**ІНСТИТУТ СИСТЕМ УПРАВЛІННЯ
МНО АЗЕРБАЙДЖАНСЬКОЇ РЕСПУБЛІКИ**

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"**

**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ**

**НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
"ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ"**

**УНІВЕРСИТЕТ МІСТА ЖИЛІНА**

---

# СУЧАСНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ

**Тези доповідей п’ятнадцятої міжнародної**

**науково-технічної конференції**

**24 – 25 квітня 2025 року**

**Том 3: секції 3, 4**

**Баку – Харків – Жиліна – 2025**

УДК 004/681.3 doi: https://doi.org/10.32620/ICT.25.t3

У збірнику подано тези доповідей п'ятнадцятої міжнародної науково-технічної конференції "Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління". Розглянуті питання за такими напрямами: теоретичні та прикладні аспекти систем прийняття рішень, оптимізації та управління системами і процесами; комп'ютерні методи та засоби інформаційно-комунікаційних технологій та управління; безпека функціонування комп'ютерних систем та мереж; інформаційні технології у цивільній безпеці; сучасні інформаційно-вимірювальні системи; інформаційні технології у цивільній безпеці.

## *ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ*

**INSTITUTE OF CONTROL SYSTEMS**
**OF THE MINISTRY OF SCIENCE AND EDUCATION**
**OF THE REPUBLIC OF AZERBAIJAN**

**NATIONAL TECHNICAL UNIVERSITY**
**KHARKIV POLYTECHNIC INSTITUTE**

**KHARKIV NATIONAL UNIVERSITY**
**OF RADIO ELECTRONICS**

**NATIONAL AEROSPACE UNIVERSITY**
**KHARKIV AVIATION INSTITUTE**

**UNIVERSITY OF ŽILINA**

---

# CURRENT DIRECTIONS OF DEVELOPMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES AND CONTROL TOOLS

**Proceedings of 15-th International**

**Scientific and Technical Conference**

**April 24 – 25, 2025**

**Volume 3: sections 3, 4**

**Baku – Kharkiv – Žilina – 2025**

UDC 004/681.3 doi: https://doi.org/10.32620/ICT.25.t3

Abstracts of reports of the 15-th international scientific and technical conference "Current directions of development of information and communication technologies and control tools" are presented in the collection. Considered issues in the following directions: theoretical and applied aspects of decision-making systems, optimization and control of systems and processes; computer methods and means of information and communication technologies and management; security of functioning of computer systems and networks; information technologies in civil security; modern information and measurement systems; information technologies in civil security.

П'ятнадцята міжнародна науково-технічна конференція "Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління" проводиться 24 та 25 квітня 2025 року в режимі ONLINE. Тези доповідей доступні в INTERNET.

**ТОМ 1**

СЕКЦІЯ 1. Теоретичні та прикладні аспекти прийняття рішень, оптимізації та управління системами і процесами

СЕКЦІЯ 5. Сучасні інформаційно-вимірювальні системи

**ТОМ 2**

СЕКЦІЯ 2. Комп'ютерні методи і засоби інформаційно-комунікаційних технологій та управління

**ТОМ 3**

СЕКЦІЯ 3. Методи швидкої та достовірної обробки даних в комп'ютерних системах та мережах

**Керівник секції**: д.т.н., проф. В. В. Косенко, НУ «ПП», Полтава
**Секретарка секції**: к.т.н. О.М. Бельорін-Еррера, НТУ «ХПІ», Харків

СЕКЦІЯ 4. Безпека функціонування комп'ютерних систем та мереж

**Керівник секції**: д.т.н., проф. О. А. Смірнов, ЦНТУ, Кропивницький
**Секретар секції**: к.т.н., доц. О. В. Сєвєрінов, ХНУРЕ, Харків

**ТОМ 4**

СЕКЦІЯ 6. Інформаційні технології у цивільній безпеці

## СЕКЦІЯ 3
# МЕТОДИ ШВИДКОЇ ТА ДОСТОВІРНОЇ ОБРОБКИ ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

**Керівник секції**: д.т.н., проф. В. В. Косенко, НУ «ПП», Полтава
**Секретарка секції**: к.т.н. О.М. Бельорін-Еррера, НТУ «ХПІ», Харків

