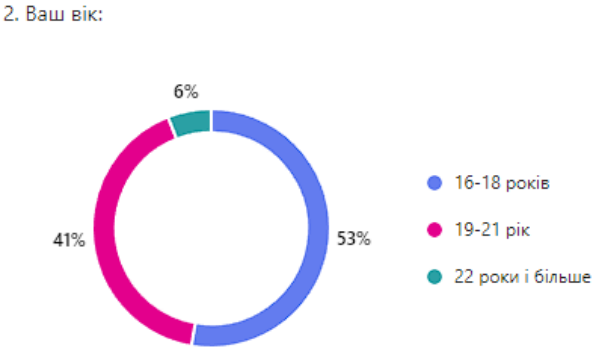


Рис. 1. Контингент опитаних

Fig. 1. Contingent of respondents

На питання як часто грають опитані респонденти в онлайн ігри більшість 32% відповіли що щодня, 30% - декілька разів на тиждень, 26% - рідко, 8% - ніколи, 4% - раз на тиждень. Загалом інформація свідчить, що в дійсності більшість опитаних так чи інакше є активними учасниками онлайн ігор (рис..2).

Для того щоб зрозуміти який на сьогодні є запити та вподобання в онлайн іграх у наявної аудиторії, було сформовано питання щодо вподобань різних жанрів ігор. Як результат отримали значну перевагу в цікавості до динамічних активних ігор. На перше місце вийшли ігри у форматі «шутер» - це 28%, «стратегії» - 24%, «симулятори» та «рольові ігри» по 15%, соціальні ігри отримали найменшу кількість вподобань що становило загалом 5% (рис.. 3.)

Рис. 2. Активність в онлайн іграх

Fig. 2. Activity in online games

Рис. 3. Вподобання молоді в іграх

Fig. 3. Youth gaming preferences

Розуміючи, що запити в опитаної аудиторії більш формуються на основі динамічних ігор, постає питання чи все ж зустрічали підлітки в онлайн іграх контент, який може виправдовувати або підтримувати терористичні дії рф. І ось в цьому випадку наші побоювання підтвердились. Не значна кількість але близько 6% відсотків з впевненістю підтвердили наявність даного контенту, 28% відповіли що інколи прослідковували, 17% не змогли чітко заперечити той факт і лише 50% впевнено відповіли що ніколи не зустрічали наявного контенту (рис.. 4). Але як показує практика не всі респонденти можуть критично оцінювати контент якщо мають вже від нього певну залежність. Тому ми умовно вважаємо що з категорії 50% є певна кількість, які не змогли критично оцінити даний контент, але це лише наше припущення.

Рис. 4. Наявність сумнівного контенту в онлайн іграх

Fig. 4. Presence of questionable content in online games

Аналізуючи результати опитування респондентів стосовно питання впливу онлайн на підсвідомість підлітків, формуючи позитивне ставлення до агресивних дій рф, отримали не менш цікаві відповіді. Переважна більшість (31% - «так» та 38% «можливо») респондентів відповіла, що онлайн ігри можуть мати вплив на підсвідомість підлітків і формувати позитивне ставлення до агресивних дій рф. Ці респонденти зазначили, що контент у таких іграх може підтримувати агресивні дії та сприяти формуванню негативних переконань. Частина респондентів висловила думку, що вплив онлайн ігор на підсвідомість підлітків є обмеженим або незначним (27%). Вони вважають, що цей вплив можна компенсувати іншими факторами, такими як освіта та виховання (рис. 5).

Враховуючи попередні результати опитування, постає питання стосовно комунікації та обговорення між підлітками або в інтернет спільноті контенту у відеоіграх стосовно формування позитивного ставлення до агресивних дій рф. Як результат дослідження визначено, що фактично 45% так чи інакше можуть обговорювати це, а 46% категорично спростували таке обговорення (рис. 6).

Рис. 6. Комунікації та обговорення між підлітками контенту у відеоіграх

Fig. 6. Communication and discussion among teenagers about video game content

Що стосується усвідомлення респондентів до контролю вмісту в онлайн іграх політичного чи пропагандистського повідомлення, в цій частині питання майже 2/3 (66%) чітко бачить важливість такої роботи.

Рис. 5. Можливість впливу онлайн ігор на підсвідомість підлітків

Fig. 5. The possibility of online games influencing the subconscious of adolescents

В той же час 24% вважає що це не є важливим, і це більше говорить про байдужість до даного процесу відповідної категорії респондентів (рис. 7).

Рис. 7. Усвідомлення щодо контролю вмісту в онлайн іграх політичного чи пропагандистського повідомлення

Fig. 7. Awareness of content control in online games of political or propaganda messages

Наступним блоком питань в даному досліджені присвячено телеграм-каналам. В цій частині спробували дізнатись про активність отримання інформації респондентами на прикладі поточної ситуацію в Україні. В цьому випадку отримали результати того що значна більшість опитаних, а це 60% щодня отримують інформацію з телеграм-каналів, близько 19% також часто користуються послугами даних каналів, незначна кількість до 8% все ж але з певною періодичністю користуються послугами. В даній ситуації лише 10% відповіли що рідко та 8% ніколи не користуються інформацією з телеграм-каналів (рис. 8). Такий підхід, говорить про тещо телеграм-канали дуже активно впливають на суспільство і в цілому, саме на підлітків, так як це найбільш зручний спосіб отримати інформацію. Враховуючи таку стрімку популярність телеграм-каналів, як основу для отримання інформаціє, наступним логічним питанням є довіри та достовірності такої інформації в даних каналах. З цією метою поставлено питання у формати «Як ви оцінюєте достовірність інформації з телеграм-каналів?». Як результат отримали

Рис. 8. Частота використання телеграм-каналів для отримання інформації про поточну ситуацію в Україні

Fig. 8. Frequency of using Telegram channels to obtain information about the current situation in Ukraine

Рис. 9. Достовірність інформації в телеграм каналах
Fig. 9. Reliability of information in Telegram channels

досить приголомшуванні результати, а саме 81% чітко відповіли що фактично частково довіряють такій інформації і 4% повністю довіряють. Незначна кількість у 8% критично ставиться до такого роду інформації (рис. 9). Наявні результати дещо насторожують, тому що фактично інформаціє з таких джерел є досить сумнівною і потребує ретельної уваги та перевірки. Немає жодної відповідальності фактично за недостовірну надану інформацію в телеграм-каналах.

Далі ми спробували дослідити це питання глибше. Для цього було поставлено наступне питання щодо відчуття вплив інформації з телеграм-каналів на емоційний стан. В цій частині отримано відповіді, що на 18% це дійсно досить сильно впливає, 44% підтвердили що це частково на них впливає, 35% стверджують що ця інформація жодним чином не впливає на емоційний стан (рис. 10).

Враховуючи вище отриману інформацію, необхідно було біль детально визначитись з контентом який найбільш цікавить опитану аудиторію. Як результат 36% цікавляться новинами, 21% цікавляться розважальним контентом, 19% цікавляться освітніми матеріалами, 12 % цікавляться соціально-політичними обговореннями (рис. 11). Фактично з даного опитування ми бачимо що досить широкий є огляд різного контенту і лише новини в цьому випадку займають лідируючі позиції.

Рис. 10. Вплив інформації з телеграм каналів на емоційний стан
Fig. 10. The influence of information from telegram channels on the emotional state

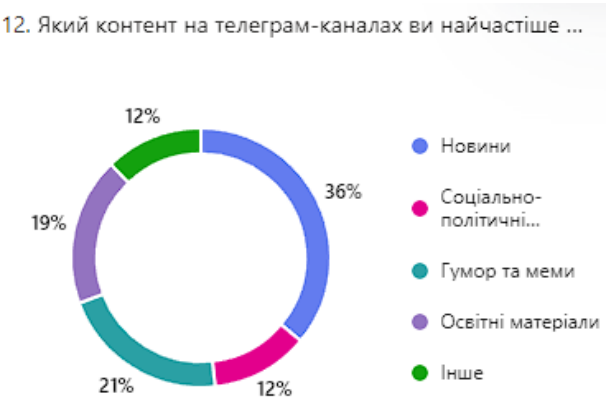


Рис. 11. Контент, який переглядається респондентами в телеграм-каналах
Fig. 11. Content viewed by respondents in Telegram channels

Для закріплення результату опитування була поставлено питання щодо можливості онлайн ігри та телеграм-канали допомоги у зниження стресу від війни. В цьому випадку 68% респондентів ствердно відповіли, що так, 18% в цьому не визначились та відповідно 14% жодним чином на це не реагують (рис. 12).

Рис. 12. Питання щодо можливості онлайн ігри та телеграм-канали допомоги у зниження стресу від війни
Fig. 12. Questions about the possibility of online games and Telegram channels helping to reduce stress from war

Для подальшого дослідженням необхідно з'ясувати, яка кількість респондентів перебувала коли-небудь у групових, закритих чи секретних чатах (Viber, Telegram, Instagram або інші), тема яких пов'язана з геополітичною ситуацією. У відповідь ствердно повідомили 83% що ніколи не користуються такими каналами, але в той же час 12% чітко надали інформацію що дійсно користуються, і лише 4% не змогли читко відповісти (рис. 13).

Рис. 13. Закриті чати в месенджерах, пов'язані з геополітичною ситуацією
Fig. 13. Closed chats in messengers related to the geopolitical situation

Враховуючи попередні відповіді про перебування у групових, закритих чи секретних чатах, додано питання стосовно наявності в цих чатах завдання або "квестів", пов'язані з передачею інформації терористичній країні рф. В більшості випадків 95% ми отримали відповідь про відсутність такої інформації, але в тойже час 2% опитаних в реальності зустрічали такі завдання і про це озвучили (рис. 14). В цьому випадку ми спробували уточнити, якого саме була формату ця інформація, як результат отримали дослівні відповіді: «Злив позицій, підпали»; «будь яка інформація за можливу грошову винагороду»

Рис. 14. Завдання та «квести», пов'язані з передачею інформації країні агресору
Fig. 14. Tasks and "quests" related to the transfer of information to the aggressor country

ОБҐРУНТУВАННЯ ДОСЛІДЖЕННЯ

Актуальність цього дослідження обумовлена зростанням впливу інтернет-середовища на молодь, особливо у сучасних умовах гібридної війни. Використання цифрових платформ ворогом для збору розвідувальних даних та проведення підривних операцій вимагає ретельного вивчення впливу інтернету, зокрема онлайн-ігор та месенджерів, на молодіжну аудиторію. Оскільки підлітки є активними користувачами таких платформ, особливо ігор із функціями реального спілкування, важливо зрозуміти, наскільки ці канали можуть сприяти поширенню ворожої пропаганди та негативно впливати на свідомість.

Основною мотивацією для проведення

дослідження стало прагнення виявити рівень загрози, пов'язаної з інформаційною маніпуляцією та пропагандою, які можуть бути приховані в популярних серед молоді інтернет-ресурсах. Дослідження спрямоване на визначення того, наскільки часто підлітки стикаються із сумнівним контентом у цифровому просторі та як це може впливати на їхні переконання, поведінку та емоційний стан.

Враховуючи, що підлітки є вразливою категорією через недостатньо сформоване критичне мислення, важливо розробити рекомендації для зниження негативного впливу інтернету. Зокрема, дослідження має на меті дати відповідь на такі запитання:

Наскільки поширені серед підлітків ситуації взаємодії з пропагандистським або деструктивним контентом?

Як вони сприймають і реагують на подібні матеріали в іграх та месенджерах?

Чи впливають онлайн-ресурси на емоційний стан молоді та їхню здатність протистояти дезінформації?

Результати цього дослідження дозволяють розробити ефективні заходи для попередження негативних наслідків впливу ворожого контенту на молодь, а також сприяють формуванню освітніх програм для розвитку критичного мислення. Це дослідження є важливим не тільки для освітньої сфери, а й для органів державної влади, які відповідають за національну безпеку, оскільки виявлення та протидія інформаційним загрозам стає ключовим компонентом у боротьбі з гібридними загрозами.

НАСТУПНІ ДОСЛІДЖЕННЯ ЗА ТЕМОЮ

Враховуючи отримані результати та актуальність дослідження, планується подальше розширення аналізу впливу інтернет-середовища на молодь у контексті гібридної війни. Майбутні дослідження можуть охоплювати такі напрями:

Поглиблений аналіз контенту онлайн-ігор та месенджерів. Необхідно детально дослідити, які саме елементи ігрового та медійного контенту містять пропаганду чи виправдання насильства. Аналіз допоможе створити систему раннього попередження щодо поширення небезпечного контенту.

Моніторинг довгострокового впливу онлайн-ігор та соціальних мереж на психологічний стан підлітків. Оцінка змін у свідомості та поведінці молоді впродовж тривалого часу дозволить визначити, які фактори найбільше впливають на формування їхніх переконань і які інструменти ефективні для нейтралізації цього впливу.

Розробка методології оцінки критичного мислення серед підлітків. Дослідження в цьому напрямі допоможуть створити освітні програми, що формуватимуть у молоді здатність до розпізнавання дезінформації та маніпуляцій.

Інтеграція технологій штучного інтелекту для автоматичного виявлення небезпечного контенту. Впровадження інструментів моніторингу в режимі реального часу може підвищити рівень безпеки онлайн-середовища.

Аналіз впливу дезінформації в телеграм-каналах та закритих чатах на суспільну думку. Вивчення механізмів, за допомогою яких поширюється недостовірна інформація, дозволить удосконалити методи боротьби з пропагандою та маніпуляціями.

Порівняльний аналіз досвіду інших країн у боротьбі з інформаційною агресією. Вивчення кращих практик та підходів, використаних у інших державах для протидії гібридним загрозам, дозволить адаптувати їх до українських реалій.

Подальші дослідження сприятимуть розробці нових інструментів для підвищення інформаційної безпеки та зниження впливу деструктивного контенту на молодь. Вони також допоможуть вдосконалити освітні та профілактичні програми, що сприятимуть формуванню стійкості молодого покоління до маніпуляцій та пропаганди.

ВИСНОВОК

Висновок: Отже, на основі проведених результатів дослідження ми можемо констатувати факти реального впливу інтернет-середовища на підлітків. Таким чином ми можемо сформувати наступні тези:

1. Частота користування інтернетом та іграми. Велика частина підлітків активно використовує інтернет для розваг, зокрема для онлайн-ігор. Найпопулярнішими жанрами є симулятори, шутери та стратегії, що свідчить про різноманітність інтересів.

2. Вплив інформації з інтернет-ресурсів. Значна кількість респондентів повідомляють про вплив інформації з телеграм-каналів на їх емоційний стан. Це підкреслює важливість критичного мислення та необхідність контролю за споживаним контентом.

3. Негативні фактори. Основними проблемами, що були виявлені, є поширення неправдивої інформації, ворожнечі та пропаганди. Підлітки визнають небезпеку таких факторів і рекомендують розвивати критичне мислення для їх мінімізації.

4. Запобігання участі у небезпечних чатах. Деякі респонденти вважають, що обмеження доступу до певного контенту та вікові обмеження можуть стати ефективними способами запобігання негативному впливу. Інші рекомендують обговорення проблем з підлітками для більшого розуміння ризиків.

Виходячи з результатів сформованих тез, ми можемо сформувати певні рекомендації, які в подальшому можуть дещо покращити наявну ситуацію, а саме:

1. Освітні програми для розвитку критичного мислення підлітків.

2. Інформаційна кампанія щодо безпечного користування інтернетом та розпізнавання дезінформації.

3. Посилення контролю за доступом до шкідливих інтернет-ресурсів.

REFERENCES

1. **Hwang, Y. W., Lee, I. Y., Kim, H., Lee, H., & Kim, D.** (2022). Current status and security trend of osint. *Wireless Communications and Mobile Computing*, 2022(1), 1290129.
2. **Glassman, M., & Kang, M. J.** (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior*, 28(2), 673-682.
3. **Hribar, G., Podbregar, I., & Ivanuša, T.** (2014). OSINT: a "grey zone"?. *International Journal of Intelligence and CounterIntelligence*, 27(3), 529-549.
4. **Miller, B. H.** (2018). Open source intelligence (OSINT): an oxymoron?. *International Journal of Intelligence and CounterIntelligence*, 31(4), 702-719.
5. **Lande, D., & Shnurko-Tabakova, E.** (2019). OSINT as a part of cyber defense system. *Theoretical and Applied Cybersecurity*, 1(1).
6. **Tabatabaei, F., & Wells, D.** (2017). OSINT in the Context of Cyber-Security. *Open Source Intelligence Investigation: From Strategy to Implementation*, 213-231.
7. **Kalpakis, G., Tsikrika, T., Cunningham, N., Iliou, C., Vrochidis, S., Middleton, J., & Kompatsiaris, I.** (2016). OSINT and the Dark Web. Open source intelligence investigation: *From strategy to implementation*, 111-132.
8. **Ziółkowska, A.** (2018). Open source intelligence (OSINT) as an element of military RECON. *Security and Defence Quarterly*, 19(2), 65-77.
9. **Stottlemyre, S. A.** (2015). HUMINT, OSINT, or something new? Defining crowdsourced intelligence. *International Journal of Intelligence and CounterIntelligence*, 28(3), 578-589.
10. **Ivanjko, T., & Dokman, T.** (2019). Open Source Intelligence (OSINT): issues and trends. *In 7th International Conference The Future of Information Sciences*, INFuture2019, 191-196. FF press.

Research on the impact of the internet environment on adolescents

Maksym Delembovskyi, Maksym Markevych, Borys Korniichuk

Abstract. This work focuses on the researched impact of the Internet environment on teenagers, which provides a detailed vision of this issue.

The main attention is paid to the study of popular messengers, as well as computer games, according to their popularity. The main ones are: "Telegram", "Instagram", "Viber", "Counter-Strike", "World of Tanks", "Dota 2".

This study revealed that a significant number of teenagers spend time in online games and messengers, in addition, they come across content that supports the aggressive actions of the aggressor state, which can affect their consciousness and emotional state.

This article analyzes the methods of attracting teenagers by the aggressor state to perform intelligence and subversive tasks.

This paper examines the perspective of filtering and restricting content for teenagers that is currently publicly available.

Keywords: teenagers, messenger, computer games, psychology, information field, public opinion, trends, misinformation

Design of radio communication modules for UAVs using atypical frequencies

Yurii Khlaponin[1], *Volodymyr Myronenko*[2]

[1,2] Kyiv National University of Construction and Architecture,
Povitryanykh Sil avenue, 31, Kyiv, 03037
[1] y.khlaponin@gmail.com, https://orcid.org/0000-0002-9287-0817
[2] volempdoge@gmail.com

Received 10.09.2024, accepted 01.11.2024
https://doi.org/10.32347//uwt.2024.15.1301

Abstract. The ongoing conflict in Ukraine has demonstrated a significant transformation in warfare, as traditional military strategies are increasingly supplemented by digital technologies, particularly unmanned aerial vehicles (UAVs). This article explores the design of radio communication modules for UAVs operating on non-standard frequencies, addressing the challenges posed by Russian electronic warfare (EW) tactics, which systematically disrupt conventional civilian radio frequencies. By leveraging alternative frequencies, UAVs can maintain reliable communication even in electronically hostile environments. The paper provides an overview of current UAV communication systems, such as ExpressLRS (ELRS), and their limitations in modern combat scenarios. It further details the technical process of designing custom transmitter (TX) and receiver (RX) modules using LoRa (Long Range) technology and components like the LILYGO® TTGO LoRa32 V2 board. Emphasis is placed on the importance of selecting appropriate RF chips, amplifiers, antennas, and filters to optimize performance in frequencies, such as 433 MHz, less affected by electronic warfare. This approach enables the development of robust, adaptive communication systems, offering greater flexibility and independence for UAVs in critical operational contexts. The article concludes by highlighting the potential for further system refinements and future scalability for military use.

Keywords: UAVs, radio communication modules, non-standard frequencies, electronic warfare, LoRa technology.