### ПРАКТИЧНІ РЕКОМЕНДАЦІЇ З НАЛАШТУВАННЯ LORAWAN-МЕРЕЖІ ДЛЯ СТАБІЛЬНОЇ РОБОТИ ТА ЗАХИЩЕНОСТІ ДАНИХ

Янко А.С., Горчаненко С.О.
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна

LoRaWAN, як енергоефективна технологія бездротового зв'язку для IoT-мереж з великою зоною покриття, відкриває широкі можливості для оптимізації бізнес-процесів та покращення якості життя [1]. Її зростаюча популярність в Україні та світі, особливо в умовах цифрової трансформації, зумовлює необхідність глибокого розуміння основних рекомендацій з її налаштування [2].

Актуальність дослідження полягає в тому, що ефективне розгортання LoRaWAN-мереж вимагає не лише технічних знань, але й стратегічного підходу до забезпечення стабільності та захищеності даних.

**Метою доповіді** є комплексний розгляд ключових аспектів конфігурації, управління безпекою та оптимізації продуктивності LoRaWAN-мережі на основі детального аналізу рекомендацій LoRa Alliance [3], зокрема документу TR007, який є одним із ключових в описі стандартів у цій галузі.

Ключові результати дослідження включають розробку практичних рекомендацій з використання OTAA для:

– безпечного з'єднання пристроїв,

– оптимізації частотного плану та каналів для забезпечення швидкого та надійного підключення,

– регулярного оновлення сесійних ключів безпеки для захисту від потенційних загроз [4],

– уникнення синхронної поведінки та накопичення трафіку для запобігання перевантаженням мережі,

– використання ADR для динамічної адаптації параметрів передачі з метою оптимізації енергоспоживання та пропускної здатності,

а також неухильне дотримання регіональних норм щодо потужності передавача та обмежень Duty Cycle для забезпечення відповідності нормативним вимогам.

Впровадження цих рекомендацій на практиці дозволяє не лише підвищити стабільність та захищеність LoRaWAN-мережі, але й забезпечити

її ефективну роботу в різних умовах [5]. LoRaWAN є надзвичайно ефективною технологією для побудови IoT-мереж, але її успішне застосування вимагає ретельного дотримання найкращих практик налаштування та управління. Результати дослідження підкреслюють важливість комплексного підходу до розгортання LoRaWAN-мереж, який враховує як технічні, так і організаційні аспекти.

Подальший розвиток LoRaWAN та її застосування в різних галузях, таких як розумні міста, промислова автоматизація, аграрний сектор та логістика, є перспективним напрямком досліджень, що відкриває нові можливості для інновацій та сталого розвитку.

**Список літератури**

1. Cordova L., & et al. Energy-Efficient LoRaWan Communication: Real-Time Applications in Aquaculture. *2024 IEEE 22nd International Conference on Industrial Informatics (INDIN)*, Beijing, China, 2024, pp. 1–6. https://doi.org/10.1109/INDIN58382.2024.10774297

2. Янко А. С., Шахно В. О. Аспект інформаційної безпеки в сучасних CRM-системах в епоху діджиталізації економіки та бізнесу. *Таврійський науковий вісник. Серія: Технічні науки*, (4), 2022. 28–33. https://doi.org/10.32851/tnv-tech.2022.4.4

3. Kjendal D. LoRa-Alliance Regional Parameters Overview. *Journal of ICT Standardization*, 9(1), 2021, pp. 35–46. https://doi.org/10.13052/jicts2245-800X.914

4. Янко, А., Прокудін, А., Філь, І., Крук, О. Виявлення атак типу LDDoS за допомогою SDN мереж з елементами машинного навчання. *Measuring and computing devices in technological processes*, (4), 2024, 287–296. https://doi.org/10.31891/2219-9365-2024-80-36

5. Katsoulis S., Koulouras G., & Christakis I. Energy-Efficient Data Acquisition and Control System using both LoRaWAN and Wi-Fi Communication for Smart Classrooms. *2024 13th International Conference on Modern Circuits and Systems Technologies (MOCAST)*, Sofia, Bulgaria, 2024, pp. 1–4. https://doi.org/10.1109/MOCAST61810.2024.10615862

## СУЧАСНІ ПІДХОДИ ДО КОРЕКЦІЇ ГРАМАТИЧНИХ ПОМИЛОК З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

Янко А.С., Мизюра М.С.
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна

Сучасні технології штучного інтелекту, зокрема методи обробки природної мови, активно впроваджуються в різні сфери життя, включаючи автоматичну корекцію граматичних помилок [1]. Ця проблема стає особливо актуальною з розвитком цифрової комунікації та зростанням обсягів багатомовного контенту.

У доповіді розглядаються ключові аспекти сучасних підходів до вирішення задач граматичної корекції [2], зокрема розглядаються методи

статистичного перекладу, моделі на основі правил, гібридні підходи та нейронні мережі.

Особлива увага приділяється моделям машинного навчання, які завдяки своїм механізмам забезпечують високу точність корекції тексту. Нейронні мережі, зокрема трансформери, демонструють значні переваги у вирішенні складних завдань, особливо для мов з багатою морфологією, таких як українська, де морфологічне різноманіття ускладнює процес корекції.

**Метою доповіді** є аналіз та оцінка сучасних підходів до корекції граматичних помилок з використанням машинного навчання, а також визначення перспектив їх розвитку та застосування для мов з обмеженими ресурсами.

Важливим аспектом є розробка метрик для оцінки якості моделей [3]. Метрики, такі як BLEU та METEOR, доповнені специфічними підходами до роботи з мовами зі складною морфологією, забезпечують об'єктивну оцінку та дозволяють порівнювати різні підходи. Проте, якість систем корекції граматичних помилок значною мірою залежить від наявності великих корпусів даних [4].

Доповідь окреслює перспективи покращення існуючих підходів, включаючи розробку багатомовних систем, які можуть використовувати знання з інших мов для покращення результатів, а також оптимізацію продуктивності моделей для реальних застосувань.

Подальші дослідження можуть зосередитися на використанні новітніх моделей трансформерів, а також на створенні багатофункціональних інструментів для підтримки мов з обмеженими ресурсами.

Дослідження також аналізує швидкість обробки даних різними сервісами машинного перекладу та робить висновок про відсутність прямого зв'язку між швидкістю та якістю перекладу.

**Список літератури**

1. Лактіонов, О. І., Педченко, Н. М., & Янко, А. С. (2024). Практичні кейси створення згорткових моделей штучного інтелекту для задач розпізнавання образів. *Системи управління, навігації та зв'язку. Збірник наукових праць*, 3(77), 136-140. https://doi.org/10.26906/SUNZ.2024.3.136

2. Лактіонов, І., Мовін, М., & Михайліченко, О. (2024). Розробка класифікатора граматичних помилок іноземної мови. *Актуальні питання гуманітарних наук*, 76(3), 87–92. https://doi.org/10.24919/2308-4863/76-3-15

3. Яковина, В., & Масюкевич, В. (2013). Огляд та аналіз метрик оцінювання якості машинного перекладу. *Вісник Національного університету "Львівська політехніка". Комп'ютерні науки та інформаційні технології*, 771, 101–107. http://nbuv.gov.ua/UJRN/VNULPKNIT_2013_771_17

4. Chen, Yu. (2024). The metamorphosis of machine translation: The rise of neural machine translation and its challenges. *Applied and Computational Engineering*, 43(1), 99–106. https://doi.org/10.54254/2755-2721/43/20230815

# ДИНАМІЧНЕ МОДЕЛЮВАННЯ ГЕТЕРОГЕННОГО КЛАСТЕРА ЗА УМОВИ НЕГАРАНТОВАНОЇ ЯКОСТІ

Рева О.А., Калмикова К.А.
Національний аерокосмічний університет
«Харківський авіаційний інститут», Харків, Україна
Калмиков А.В.
Представництво «Оракл Іст Сентрал Юроп Сервісис Б.В.», Київ, Україна