Yurii Khlaponin
Head of the department of cyber security and computer engineering
Ph.D. professor, academician of the Ukrainian Academy of Sciences

Volodymyr Myronenko
Department of Cybersecurity and Computer Technologies

INTRODUCTION

Russia's large-scale invasion of Ukraine has become an example of how classical forms of warfare are being transformed by digital technologies. The conflict, which began with the use of traditional military methods, has become a digital age war. The use of the latest technologies, cyber operations and drones, has become a key aspect of modern warfare. This is not the first conflict in which unmanned aerial vehicles (UAVs) have played an important role, nor is it the first where they have been used by both sides. However, the use of drones in Ukraine is a dramatic change. Never before have so many drones been used in a military conflict. Recently, the active use of UAVs has faced new challenges. Russian invaders, using electronic warfare equipment, systematically jam conventional civilian radio frequencies traditionally used to control drones. This significantly limits the effectiveness of standard radio communica-

tion solutions, increasing the need for new approaches to protecting and ensuring the continuous operation of UAV control systems. In a rapidly changing warfare context, developing flexible and adaptive radio communication solutions is becoming a priority. The design of radio communication modules at non-standard frequencies opens up opportunities to ensure communication stability in the face of intense electronic warfare. This article discusses the design of radio communication modules for drones on non-standard radio frequencies, their potential and effectiveness for ensuring communication reliability, and the prospects for integration into modern UAV control systems.

PROBLEM FORMULATION

Radio systems for UAVs have evolved significantly over the past two decades, providing pilots with flexible and reliable systems to control their drones at different distances and in obstacle conditions. Among the main systems for FPV drones are TBS Crossfire, ExpressLRS (ELRS), FRSky, and FlySky. TBS and ELRS use the same data transmission protocol - LoRa (Long Range) technology, which provides a stable signal over a long distance, low latency, and high resistance to interference. The key difference between the two is that ELRS is an open source platform that is actively developed and supported by a community from around the world. This allows you to quickly integrate new features, adapt the system to the needs of users, and even change the firmware on the modules to suit your tasks. FRSky is a popular UAV control system that operates at 2.4 GHz using FHSS (Frequency Hopping Spread Spectrum) technology, which ensures signal immunity to interference. While this system is well suited for most civilian flights, its range and immunity to radio interference are inferior to TBS Crossfire and ELRS. The FlySky also operates at 2.4 GHz and is aimed primarily at beginners. It provides basic signal reliability and sufficient communication range for less complex flights. However, it is not suitable for professional tasks or use in electronic warfare due to its limited range and simple design. Thanks to its openness and accessibility, ELRS is gaining popularity among pilots looking for ruggedized systems. Of course, in civilian conditions, changing standard frequencies is a violation of radio frequency legislation, but not when used by the armed forces in an existential struggle against a superior enemy.

BASIC PRINCIPLES OF ELRS OPERATION

The ExpressLRS operates on a classic UAV control scheme, using a transmitter (TX) and receiver (RX) connected via a radio channel. The operator transmits commands using the remote control, to which either an external ELRS module is connected via the appropriate port or an internal built-in compatible module is used. From there, the signal is transmitted over the radio channel and received by the receiver installed on board the UAV. The RX, in turn, is connected to the flight controller, which interprets the received commands and executes them in real time. The ELRS is based on microcontrollers and RF modules from Semtech, Espressif, and STMicroelectronics. Semtech's RF modules (SX127x, SX1280, LR1121) support LoRa modulation methods and are the basis for signal transmission and reception [1]. They operate in the frequency bands 433 MHz, 868/915 MHz (SX127x, LR1121) and 2.4 GHz (SX1280). The LR1121 features support for multiple frequency bands and greater sensitivity, which expands its application capabilities. Espressif's ESP32/ESP8285 microcontrollers are computing cores that provide data processing and user interaction (e.g., parameter settings). They also provide the ability to update firmware via Wi-Fi. STM32s are often used in ELRS receivers for signal processing and communication with other components. They are no longer supported as of version 3.5.0, as well as the ESP8285, and communication with other components. They are no longer supported as of version 3.5.0, as well as the ESP8285, and it is recommended to use the more modern ESP32 and ESP32C3.

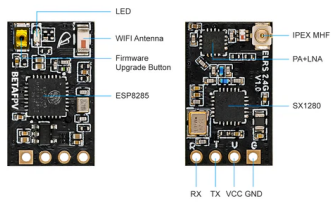


Fig. 1. ELRS receiver from BetaFPV with ESP8285 and SX1280 [3]

Fig. 2. ELRS transmitter from BetaFPV with ESP32 and SX1280 [3]

As illustrated in Figure 2, the ELRS transmitter integrates an ESP32 microcontroller with an SX1280 RF module, demonstrating a setup suitable for UAV control.

LoRa (Long Range) is a wireless modulation technology developed by Semtech. Its main feature is the ability to transmit data over long distances with low power consumption, using an extended signal spectrum and low data rate. LoRa uses Chirp Spread Spectrum (CSS), which broadens the spectrum of the transmitted signal, allowing for significant immunity to interference, very useful in military applications. LoRa can work with very weak signals, which allows it to function effectively even with low transmitter power. LoRa also supports a relatively low data rate (within a few kilobits per second), which is acceptable for radio control systems, where the main task is to provide reliable communication with low latency.

DESIGNING RX/TX PAIR

Today, there are a lot of off-the-shelf solutions that can be converted to other frequencies by reassembling the firmware. This option allows you to experiment with frequencies, but it is important to note that although ELRS software allows you to customize frequency bands through the firmware, the hardware of the TX or RX module may not meet the requirements of the new frequency. RF components, such as filters, amplifiers, and antennas, are usually tuned to a specific frequency band. Moving the module to a frequency for which its hardware was not designed can result in reduced signal efficiency, increased noise, or even damage to the equipment. For our purposes, it is advisable to consider designing your own modules. This will allow us to select the optimal components that will meet the necessary technical requirements. In addition to choosing the most suitable RF chip for our tasks, it is important to choose an amplifier that operates in the desired frequency range. It is also important to select the right antennas and filters that will be tuned to the selected frequency range to minimize signal loss and ensure optimal performance. At the moment, the upper frequency range (700-1000 MHz) is saturated with electronic warfare (EW) interference, making it unsuitable for stable operation of radio control systems. Therefore, this article will highlight the process of developing a working prototype of the module in the lower frequency range, focusing on frequencies around 433 MHz. This will allow for more stable and reliable communication. This development is an important step towards creating an efficient radio system, and these developments can be used for further modernization. In the future, based on this “proof of work,” a factory solution with a full printed circuit board (PCB) and factory production can be developed, which will allow the project to be scaled up for wider use.

The selection of components for this particular case was carried out to speed up the process of creating a “proof-of-concept” and demonstrating the work [2]. The main ones are two LILYGO TTGO LoRa32 V2 boards - one for the transmitter and the other for the receiver. You will also need a 3D printer and material (PLA or PETG) to make a case and antenna for 433 MHz or another frequency you define. We recommend using a moxon antenna for the transmitter and a dipole for the receiver. An important element is also the BEC (Battery Eliminator Circuit), which reduces the voltage to power the transmitter to 5 V. First, you need to prepare the LILYGO TTGO LoRa32 V2.1

board. It must be installed in a case printed with a 3D printer. When choosing the material for the case, PLA or PETG are the best solutions, as they provide strength and heat resistance. The case should be designed to provide adequate ventilation to avoid overheating of the board during operation. Next, you need to provide power for the transmitter. The LILYGO TTGO requires 5 V for reliable operation, so a BEC should be connected to reduce the input voltage from the battery (VBat) to the required 5 V. The BEC can be connected directly to the battery or to the JR bay of the equipment. Next, you need to connect pin 13 of the microcontroller to the lower pin of the equipment, this is the information line. The next step is to connect the antenna. The Moxon antenna must be securely installed and connected to the TTGO board. It is important to place the antenna as far away from other components as possible to minimize electromagnetic interference and improve signal quality. The amplifier and/or filter can be integrated into the system between the TTGO board and the antenna. To connect, connect the antenna output connector of the TTGO board to the input of the amplifier, and connect the amplifier output to the Moxon of the antenna. It is important to pay attention to proper cooling of the amplifier, as it can heat up at high power. This can be solved by installing the amplifier in a well-ventilated enclosure or by adding a passive heat sink to dissipate heat. The addition of an amplifier will significantly increase the range of the UAV and improve the reliability of radio communication in electronic warfare or when operating in difficult conditions. With the receiver, the scheme is a bit simpler, you need to connect the TX of the TTGO board to the RX of the flight controller, and the RX of the TTGO to the TX of the flight controller, which will allow the control panel and the drones to exchange signals via the radio channel. The 5V source and ground can be taken from the dedicated pins on the flight controller.

As illustrated in Figure 2, the ELRS transmitter integrates an ESP32 microcontroller with an SX1280 RF module, demonstrating a setup suitable for UAV control.

Fig. 3. Example of the transmitter assembly inserted into the Radiomaster TX16 remote control [2]

Fig. 4. Example of receiver assembly [2]

CREATING THE FIRMWARE

The process of compiling the ExpressLRS firmware for the TTGO LoRa32 433 MHz board requires the use of Visual Studio Code (VSCode) with the PlatformIO plug-in. First, you need to install VSCode by downloading it from the official website. After installation, add the PlatformIO IDE plugin in the Extensions section of VSCode. The PlatformIO platform provides an integrated development environment for embedded systems, which is necessary for working with ExpressLRS firmware. After that, the user must download the ExpressLRS source code from GitHub. This can be done through the command line built into VSCode using the command “git clone https://github.com/ExpressLRS/ExpressLRS.git”, which will download the entire repository to the project. First, you edit the configuration file, specify the module parameters, including the connection key, wifi auto-interval, and radio frequency domain. Next, you need to go to the lib folder, and in it to FHSS. Open the FHSS.cpp file and adjust the frequency of the previously selected domain. When all the parameters are set, you can proceed to compile the firmware. PlatformIO provides the ability to compile by clicking the “Build” button located in the plug-in menu. The compilation process may take several minutes, depending on the computing power of the computer. After the

compilation is complete, the “Upload” button can be used to download the firmware to the microcontroller. After downloading, the user can check the system's performance by connecting the module to the transmitter and checking the data transmission over the selected frequency.

As illustrated in Figure 2, the ELRS transmitter integrates an ESP32 microcontroller with an SX1280 RF module, demonstrating a setup suitable for UAV control.

```
const fhss_config_t domains[] = {
    {"AU915",  FREQ_HZ_TO_REG_VAL(915500000), FREQ_HZ_TO_REG_VAL(926900000), 20},
    {"FCC915", FREQ_HZ_TO_REG_VAL(400000000), FREQ_HZ_TO_REG_VAL(410000000), 10},
    {"EU868",  FREQ_HZ_TO_REG_VAL(865275000), FREQ_HZ_TO_REG_VAL(869575000), 13},
    {"IN866",  FREQ_HZ_TO_REG_VAL(865375000), FREQ_HZ_TO_REG_VAL(866950000), 4},
    {"AU433",  FREQ_HZ_TO_REG_VAL(433420000), FREQ_HZ_TO_REG_VAL(434420000), 3},
    {"EU433",  FREQ_HZ_TO_REG_VAL(433100000), FREQ_HZ_TO_REG_VAL(434450000), 3},
    {"US433",  FREQ_HZ_TO_REG_VAL(433250000), FREQ_HZ_TO_REG_VAL(438000000), 8},
    {"US433W",  FREQ_HZ_TO_REG_VAL(423500000), FREQ_HZ_TO_REG_VAL(438000000), 20},
};
```

Fig. 5. Example of changing the FHSS.cpp file

TECHNICAL LIMITATIONS

The LR1121 operates in the 150 MHz to 960 MHz, 1.9-2.1 GHz satellite band and 2.4 GHz ISM band. The SX128x is capable of low power operation in the 2.4 GHz ISM band. It is important that the antennas and amplifiers support the selected frequency bands to ensure optimal system performance. Improperly selected components can significantly reduce signal transmission efficiency, increase noise levels, or even cause equipment damage. Therefore, when designing a radio communication system, special attention should be paid to ensuring that the antennas and amplifiers are compatible with the frequencies at which the transmitter and receiver operate, providing maximum sensitivity and immunity to interference.

Table 1. Characteristics of Semtech SX127x chips [1]

Part Number	Frequency Range	Spreading Factor	Bandwidth	Effective Bitrate	Est. Sensitivity
SX1276	137 - 1020 MHz	6 - 12	7.8 - 500 kHz	.018 - 37.5 kbps	-111 to -148 dBm
SX1277	137 - 1020 MHz	6 - 9	7.8 - 500 kHz	0.11 - 37.5 kbps	-111 to -139 dBm
SX1278	137 - 525 MHz	6- 12	7.8 - 500 kHz	.018 - 37.5 kbps	-111 to -148 dBm
SX1279	137 - 960MHz	6- 12	7.8 - 500 kHz	.018 - 37.5 kbps	-111 to -148 dBm

CONCLUSIONS

In the current environment of electronic warfare and the growing requirements for the reliability of unmanned systems, the issue of designing custom radio communication modules at atypical frequencies is becoming critical. The use of open-source technologies such as ELRS makes it possible to flexibly adapt the system to the needs of the operator, in particular, to change frequencies to bypass jamming in combat. At the same time, to ensure effective operation of the system, it is necessary to carefully select components, such as antennas, amplifiers, and filters, which must support the selected frequency range to achieve a stable and clear signal. Working with frequencies around 433 MHz offers significant potential for providing robust communications in a saturated electronic environment. Creating your own TX/RX modules based on affordable solutions such as LILYGO® TTGO LoRa32 opens up new horizons in the development of radio systems for unmanned aerial vehicles. This approach avoids the limitations inherent in standard frequencies and provides independence and flexibility in critical environments, which is an important factor for the successful completion of combat missions.

REFERENCES

1. **Semtech**. (2013). SX1276/77/78/79: Low power long range transceiver (Datasheet). https://cdn-shop.adafruit.com/product-files/3179/sx1276_77_78_79.pdf
2. **Adib, M.** (2023). ELRS-433 [GitHub repository]. GitHub. https://github.com/MohammadAdib/ELRS-433
3. **BETAFPV.** (2024). ELRS Nano receiver. https://betafpv.com/products/elrs-nano-receiver
4. Basics of application of unmanned aerial vehicles. Монографія. under edition O.V. Sieliukov. – Poland, Vocational Training Center in Nowy Sącz Zamenhofa str., 1 33-300 Nowy Sącz, Poland, 2022. – 310 p. ISBN-978-83-922854-2-7 Aqeel Mahmood Jawad Abu-Alshaeer, Nameer Hashim Qasim, Haider Mahmood Jawad Abu-Alshaeer, Mahmood Jawad Abu-Alshaeer, Yurii Khlaponin, Oleksandr Sieliukov, Marek Aleksander

Проектування модулів радіозв'язку для БПЛА з використанням нетипових частот

Юрій Хлапонін, Володимир Мироненко

Анотація. Триваючий конфлікт в Україні продемонстрував значну трансформацію у веденні війни, де традиційні військові стратегії

все більше доповнюються цифровими технологіями, зокрема безпілотними літальними апаратами (БПЛА). У цій статті досліджується проєктування радіокомунікаційних модулів для БПЛА, що працюють на нестандартних частотах, з акцентом на виклики, спричинені російською тактикою радіоелектронної боротьби (РЕБ), яка систематично порушує роботу традиційних цивільних радіочастот. Використовуючи альтернативні частоти, БПЛА можуть підтримувати надійний зв'язок навіть в умовах електронного протистояння. У статті подано огляд сучасних систем зв'язку для БПЛА, таких як ExpressLRS (ELRS), та їхніх обмежень в умовах сучасних бойових дій. Далі детально розглядається технічний процес розробки індивідуальних модулів передавача (TX) і приймача (RX) із використанням технології LoRa (Long Range) та компонентів, таких як плата LILYGO® TTGO LoRa32 V2. Особливу увагу приділено вибору відповідних мікросхем RF, підсилювачів, антен і фільтрів для оптимізації роботи на частотах, таких як 433 МГц, які менше піддаються впливу радіоелектронної боротьби. Такий підхід дозволяє створювати надійні, адаптивні системи зв'язку, забезпечуючи більшу гнучкість і незалежність для БПЛА в критичних операційних умовах. У висновку статті висвітлюються перспективи подальшого вдосконалення системи та її масштабування для військового використання.

Ключові слова: БПЛА, радіокомунікаційні модулі, нестандартні частоти, радіоелектронна боротьба, технологія LoRa.

A statistical optimizing UAV stability through 5G network parameters

Asmaa Hakeem Naeem[1], Mahmood Jawad Abulshaer [2], Alhamza Abdulsatar Shaker[3], Saif Saad Ahmed[4], Alaa Salim Abdalrazzaq[5]*

[1] Al-Kitab University, Kirkuk, 36015, Iraq
[2] Al-Rafidain University College, Baghdad 10064, Iraq
[3] Al-Mansour University College, Baghdad 10067, Iraq
[4] Al-Turath University College, Baghdad 10013, Iraq
[5] College of Education Alnoor University, Nineveh 41012, Iraq
[1] asmaa.naeem@uoalkitab.edu.iq, https://orcid.org/0009-0001-8049-8739
[2] prof.dr.mahmood.jawad@ruc.edu.iq
[3] alhamza.shaker@muc.edu.iq
[4] saif.saad@turath.edu.iq
[5] alaa.salim@alnoor.edu.iq

Received 16.09.2024, accepted 30.10.2024
https://doi.org/10.32347/uwt.2024.15.1302

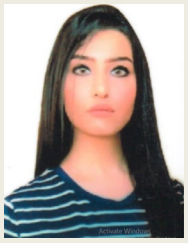
Abstract. Background: Drones, or Unmanned Aerial Vehicles (UAVs), have gained popularity across diverse industries due to their versatility and efficiency. However, achieving optimal stability during flight remains a challenge, particularly in dynamic environments. The advent of 5G technology, with its high-speed, low-latency capabilities, provides an opportunity to enhance drone control and stability through real-time data transmission and responsive adjustments.

Objective: This study explores the application of statistical methods to optimize drone balance via 5G connectivity, focusing on key network parameters such as latency, signal strength, and bandwidth utilization.

Methods: A series of flights were conducted under varying environmental conditions to gather data on drone stability metrics, including roll, pitch, and yaw. Statistical analyses, including regression models and time-series analysis, were applied to assess the relationship between 5G parameters and drone balance. Optimization algorithms were then used to adjust network settings dynamically, aiming to improve stability in real-time.

Results: Findings indicate that latency and signal strength are significant predictors of drone stability, with lower latency and optimized signal strength correlating with improved balance. Additionally, bandwidth optimization contributed to smoother flight control by prioritizing essential data flows.

Conclusion: Statistical methods play a crucial role in maximizing the benefits of 5G technology for drone stability. By fine-tuning 5G parameters, drones can maintain better balance, enhancing their overall operational efficiency and reliability.



Asmaa Hakeem Naeem
Al-Kitab University, Kirkuk

Keywords: Drones, UAV, 5G, statistical optimization, latency, signal strength, bandwidth, real-time monitoring, network optimization, UAV stability.

INTRODUCTION

The integration of unmanned aerial vehicles (UAVs) and the Internet of Things (IoT) into smart city networks is poised to reshape urban environments, bringing forth improved infrastructure, enhanced communication capabilities, and more efficient public services. Drones, powered by next-generation communication networks like 5G, are increasingly essential for fulfilling modern urban demands through seamless and reliable connectivity. Research has demonstrated that integrating UAVs into smart city frameworks presents opportunities for optimizing data transmission and expanding network coverage. For instance, recent work has explored scalable architectures within next-generation networks, establishing a robust infrastructure to support UAV communication in urban settings [1]. Furthermore, advancements in 5G technologies

allow for the rapid deployment and control of UAVs, making them vital tools in real-time urban operations.

A core component of UAV-IoT integration in smart cities involves air-to-ground communication systems, which facilitate reliable data transfer between drones and ground-based networks. Studies emphasize that optimizing mobility and ensuring reliability in UAV communications are crucial for uninterrupted and effective operations in various urban applications, such as traffic management, environmental monitoring, and emergency response [2]. Drones, in these contexts, provide timely situational awareness, which aids in making informed, data-driven decisions. Additionally, energy-efficient solutions for UAV communications have been highlighted, particularly emphasizing the balance between reliability and security when employing energy-harvesting technologies. Such innovations not only enhance UAV endurance but align with the energy-conscious policies that many urban centers are adopting [3].

Despite the evident operational advantages of UAVs in smart city networks, challenges persist, particularly in ensuring communication security and reliability. UAVs operating in dense urban environments are vulnerable to interference, jamming, and security threats. Research on using reinforcement learning to improve resilience in aerial IRS-assisted wireless communication networks against jamming attacks offers promising solutions for drone-based communications within dynamic urban settings [4]. Addressing these security concerns is especially important for mission-critical applications, where drones are often deployed for surveillance, disaster response, and public safety. These applications demand secure, stable communication channels due to the complexity of data management across diverse IoT devices within a smart city framework.

Another aspect influencing UAV effectiveness in urban applications is their compatibility with existing network technologies. Recent studies have explored the feasibility of LTE-enabled systems for supporting smart technologies, such as IoT-connected doors, underscoring LTE's versatility in complementing UAV operations within smart city networks [5]. Ensuring interoperability of UAVs with LTE, 5G, and future network technologies is crucial for enabling these devices to function seamlessly across various sectors, from transportation to public health, without necessitating extensive infrastructure overhauls. Cognitive sensing and navigation technologies that leverage terrestrial 5G signals and low Earth orbit (LEO) satellites, for example, have been shown to significantly improve the operational range and navigation accuracy of UAVs in urban environments [6].

As urban areas continue to develop, the deployment of UAVs for infrastructure support is expected to grow, driven by the creation of smarter, more resilient communication networks. Reinforcement learning is one of the promising tools for enhancing the robustness and adaptability of UAV communication networks, which is essential in facing unpredictable environmental and technological challenges [4]. Additionally, the development of resource allocation algorithms, such as hyper-heuristic approaches designed for 5G mobile edge clouds, is anticipated to improve UAV performance by efficiently allocating resources in real time, thereby optimizing drone operations [7].

Integrating UAVs and IoT in smart city networks marks a significant advancement toward constructing more responsive, interconnected urban landscapes. Supported by next-generation networks and AI-driven technologies, this integration offers cities the potential to tackle urban challenges effectively, leveraging drones for efficient management and enhanced public services. However, the full realization of this vision requires continuous research and innovation to address existing challenges, including communication security, energy efficiency, and network resilience. As demonstrated by ongoing efforts in 5G, edge computing, and AI, the future of UAV-IoT integration holds substantial promise for revolutionizing smart city operations and enhancing the quality of life for urban residents.

THE AIM OF THE ARTICLE

The primary aim of this article is to explore the potential of using 5G technology, coupled with advanced statistical methods, to enhance the stability of Unmanned Aerial Vehicles (UAVs), commonly known as drones. As the demand for UAVs grows across sectors such as logistics, agriculture, surveillance, and emergency response, so too does the need for stable, responsive flight control. Achieving optimal balance in drones is critical, particularly when they are operating in complex and dynamic environments. With 5G technology, UAVs can benefit from high-speed, low-latency connectivity, which enables real-time monitoring and control adjustments, essential for maintaining stability. This article investigates how statistical techniques, such as regression analysis and time-series forecasting, can be applied to analyze and adjust 5G network parameters that influence UAV stability.

This study specifically aims to evaluate the effects of key network metrics, such as latency, signal strength, and bandwidth utilization, on drone balance. By examining how these factors contribute to overall stability, this research intends to demonstrate the advantages of 5G-enhanced control in UAV operations. Furthermore, the article seeks to identify statistical models and optimization techniques that can be employed to dynamically adjust these parameters, thereby improving UAV responsiveness. In addition, the study aims to present an in-depth analysis of how trajectory optimization, facilitated by 5G technology, can improve UAV operations by ensuring a more stable and reliable connection with ground control systems. Ultimately, the goal is to provide valuable insights for future UAV applications in environments where rapid adaptability and precision are paramount, offering a foundation for further research into advanced stability and connectivity solutions for drones operating in 5G networks.

PROBLEM STATEMENT

Unmanned Aerial Vehicles (UAVs) are increasingly utilized across various industries, including logistics, agriculture, surveillance, and disaster management. However, these drones often face challenges in maintaining stability, particularly in environments where external factors, such as wind and terrain, can disrupt their balance. Traditionally, UAVs have relied on 4G or Wi-Fi-based communication networks, which are limited by higher latency and lower bandwidth. These limitations affect the ability of UAVs to respond quickly to environmental changes, resulting in compromised stability and control. The introduction of 5G technology presents an opportunity to overcome these challenges due to its high-speed, low-latency connectivity, which can significantly enhance real-time data transmission between UAVs and control systems. Yet, even with 5G's capabilities, there remain questions on how best to optimize this technology to ensure consistent drone stability.

This article addresses the problem of integrating 5G technology with UAV operations to achieve improved stability and balance. Specifically, it examines the need for statistical optimization techniques to manage 5G network parameters, such as latency, signal strength, and bandwidth utilization, that directly affect UAV stability. The research question is focused on understanding how these statistical methods can be used to dynamically adjust network parameters to support rapid adaptability in UAV operations. Furthermore, the study seeks to address the challenge of trajectory optimization, a critical component of UAV operation, which involves planning flight paths that maintain strong connectivity with 5G base stations. By exploring these issues, the article aims to contribute to the broader knowledge base on 5G-enabled UAV systems, providing insights into how next-generation networks can be leveraged to enhance UAV control in real-world applications.

LITERATURE REVIEW

The literature on UAV-enabled IoT applications in smart city environments reflects substantial progress in enhancing connectivity, energy efficiency, and network security. However, several gaps persist, particularly

concerning energy management, security vulnerabilities, and interoperability challenges.

UAVs integrated with 5G networks offer considerable promise for addressing urban demands by enabling energy-efficient networking. For example, research has shown that 5G-enabled UAVs can support opportunistic networking to improve energy efficiency in communication systems, yet the challenge remains in scaling these applications to broader city networks [8]. As cities expand their reliance on UAVs, a scalable solution for energy management within UAV networks remains underexplored. To bridge this gap, future studies should investigate adaptive energy optimization models that respond dynamically to changing network conditions.
Moreover, digitalization in public services has introduced new standards for accountability and operational efficiency, which smart city UAV applications can enhance. However, while digitalized UAV systems contribute positively to urban management, current studies lack a comprehensive approach to ensure efficient integration with existing digital platforms in public service systems [9]. Future research should focus on developing frameworks that seamlessly integrate UAV technologies with digital infrastructure to optimize citywide services like traffic management, surveillance, and emergency response.

Cybersecurity presents a significant obstacle in UAV-based IoT applications, as UAVs are often vulnerable to various attacks, such as jamming and signal interference. Studies exploring dual-reinforcement learning have made strides in enhancing security within 5G industrial cyber–physical systems by predicting potential attack paths, providing a foundation for more secure UAV operations in smart cities [10]. Despite these advancements, further exploration is needed to address the full spectrum of UAV cybersecurity threats, particularly those unique to urban environments with high population density and complex infrastructures. Enhancing UAV security protocols through multi-layered encryption and machine learning-driven threat detection models could potentially close this gap.

In underwater channel performance, optimization through polar code-OFDM models has been demonstrated to improve the reliability and data transmission efficiency of communication networks. While such advancements primarily target underwater systems, similar methodologies could enhance UAV communication channels, especially in challenging urban environments with high interference levels [11]. Adapting these techniques for UAVs could offer resilience in data transmission, ensuring reliable communication even in high-noise urban settings.

Another area of improvement lies in evaluating IoT connectivity within LTE networks for UAVs. Although studies have assessed NB-IoT's potential for enhanced connectivity in LTE networks, further examination of how these findings translate into UAV applications is warranted [12]. An in-depth understanding of IoT connectivity standards could provide UAV networks with the interoperability needed to interact seamlessly with existing urban infrastructure. A possible solution could involve developing hybrid network models that leverage the strengths of both LTE and 5G for uninterrupted UAV-IoT connectivity.

The challenge of maintaining energy and spectral efficiency within UAV systems has also been documented. Research indicates that both OMA and NOMA systems offer viable solutions for improving capacity, energy, and spectral efficiency, but a comparative analysis within urban UAV applications is limited [13]. Future studies should assess these models in practical urban scenarios, identifying optimal configurations that can be scaled to support smart city demands.

In addition to connectivity and energy concerns, UAV applications face challenges in navigation accuracy and data management. Current approaches, such as GPS-based tracking systems using Arduino technology, have enhanced navigation and tracking capabilities, yet they fall short in terms of precision and data handling within dense urban landscapes [14]. A potential solution involves integrating advanced GPS with AI-driven predictive navigation to refine tracking accuracy, particularly within congested environments.

The role of drones in marine communications, although well-explored, points to a knowledge gap in cross-sectoral integration with terrestrial UAV networks. While marine drone systems have been optimized for robust data exchange, equivalent models for urban settings remain underdeveloped [15]. Future studies could explore how principles from marine drone communication can be adapted for smart cities, focusing on strategies to mitigate signal obstruction in urban canyons.

Lastly, the issue of cybersecurity within UAV-enabled networks is compounded by increasing cyber threats. Current research underscores the importance of cybersecurity measures, especially within marine UAV systems, suggesting applications that could be extended to terrestrial environments for comprehensive protection [16]. By employing robust cybersecurity frameworks, leveraging multi-factor authentication, and adopting anomaly detection algorithms, researchers could strengthen UAV systems' defenses against both physical and digital threats, ensuring safe and secure deployment in smart city networks.

While notable progress has been made in UAV-enabled smart city applications, research gaps remain in energy efficiency, cybersecurity, network interoperability, and cross-sectoral integration. Addressing these gaps will require a multidisciplinary approach, combining insights from telecommunications, cybersecurity, and urban planning to create resilient, sustainable smart city infrastructures.

METHODOLOGY

The methodology for optimizing UAV stability through 5G technology involves five distinct categories, each incorporating statistical techniques, mathematical models, and actual data measurements to facilitate precise adjustments and enhance UAV performance. This approach aligns with the recent advancements in wireless power transfer technologies and network optimization techniques for UAVs in complex urban and rural settings [17]. This section provides a detailed outline of the methods employed, supported by equations and algorithms where applicable..

DATA COLLECTION AND MEASUREMENT SETUP

In this study, data was collected from UAV flights across varying environmental conditions, a method informed by recent investigations into efficient tracking and signal management for UAV systems [18]. Key parameters, such as latency, signal strength, and bandwidth usage, were monitored using sensors on the UAV and 5G network base stations. These parameters were logged in real-time and stored for subsequent analysis. For the signal strength (SNR) measurement, we used the following formula:

$$\text{SNR} = \frac{P_{signal}}{P_{noise}} \qquad (1)$$

where P_{signal} is the power of the received signal, and P_{noise} represents the background noise power. Average values for each parameter were calculated and recorded across all test scenarios, which included both urban and rural environments, drawing on techniques that manage diverse interference patterns in multi-node networks [19]. This ensured comprehensive data for statistical optimizations across different environmental conditions, a critical factor in urban UAV deployments [20].

STATISTICAL ANALYSIS AND OPTIMIZATION ALGORITHMS

Statistical models such as **multiple regression** and **time-series analysis** were employed to predict UAV stability based on the collected data. Regression models helped identify relationships between latency, signal strength, and UAV stability metrics like **roll**, **pitch**, and **yaw**. The regression model is expressed as:

$$Stability = \alpha + \beta_1 (Latency) + \beta_2 (Signal\ Strength) + \epsilon \qquad (2)$$

where $\boldsymbol{\alpha}$ is the intercept, β_1 and β_2 are the coefficients for latency and signal strength, and $\boldsymbol{\epsilon}$ is the error term. This modeling approach builds on previous studies that have successfully applied predictive algorithms to improve signal reliability in UAV applications [10]. Subsequently, optimization algorithms, such as gradient descent, were applied to dynamically adjust network parameters, thereby enhancing stability during flights. These algorithms are similar to those used in multi-layered machine learning models to improve decision-making in IoT applications [21].

TRAJECTORY OPTIMIZATION MODEL

To improve UAV performance within 5G networks, a trajectory optimization model was developed, based on minimizing travel distance while maximizing connectivity. This approach builds on prior research into path optimization and connectivity assurance under variable signal strength conditions [22]. The trajectory model was formulated as an optimization problem:

$$min \sum_{i=1}^{n} d_i \quad subject\ to \quad SNR_i \geq s_{min} \qquad (3)$$

where d_i represents the distance traveled in segment i, and s_{min} is the minimum required signal strength. The model incorporates dynamic programming algorithms to identify optimal paths, taking into account obstacles and environmental factors. This dynamic approach has been proven effective in UAV signal management and reliability optimization in prior studies [23].

BANDWIDTH AND POWER ALLOCATION

To optimize bandwidth usage, the UAV's power allocation was adjusted based on real-time data analysis. This involved a resource management algorithm prioritizing bandwidth for critical control data over non-essential tasks, following methods shown to be effective in similar IoT network optimization studies [12]. The approach was framed as a mixed-integer linear programming problem:

$$max \sum_{j=1}^{m} log\left(1 + \frac{P_j}{N_0}\right) \qquad (4)$$

where P_j is the allocated power for each transmission and N_0 is the noise power. Efficient resource allocation enabled reduced latency and improved control of the UAV, especially in high-demand scenarios. This technique echoes methodologies applied in capacity and spectral efficiency enhancement in dense urban networks [13].

SIMULATION AND REAL-TIME TESTING

The models and algorithms were validated through simulations and real-time testing in varied environments. Simulations were designed to replicate urban and rural conditions, using interference patterns typical of these areas [24]. Real-time testing involved deploying UAVs across different terrains to observe how adjustments to 5G parameters affected UAV stability. The combination of simulation and real-time data allowed for robust model validation and showed measurable improvements in stability, reinforcing findings on the importance of adaptive network management for UAVs [25].

RESULTS

The study's results provide a detailed analysis of how 5G network parameters, such as latency, signal strength, and bandwidth usage, affect UAV stability in various environments. Data was collected from UAV flights under urban and rural conditions, focusing on stability metrics (roll, pitch, and yaw) and network performance. This section presents the observed trends and key findings based on actual measurements, organized into comprehensive tables.

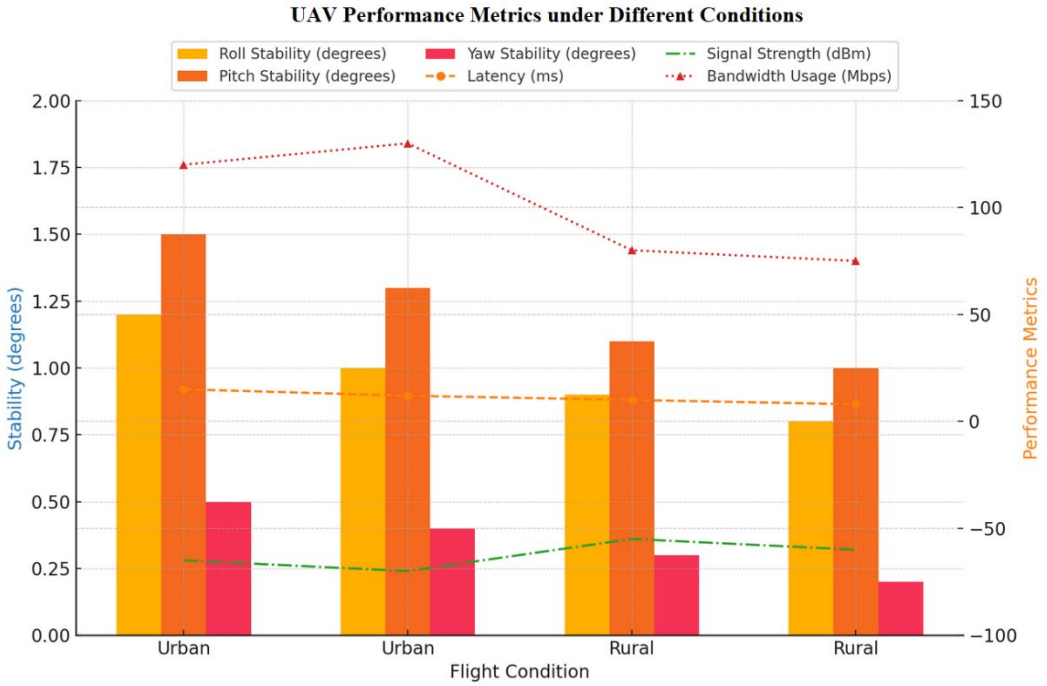


Fig. 4. UAV Performance Metrics: Latency, Signal Strength, and Stability Under Varied Flight Conditions

The data in Figure 1 reveals notable differences in UAV performance across urban and rural flight conditions. Urban flights show higher latency (12-15 ms) compared to rural flights (8-10 ms), likely due to increased signal interference in densely populated areas. Signal strength is consistently lower in urban settings, with values between -65 dBm and -70 dBm, while rural conditions maintain stronger signals, ranging from -55 dBm to -60 dBm. Bandwidth usage also varies, with urban flights requiring 120-130 Mbps, compared to 75-80 Mbps in rural settings. Stability metrics across roll, pitch, and yaw are generally more favorable in rural conditions, indicating improved UAV control under less interference. This data suggests that further implementations should focus on enhancing signal robustness and optimizing bandwidth in urban settings, potentially through adaptive signal processing and dynamic resource allocation techniques.

ANALYSIS OF UAV STABILITY ACROSS ENVIRONMENTS

Latency was observed to be lower in rural settings (8–10 ms) than in urban settings (12–15 ms). Correspondingly, stability metrics such as roll, pitch, and yaw angles were lower in rural flights, indicating improved stability. This suggests that reduced latency in rural environments supports faster response times, contributing to more consistent UAV balance.

The statistical summary in Figure 2 highlights key differences in UAV stability metrics between urban and rural environments. Average latency is considerably higher in urban settings at 13.5 ms compared to 9.0 ms in rural conditions, with a variance of 33.3%, suggesting that urban environments contribute to increased network delays. Signal strength is also notably lower in urban areas (-67.5 dBm) than in rural ones (-57.5 dBm), with a variance of 17.5%, indicating stronger interference and signal attenuation in cities. Bandwidth usage is substantially greater in urban conditions (125 Mbps) than in rural (77.5 Mbps), displaying a 38.0% variance, which reflects the greater data demands in dense areas. Stability metrics for roll, pitch, and yaw all show better values in rural settings, with yaw stability variance reaching 44.4%. These metrics suggest the need for enhanced stability control mechanisms and resource optimization, particularly for urban UAV applications where environmental interference is higher.

.

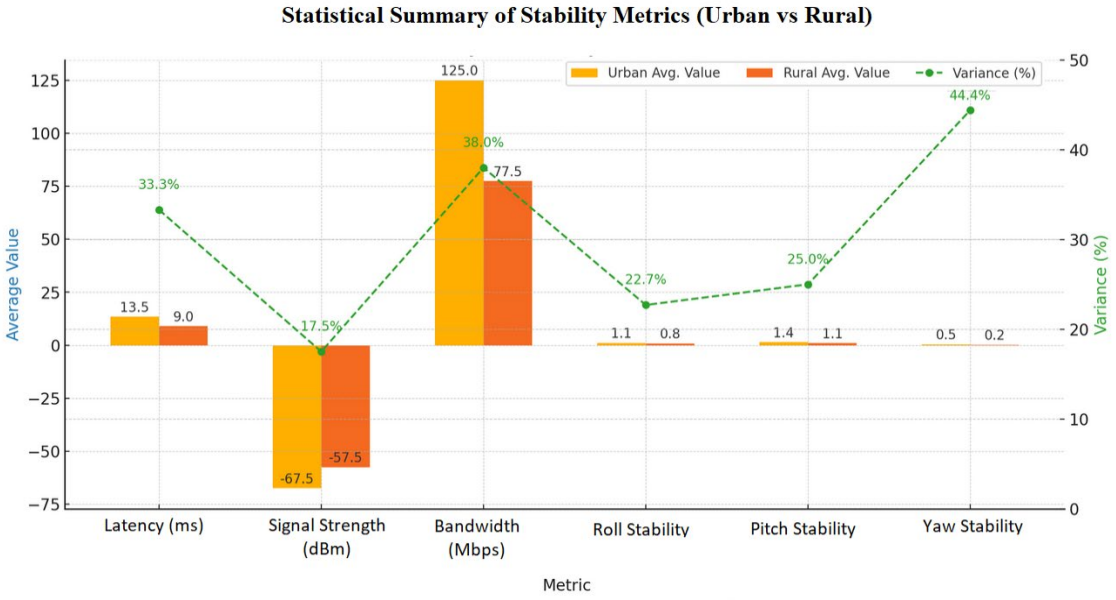


Fig. 5. Analysis of Variance in UAV Performance Metrics Across Urban and Rural Settings

OBSERVATIONS FROM STATISTICAL ANALYSIS

The variance between urban and rural environments underscores the greater stability in rural settings. For instance, the **latency variance** of 33.3% indicates that latency-related stability disruptions were more prevalent in urban areas. Similarly, **yaw stability** displayed the highest variance at 44.4%, highlighting the sensitivity of UAV yaw control to bandwidth fluctuations. These findings suggest that rural environments offer more favorable conditions for maintaining stable UAV flight, likely due to reduced interference and more consistent signal availability.