Розміщення додатків у хмарній інфраструктурі з використанням технологій K8s дозволяє значно поліпшити доступність, масштабування сервісу, ефективність використання ресурсів. При цьому привабливим є спільне розташування різнорідних контейнерізованих додатків, що спрощує управління, але робить кластер гетерогенним, у якому контейнери сильно відрізняються за вимогами та мають негарантовану якість обслуговування, де забезпечений ресурс (request) не дорівнює дозволеному (limit). Стандартні механізми планування кластера враховують лише гарантовані ресурси, а запровадження спеціалізованих алгоритмів має певні обмеження з огляду на велику ціну помилки. З урахуванням цього прагматичним виглядає застосування стандартних засобів за умови оптимальної конфігурації. Так як взаємодію множини процесів та загальне споживання ресурсів у часі фактично неможливо визначити аналітичними моделями то доцільно застосувати моделювання конфігурацій на основі подій з урахуванням історичних або прогнозованих даних. На жаль, доступні та відомі інструменти емуляції процесів планування [1] кластера K8s не дозволяють досліджувати поведінку ресурсів у часі.

**Метою доповіді** є опис технології моделювання поведінки кластера з реальними конфігураціями контейнерізованих додатків та стандартними засобами, що обґрунтовує оптимальні варіанти за критеріями використання ресурсів, доступності, стабільності сервісу. Для дослідження поведінки кластера моделюється множина послідовностей додавання додатків в кластер з плануванням їх розміщення на інфраструктурі з імітацією використання ресурсів за історичними даними у часі. В доповіді показані результати моделювання на основі практичних даних споживання ресурсів додатками, що дозволило дослідити конкуренцію між ними, та довести дієвість запропонованих принципів комплексного урахування вимог додатків у гетерогенному кластері, зокрема для справедливого надання ресурсів на основі нормалізації вимог до ресурсів, яке забезпечує відповідну якість сервісу за умови мінімізації використаної інфраструктури.

**Список літератури**

1. Kubernetes scheduler simulator. [Електронний ресурс]. – Режим доступу: https://github.com/kubernetes-sigs/kube-scheduler-simulator/. –

# IMAGE REPRESENTATION BY ATOMIC WAVELETS: FEATURES FOR IMAGE CLASSIFICATION

Makarichev V.O., Lukin V.V., Brysina I.V.
National Aerospace University
"Kharkiv Aviation Institute", Kharkiv, Ukraine

Digital images are an essential part of big data [1]. They have many applications that produce a high impact on the efficiency and performance of various systems and technological processes. A particular feature of this type of data is its size. This leads to huge expenses required for analyzing, processing, storing, and transferring such data via communicational networks. For this reason, image compression algorithms are used in order to reduce memory, time, and traffic costs [2]. There are two types of image compression techniques: lossless and lossy. In general, lossy algorithms provide a significantly higher compression ratio. Although, they produce distortions that depend on applied method settings. However, often, loss of quality is invisible to the human eye, which makes lossy methods acceptable for compression of some kinds of images, especially digital photos. Image classification is an important task of machine learning (ML) and computer vision (CV) [3]. It has many practical applications, including security systems, healthcare and medicine, autonomous vehicles, precise agriculture, etc. There are many approaches to solving this problem. The use of deep convolutional neural networks (CNN) is among them. A wide range of different architectures has shown their high performance [4]. CNN-based classifiers take an image, extract high-level features, and predict its class. Wherein, an input of such models is a matrix of raw pixel data. Therefore, in order to apply some model to a given image, which is usually stored in compressed format, a decompression procedure is needed that requires additional computational resources. These additional costs might be a blocker for applying models in real time in embedded devices if an input image has a great number of pixels. For this reason, the problem of reduction of decompression expenses is relevant.

**In this talk,** we consider digital image representation by atomic wavelets proposed in [5]. It is based on discrete atomic transform (DAT) that provides a combination of compression and encryption features. Due to the functional properties of atomic wavelets, this transform provides decomposition into DAT components, which might be useful for further classification by CNN-based models. **The aim of the current research** is to prove this hypothesis. We consider a set of state-of-the-art architectures, including MobileNetV2, VGG16, VGG19, ResNet50, NASNetMobile, and NASNetLarge. We apply models with weights trained on the ImageNet dataset. **It is shown that** the use of DAT-features of an image instead of its raw pixel matrix preserves a high percentage of the best predicted class, as well as the top 5 best predicted classes. This means that the complete reconstruction of an image compressed by DAT is not required. So, a huge computational resource can be reduced, when analyzing images with a great

number of pixels, especially digital photos produced by current cameras and mobile devices. For the illustration of the suggested approach, a dataset of 130 digital photos has been collected. The total size is 18.96 GB (raw data) and 1.35 GB in JPEG format. Each image has been processed by DAT with such quality loss settings that provide the absence of visual distortions (PSNR > 35 dB). The total size of compressed and encrypted data is 1.1 GB. After that, we have applied pretrained MobileNetV2, VGG16, VGG19, ResNet50, NASNetMobile, and NASNetLarge models to both source images and their representations by DAT-components. The aggregated results are shown in Fig. 1.