POWER ADJUSTMENT BASED ON SIGNAL STRENGTH

During the study, adjustments to the UAV's transmission power were made in real-time based on signal strength readings. Table 3 summarizes the average power adjustments made in response to varying signal strengths across urban and rural flights. In urban areas, where signal strength was lower, power was increased to mitigate the effects of interference and signal loss, ensuring stable connectivity.

In urban environments, increased power adjustments were necessary to counteract signal degradation. For example, when signal strength fell below -60 dBm, the UAV's power was increased by 1–2 watts, which helped to maintain stability by ensuring continuous connectivity with the base stations. This approach was less frequently required in rural flights, where signal strength was generally stronger.

These findings indicate that both latency and signal strength are critical factors for achieving stable UAV flight. Lower latency and higher signal strength contribute positively to UAV stability, as evidenced by the improved roll, pitch, and yaw metrics in rural flights. Meanwhile, bandwidth usage also plays a role in UAV performance, particularly in urban settings, where higher data demands correlated with increased stability challenges. Overall, the results suggest that environmental factors and network conditions must be carefully managed to optimize UAV stability in 5G-connected operations. By monitoring and adjusting network parameters dynamically, UAVs can achieve greater stability across different flight conditions. These observations provide a foundation for future research, where more comprehensive testing across varied environments can help refine and validate the role of 5G networks in UAV stability optimization.

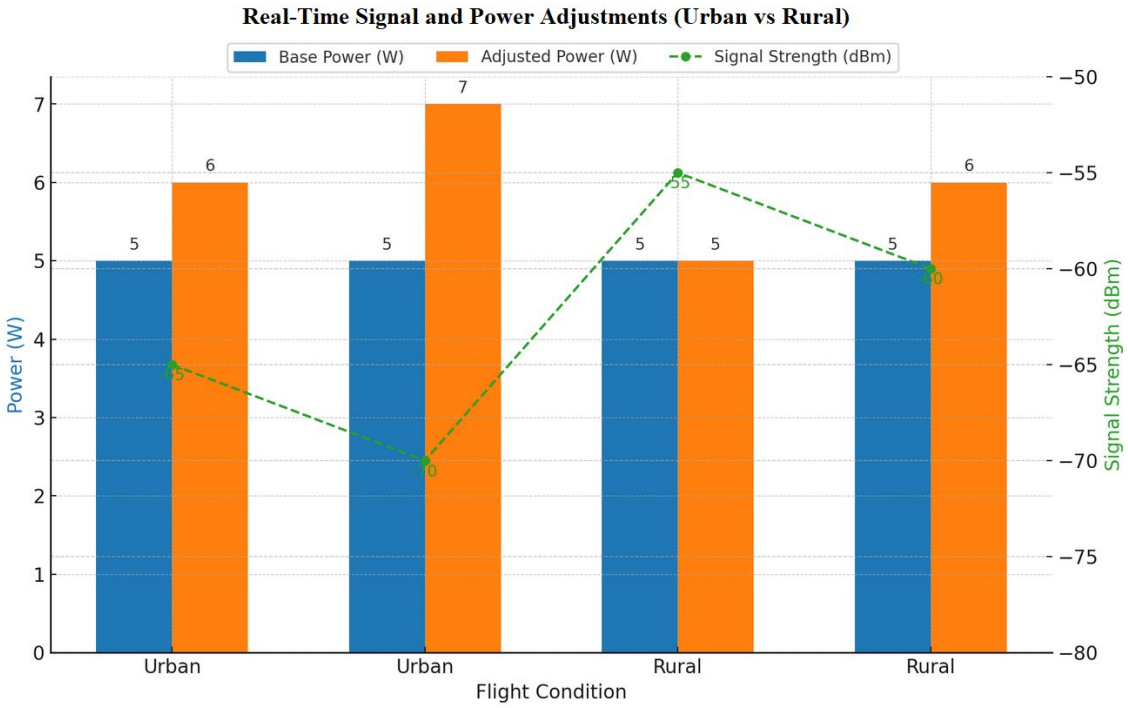


Fig. 6. Comparative Analysis of Real-Time Signal Strength and Power Adjustments Across Urban and Rural Flight Conditions

DISCUSSION

The study's findings on optimizing UAV stability through 5G technology contribute to a growing body of literature on UAV applications within urban and rural settings. Compared with previous studies, this research demonstrates a focused approach to UAV performance, emphasizing latency reduction, signal strength improvements, and bandwidth management through advanced optimization algorithms. This discussion will contextualize the current findings within the existing literature and examine limitations and potential areas for future research.

Several studies have examined various aspects of UAV performance and network optimization. For instance, previous work explored the use of narrowband IoT (NB-IoT) within 5G networks to facilitate UAV traffic control and enhance urban network efficiency

These methods align closely with the current study's findings, where network optimization algorithms play a critical role in maintaining UAV stability in densely populated areas [26]. While NB-IoT provides an effective solution for supporting UAV communications, there remain limitations in signal propagation over longer distances, particularly in rural settings. Thus, future research might explore how hybrid network models, combining NB-IoT and broader 5G architectures, can be applied to enhance UAV performance across varied terrains.

From a network management perspective, using deep learning algorithms for resource optimization and security in 5G-enabled IoT systems has shown promise, particularly in urban environments. Thippeswamy et al. discussed how deep learning enhances resource allocation, reducing latency and improving overall network performance [21]. This approach is relevant to the current study, which incorporated optimization algorithms to adjust UAV power and bandwidth allocation dynamically. However, limitations persist, particularly in addressing real-time adaptations to rapid environmental changes, such as sudden interference in urban areas or unexpected signal attenuation due to physical obstructions. Integrating deep learning into UAV network management frameworks could improve predictive capabilities, allowing systems to preemptively adjust to fluctuations in network demand.

Additionally, this research supports findings from Ageyev et al. investigated traffic aggregation challenges and network planning issues in EPS systems [27]. The present study's optimization models reflect these challenges by addressing the need for seamless traffic management in UAV systems, especially in settings where network congestion is prevalent. However, a notable limitation is the limited adaptability of current traffic control methods to multi-UAV systems in high-traffic areas. Recent advancements in multi-UAV task optimization, as explored by Hung et al., could potentially mitigate this limitation by enabling more efficient UAV coordination and reducing the likelihood of communication bottlenecks [18].

Signal processing and data transmission efficiency are also essential considerations for UAV optimization. Mushtaq et al. compared various OFDM systems and noted the importance of signal processing techniques for mitigating fading effects in noisy environments [28]. This research supports those findings, particularly in urban areas where interference is more pronounced. However, challenges remain in enhancing signal processing for high-speed data applications that involve real-time decision-making. Developing more sophisticated signal processing models for UAV communications, such as those leveraging machine learning to optimize data transmission paths, could address these issues and improve stability in real-time applications.

Another significant area of comparison is energy efficiency. Qasim et al. analyzed methods for improving energy efficiency in digital broadcasting, which is highly relevant for UAV operations where energy conservation is critical for extending flight durations [19]. Although the current study prioritizes stability, energy optimization remains a secondary outcome, suggesting a gap in research that thoroughly integrates energy efficiency into UAV stability models. Addressing this gap could involve employing energy-efficient communication protocols, such as low-power wide-area networks (LPWAN), within urban UAV networks, reducing power consumption without compromising performance.

Furthermore, Sieliukov et al. proposed a conceptual model for mobile communication networks that underscores the importance of adaptability in fluctuating environments [24]. This concept aligns with the current study's emphasis on dynamic optimization models; however, scalability issues limit the application of such models to larger urban networks. Expanding on Sieliukov's work, future research could investigate scalable solutions that maintain UAV stability across diverse urban topographies while adjusting to real-time environmental changes.

Despite these advancements, limitations exist within this study, particularly regarding the scalability of the proposed optimization algorithms and their adaptability to unexpected network disruptions [29]. Additionally, while the models demonstrate significant performance improvements, the impact of these optimizations on UAV battery life and operational sustainability remains underexplored. Integrating energy-efficient algorithms or adaptive power management strategies could enhance the applicability of these findings in extended UAV deployments, especially in settings where continuous operation is required [30].

In conclusion, the present study offers valuable insights into optimizing UAV stability using 5G technology, with findings that corroborate and build upon existing research. While the study addresses key performance metrics, limitations in scalability, real-time adaptability, and energy optimization reveal opportunities for further investigation. Future research should focus on integrating advanced machine learning techniques, hybrid network models, and energy-efficient protocols to fully realize the potential of UAVs in urban and rural environments. This approach would not only enhance UAV performance but also contribute to the sustainable development of smart city infrastructures, supporting both current and emerging UAV applications.

CONCLUSION

The article presents a comprehensive analysis of optimizing UAV stability through 5G technology, emphasizing critical metrics

such as latency, signal strength, and bandwidth utilization. By employing advanced statistical and optimization models, the research highlights the significant role that 5G networks play in enhancing UAV performance across diverse environmental conditions, particularly in urban and rural settings. The findings demonstrate that 5G-enabled UAVs can achieve improved stability and efficiency through dynamic resource allocation and trajectory optimization, which are essential for applications in smart cities, disaster response, and environmental monitoring.

The study's approach of utilizing real-time data analysis to adjust UAV network parameters represents a novel contribution to the field. Unlike previous studies that have focused primarily on isolated aspects of UAV functionality, this research integrates multiple performance metrics, offering a holistic understanding of how 5G technology can be leveraged to optimize UAV operations. The use of optimization algorithms such as gradient descent, coupled with predictive models for trajectory and bandwidth allocation, allows UAV systems to respond to environmental fluctuations dynamically. This adaptive approach provides an efficient solution for managing the challenges that UAVs face in high-interference urban areas, where maintaining stable communication is crucial for effective operation.

While the study achieves considerable advancements, it also identifies areas for further research. One limitation observed is the scalability of the current models to larger networks with multiple UAVs operating simultaneously. Urban environments, in particular, pose unique challenges due to high-density infrastructure and frequent signal obstructions. Future research should focus on developing scalable optimization models capable of supporting multi-UAV deployments within such complex environments. Additionally, implementing machine learning techniques for predictive network management could further enhance the adaptability of UAV systems, allowing them to proactively respond to anticipated changes in signal strength and latency.

Another area for future exploration is energy efficiency. Although the research demonstrates improved UAV stability, the impact of these optimizations on energy consumption was not fully explored. Given that energy efficiency is critical for extended UAV operations, future studies could integrate energy management algorithms that minimize power usage without compromising performance. Such an approach would be particularly beneficial in applications where UAVs are required to operate continuously over long durations, such as in agricultural monitoring or border surveillance.

The study also lays the groundwork for exploring hybrid network models that combine 5G with other wireless communication technologies. Hybrid models could offer enhanced connectivity for UAVs in areas where 5G infrastructure is limited, thereby extending the operational range and versatility of UAVs. As 5G networks continue to expand, the integration of additional communication protocols, such as narrowband IoT and low-power wide-area networks, could facilitate seamless UAV operation across both urban and rural areas.

In terms of novelty, the research contributes a unique perspective by linking UAV stability directly with real-time 5G network optimization. This real-time approach is particularly innovative, as it enables UAVs to make instantaneous adjustments to network parameters based on environmental data. The adaptive models developed in this study represent a significant step forward in UAV technology, offering practical solutions for enhancing stability and performance in dynamic settings. By addressing both urban and rural applications, the study demonstrates the versatility of 5G technology in optimizing UAV functions for a wide range of use cases.

The article provides valuable insights into the optimization of UAV systems through 5G technology, with implications for both current and future UAV applications. The integration of predictive models and optimization algorithms not only enhances UAV stability but also opens new possibilities for deploying UAVs in complex environments. As technology continues to advance, further research into

scalable, energy-efficient, and hybrid communication solutions will be essential to fully realize the potential of UAVs in various sectors, from smart cities to environmental conservation.

REFERENCES

1 **N. H. Qasim, D. A. Jumaa, F. Rahim, A. M. Jawad, A. M. Khaleefah, G. Zhyrov, and H. Ali**: (2024). Simplifying IP multimedia systems by introducing next-generation networks with scalable architectures, *Edelweiss Applied Science and Technology*, 8, (4), 2042-54

2 **J. Zhou, D. Tian, Y. Yan, X. Duan, and X. Shen**: (2024). Joint Optimization of Mobility and Reliability-Guaranteed Air-to-Ground Communication for UAVs'', *IEEE Transactions on Mobile Computing*, 23, (1), 2024, 566-80

3 **T. N. Nguyen, L. T. Tu, P. Fazio, T. V. Chien, C. V. Le, H. T. T. Binh, and M. Voznak**. (2024). On the Dilemma of Reliability or Security in Unmanned Aerial Vehicle Communications Assisted by Energy Harvesting Relaying. *IEEE Journal on Selected Areas in Communications*, 42, (1), 52-67.

4 **Z. U. A. Tariq, E. Baccour, A. Erbad, and M. Hamdi**. (2024). Reinforcement Learning for Resilient Aerial-IRS Assisted Wireless Communications Networks in the Presence of Multiple Jammers. *IEEE Open Journal of the Communications Society*, 5, 15-37

5 **N. H. Qasim, F. Rahim, and N. Bodnar**: (2024). A comprehensive investigation of an LTE-enabled smart door system using the Arduino UNO. *Edelweiss Applied Science and Technology*, 8, (4), 697-708.

6 **M. Neinavaie, and Z. M. Kassas**. (2024). Cognitive Sensing and Navigation With Unknown OFDM Signals With Application to Terrestrial 5G and Starlink LEO Satellites. *IEEE Journal on Selected Areas in Communications*, 42, (1), 146-60.

7 **N. M. Laboni, S. J. Safa, S. Sharmin, M. A. Razzaque, M. M. Rahman, and M. M. Hassan**. (2024). A Hyper Heuristic Algorithm for Efficient Resource Allocation in 5G Mobile Edge Clouds. *IEEE Transactions on Mobile Computing*, 23, (1), 29-41.

8 **N. H. Qasim, and A. M. Jawad**. (2024). 5G-enabled UAVs for energy-efficient opportunistic networking'', *Heliyon*, 10, (12), e32660

9 **N. J. M. Omar S.S., Qasim N. H., Kawad R. T., Kalenychenko R.** (2024). The Role of Digitalization in Improving Accountability and Efficiency in Public Services., *Revista Investigacion Operacional*, 45, (2), 203-24.

10 **X. Li, X. Hu, and T. Jiang**. (2024). Dual-Reinforcement-Learning-Based Attack Path Prediction for 5G Industrial Cyber–Physical Systems. I*EEE Internet of Things Journal, 11*, (1), 50-58.

11 **S. D. Abdulameer, N. A. Taher, S. R. Alatba, N. H. Qasim, and O. Dorenskyi**. (2024). Optimization of Underwater Channel Performance through Polar Code-OFDM Models'. 'Book Optimization of Underwater Channel Performance through Polar Code-OFDM Models' (2024, edn.), 3-10

12 **N. H. Qasim, A. J. Salman, H. M. Salman, A. A. AbdelRahman, and A. Kondakova**. 'Evaluating NB-IoT within LTE Networks for Enhanced IoT Connectivity', in Editor (Ed.)^(Eds.): 'Book Evaluating NB-IoT within LTE Networks for Enhanced IoT Connectivity' (IEEE, 2024, edn.), pp. 552-59

13 **M. M. Salih, B. M. Khaleel, N. H. Qasim, W. S. Ahmed, S. Kondakova, and M. Y. Abdullah**. (2024). Capacity, Spectral and Energy Efficiency of OMA and NOMA Systems, in Editor (Ed.)^(Eds.): 'Book Capacity, Spectral and Energy Efficiency of OMA and NOMA Systems' (2024, edn.), 652-58.

14 **A. J. M. Jawad, A. M. Abed, N. H. Qasim, and A. A. AbdelRahman**. (2024). Design and Implement a GPS Car Tracker on Google Maps Using Arduino. Book Design and Implement a GPS Car Tracker on Google Maps Using Arduino, 284-93 [15] Q. Nameer Hashim, A.-H. Hayder Imran, S. Iryna, and J. Aqeel Mahmood: ''Modern Ships and the Integration of Drones – a New Era for Marine Communication'', *Development of Transport*, 4, (19), 2023

15 **Q. Nameer, J. Aqeel, and M. Muthana**. (2023). The Usages of Cybersecurity in Marine Communications. *Transport Development*, 3, (18), 2023.

16 **A.-A. M. G. Jawad A. M., & Qasim N. H.** (2023). Emerging Technologies and Applications of Wireless Power Transfer'', *Transport Development*, 4, (19).

17 **H. A. Hung, H. H. Hsu, and T. H. Cheng**: (2024). Optimal Sensing for Tracking Task by Heterogeneous Multi-UAV Systems. *IEEE Transactions on Control Systems Technology*, 32, (1), 282-89

18 **N. Qasim, Shevchenko, Y.P., and Pyliavskyi, V**. (2019). Analysis of methods to improve energy efficiency of digital broadcasting'',

Telecommunications and Radio Engineering, 78, (16).

19 **N. Qasim, and L.-C. Nataliia**. The Role of Drones for Evolving Telecommunication and Internet.

20 **S. Naik, P. Thippeswamy, A. Raghavan, M. Rajgopal, and A. Sujith**. (2024). '*Efficient network management and security in 5G enabled internet of things using deep learning algorithms Keywords: 5G enabled IoT Deep learning Network management Network security Predictive modelling*' (2024. 2024)

21 **A. Gnanaraj, F. Abbasali, A. Kumar, S. Subramanian, and M. Chinnathambi**. (2024). Hyperelliptic curve based authentication for the internet of drones. *International Journal of Reconfigurable and Embedded Systems (IJRES)*, 13, 133.

22 **V. L. Dao, E. Uhlemann, and S. Girs**. (2024). Dealing With Jamming Attacks in Uplink Pairwise NOMA Using Outage Analysis, Smart Relaying, and Redundant Transmissions. *IEEE Open Journal of the Communications Society*, 5, 112-26.

23 **Q. N. H. Sieliukov A.V., Khlaponin Y. I.** (2022). Conceptual model of the mobile communication network. *The Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things «TTSIIT»*, 20-22.

24 **N. Qasim, Khlaponin Y., & Vlasenko M.** (2022). Formalization of the Process of Managing the Transmission of Traffic Flows on a Fragment of the LTE network. *Collection of Scientific Papers of the Military Institute of Taras Shevchenko National University of Kyiv*, 75, 88–93.

25 **N. Qasim, A. Jawad, H. Jawad, Y. Khlaponin, and O. Nikitchyn**. (2022). Devising a traffic control method for unmanned aerial vehicles with the use of gNB-IOT in 5G. *Eastern-European Journal of Enterprise Technologies*, 3, 53-59.

26 **D. Ageyev, D. Yarkin, and Q. Nameer**. (2014). Traffic aggregation and EPS network planning problem, in Editor (Ed.)^(Eds.): 'Book Traffic aggregation and EPS network planning problem' (2014, edn.), 107-08.

27 **A.-S. Mushtaq, A.-A. Ali Ihsan and N. Qasim** (2015). 2D-DWT vs. FFT OFDM Systems in fading AWGN channels, *Radioelectronics and Communications Systems*, 58, (5), 228-33.

28 **Q. Nameer**: (2014). Aggregated Self-Similar Traffic Parameters Determination Methods for EPS network planning Scholars, *Journal of Engineering and Technology*, 2, (5A), 727-32

29 **Y. Zhang, Y. Huang, C. Huang, H. Huang, and A. T. Nguyen**. (2024). Joint Optimization of Deployment and Flight Planning of Multi-UAVs for Long-Distance Data Collection From Large-Scale IoT Devices, *IEEE Internet of Things Journal*, 11, (1), 791-804.