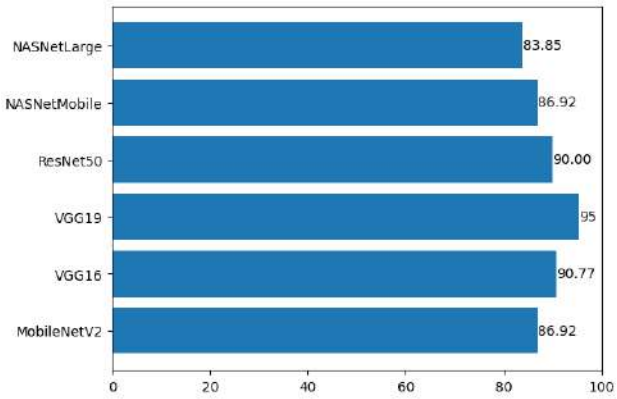


Fig. 1. Mean percentage of the best class similarity ensured by DAT-representation

The obtained results presented as the mean percentage of the best class similarity show that DAT-representation of a digital image is ML/CV-oriented. It is also possible to state that the CNN VGG19 produces the best results, where the mean percentage for it is about 95.

**References**

1. Gonzalez R. C., Woods R. E. Digital image processing, 4th ed. Pearson: New York, NY, USA, 2018.

2. Sayood K. Introduction to Data Compression, 5th ed. Morgan Kaufman: Cambridge, MA, USA, 2017.

3. Szelinski R. Computer Vision: Algorithms and Applications, 2nd ed. Springer Cham, 2022. DOI: https://doi.org/10.1007/978-3-030-34372-9.

4. Parka J., Jung Y. A review and comparison of convolution neural network models under a unified framework. *Communications for Statistical Applications and Methods*. 2022, No. 29. P. 161-176. DOI: https://doi.org/10.29220/CSAM.2022.29.2.161.

5. Makarichev V., Lukin V., Illiashenko O., Kharchenko V. Digital Image Representation by Atomic Functions: The Compression and Protection of Data for Edge Computing in IoT Systems. *Sensors*. 2022. Vol. 22, Art. no. 3751. P. 1-24.

# HYBRID NAVIGATION METHOD FOR AUTONOMOUS UAV FLIGHT UNDER RADIO SUPPRESSION CONDITIONS

Ovdiyuk E.
National Aerospace University
“Kharkiv Aviation Institute”, Kharkiv, Ukraine

In the current conditions of protecting infrastructure from aggressor attacks, a key role is assigned to the **detection and destruction of enemy UAVs**, including both reconnaissance and strike drones. These aerial threats can cause significant damage and disrupt critical operations, making their neutralization a high priority. One of the potentially effective means of achieving this objective is the **deployment of strike UAVs equipped with modern, intelligent control systems**.

The development of such control systems includes not only hardware integration but also advanced software capable of autonomous operation. This includes analysis of enemy UAV behavior, flight characteristics, and development of algorithms for **detection, tracking, and targeting**, as discussed in the works *"Simulation System for Modelling UAV Visual Guidance"* [1] and *"Comparative Analysis Region of Interest (ROI) Tracking Methods"* [2].

Recent advancements in deep learning-based object detection—such as the **Faster R-CNN** architecture combined with lightweight networks like **ShuffleNet** for efficient prefiltering—have shown great potential for integration into UAV platforms. These technologies enable precise identification of key targets during **autonomous missions**, supporting rapid, reliable decision-making processes [5].

However, a major challenge during UAV operation and testing in realistic environments is **terrain navigation**, especially using **GNSS systems** that are highly susceptible to signal jamming in active combat zones. In such conditions, **CRPA antennas** are often employed to maintain satellite connectivity, even under intentional radio interference. Yet, these solutions show diminishing effectiveness over time as **jamming systems continue to evolve**, while CRPA technology demands costly and time-consuming modernization, making them a less sustainable long-term option.

The primary purpose of this paper is to propose a **new hybrid UAV navigation approach** that allows for reliable autonomous flight even in **radio-suppressed environments**. While these methods cannot fully replace traditional GNSS-based systems, they serve as crucial **supplementary technologies** to maintain continuous UAV positioning when satellite signals are degraded or unavailable. This ensures uninterrupted mission execution, especially during critical phases close to or within the battlefield, and facilitates improved targeting operations.

The study *"Autonomous UAV flight using the Total Station Navigation System in Non-GNSS Environments"* [3] offers a viable solution for navigation under such constraints. Among the **key methods** considered for integration into hybrid systems are:

1. **SLAM (Simultaneous Localization and Mapping)** — enabling UAVs to build maps and localize themselves in unfamiliar environments in real time [3].

2. **Cooperative Navigation** — where UAVs with GNSS access can transmit positioning data to those operating in denied environments, thus extending mission capability and maintaining formation coherence [3].

3. **Marker Recognition Navigation** — involves the use of visual markers to correct or confirm UAV positioning. Though limited in some combat scenarios, this method can be particularly effective in controlled or semi-structured environments [3]. For example, it can enhance **automatic landing systems**, improving overall **trajectory accuracy** and reliability during descent and touchdown [4].

Furthermore, the integration of **deep learning for object recognition**, advanced **data augmentation**, and robust **feature selection** methods greatly enhances the **autonomy and resilience** of UAV systems. Lightweight neural networks offer distinct advantages for real-time processing onboard UAVs, especially in **resource-limited conditions**.

When these techniques are integrated with GNSS or used as fallback systems, they form the backbone of a **robust hybrid navigation system** for modern combat UAVs—capable of operating effectively even under full GNSS denial.

Future work should explore **advanced data fusion methods**, improve real-time performance, and conduct **field testing across diverse scenarios** to validate system robustness and operational efficiency.

**References**

1. Dergachov K., Ovdiyuk E., Dubinin V., Hurtovyi O., Bilozerskyi V. Simulation system for modeling UAV visual guidance // Proceedings of the 14th International Conference on Dependable Systems, Services and Technologies (DESSERT'2024).

2. Dergachov K., Ovdiyuk E., Dubinin V. Comparative analysis of region of interest (ROI) tracking methods // Proceedings of the International Scientific and Technical Conference "Integrated Computer Technologies in Mechanical Engineering: Synergetic Engineering" (ICTM-2024), December 23, 2024.

3. Ishii A., Yasuno T., Amakata M., Sugawara H., Fujii J., Ozasa K. Autonomous UAV flight using the Total Station Navigation System in non-GNSS environments // ISARC. Proceedings of the International Symposium on Automation and Robotics in Construction. 2020. Vol. 37. P. 685–692. IAARC Publications.

4. Dergachov K., Bahinskii S., Piavka I. The algorithm of UAV automatic landing system using computer vision // 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT). 2020, May. P. 247–252. IEEE.

5. Takahashi Y., Fujii J., Amakata M., Yamashita T. An application of AI technology to UAV's river patrol and the features value of datasets // Proceedings of the 10th International Conference on Structural Health Monitoring of Intelligent Infrastructure (SHMII-10). 2021.

# ATOMIC WAVELET REPRESENTATION FOR COLOR IMAGE CLUSTERING

Makarichev V.O., Lukin V.V., Brysina I.V.
National Aerospace University
"Kharkiv Aviation Institute", Kharkiv, Ukraine

Data is a crucial part of the majority of human activity. It is widely utilized in different systems and processes, including industrial manufacturing, healthcare and social communication, economics, education, etc. In a sense, data is the lifeblood of social interaction and technology development. There are many types of data, and digital images constitute a particular one of them. They are widely used in security systems and robotics, unmanned aerial vehicles and autonomous car driving, remote sensing, environmental monitoring, medicine, etc. A lot of methods for solving image processing [1] and computer vision [2] problems have been recently developed. Their principal feature is the need to process large volumes of numerical data, since modern sensors produce images of a very high resolution with a huge number of pixels. For this reason, time and spatial complexity reduction for both existing and new algorithms is an important task. In addition, the necessity to perform computations at the edge devices in real time makes it of great relevance. **In the current research,** we consider the problem of accelerating machine learning (ML) and computer vision (CV) algorithms by applying image representation given by atomic wavelets [3].