Статистична оптимізація стабільності БПЛА через параметри мережі 5G

Асма Хакім Наїм, Махмуд Джавад Абулшаер, Альхамза Абдулсатар Шакер, Саіф Саад Ахмед, Ала Салім Абдалраззак

Анотація. Довідка: дрони, або безпілотні літальні апарати (БПЛА), набули популярності в різних галузях завдяки своїй універсальності та ефективності. Однак досягнення оптимальної стабільності під час польоту залишається проблемою, особливо в динамічних середовищах. Поява технології 5G

з її високошвидкісними можливостями з малою затримкою дає можливість покращити контроль і стабільність безпілотників завдяки передачі даних у реальному часі та оперативним налаштуванням.

Мета: це дослідження вивчає застосування статистичних методів для оптимізації балансу дронів через підключення 5G, зосереджуючись на ключових параметрах мережі, таких як затримка, потужність сигналу та використання пропускної здатності.

Методи: серію польотів було проведено в різних умовах навколишнього середовища, щоб зібрати дані про показники стійкості дрона, включаючи крен, тангаж і поворот. Статистичний аналіз, включаючи регресійні моделі та аналіз часових рядів, було застосовано для оцінки зв'язку між параметрами 5G і балансом дронів. Потім були використані алгоритми оптимізації для динамічного налаштування параметрів мережі з метою підвищення стабільності в режимі реального часу.

Результати. Отримані дані вказують на те, що затримка та потужність сигналу є значущими показниками стабільності дрона, причому менша затримка та оптимізована потужність сигналу корелюють із покращеним балансом. Крім того, оптимізація пропускної здатності сприяла більш плавному керуванню польотом завдяки пріоритетності основних потоків даних.

Висновок: статистичні методи відіграють вирішальну роль у максимізації переваг технології 5G для стабільності дронів. Завдяки точному налаштуванню параметрів 5G дрони

можуть підтримувати кращий баланс, підвищуючи загальну ефективність і надійність.

Ключові слова: дрони, БПЛА, 5G, статистична оптимізація, затримка, потужність сигналу, пропускна здатність, моніторинг у реальному часі, оптимізація мережі, стабільність БПЛА.

Система моніторингу банківської інфраструктури

Олег Кузін[1]

[1] Державний торговельно-економічний університет
Україна, 02156, м. Київ, вул. Кіото, 19
[1] o.kuzin@knute.edu.ua, orcid.org/0009-0009-3592-0345

Received 17.09.2024, accepted 30.10.2024
https://doi.org/10.32347/uwt.2024.15.1801

Анотація. У сучасних умовах цифрової трансформації фінансового сектору стабільність і безперебійна робота банківської інфраструктури є запорукою успіху. Відмовостійкість комп'ютерних систем є одним із ключових факторів успішної роботи сучасних організацій, особливо в таких критичних галузях, як банківська сфера. Забезпечення постійної доступності банківських сервісів є вкрай важливим для безперебійної роботи платіжних систем, обробки транзакцій і доступу до рахунків клієнтів. Одним з основних інструментів для підтримки відмовостійкості є моніторинг показників систем, який дозволяє виявляти проблеми до того, як вони стають критичними, та вживати заходи для запобігання збоям.

У цій роботі розглянуто систему моніторингу інформаційного середовища банку, проведено аналіз ключових показників забезпечення відмовостійкої роботи системи. Окремо розглянуто такі особливості як критичність досліджуваних параметрів, частота опитування підсистем, часова чутливість та порогові значення.

В рамках дослідження виділено стабільні і аномальні значення параметрів об'єктів моніторингу і на їх основі сформовані шаблони поведінки системи. Як результат, визначені рівні ескалації, методи сповіщень та застосування додаткових автоматизацій для стабілізації роботи підсистем.

Ключові слова: Відмовостійкість, інформаційне середовище, система моніторингу, моделювання.

Олег Кузін
аспірант кафедри цифрової економіки та системного аналізу

МЕТА ТА МЕТОДИ ДОСЛІДЖЕННЯ

Метою цього дослідження є моніторинг банківської системи щодо покращення працездатності інфраструктури в умовах потенційних загроз під час військової агресії.

Під час дослідження використовувалися методи системного аналізу та комплексного аналізу.

ВСТУП

Умови роботи банківської системи України суттєво змінилися з початком повномасштабного вторгнення російської федерації, коли критичні інфраструктури опинилися під постійною загрозою фізичних пошкоджень, кібератак та регулярних збоїв в енергопостачанні [3]. Відключення електроенергії, перебої з інтернет-зв'язком і атаки на цифрові ресурси стали постійними викликами для банківської інфраструктури, яка відіграє важливу роль у фінансовій стабільності країни [4]. У таких умовах надзвичайно важливим стає безперервний контроль за станом IT-систем банків, де навіть короткочасний збій може призвести до великих втрат та порушення роботи критичних сервісів, таких як платежі, банкомати, обслуговування рахунків [5]. Саме системи моніторингу відіграють ключову роль у забезпеченні стабільної роботи інфраструктури банків під час кризових ситуацій, дозволяючи вчасно виявляти загрози та запобігати відмовам. Ефективний моніторинг не тільки допомагає швидко реагувати на несправності, а й прогнозувати потенційні ризики, що особливо

важливо в умовах, коли від стабільної роботи банків залежить економічна та соціальна стабільність країни.

Відмовостійкість — це здатність системи функціонувати навіть у випадку відмови одного або кількох компонентів. У банківських системах це означає безперервну роботу банкоматів, інтернет-банкінгу, процесингу карткових платежів та інших важливих операцій навіть під час технічних проблем. Для цього необхідно впровадити механізми резервування, автоматичної заміни несправних компонентів і ефективного моніторингу.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Моніторинг показників систем допомагає вчасно виявляти потенційні проблеми і попереджати збої. Системи моніторингу, дозволяють збирати дані про стан серверів, мереж, баз даних та інших компонентів IT-інфраструктури, а також забезпечують інструменти для аналізу та побудови прогнозів.

Основні функції моніторингу:

- **Виявлення проблем на ранніх стадіях.** Моніторинг дозволяє виявляти проблеми до того, як вони перетворяться на критичні збої, що впливають на роботу системи.
- **Прогнозування відмов.** На основі історичних даних можна побудувати прогнози і визначити, коли певний компонент системи може вийти з ладу.
- **Автоматизація процесів реагування**. За допомогою тригерів можна налаштувати автоматичне сповіщення або навіть автоматичне переключення на резервне обладнання у випадку виявлення критичних проблем.

Основні показники моніторингу

Щоб забезпечити відмовостійкість, важливо відстежувати ряд ключових показників системи. Основні з них включають:

- Завантаження процесора (CPU Load):

Високе завантаження процесора може призвести до перевантаження і збою у роботі серверів. Системи моніторингу дозволяють відслідковувати рівень завантаження і вчасно попереджати про критичні ситуації. Аналізуючи історичні дані, можна спрогнозувати сповільнення роботи підсистем внаслідок перевантаження і вчасно вжити заходів для підвищення продуктивності. Найбільше процесорне навантаження відбувається в робочі дні з 09:00 до 18:00 (Рис.1) і саме аналіз цих часових проміжків дозволяє робити висновки і прогнози завантаження і швидкодії бізнес-застосунків.

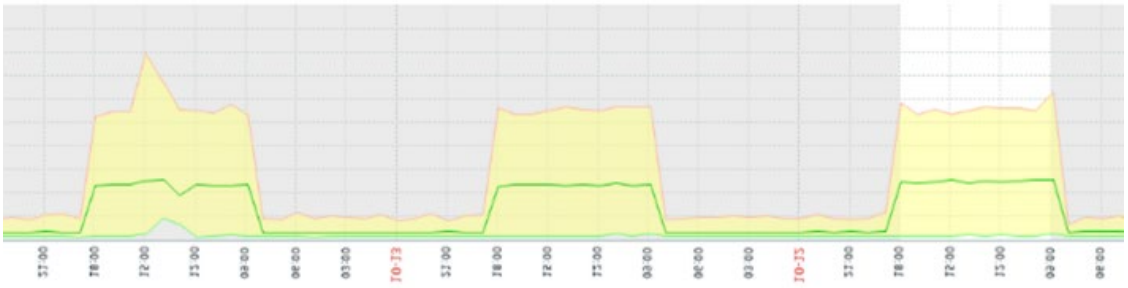


Рис. 1. Завантаження процесора в бізнес-час

Fig. 1. Processor load during business hours

Використання оперативної пам’яті (RAM Usage):

Надмірне використання оперативної пам’яті може призвести до уповільнення або відмови системи. Моніторинг використання пам’яті дозволяє оптимізувати ресурси і запобігати відмовам. Аналіз графіків використання оперативної пам’яті дозволяє виявити години навантаження серверних застосунків, виявити складні для обладнання часові рамки і виявити тенденції завантаження серверних застосунків, щоб уникнути перевантаження та витоків пам’яті.

- Вільне місце на диску (Disk Space Usage):

Моніторинг вільного місця на диску є одним із найважливіших елементів для забезпечення стабільної роботи IT-систем,

де зберігаються великі обсяги даних, зокрема бази даних, транзакційна інформація, журнали подій та інші критичні файли. Аналіз використання дискового простору кожної підсистеми дозволяє встановити порогові значення, при перевищенні яких потрібно вживати дій по очищенню дискового простору, або планувати покупку дискових накопичувачів, згідно тенденції використання, як зазначено на Рис.2. Окремої уваги потребує моніторинг вільного дискового простору в системних областях, при переповненні яких виникають проблеми не просто із застосунками, а і з операційною системою.

Рис. 2. Прогнозування покупки дискових накопичувачів згідно тенденції використання
Fig. 2. Forecasting disk drive purchases according to usage trends

- Мережеві показники:

Пропускна здатність (Network Bandwidth) і затримки (Latency) — ці параметри визначають ефективність передачі даних і швидкість доступу до системи [7]. Мережеві ресурси використовуються для обробки транзакцій, обміну даними між офісами, клієнтськими запитами до інтернет-банкінгу, підтримки систем електронної пошти та інтеграції з платіжними системами. Моніторинг пропускної здатності мережі допомагає вчасно виявляти потенційні проблеми, попереджувати їх і забезпечувати стабільну роботу мережевої інфраструктури. Аналіз історичних даних системи моніторингу мережі дозволяє визначити пікові періоди використання мережі протягом бізнес-часу та поза ним. Ці показники дають можливість спрогнозувати навантаження мережевої інфраструктури, виявити окремі «пляшкові горла» трафіку, на яких виникають затримки, виявити аномалії (Рис.3) і попередити витоки інформації [1]. Постійний моніторинг пропускної здатності мережі і її окремих вузлів допомагає у прийнятті рішень про масштабування підсистем і модернізацію мережі для досягнення необхідних швидкостей передачі даних.

Рис. 3. Аномальне споживання трафіку системою при оновленні версії серверної компоненти
Fig. 3. Abnormal traffic consumption by the system when updating the version of the server component

- Температура обладнання:

Перегрів серверів, мережевого обладнання чи систем зберігання даних може призвести до серйозних збоїв, пошкодження компонентів або втрати інформації. Своєчасне виявлення підвищених температур дозволяє вжити заходів для охолодження або оптимізації навантаження, що знижує ризик відмов системи. Ефективний моніторинг допомагає підтримувати обладнання в межах рекомендованих температурних параметрів, продовжуючи його термін служби. Таким чином, аналізуючи графіки коливання температур обладнання, можна виявити несприятливі тенденції і вчасно вжити заходів з дотримання оптимальних температурних режимів серверної кімнати, створити автоматизації по увімкненню додаткових систем кондиціонування при

невеликому перевищенні температур, як показує графік на Рис.4, або прийняти рішення [2] по активації системи пожежогасіння при критичному перевищенні температури.

Рис. 4. Впровадження додаткової системи охолодження
Fig. 4. Implementation of an additional cooling system

ПРОГНОЗУВАННЯ ВІДМОВ

Окрім виявлення проблем у реальному часі, системи моніторингу допомагають у прогнозуванні можливих відмов. Наприклад, якщо система моніторингу збирає дані про зростання завантаження серверів протягом кількох місяців, це може свідчити про наближення критичного навантаження, і керівництво банку може ухвалити рішення про модернізацію обладнання або розширення ресурсів.

АВТОМАТИЗАЦІЇ ТА СПОВІЩЕННЯ

Сповіщення від системи моніторингу є критично важливими для своєчасного реагування на проблеми в банківській інфраструктурі, дозволяючи оперативно усувати збої до того, як вони стануть критичними [8]. Важливим критерієм є правильне налаштування порогових значень, коли система має генерувати сповіщення – це дозволяє уникнути як надмірної кількості "шуму", так і пропуску серйозних інцидентів. Система повинна враховувати не лише поточний стан компонентів, але й тривалість аномалій, щоб запобігти реакції на тимчасові сплески навантаження. Ескалація оповіщень залежно від рівня критичності дозволяє залучати потрібних фахівців у випадку серйозних відмов. Нарешті, важливою є інтеграція сповіщень з автоматизованими процесами реагування, щоб забезпечити мінімальний час простою в разі критичних подій.

Автоматизація є важливою частиною процесу забезпечення відмовостійкості [6]. Системи моніторингу можуть автоматично генерувати сповіщення, створювати резервні копії даних або ініціювати переключення на резервні сервери без участі людини, особливо в в умовах, коли час на реакцію обмежений, а швидкість відновлення роботи системи є критичним фактором.

Консолідація даних моніторингу.
Консолідована панель (Дашборд) є зручним інструментом для візуалізації основних показників моніторингу в реальному часі, що дозволяє швидко оцінювати стан всієї IT-інфраструктури. Вона об'єднує на одному екрані критичні метрики і надає можливість оперативно відстежувати потенційні проблеми (Рис.5). Графіки та індикатори допомагають легко виявляти відхилення від нормальних значень і прогнозувати можливі збої. Дашборд також дозволяє налаштовувати рівні попереджень і сповіщень для кожного з показників, забезпечуючи швидкий доступ до критичної інформації для своєчасного реагування і підтримки відмовостійкості та ефективного управління IT-інфраструктурою.

Рис. 5 Приклад консолідованої панелі моніторингу ключових показників
Fig. 5. Example of a consolidated key performance indicator dashboard

ВИСНОВОК

Система моніторингу банківської інфраструктури відіграє ключову роль у забезпеченні її стабільної та відмовостійкої роботи, особливо в умовах воєнного стану та постійних технічних викликів.

Використання інструментів моніторингу дозволяє не тільки виявляти проблеми на ранніх етапах, але й прогнозувати потенційні загрози для всіх критичних компонентів системи. Завдяки постійному контролю за ключовими показниками, такими як завантаження процесора, використання оперативної пам'яті, стан мережевих ресурсів та температура обладнання, можна запобігти серйозним збоям і забезпечити безперебійну роботу банківських сервісів. Крім того, впровадження автоматизацій та оповіщень значно підвищує ефективність управління інфраструктурою, дозволяючи швидко реагувати на зміни та забезпечувати її надійність. Таким чином, системи моніторингу є невід'ємним інструментом для підтримки безпеки і стабільності банківської інфраструктури в умовах сучасних викликів.

REFERENCES

1. **Khlaponin, Y., Kozubtsova, L., Kozubtsov, I., & Shtonda, R.** (2022). Funktsiyi systemy zakhystu informatsiyi i kiberbezpeky krytychnoyi informatsiynoyi infrastruktury. *Elektronne fakhove nau-kove vydannya «Kiberbezpeka: osvita, nauka, tekhnika»*, 3(15), 124–134. https://doi.org/10.28925/2663-4023.2022.15.1241341
2. **Humennyy, D., Kuzin, O., & Shabala, YE.** (2024). Radarnyy zakhyst ta aktyvne perekhoplennya droniv-kamikadze. Pidvodni Tehnologii, 1(14), 98–106. https://doi.org/10.32347/uwt.2024.14.1301.
3. **Nastasyak, R. V., and O. O. Perepolkina.** Funktsionuvannya bankivs′koyi systemy ukrayiny v umovakh voyennoho stanu. Or-hanizatsiynyy komitet konferentsiyi: 234.
4. Postanova Pravlinnya Natsional′noho banku Ukrayiny «Pro robotu bankivs′koyi systemy v period zaprovadzhennya voyennoho stanu» vid 24.02.2022 № 18. URL: https://zakon.rada.gov.ua/laws/show/v0018500-22#Text.
5. Metodychni vkazivky z inspektuvannya bankiv « Systema otsinky ryzykiv » [Elektronnyy resurs] // NBU. Rezhym dostupu do resursu: https://bank.gov.ua/admin_uploads/article/Organizacijna_struktura_sistemi_upravlinnya_rizikami_2018-09-18_19_pr.pdf?v=6
6. **Kasovska I. V., Shapovalenko O. D., Lutsenko I. M.** (2021). Prohramni kompleksy merezhevoho monito-rynhu dlya pidvyshchennya efektyvnosti zakhy-stu merezh. *Suchasnyy zakhyst informatsiyi*, №1(45), 47–52.
7. **Kuznyuk K. V., Kovalenko O. Ye.** Doslidzhennya tekhnolohiy ta rozroblennya zasobiv rozshyrennya funktsional′nosti system monitorynhu komp'yuternykh merezh. *Informatsiyni tekhnolohiyi: ekonomika, tekh-nika, osvita: Zb. materialiv KHIII mizhnar. nauk.-prakt. Konf*
8. **Koskinen Marko.** (2024). Integrating open-source computer and network monitoring software to an automation supervision system.
9. https://www.zabbix.com/features, [Accessed 10.10.2024].

Banking infrastructure monitoring system

Oleg Kuzin

Annotation. In today's conditions of digital transformation of the financial sector, the stability and uninterrupted operation of the banking infrastructure is the key to success. The fault tolerance of computer systems is one of the key factors in the successful operation of modern organizations, especially in such critical industries as banking. Ensuring the constant availability of banking services is extremely important for the uninterrupted operation of payment systems, transaction processing and access to customer accounts. One of the main tools for maintaining fault tolerance is the monitoring of system indicators, which allows you to detect problems before they become critical and take measures to prevent failures.

This work examines the monitoring system of the bank's information environment, analyzes the key indicators of ensuring the system's fault-tolerant operation. Such features as the criticality of the studied parameters, the frequency of polling subsystems, time sensitivity and threshold values are separately considered.

Within the framework of the study, stable and abnormal values of the parameters of the monitoring objects were selected, and based on them, patterns of system behavior were formed. As a result, escalation levels, notification methods and application of additional automations to stabilize subsystems are defined.

Keywords: Fault tolerance, information environment, monitoring system, modeling.

Моделі побудови мереж інтернету речей для управління інфраструктурою міста

Анастасія Кондакова[1], Олександр Корецький[2]

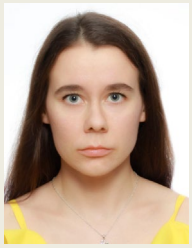
[1] Київський національний університет будівництва і архітектури
пр-т Повітряних Сил, 31, м.Київ, Україна, 03037
[2] Державний університет інформаційно-комунікаційних технологій
вул. Солом'янська, 7, м. Київ, Україна, 03110,
[1] a_kondakova@ukr.net, https://orcid.org/0000-0003-1302-2244
[2] okoretsky@gmail.com, https://orcid.org/0009-0001-4809-7556

Received 17.09.2024, accepted 30.10.2024
https://doi.org/10.32347/uwt.2024.15.1901

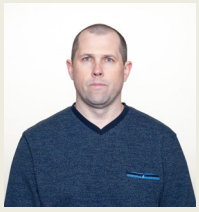
Анотації. У роботі розглядаються сучасні підходи до впровадження технологій IoT для ефективного управління міською інфраструктурою. Основна увага приділена аналізу мережевих архітектур, що використовуються для збирання та передачі даних у системах розумних міст. Порівнюються різні моделі побудови мереж, зокрема однохопові та багатохопові мережі, а також топології WSN. Робота акцентує на перевагах і недоліках цих мереж у контексті енергоспоживання, масштабованості та стабільності. Особлива увага приділяється ієрархічним моделям, що дозволяють знизити енерговитрати та підвищити ефективність мережі. Проаналізовано застосування IoT у ключових сферах міської інфраструктури, таких як транспорт, енергетика та водопостачання. Також детально розглянуто питання кібербезпеки IoT-систем, включаючи автентифікацію, шифрування даних та забезпечення надійності зв'язку. Окремо обговорюється роль CPS та сенсорних вузлів, які забезпечують моніторинг і контроль міських ресурсів у реальному часі. Розглянуто математичні моделі для оптимізації трафіку в мережах IoT, зокрема використання теорії черг для забезпечення QoS. Зроблено висновки щодо ефективності впровадження IoT для управління міськими ресурсами, що дозволяє підвищити надійність міської інфраструктури та покращити умови життя мешканців. Обґрунтовано застосування в IoT-системах мікросервісного програмного забезпечення та визначені напрямки наукових досліджень, спрямованих та його втілення в IoT-системи управління інфраструктурними об’єктами.