Image clustering splits pixels into groups of similar samples named clusters. It belongs to unsupervised ML and does not require labeled data [4]. There are many methods for clustering data, in particular remote sensing images [5]. Here, we consider the K-means algorithm, which is often used as a preprocessing stage for other techniques. **Our aim is** to show that it can be accelerated using an atomic wavelet representation of an image, namely DAT-representation [3].

**In this talk,** we present an investigation on the efficiency of applying K-means to DAT-representation of images and compare results to the use of the Haar wavelet, which is considered a baseline. We use a set of classic aerial images available at the following USC-SIPI resource: https://sipi.usc.edu/database/database.php?volume=aerials. We have performed K-means clustering of each image sample and its representations by Haar wavelet and DAT for k = 2, 3, …, 20. After that, we've compared results using the cluster similarity metric, which is the percentage of pixels that preserve their cluster. Fig. 1 shows the aggregated results.

It follows that DAT-representation of an image, i.e. its decomposition into atomic wavelet components, on average, provides higher cluster similarity, than the Haar wavelet representation. This is mainly due to better approximation properties of atomic functions that constitute the core of the transform DAT [3].

Next, this implies that the cluster similarity provided by DAT-components remains high even for a large number of clusters. This means that the use of an

image features, stored in a DAT file, provide nearly the same results, when applying the K-means algorithm. Hence, a complete image decompression is not needed.

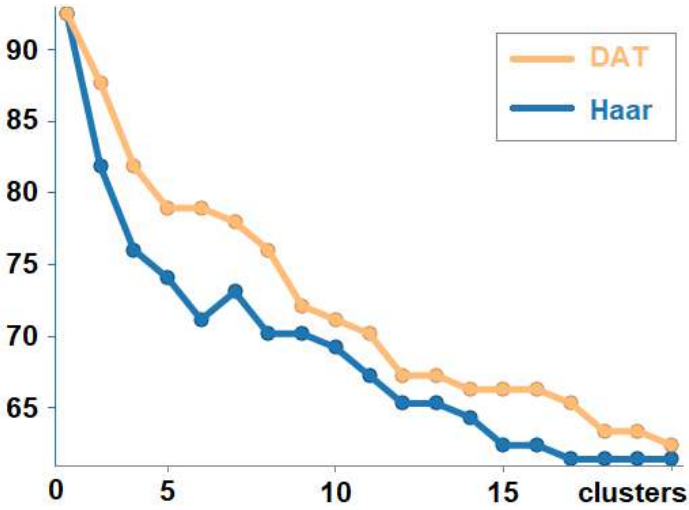


Fig. 1. Mean similarity (%) of clusters produced by Haar and DAT representations compared to the source image clusters

Thus, the DAT-representation of a digital image is ML/CV-oriented. In combination with compression and encryption features [3], this makes DAT a promising image processing method.

**References**

1. Gonzalez R. C., Woods R. E. Digital image processing, 4th ed. Pearson: New York, NY, USA, 2018.

2. Szelinski R. Computer Vision: Algorithms and Applications, 2nd ed. Springer Cham, 2022. DOI: https://doi.org/10.1007/978-3-030-34372-9.

3. Makarichev V., Lukin V., Illiashenko O., Kharchenko V. Digital Image Representation by Atomic Functions: The Compression and Protection of Data for Edge Computing in IoT Systems. *Sensors*. 2022. Vol. 22, Art. no. 3751. P. 1-24. DOI: https://doi.org/10.3390/s22103751.

4. Oyewole G. J., Thopil G. A. Data clustering: application and trends. *Artif. Intell. Rev*. 2023. Vol. 56. P. 6439-6475. DOI: https://doi.org/10.1007/s10462-022-10325-y.

5. Maryam M., Ahsan S., Bushra Z., Amsa S., Nouman A. Remote Sensing Image Classification: A Comprehensive Review and Applications. Mathematical Problems in Engineering. 2022. Art. ID 5880959. P. 1-24. DOI: https://doi.org/10.1155/2022/5880959.