Дослідження відкриває нові перспективи для застосування IoT у розумних містах та вказує на необхідність подальшого вивчення питань безпеки та енергозбереження в таких системах.

Ключові слова: IoT, міська інфраструктура, розумні міста, WSN, енергоефективність, CPS, мікросервісне програмне забезпечення



Анастасія Кондакова
Аспірант кафедри кібербезпеки та комп'ютерної інженерії, КНУБА



Олександр Корецький
Аспірант кафедри штучного інтелекту ДУІКТ

ПОСТАНОВКА ПРОБЛЕМИ

У сучасних умовах інтенсивної урбанізації та стрімкого зростання міст технології, які дозволяють ефективно управляти міською інфраструктурою, набувають дедалі більшої актуальності. Однією з найбільш перспективних концепцій у цьому контексті є Інтернет речей (далі IoT), що забезпечує обмін даними між пристроями та системами для автоматизованого контролю й управління міськими ресурсами [№][№]. У таких містах, як Сінгапур та Барселона, впровадження IoT сприяло значному підвищенню ефективності використання ресурсів і скороченню операційних витрат,

дозволивши оперативно реагувати на зміни інфраструктурних потреб. Інтеграція IoT з міською інфраструктурою дає змогу підвищити ефективність використання ресурсів, зменшити операційні витрати та покращити якість життя мешканців [№].

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ

Останні дослідження у сфері IoT для розумних міст охоплюють кілька ключових напрямків. Одним із важливих аспектів є управління міськими ресурсами та підвищення енергоефективності. Зокрема, Маркуц [1] акцентує на використанні IoT для автоматизованих систем управління ресурсами, що сприяє енергозбереженню, тоді як Gómez [4] розглядає застосування IoT для моніторингу екологічних параметрів у міському середовищі. Інші дослідження зосереджені на архітектурі мереж та протоколах передачі даних. Публікації [5; 7; 8] описують різноманітні підходи до побудови IoT-мереж у розумних містах, включаючи розробки, які забезпечують масштабованість і стабільність мережевої інфраструктури. Також велика увага приділяється питанням безпеки. Aggarwal [2] і Garcia-Retuerta [3] аналізують виклики кібербезпеки та захисту даних в IoT-системах, що включає проблеми автентифікації та шифрування інформації. Хоча ці питання активно вивчаються, багато аспектів, зокрема кібербезпека та оптимізація енергоспоживання, залишаються невирішеними та потребують подальших досліджень [9; 10].

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є дослідження можливостей ефективного застосування технологій IoT для управління міською інфраструктурою, зокрема через розробку енергоефективних, надійних та безпечних мережевих архітектур. Завданнями є аналіз існуючих моделей побудови однохопових і багатохопових мереж, а також топологій бездротових сенсорних мереж (далі WSN), щоб визначити найбільш оптимальні підходи для застосування в умовах розумних міст. Особлива увага приділяється питанням енергоспоживання, масштабованості, кібербезпеки та інтеграції IoT-систем у ключові сфери міської інфраструктури, такі як транспорт, енергетика та водопостачання

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Для належної роботи IoT у розумних містах ключовим аспектом є вибір мережевої архітектури, здатної ефективно обробляти та передавати великі обсяги даних. Основним завданням є досягнення балансу між енергоефективністю та надійністю передачі інформації на великі відстані.

Однохопові мережі забезпечують підключення сенсорних вузлів безпосередньо до базової станції. Їх перевагою є висока швидкість передачі даних через мінімальну кількість проміжних вузлів, що зменшує затримки. Однак значне енергоспоживання та обмежена масштабованість у великих міських територіях є недоліками, що обмежують застосування таких мереж у масштабних IoT-системах [1].

На відміну від однохопових систем, багатохопові мережі передають дані через проміжні вузли, що знижує енергоспоживання, оскільки кожен вузол підтримує зв'язок із найближчими вузлами. Така архітектура дозволяє розширити зону покриття без значного збільшення кількості базових станцій і робить мережу більш гнучкою та надійною для використання в умовах розумних міст [7]. Ієрархічна модель є підтипом багатохопової мережі, де деякі вузли виступають кластерними головними вузлами, збираючи дані від інших і передаючи їх на базову станцію. Це зменшує навантаження на мережу, підвищує енергоефективність і забезпечує високу масштабованість та стабільність системи [3].

Багатохопові мережі є особливо актуальними для розумних міст через їхню

здатність адаптуватися до втрат вузлів або змін у мережевих умовах. Вони забезпечують надійність для критичних систем, таких як транспорт, енергетика та водопостачання. Крім того, ці мережі легко адаптуються до збільшення кількості вузлів у міру розширення міста.

Топологія бездротових сенсорних мереж (далі WSN) є важливим аспектом побудови IoT-систем, оскільки вона впливає на стабільність і масштабованість системи. Плоска топологія, у якій усі вузли є рівноправними, є простою і дешевою у побудові, але має обмежену ефективність і масштабованість, що критично для великих міст [7]. У разі збільшення кількості вузлів вона може призводити до перевантаження мережі та затримок у передачі даних.

Ієрархічна топологія, що передбачає кластеризацію вузлів, є більш ефективною, оскільки знижує навантаження на окремі вузли і підвищує енергоефективність. Головні вузли виконують функції обробки та фільтрації даних, що сприяє стабільності та ефективності мережі. Ієрархічні топології добре підходять для великих міст, оскільки забезпечують стійкість і адаптивність [9].

У міському розвитку концепція розумних міст покладається на WSN, оскільки вони дозволяють ефективно управляти великими обсягами даних і мінімізувати енергоспоживання. Наприклад, у транспортних системах WSN можуть використовуватися для моніторингу транспортних потоків і управління світлофорами, що зменшує затори та скорочує час пересування [5].

У сфері енергетики WSN застосовуються для моніторингу споживання енергії будівлями, а також для оптимізації роботи електричних мереж. Сенсорні вузли інтегруються в системи управління електропостачанням для виявлення проблемних ділянок і автоматичного регулювання навантаження. Водопостачальні системи також використовують WSN для моніторингу тиску та рівня води в резервуарах, що дозволяє своєчасно попереджати аварії або витоки води [6].

Інші типи топологій, як-от зіркоподібна або кільцева, мають обмежене застосування у великих IoT-системах через слабку масштабованість і вразливість до відмов окремих вузлів. Наприклад, у зіркоподібній топології відмова центрального вузла може призвести до збоїв у всій мережі [1].

Сенсорні вузли, що відповідають за збір даних із фізичного середовища, є основним компонентом WSN у розумних містах. Вони можуть вимірювати різні параметри, як-от температура, тиск чи рівень забруднення, і моніторити стан критичної інфраструктури, зокрема мостів, доріг та енергомереж. Енергоефективність є важливою вимогою до таких вузлів, оскільки вони зазвичай працюють на обмежених енергетичних ресурсах.

Топологія бездротових сенсорних мереж (далі WSN) є важливим аспектом побудови IoT-систем, оскільки вона впливає на стабільність і масштабованість системи. Плоска топологія, у якій усі вузли є рівноправними, є простою і дешевою у побудові, але має обмежену ефективність і масштабованість, що критично для великих міст [7]. У разі збільшення кількості вузлів вона може призводити до перевантаження мережі та затримок у передачі даних.

Ієрархічна топологія, що передбачає кластеризацію вузлів, є більш ефективною, оскільки знижує навантаження на окремі вузли і підвищує енергоефективність. Головні вузли виконують функції обробки та фільтрації даних, що сприяє стабільності та ефективності мережі. Ієрархічні топології добре підходять для великих міст, оскільки забезпечують стійкість і адаптивність [9].

У міському розвитку концепція розумних міст покладається на WSN,

оскільки вони дозволяють ефективно управляти великими обсягами даних і мінімізувати енергоспоживання. Наприклад, у транспортних системах WSN можуть використовуватися для моніторингу транспортних потоків і управління світлофорами, що зменшує затори та скорочує час пересування [5].

У сфері енергетики WSN застосовуються для моніторингу споживання енергії будівлями, а також для оптимізації роботи електричних мереж. Сенсорні вузли інтегруються в системи управління електропостачанням для виявлення проблемних ділянок і автоматичного регулювання навантаження. Водопостачальні системи також використовують WSN для моніторингу тиску та рівня води в резервуарах, що дозволяє своєчасно попереджати аварії або витоки води [6].

Інші типи топологій, як-от зіркоподібна або кільцева, мають обмежене застосування у великих IoT-системах через слабку масштабованість і вразливість до відмов окремих вузлів. Наприклад, у зіркоподібній топології відмова центрального вузла може призвести до збоїв у всій мережі [1].
Сенсорні вузли, що відповідають за збір даних із фізичного середовища, є основним компонентом WSN у розумних містах. Вони можуть вимірювати різні параметри, як-от температура, тиск чи рівень забруднення, і моніторити стан критичної інфраструктури, зокрема мостів, доріг та енергомереж. Енергоефективність є важливою вимогою до таких вузлів, оскільки вони зазвичай працюють на обмежених енергетичних ресурсах.

Сенсорні вузли можуть бути як стаціонарними, так і мобільними. Стаціонарні вузли забезпечують стабільність передачі даних, тоді як мобільні вузли дозволяють охоплювати більші території для динамічного моніторингу. Однак мобільні вузли потребують оптимізації енергоспоживання та підтримки надійного зв'язку під час руху [7].

Важливу роль відіграють вузли-шлюзи, які забезпечують передачу даних між сенсорними вузлами та центральною системою управління. Вони обробляють дані від сенсорів і передають їх на базові станції або сервери для аналізу. Це зменшує навантаження на сенсорні вузли і знижує енерговитрати. Вузли-шлюзи мають більше енергетичних та обчислювальних можливостей, що дозволяє їм управляти потоком даних, забезпечувати безпеку комунікацій і координувати роботу різних елементів мережі. Вони можуть також інтегруватися з іншими системами, такими як хмарні платформи або кібер-фізичні системи (далі CPS), що підвищує загальну ефективність.

IoT-технології в міській інфраструктурі створюють можливості для автоматизації процесів управління та підвищення ефективності використання ресурсів. Однією з ключових технологій є кібер-фізичні системи, що забезпечують контроль і моніторинг ресурсів у реальному часі. Одним із важливих напрямів застосування IoT є енергетична сфера. Сенсори можуть моніторити споживання енергії, виявляти проблемні ділянки та оптимізувати роботу електричних мереж, що підвищує надійність енергопостачання і знижує втрати енергії. Автоматизовані системи також дозволяють інтегрувати відновлювані джерела енергії, такі як сонячні та вітрові електростанції, сприяючи сталому розвитку міст.

Інший важливий напрям IoT – управління транспортними системами. Сенсори, розміщені на дорогах і транспортних засобах, дозволяють збирати дані про транспортні потоки, які використовуються для оптимізації роботи світлофорів, громадського транспорту та паркувальних майданчиків. Це знижує рівень заторів і скорочує час пересування мешканців міста, а також зменшує забруднення повітря [5].

У водопостачанні сенсори можуть моніторити тиск у трубопроводах, рівень води в резервуарах і якість води. Дані в реальному часі допомагають попередити

аварії або витоки води, знижуючи витрати на ремонт та експлуатацію.

Оскільки IoT-системи широко використовуються для управління критичними елементами міської інфраструктури, безпека таких систем є пріоритетом. Зростання кількості підключених пристроїв підвищує ризик кібератак, що вимагає надійних методів захисту даних і безпеки мережевих взаємодій [8].

Автентифікація користувачів є одним із ключових методів забезпечення безпеки IoT. Вона гарантує, що лише авторизовані користувачі та пристрої мають доступ до мережі. Однак класичні підходи не завжди підходять для IoT через обмежені обчислювальні потужності сенсорних вузлів. Тому розробляються нові полегшені протоколи автентифікації, які забезпечують безпеку без надмірного навантаження на ресурси [9].

Ще одним важливим аспектом безпеки є шифрування даних. IoT-системи використовують алгоритми AES або RSA для захисту інформації, проте через обмежені ресурси сенсорів часто застосовують полегшені варіанти цих алгоритмів. Також важливими є захищені протоколи зв’язку, як-от TLS або DTLS, що знижують ризик перехоплення даних. Проте складні алгоритми можуть підвищити енергоспоживання, тому необхідно знайти баланс між безпекою та енергоефективністю.

Ситуаційні центри управління є ключовими компонентами IoT-систем у містах. Вони забезпечують координацію міської інфраструктури в режимі реального часу, дозволяючи оптимізувати процеси, як-от керування транспортними потоками та водопостачанням. Дані з сенсорів допомагають автоматично реагувати на аварії або надзвичайні ситуації [6].

Нарешті, для стабільної роботи IoT-систем необхідно впроваджувати стандарти якості обслуговування (далі QoS), що визначають затримку передачі даних, ширину смуги пропускання, надійність зв’язку та безпеку. Наприклад, затримка передачі даних у транспортних або енергетичних мережах може призвести до серйозних наслідків, як-от затори або перебої в електропостачанні [6].

Ще одним важливим показником є ширина смуги пропускання. У міських IoT-системах кількість підключених пристроїв може бути дуже великою, і для ефективної роботи системи необхідно забезпечити достатню пропускну здатність мережі. Якщо пропускна здатність недостатня, це може призвести до перевантаження мережі та зниження швидкості передачі даних, що негативно вплине на функціонування всієї міської інфраструктури [8]. Особливо важливо забезпечити необхідну пропускну здатність для критичних систем, таких як моніторинг та управління міськими ресурсами. Надійність зв'язку також є ключовим аспектом для IoT-систем, оскільки стабільне та безперебійне з'єднання між усіма компонентами інфраструктури є критично важливим для їхньої безперервної роботи. Наприклад, у разі збоїв у з'єднанні енергетичних мереж або систем безпеки можуть виникати серйозні наслідки, як-от перебої в електропостачанні або затримки у реагуванні на надзвичайні ситуації [9]. Таким чином, забезпечення стабільного зв'язку є важливим завданням для ефективного функціонування розумних міст.

Одним із найважливіших аспектів QoS в IoT-системах є безпека, яка відіграє ключову роль у захисті конфіденційних даних і збереженні цілісності систем. Для цього застосовуються захищені протоколи зв'язку та шифрування даних, що гарантує захист переданої інформації від несанкціонованого доступу. З огляду на зростання кількості IoT-пристроїв у міській інфраструктурі, виникає необхідність оптимізації процесу передачі даних, щоб уникнути перевантажень мережі та забезпечити стабільну роботу всієї системи.

Математичні моделі є важливим інструментом для оптимізації трафіку в мережах IoT, допомагаючи прогнозувати трафік і приймати рішення щодо його

обробки. Однією з найбільш ефективних моделей для аналізу й оптимізації трафіку в IoT-системах є теорія черг, яка дозволяє моделювати поведінку мережі під різними навантаженнями, тим самим забезпечуючи високу якість обслуговування. Основний підхід, заснований на цій теорії, полягає в моделюванні процесу обробки даних, які надходять від численних сенсорних вузлів через вузли-шлюзи та базові станції. У міру збільшення обсягу трафіку теорія черг допомагає уникнути перевантаження каналів зв'язку і підвищити ефективність використання мережевих ресурсів. Використання таких математичних моделей дозволяє передбачати можливі затримки та рівномірно розподіляти навантаження між різними елементами мережі [9].

Різні типи моделей черг можуть бути застосовані для IoT-систем залежно від конкретних сценаріїв. Наприклад, модель M/M/1, де один сервер обслуговує заявки, що надходять із певною частотою, є корисною для прогнозування трафіку у вузлах IoT-систем із обмеженою пропускною здатністю. Для складніших сценаріїв можуть бути використані інші моделі, як-от M/M/c або M/G/1, де кілька серверів обробляють чергу заявок, або ж обробка здійснюється зі змінною швидкістю [9]. Такі підходи дозволяють враховувати різні фактори, що впливають на трафік, зокрема час доби, інтенсивність транспортних потоків або інші чинники міського середовища.

Агрегований трафік від IoT-пристроїв у розумних містах змінюється залежно від різних умов, наприклад, часу доби або інтенсивності транспортних потоків. Моделі, що використовують агреговані потоки даних, дозволяють прогнозувати зміни трафіку в реальному часі та динамічно адаптувати роботу мережі для зменшення затримок [10]. Застосування таких моделей є важливим у системах управління міським транспортом, де вони допомагають оптимізувати роботу світлофорів, скоротити час очікування для водіїв і знизити загальне навантаження на транспортну інфраструктуру. Подібні підходи можуть бути застосовані для управління іншими міськими ресурсами, такими як електромережі або системи водопостачання [8].

Один із ключових аспектів, який враховують у математичних моделях управління трафіком IoT-систем, — це параметри QoS. Ці параметри включають затримку передачі даних, ширину смуги пропускання, надійність зв'язку та пріоритетність даних. Застосування теорії черг дозволяє оптимізувати ці показники для досягнення високої ефективності роботи системи. Наприклад, такі моделі допомагають визначити оптимальні рівні затримок і пропускної здатності для кожного типу трафіку, що дозволяє забезпечити пріоритетну обробку критичних даних, таких як інформація про аварії чи небезпеки [9].

Важливим фактором підвищення ефективності управління трафіком IoT-систем в процесі управління інфраструктурою міста є методи, способи та вид програмного забезпечення яке буде застосовуватися в межах як управління самою системою так і застосування самої системи, пов’язаними з нею елементами IoT та кінцевими користувачами.

Існуючі тенденції розвитку способів та методі розробки та застосування програмних продуктів в сучасних мережах IoT, з врахуванням масованого втілення телекомунікаційних мереж та систем п’ятого покоління, а саме 5G/IMT-2020, виводить на перший план застосування таких типів архітектури програмного забезпечення (ПЗ) як безсерверні та мікросерверні масиви ПО [11,12]. Їх перевагами є відсутність проміжних елементів накопичення та обробки даних, що значно підвищує швидкість функціонування мережі та отримання результатів її застосування. При цьому саме мікросервісна архітектура ПЗ забезпечує можливість одночасного ефективного застосування різними користувачами ПЗ різного призначення в інфраструктурних рішеннях, до яких в першу чергу відносяться IoT-систем.

Побудована по мікросервісній архітектурі ПЗ уявляє собою набір окремих програмних продуктів та логіку їх застосування. При цьому побудоване таким чином ПЗ може включати в себе окремі функціональні блоки а бо мати атомарну структуру [11, 12].

В свою чергу, саме найбільш сучасна на перспективна атомарна структура мікросервісного ПЗ дозволяє більш ефективно використати вільні обчислювальні можливості мережі, мати можливість до швидкого клонування окремих елементів ПО, активно застосовувати при функціонуванні сумісно з граничними туманні обчислення та залучати до управління мікросервісногог ПЗ елементи штучного інтелекту (ШІ). Особливо важливе залучення ШІ при аналізі трафіку запитів до масиву мікросервісного ПО на етапі визначення навантаження на IoT-систему, виключення впливу додаткових затримок і змін структури потоків корисних даних в мережі [12, 13].

Важливою властивістю мікросервісног підходу до побудови ПЗ є можливість до мінімізації якості розробки та взаємодії різни[елементьd такого ПЗ, при створення різними виробниками та залученні до їх застосування різних програмно-апаратних комплексів.

Зі всього переліку чинників, негативних факторів та параметрів, які можуть чинити вплив на якість функціонування IoT-системи в умовах застосування масивів мікросервісного ПЗ, створеного, як совокупність елементів від різних розробників та реалізованого на різних типах програмно-апаратних комплексів найбільш значущим буде чинник затримки, який визначається часом відклику мережі на запит окремого користувача [11, 12].

Є очевидним, що наукові дослідження по мінімізації вказаного часу затримки повинні проводитись в напрямку своєчасного аналізу навантаження на контролери програмно-орієнтованої мережі. Результати аналізу якого, через подальший розподіл трафіку запитів можуть забезпечити виключення впливу як особливостей розробки елементів ПЗ так і вплив можливостей програмно-апаратних комплексів на загальну ефективність управління всієї IoT-системи [13, 14].

Таким чином, побудови мереж інтернету речей для управління інфраструктурою міста при умові залучення до її функціонування мікросервісного ПЗ вимагає проведення ряду наукових досліджень. Основними з напрямків якого можуть бути:

- розробка механізмів аналізу навантаження в IoT-системах, які б дозволили мінімізувати час визначення додаткових затримок трафіку і зміни структури потоків корисних даних.

– побудова структури взаємодії туманних та граничних обчислень в межах мікросервісного ПЗ з урахуванням змін динамічності користувачів;

– розробка нових, науково обґрунтованих моделей взаємодії туманних і граничних обчислень, які, за рахунок раціонального вибору пристроїв туманних обчислень які повинні забезпечити функціонування мікросервісного ПЗ при умові мінімізації часу виконання завдань;

– розробка та удосконалення методик та методів прогнозування навантаження на контролер програмно конфігурованих мереж, які повинні забезпечити виключення залежності ПЗ управління мережами від особливостей функціонування апаратно-програмованих комплексів різних виробників.

Вирішення вище поданих завдань в цілому, через зменшення часу відпрацювання окремих запитів та часткових завдань, буде сприяти підвищенню якості функціонування мереж інтернету речей при залучені її до управління інфраструктурою міста.

ВИСНОВКИ

Таким чином, математичні моделі, зокрема теорія черг, є важливими інструментами для управління трафіком в IoT-системах розумних міст. Вони дозволяють не тільки уникнути

перевантажень, але й забезпечити стабільну та ефективну роботу системи, що є критично важливим для міської інфраструктури великих агломерацій. Успішне впровадження IoT-систем для управління міською інфраструктурою відкриває нові можливості для оптимізації використання ресурсів, підвищення надійності міських сервісів і покращення умов життя мешканців. Однак для досягнення цих цілей необхідно ретельно підходити до вибору мережевої архітектури, забезпечення безпеки і управління агрегованим трафіком, перейти до застосування найбільш раціональної архітектури програмного забезпечення для управління трафіком системи та її застосування при управління міською інфраструктурою.

В якості раціональної архітектури програмного забезпечення в роботі запропоновано застосувати мікросервісне програмне забезпечення. А саме, визначені його особливості та переваги і подані напрямки подальших наукових досліджень, які будуть направлені на ефективне застосування вказаного програмного забезпечення для управління інфраструктурою міста через IoT-систему.

REFERENCES

1. **Markuts V.** (2023). Zastosuvannia tekhnolohii Internetu rechei v avtomatyzovanykh systemakh upravlinnia resursamy. *Stratehiia ekonomichnoho rozvytku Ukrainy*, No.52, 97–111. https://doi.org/10.33111/sedu.2023.52.097.111,
2. **Aggarwal A.** (2019). Internet of things driven perceived value co-creation in smart cities of the future: a PLS-SEM based predictive model. *Journal of Computational and Theoretical Nanoscience*, Vol. 16. No. 9. 4053–4058. DOI: https://doi.org/10.1166/jctn.2019.8292.
3. **Garcia-Retuerta, D., Chamoso, P., Hernández, G., Guzmán, A., Yigitcanlar, T., Corchado, J.** (2021). An efficient management platform for developing smart cities: Solution for real-time and future crowd detection. *Electronics*, Vol. 10 (7), 765. https://doi.org/10.3390/electronics10070765.
4. **Gómez J. E.** (2017). IoT for environmental variables in urban areas. *Procedia computer science*, Vol. 109, 67–74. https://doi.org/10.1016/j.procs.2017.05.296.
5. IoT-enabled smart cities: A hybrid systematic analysis of key research areas, challenges, and recommendations for future direction | Discover Cities [Springer] Available at: https://link.springer.com/article/10.1007/s42162-022-00195-2
6. **Madakam S., Ramaswamy R., Date H.** (2019). Quality of life. Palava smart city: A case study". Global Business Review, Vol. 20 (3), 708–742. DOI: https://doi.org/10.1177/097215091772182
7. Networking Architectures and Protocols for IoT Applications in Smart Cities: Recent Developments and Perspectives [MDPI] Available at: https://www.mdpi.com/2079-9292/12/11/2490
8. Networking architectures and protocols for smart city systems | Journal of Internet Services and Applications [SpringerOpen] Available at: https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0097-0
9. On Wireless Sensor Network Models: A Cross-Layer Systematic Review [MDPI] Available at: https://www.mdpi.com/2224-2708/12/4/50
10. Wireless Sensor Networks: Applications | IntechOpen Available at: https://www.intechopen.com/chapters/73287
11. **Ekaterina Oleynik, Sergey Revnivykh** (2011). GLONASS Status and Modernization. CGSIG Meeting, September. https://web.archive.org/web/20130921061015/http://www.navcen.uscg.gov/pdf/cgsicMeetings/51/3_GLONASS_CGSIC_Oleynik.pdf
12. **Shin Y., Kim E.** (2018). PF-DOP hybrid path planning for safe and efficient navigation of unmanned vehicle systems. In Proceedings of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS+ 2018, Miami, FL, USA, 24–28 September 2018; Institute of Navigation: Manassas, VA, USA, 2501–2517. DOI: 10.33012/2018.15978.
13. **Koretskyi Oleksandr** (2024) Architecture of multifunctional application software microservices. Сучасний захист інформації, 3(59), 85–93. DOI:10.31673/2409-7292.2024.030009.
14. **Y. Romani O.** (2022). Tibermacine and C. Tibermacine, "Towards Migrating Legacy Software Systems to Microservice-based Architectures: a Data-Centric Process for Microservice Identification," 2022 IEEE 19th International Conference on Software Architecture Companion (ICSA-C), Honolulu,

HI, USA, 2022, pp. 15-19, doi: 10.1109/ICSA-C54293.2022.00010.

Models for building Internet of Things networks for city infrastructure management

Anastasia Kondakova, Oleksandr Koretskyi,

Abstracts. The work considers modern approaches to the implementation of IoT technologies for effective management of urban infrastructure. The main focus is on the analysis of network architectures used for data collection and transmission in smart city systems. Various network construction models are compared, including single-hop and multi-hop networks, as well as WSN topologies. The work focuses on the advantages and disadvantages of these networks in the context of energy consumption, scalability and stability. Special attention is paid to hierarchical models that allow to reduce energy costs and increase network efficiency. The application of IoT in key areas of urban infrastructure, such as transport, energy and water supply, is analyzed. The issue of cyber security of IoT systems, including authentication, data encryption and ensuring communication reliability, is also discussed in detail. The role of CPS and sensor nodes that provide real-time monitoring and control of urban resources is discussed separately. Mathematical models for traffic optimization in IoT networks are considered, in particular, the use of queuing theory to ensure QoS. Conclusions have been drawn regarding the effectiveness of IoT implementation for urban resource management, which allows to increase the reliability of urban infrastructure and improve the living conditions of residents. The use of microservice software in IoT systems is substantiated and the directions of scientific research aimed at and its implementation in IoT-systems of management of infrastructure objects.

The study opens up new perspectives for the application of IoT in smart cities and indicates the need for further study of security and energy conservation issues in such systems.

Keywords: IoT, urban infrastructure, smart cities, WSN, energy efficiency, CPS, microservice software

Концептуальна модель формування обмежень щодо використання земель

Ольга Петраковська[1], Марія Михальова[2]

[1,2] Київський національний університет будівництва і архітектури
пр-т Повітряних Сил, 31, м.Київ, Україна, 03037
[1] petrakovska.os@knuba.edu.ua, orcid.org/0000-0002-9437-9730
[2] mykhalova.myu@knuba.edu.ua, orcid.org/0000-0002-2242-5507

Received 17.09.2024, accepted 30.10.2024
https://doi.org/10.32347/uwt.2024.15.1902

Анотація. Одним із найважливіших механізмів забезпечення ефективного та сталого використання земельних ресурсів є планування землекористування. Підвищення збалансованості використання земель, зокрема при формуванні обмежень вимагає комплексного підходу, що включає раціональне планування землекористування, законодавче та нормативно-правове регулювання, забезпечення екологічної стабільності, суспільну значущість, розвиток інфраструктури, залучення зацікавлених сторін та гарантування їх прав власності та користування, впровадження сучасних технологій.

Метою цього дослідження є представлення ідеології побудови концептуальної моделі формування обмежень щодо використання земель. Під час цього дослідження використовувалися методи факторного та системного аналізу, а також комплексного аналізу. Методом структурно-функціонального моделювання отримано концептуальну модель формування обмежень щодо використання земель.

Ключові слова: земельні ресурси, обмеження щодо використання земель, зацікавлені особи, просторовий розвиток, концептуальна модель.

ВСТУП

Земельні ресурси – найбільше важливий ресурс у процесі економічного та соціального розвитку кожної країни. Тому ефективне управління та використання земельних ресурсів є ключовим питанням

сталого розвитку більшості країн світу. Складність забезпечення збалансованого розвитку зумовлена міждисциплінарністю завдань, які необхідно вирішувати при комплексному врахуванні багатьох, часом суперечливих факторів і великою кількістю зацікавлених сторін.

Одним із найважливіших механізмів забезпечення ефективного та сталого використання земельних ресурсів є планування землекористування.

Це процес, який регулює використання земель шляхом реалізації різноманітних планів з урахуванням природних, містобудівних, соціально-економічних та екологічних умов. Існує також поділ території на різні зони з визначеними регламентами та обмеженнями використання земель як складова планування землекористування.

Земля — це вразливий ресурс, що потребує захисту та регулювання з боку держави. Враховуючи складові права власності на землю всі обмеження цих прав можна розглядати в економічному, соціальному і екологічному аспектах.

Забезпечення збалансованого, ефективного використання земель, зокрема при формуванні обмежень вимагає комплексного підходу, що включає раціональне планування землекористування, законодавче та нормативно-правове регулювання, забезпечення екологічної стабільності і суспільної значущості, розвиток інфраструктури, врахування інтересів зацікавлених сторін та гарантування їх прав власності та користування, впровадження сучасних технологій. Окрім цього, основою будь якого управлінського рішення є аналіз і оцінка факторів, які обумовлюють кінцевий результат. Застосування комплексного підходу дозволяє забезпечити збалансований просторовий розвиток, включаючи соціальну, екологічну та економічну складову.

МЕТА ТА МЕТОДИ ДОСЛІДЖЕННЯ

Метою цього дослідження є представлення ідеології побудови концептуальної моделі формування обмежень щодо використання земель.

Під час дослідження використовувалися методи факторного, системного аналізу, та комплексного аналізу. Методом структурно-функціонального моделювання отримано концептуальну модель формування обмежень щодо використання земель.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Просторовий розвиток – це процес, в наслідок якого відбуваються зміни в інтенсивності і розосередженні різних видів діяльності в певному просторі та зв`язків між ними, і безпосередньо пов'язаний із територіальними (містобудівними) системами, які є сукупністю просторово-організованих і взаємопов'язаних технічно освоєних територій, будівель і споруд, доріг і інженерних споруд, спільно з природними компонентами. Неодмінною умовою збалансованого просторового розвитку є врахування взаємозв'язків між основними структурними елементами територій, оцінка і прогнозування наслідків їх збереження і порушення. Встановлення обмежень щодо використання земель безпосередньо пов’язано із завданнями просторового планування і складовими прав власності на землю [1, 8, 9, 12].

Особливості різних етапів розвитку просторового планування в Україні ілюструють трансформацію підходів до накладання обмежень на використання земель.

Ретроспектива формування обмежень щодо землекористування ілюструє, що цей процес розвивався у відповідь на зміну суспільних пріоритетів, економічний тиск, екологічні проблеми та правові конфлікти і відображає постійну адаптацію суспільства до нових умов та викликів. Сучасні обмеження у використанні земель стають ще більш багатогранними. Вони враховують як екологічні, так і соціальні, економічні аспекти, зокрема права місцевих громад, збереження біорізноманіття, запобігання деградації земель та вплив на зміни клімату. З’являються нові технології та підходи, які дозволяють більш точно визначати необхідні обмеження та їх вплив на навколишнє середовище. Це поняття еволюціонувало від простих обмежень, спрямованих на збереження земельних ресурсів у локальному масштабі, до складної системи норм і стандартів, які враховують глобальні виклики [2, 4, 5, 7].

Посилення уваги до обмежень у використанні земель спрямовано на забезпечення збалансованості економічних, екологічних і соціальних складових розвитку територій і використання окремих земельних ділянок.

На основі результатів, отриманих в [11, 14,15] запропонована концептуальна модель формування обмежень щодо використання земель як одного з механізмів забезпечення збалансованого просторового розвитку територій (Рис. 1).

В основу побудови концептуальної моделі покладені принципи які визначають ключові пріоритети та правила, за якими мають формуватися обмеження, враховуючи їх соціальний, екологічний і економічний вплив і наслідки.

Проведений авторами аналіз ілюструє, що всі обмеження мають кількісті і якісні характеристики. Об’єктом встановлення обмежень можуть бути сформовані земельні

ділянки, сукупність земельних ділянок/земельний масив або територія.

своєї дії при переході права власності на земельну ділянку, така інформація має бути вже зафіксована при набутті прав власності.

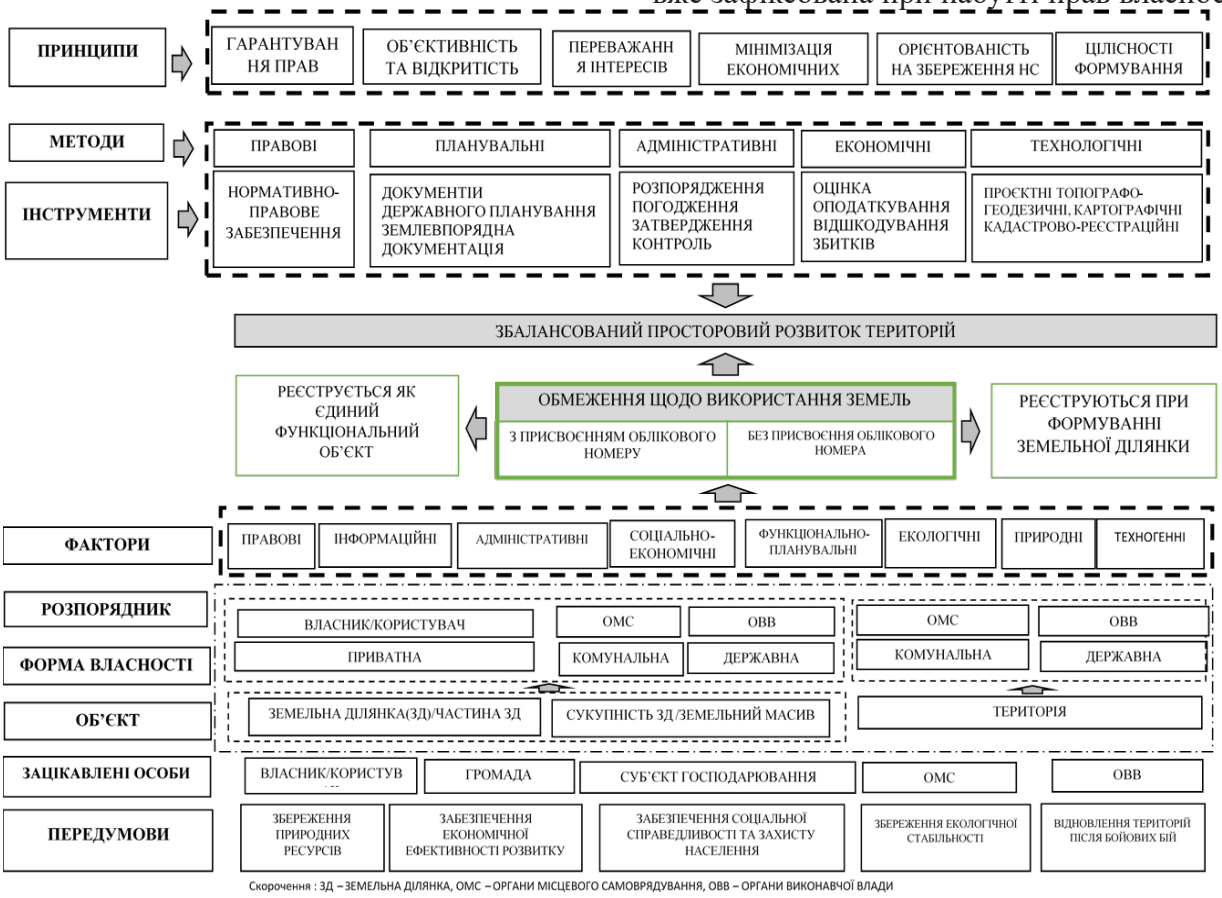


Рис. 1. Концептуальна модель формування обмежень щодо використання земель
Fig. 1. Conceptual model of land use restrictions formation

При цьому обмеження прав власності можуть бути спрямовані на різні складові прав: право володіння, право користування, право розпорядження. У випадку, коли об'єктом обмеження є сформована земельна ділянка, заборони можуть розповсюджуватись на всю земельну ділянку або її частину. У разі коли земельні ділянки не сформовані, мова йде про земельні масиви вільні від забудови або забудовані території.

З точки зору контролю за дотриманням обмежень набуває значення форма власності земель, які потрапляють в зону дії обмежень. У разі державної і комунальної власності при вирішенні цих питань не виникає додаткових проблем. У разі приватної власності на землю, власник має бути проінформований про всі обмеження, які накладаються на його земельну ділянку. Враховуючи що обмеження не припиняють

Однак обмеження також можуть бути встановлені в про-цесі використання земельної ділянки. В такому випадку встановити обмеження на землях приватної власності можна тільки за згодою власника або через суд.

В результаті дослідження світового досвіду встановлення обмежень, авторами було систематизовано передумови їх формування:

- збереження природних ресурсів;
- забезпечення економічної ефективності розвитку території;
- забезпечення соціальної справедливості та захисту населення;
- збереження екологічної стабільності.

Зокрема, в Україні, після повномасштабного вторгнення Росії на територію України, виникла додаткова

необхідність у встановленні обмежень щодо використання земель, пов'язані з бойовими діями, руйнуваннями і необхідністю відновлення територій. Необхідність вже зараз готувати підґрунтя для відновлення і розвитку територій не визиває сумніву і є дуже важливим кроком в майбутнє. Але ці підґрунтя мають бути виваженими і зорієнтованими на ефективний результат від застосування та законодавчо врегульованими.

Взаємоузгодження державних, громадських та приватних інтересів є одним із принципів формування обмежень [10]. Одним із механізмів забезпечення такого взаємоузгодження є проведення громадських слухань і громадських обговорень [19]. В роботі була проведена ідентифікація зацікавлених осіб і визначені, враховуючи мету дослідження, основні три групи респондентів інтереси, яких принципово відрізняються:

- землевласник/землекористувач;
- територіальна громада;
- орган місцевого самоврядування/ органу виконавчої влади;
- фахівець з питань щодо встановлення обмежень (землевпорядник, містобудівельник, геодезист, архітектор тощо).

Такий вибір зацікавлених осіб обумовлений наступним. Власників і користувачів в першу чергу цікавить вплив обмежень на їх нерухомість. Територіальна громаду представляють мешканці, які в свою чергу теж є землекористувачами земель комунальної власності. Органи місцевого самоврядування і виконавчої влади опікуються інтересами громад і загальними суспільними. Фахівці з питань встановлення обмежень зацікавлені в досконалих технологічних процедурах встановлення обмежень як об'єкту містобудівного планування, землеустрою, кадастру, екологічної оцінки тощо.

Врешті решт, щоб правильно реалізувати процес формування обмежень і забезпечити їх обґрунтованість і соціально-економічну і екологічну збалансованість, необхідно ретельно вивчити та проаналізувати фактори, які впливають на цей процес, а також визначити вагомість кожного з них. Обґрунтованість встановлення обмежень у використанні земель, їх легітимність та доцільність може бути досягнуто при врахуванні низки факторів, які обумовлюють цей процес і визначають його наслідки.

У роботі [14] були проаналізовані результати дослідження щодо публікацій вітчизняних та закордонних науковців, нормативно-правової бази, державних інформаційних ресурсів, відкритих даних та різних видів документації з питань встановлення різних видів обмежень, таких як містобудівні та землевпорядні. Це дослідження виявило сукупність факторів, які необхідно враховувати при формуванні обмежень щодо використання земель, на основі детального аналізу літературних джерел, практичного досвіду та нормативно-правового регулювання.

Вся сукупність досліджуваних факторів, авторами об'єднано у вісім тематичних груп: правові; адміністративні; інформаційні; екологічні; природні; соціально-економічні; функціонально-просторові; техногенні [14].

Обмеження можна вважати сформованим з моменту внесення інформації в державний земельний кадастр [16,20]. Проведений аналіз набуття легітимності дозволив визначити два варіанти реєстрації обмежень щодо використання земель. В першому випадку до ДЗК вносяться відомості про обмеження у використанні земель на підставі землевпорядної документації, договору, рішення суду [17, 18]. В такому випадку обмеження щодо використання земель реєструються як єдиний функціональний об'єкт. В результаті реєстрації в державному земельному кадастрі об'єкту присвоюється обліковий номер. В другому випадку встановлення обмежень здійснюється у процесі державної реєстрації земельних ділянок. Обмеження щодо використання земель встановлюються виключно в межах земельної ділянки, яка формується. В такому випадку обмеження реєструється в державному земельному кадастрі без присвоєння облікового номера.

ВИСНОВОК

В результаті систематизації і структуризації сукупності обмежень та аналізу передумов та принципів їх встановлення визначено, що обмеження можуть впливати на соціальні, економічні і екологічні аспекти використання земельних ділянок і розвитку земель. На підставі результатів дослідження авторами розроблено концептуальну модель формування обмежень щодо використання земель.

Запропонована модель ілюструє, що встановлення обмежень має базуватися на комплексному підході та врахуванню особливостей об'єкта та суб'єкта, факторів впливу, а також залученості зацікавлених сторін та врахуванні державних, громадських та приватних інтересів.

REFERENCES

1. **Almulhim, A.I.; Bibri, S.E.; Sharifi, A.; Ahmad, S. & Almatar, K.M.** (2022). Emerging Trends and Knowledge Structures of Urbanization and Environmental Sustainability: A Regional Perspective. Sustainability, 14, 13195
2. **Barker, Kate.** (2006). Barker Review of Land Use Planning, Final Report – Recommendations, 5 Decem-ber, HM Treasury.
3. **Coad, L., A. Campbell, L. Miles, and K. Humphries.** (2008). The Costs and Benefits of Protected Areas for Local Livelihoods: a review of the current literature. Working Paper. UNEP World Conservation Monitoring Centre, Cambridge, U.K.
4. **Fernandes, E.** (2008). Sustainable Land Management: Sourcebook. https://doi.org/10.1596/978-0-8213-7432-0.
5. **Garrett Power.** (2013). Constitutional Limitations on Land Use Controls, Environmental Regulations and Governmental Exactions U of Maryland Legal Studies Research Paper No. 2013-1
6. **Kalfas, D.; Kalogiannidis, S.; Chatzitheodoridis, F.; Toska, E.** (2023). Urbanization and Land Use Planning for Achieving the Sustainable Development Goals (SDGs): A Case Study of Greece. Urban Sci. 2023, 7, 43.
7. **Kim, J.H.** (2011). Linking land use planning and regulation to economic development: A literature review. J. Plan. Lit. 26, 35–47
8. **Land Use Restrictions as Barriers to Entry** (2008). the Competition Committee (Working Party No. 2 on Competition and Regulation)
9. **Palmer, Robert; Nursey-Bray, Melissa.** (2007). "Rio Declaration on Environment and Development". In Robbins, Paul (ed.). Encyclopedia of Environment and Society. Vol. 4. Thousand Oaks: Sage Publications. pp. 1512–1514. ISBN 9781412927611.
10. **Parmar, B.L., Freeman, R.E., Harrison, J.S. et al.** (2010). "Stakeholder Theory. The state of the art" Management Faculty Publications. 99.
11. **Petrakovska O. and Mykhalova M.** (2018). Socio-economic and ecological aspects of land management in cities, ACTA Scientiarum Polonorum, Formatio Circumiectus Zeszyt 17 (4) 2018 pp. 103-109.
12. **Trehub M., Trehub Y**. (2015). Substantiation of land management methods of industrial cities. Theoretical and Practical Solutions of Mineral Resource. 2015. P. 449-452. DOI: https://doi.org/10.1201/b19901
13. **Webster, Chris and Lawrence Wai-Chung Lai** (2003). Property Rights, Planning and Markets. Edward Elgar: London, 2003
14. **Petrakovska O.S., Mykhalova M.Iu.** (2024). Faktory, shcho obgruntovuiut formuvannia obmezhen vykorystannia zemel Mistobuduvannia ta terytorialne planuvannia, (85), 454–461. https://library.knuba.edu.ua/books/zbirniki/02/2024/202485.pdf
15. Pro zatverdzhennia Poriadku vedennia Derzhavnoho zemelnoho kadastru. Postanova Kabinetu Ministriv № 1051, 17.10.2012 [Elektronnyi resurs]. Rezhym dostupu: http://zakon2.rada.gov.ua/laws/show/1051-2012
16. Pro zatverdzhennia Poriadku rozroblennia, onovlennia, vnesennia zmin ta zatverdzhennia mistobudivnoi dokumentatsii. Postanova KMU № 926 vid 01.09.2021 [Elektronnyi resurs]. – Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/926-2021-%D0%BF#Text
17. Pro zemleustrii. Zakon Ukrainy 858-IV (2003). [Elektronnyi resurs]. – Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/858-15
18. Pro rehuliuvannia mistobudivnoi diialnosti. Zakon Ukrainy 3038-VI v redaktsii 27.10.2022 [Elektronnyi resurs]. – Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/3038-17#Text

19. **Trehub, M., Trehub, Yu., Zabolotna, Yu., & Yankin, O.** (2022). Propozytsii shchodo vdoskonalennia metodyky derzhavnoi reiestratsii sanitarno-zakhysnykh zon. Prostorovyi rozvytok, (1), 268–276. https://doi.org/10.32347/2786-7269.2022.1.268-276

Conceptual model of land use restrictions formation

Olga Petrakovska, Mariia Mykhalova

Abstract. One of the most important mechanisms for ensuring efficient and sustainable use of land resources is land use planning. Improving the balance of land use, in particular in the formation of restrictions, requires an integrated approach, including rational land use planning, legislative and regulatory regulation, ensuring environmental sustainability, social significance, infrastructure development, stakeholder involvement and guaranteeing their property and use rights, and the introduction of modern technologies.

The purpose of this study is to present the ideology of building a conceptual model of land use restrictions. In the course of this study, the methods of factor and system analysis, as well as complex analysis were used. By the method of structural and functional modeling, a conceptual model of the formation of restrictions on land use was obtained.

Keywords: land resources, restrictions on land use, stakeholders, spatial development, conceptual model.

GUIDELINES FOR AUTHORS

Publication requirements

For publication in the *Smart Technologies: Industrial and Civil Engineering* journal are accepted original materials of the research and discussion character (mostly individual, in English, the number of authors not more than three) in volume of 8 − 12 pages (A4), including tables, drawings and a list of literature. The Articles (mostly individual, in English, no more than 3 authors and no less than 20 sources) are subject to double review, including by independent specialists engaged by the editors, and DOI digital identification. The authors submit to the publisher the copyright to texts and written permissions to reproduce drawings and tables from previously unpublished or copyrighted materials. The editorial board follows the ethical standards of scientific publication.

To the article attached (cybersec@knuba.edu.ua) **Application** for publication (7 files collected in the "Documents" folder):

1) information ***about the article*** − *Form 1*
1) information ***about the authors*** (status: *h*-index, last name, first name, patronymic, degree, academic rank, place of work, address, post; contacts: photo of the author (.jpg), mobile phone, e-mail, ORCID identifiers and Scopus Author ID) − *Form 2* (word)
2) two external ***reviews*** − *Form 3*
3) expert ***conclusion*** − *Form 4*
4) ***agreement*** on the free use of copyright − *Form 5*
5) certified ***translation*** of the article into English
6) ***recommendation*** for printing (extract from the protocol of the institution where the author works)

Requirements to the article

Terms:

- sheet parameters: A4 format, upper and lower fields 2,5 cm, left and right 2 cm; font Times New Roman; footers 1,0 cm, paragraph indentation 0,5 cm; the size of the main text 12, annotations and literature 11, line spacing 1
- the article (.doc) is formatted in two columns of 8 cm with a gap of 1 cm; set up automatic word transfer
- the names of the tables and signatures under the drawings (size 11) are placed on the left of the graphic object; in Cyrillic texts − duplicate in English (line below)
- in the list of references – not less than 20 references (mainly on scientific articles and monographs); after the surname the year of publication is indicated (APA standard)
- the list of references is duplicated in English (verbatim), while the original data is transliterated (https://translit.kh.ua/#lat), indicating in brackets the original language, for example (in Ukrainian), (in Poland), (in English)
- referring to the Internet resource, the full name and the source data of the publication should be indicated
- at the end of the English-language articles the annotation is given in Ukrainian; in other articles − in English

Structuring:

- source data (font Arial): title of the work (n/a, font 14), author's first and last name (italics, font 12), place of work, postal address, e-mail, ORCID (font 10); if there are several authors − they are marked with digital footnotes; 5 empty lines is left between the upper field of the page, the source data and the main text of the article
- structural subdivisions:

Article (8 – 12 pp. font 12):	*Annotation*: (not less than 1800 characters – 0,5 pp. font 11)
- ANNOTATION	- PURPOSE
- INTRODUCTION	- METHODOLOGY
- PURPOSE AND METHODS	- RESULTS OF THE RESEARCH
- RESULTS AND EXPLANATIONS	- SCIENTIFIC NOVELTY
- CONCLUSIONS AND RECOMMENDATIONS	- PRACTICAL SIGNIFICANCE
- ACKNOWLEDGMENT (if necessary)	- KEYWORDS (5 − 8 words)
- REFERENCES (not less than 20 references)	

- title of the article − informative and short; the annotation structure is similar to the structure of the article, without the use of shortenings and abbreviations, all explanations are given in the text; link − no more than 5 sources in one place
- tables and figures are placed after the first mention of them, large (full width of the sheet) − from the top or bottom of the page (without breaking the two columns of the text simultaneously)
- Illustrations − in .jpg, .tif format with the resolution of at least 300 dpi

Design:

- write straight: numbers, Greek letters, Cyrillic alphabet, trigonometric functions (tan, sin, etc.), fixed expressions (max, const, etc.), chemical elements; italics − English formula symbols, Roman numerals, exploration numbers
- between formulas, drawings, tables and text leave 1 empty line
- formulas (size 12-9-7-16-12) are typed in MathType and centered; numbering − to the right of the column; tables and figures − do not exceed the area printed sheet
- shortened words "Table", "Fig." are written with capital letter (in the text − light, in the name − n/a); The text in the drawing field is minimized, explanations are given in the signatures under the drawings
- as punctuation marks only a point and a comma are used (standard ARA); the number of pages (range) is indicated without their designation
- examples of article design and archive of journals – see http://uwtech.knuba.edu.ua

Publication statement
in an international scientific journal

_____
(journal name)

Form 1

INFORMATION ABOUT THE ARTICLE

Language of the article	**Author(s)** (name, surname − *in the language of the article*) (subject area) / (number of pages)	**Documents (+/−)**							**Article Title**	**Order** (number of copies)
		About the article (*F.1*)	About the authors (*F.2*)	Two reviews (*F.3*)	Exp. conclusion (*F.4*)	Agreement (*F.5*)	Approved Translation	Recommendation	**Reviewers** (name, surname, scientific degree, academic status − *in the language of the article*)	Payment (€) Date
		1	2	3	4	5	6	7		Signature
									Rev.1: *Rev.2*:	

Form 2

INFORMATION ABOUT THE AUTHORS
(*in the language of the article*)

Data			Contacts	
h-index (*Scopus*)	Full Name scientific degree, academic status	Place of work, position, address, index	The author's photo (.jpg, 300 dpi)	Cell-phone e-mail ORCID *Scopus Author ID* *Researcher ID*

* – indicate availability by sign

Form 3

REVIEW
(two, external)

Must contain:
1) *Title of the article*, *Surname of the author(s)*
2) *Evaluation of the work* (originality, correspondence with the title and text of the article, methods and purpose of work, terminology, style of presentation, grammar)
3) Information about *the Quality of the article* (content, translation in English) and the lack of *Plagiarism*
4) *Remarks* and *Adjustments* (or indication of the necessity to transfer the article to another reviewer)
5) *Recommendation* (for publication, further elaboration, re-review, refusal to publish)
6) Information about the *Reviewer* (name, surname, degree, academic rank, place of work in the language of the article)
7) *Date*, *Signature* (approved)

Form 4

(Sample)

APPROVED

(position, scientific degree,
academic status)

Full Name

« ___ » _____ 202 ___

EXPERT CONCLUSION No ____

on the possibility of publishing materials
in the press and other sources of information

Kyiv National University of Construction and Architecture Expert Commission, having reviewed the materials

_____
(name, surname of the author(s))

_____
(Article Title)

_____

_____

which consists of ____ pages, notes that they do not have any information that would be a subject to publication ban in accordance with "The Expanded list of information containing the state secret in the Ministry of Education and Science of Ukraine − 2001"

Conclusion: these materials are allowed to be published openly

The Head of the Expert Group

Full Name

Form 5

AGREEMENT No _____

on free use of copyright in the *Smart Technologies: Industrial and Civil Engineering* periodical Edition

Kyiv « ___ » _____ 20 ___

The Editorial Board of the *Smart Technologies: Industrial and Civil Engineering* journal, the founder of which is the Kyiv National University of Construction and Architecture, having the legal address: KNUCA, Povitrianykh Syl Ave, 31, Kyiv, Ukraine, 03037, in the person of the chief editor, doctor of technical sciences, professor M. Sukach, on the one hand (hereinafter − Editorial), and the owner(s) of the property rights and copyright in the person of

_____ _____ _____,
(Full Name) (scientific degree, academic status)..... (ORCID)

_____ _____ _____,
(Full Name) (scientific degree, academic status)..... (ORCID)

_____ _____ _____,
(Full Name) (scientific degree, academic status)..... (ORCID)

on the other hand (hereinafter − the Author(s)), who altogether referred to as the Parties, guided by the Civil Code, the Law of Ukraine "On Copyright and Related Rights", other legislative and regulatory acts of Ukraine, entered into this Agreement as follows.

§ 1

1.1. The author (s) declare that they are valid writers of the Scientific Work / Article titled as

_____

_____
(original language)

which is the result of their joint creative work and that they have the exclusive copyright in relation to the above mentioned work.

1.2. The author (s) declare that the Work/Article does not violate the copyrights of any third party, does not contain any borrowings (plagiarism), and there are no other circumstances that may cause the Editorial Board to be liable to any third party as a the result of the use or publication of the Work/Article.

1.3. The author (s) declare that they have the right to dispose of the materials contained in the Work/Article, including texts, photographs, maps, plans, etc., and that the use of these materials in the Work/Article does not violate the rights of the third party.

1.4. The author (s) confirm that they are familiar with the article design requirements. The text of the Work/Article has been prepared in accordance with the editorial requirements regarding the publication in the *Smart Technologies: Industrial and Civil Engineering* periodical.

1.5. The author (s) declare that the Work/Article has not been previously published in full or in part (or under the same or another name) and that it has not been transmitted for publication to any other periodical publication in accordance with the Law of Ukraine "On Copyright and Related Rights".

§ 2

2.1. The author (s) provide the Editorial with free and no restrictions on the territory, time and number of copies full copyright of the Work/Article for the purpose of its publication in the *Smart Technologies: Industrial and Civil Engineering* periodical in printed and electronic form, with the following terms of use:

a) storage on any media devices;

b) reproduction of the Work/Article, its parts or fragments by any known methods, copying Work/Article or parts and fragments thereof by any technique, including printing, risography, magnetic recording and digitization;

c) saving on a computer and placing in private and public computer networks (including the Internet) and distribution over the networks;

d) dissemination of the original and / or copies of the Work/Article, its separate parts or fragments, distribution and transfer to the use of the original or copies thereof.

2.2. The author(s) agree that the editorial work and duplication of the periodical publication shall be made with the voluntary contributions of the Publishers.

§ 3

3.1. The author(s) and the Editorial Board agree that the Editor will also be entitled to:

a) make the necessary design of the Work/Article on the results of the editorial work;

b) determine independently the number of publications, the printing of additional copies and the circulation of the Work / Article, the number of copies of individual editions and additional copies;

c) the publication of the Work/Article in other editions related to the activities of the Editor than those specified in paragraph 2.1.

§ 4

4.1. The author (s) and Editorial hereby state that free use of the copyright under this agreement is free of charge.

4.2. Any changes to this Agreement must be made in hard copies.

4.3. Questions not regulated by the provisions of this Agreement shall be subject to the rules of the Civil Code and the Law of Ukraine "On Copyright and Related Rights".

4.4. Any disputes that may arise during the execution and during the term of this Agreement will be resolved within the territorial jurisdiction of the place where the Editorial is located.

The Agreement is made in 2 (two) identical copies − one to each of the Parties.

AUTHOR(S):	EDITORIAL BOARD:
1. _____ _____ (Signature) (Full Name)	International scientific journal *Smart Technologies:* *Industrial and Civil Engineering* Povitrianykh Syl Ave, 31, 31, Kyiv, Ukraine, 03037 cybersec@knuba.edu.ua
2. _____ _____ (Signature) (Full Name)	
3. _____ _____ (Signature) (Full Name)	_____ Y. Khlaponin

INTERNATIONAL SCIENTIFIC JOURNAL

Scientific Edition

SMART TECHNOLOGIES:

INDUSTRIAL AND CIVIL ENGINEERING

Issue 2(15), 2024

Articles are published in the author's wording

- Design, style and contents of the magazine are subject to copyright and are protected by law
- The authors of the publications are responsible for the content and validity of the data given there
- The editorial staff reserves the right to edit and reduce the materials submitted
- All the articles have been positively evaluated by independent reviewers
- Reprints of material placed in the journal are allowed only with the written consent of the editorial board

Article reviewers

Nader Asnafi	PhD, Ass.Prof.
Goran Bryntse	PhD, Ass.Prof.
Stanislav Fic	Dr. hab eng, Prof.
Mykola Kuzminets	Dr.Tech.Sc, Prof.
Oleg Limarchenko	Dr.Tech.Sc., Prof.
Andrzej Marczuk	Dr hab eng, Prof.
Volodymyr Musiyko	Dr.Tech.Sc., Prof.
Bogdan Norkin	Dr.Phys. and Math.Sc.
Oleksandr Ovchinnikov	Dr.Tech.Sc., Prof.
Yurii Romasevych	Dr.Tech.Sc, Prof.
Eugene Shkvar	Dr.Tech.Sc, Prof.
Viktor Skachkov	Dr.Tech.Sc., Prof.

The journal is indexed in world databases

Google Academy	http://scholar.google.com.ua	CrossRef	https://www.crossref.org
Index Copernicus	www.journals.indexcopernicus.com	Ulrichs Web	http://ulrichsweb.serialssolutions.com
Web ИРБИС	http://irbis-nbuv.gov.ua		

The original layout is made in the editorial office of the journal Smart Technologies: Industrial and Civil Engineering

Responsible for the issue	*Dmytro Mischuk*
Linguistic consultant	*Anastasiia Khlaponina*
Computer layout	*Anna Liubushkina*
Editing and proofing	*Olha Tokarenko*
Layout and cover	*Anton Khaddad*

Journal Editorial Staff

KNUCA, Povitrianykh Syl Ave, 31, Kyiv, Ukraine, 03037,
Labor. corp., of. 361, Kyiv, Ukraine, 03037
+38 044 244 96 45, +38 050 311 0373
http://uwtech.knuba.edu.ua/, cybersec@knuba.edu.ua

Publisher and manufacturer

LLC “Lira-K Publishing”
Certificate No. 3981, DK series.
03142, Kyiv, str. V. Stusa 22/1
Phone (050) 462-95-48; (067) 820-84-77
Website: lira-k.com.ua, editor: zv_lira@ukr.net

Signed for printing on 18.06.2024 Format 60×84 1/8
Paper offset. Printing offset. Times New Roman
Cond. print. sheets 11,16. Circulation 100 copies

SMART TECHNOLOGIES

INDUSTRIAL AND CIVIL ENGINEERING

INTERNATIONAL SCIENTIFIC JOURNAL