# LOSSY COMPRESSION AND POST-FILTERING OF IMAGES CONTAMINATED BY POISSON NOISE

Rebrov V.S., Lukin V.V.
National Aerospace University
"Kharkiv Aviation Institute", Kharkiv, Ukraine

Images serve nowadays as one of the most widespread sources of information.

Their quality can be degraded by the noise and the image size and/or their number can be too large [1]. Then, such image data have to be compressed in a lossy manner taking into account the noise presence [2]. HEIF coder [3] is a good candidate for this purpose.

However, a possibility and peculiarities of its application to single component noisy images have been studied in [2] under assumption that that noise is additive, white, and Gaussian. Meanwhile, noise can be signal-dependent. Then, a question is how to perform lossy compression in this case.

There are two ways described in [4] for better portable graphics (BPG) coder. One way consists in direct application of a coder to a noisy image. However, for signal-dependent noise, this leads to different degree of noise suppression and loss of fine details in dark regions. Another way is to apply a proper variance stabilizing transform (VST) with providing additive nature of the noise with known variance and convenient range of image representation (e.g., 8-bit). In our work, we consider just this approach.

Then, it is possible to carry out compression of converted image in optimal operation point (OOP) if it exists or with a smaller compression ratio (CR) with post-filtering using, e.g., a block matching 3-dimensional (BM3D) filter [5]. The noise filtering effect of lossy compression and post-filtering are specific. Because of this, we present below data (output values of peak signal-to-noise values) for the following approaches:

1) Filtering of original image by BM3D (to understand what is the potential of image denoising);

2) Lossy compression in OOP with parameters recommended in [2], this approach provides a rather large CR;

3) Post-filtering of images compressed in OOP with optimal BM3D parameter after decompression;

4) A more "careful" lossy compression of a noisy image after VST with further post-filtering using BM3D with optimal parameter.

Note that the corresponding inverse VST is carried out after decompression and post-filtering in all considered cases.

The results obtained for the test images Frisco (having relatively simple structure) and Fr03 having a rather complex structure (with many edges, textures and fine details) are presented in Table below. Recall that input PSNR is equal to 27.9 dB for Fr03 and 27.4 dB for Frisco images, respectively.

Table. PSNR (dB) for different image processing approaches

| Test image | PSNR for ideal denoising | PSNR in OOP | PSNR in OOP with post-filtering | "Careful" compression with post-filtering |
|---|---|---|---|---|
| Fr03 | 31.6 | 28.06 | 28.75 | 30.39 |
| Frisco | 37.53 | 34.04 | 34.6 | 36.68 |

As seen, ideal denoising (approach 1) produces PSNR improvement but this improvement considerably depends on image complexity (it is significantly larger for the simple structure image Frisco). OOPs exist for both test images (PSNR in OOP is larger than input PSNR. Meanwhile, PSNR in OOP is about 3 dB smaller than for ideal denoising, i.e. denoising due to lossy compression is essentially less efficient compared with ideal denoising.

About 0.6 dB improvement of the output PSNR can be provided by post-filtering of images compressed in OOP. However, such an improvement practically cannot be noticed by visual inspection.

Finally, "careful" lossy compression with further post-filtering is less efficient than ideal denoising but it produces about 2 dB better output PSNR than for compression in OOP.

The CR provided for compression in OOP is usually between 10 and 20 whilst for the last approach ("careful" compression with post-filtering) the attained CR is about two times smaller. This is the payment for better quality. The optimal β for the BM3D filter for the approach 2 is slightly less than 2 an it is slightly larger than 2 for the last approach. The proposed approach tested for Poisson noise can be adapted to other types of signal-dependent noise.

**References**

1. Gonzalez, R. C., & Woods, R. E. *Digital image processing*, 4th ed. Pearson: New York, NY, USA, 2018.

2. Kryvenko, S., Rebrov, V., Lukin, V., Golovko, V., Sachenko, A., Shelestov, A., & Vozel, B. Post-Filtering of Noisy Images Compressed by HEIF. *Applied Sciences*, 2025, vol. 15, iss. 6. DOI: https://doi.org/10.3390/app15062939.

3. Lainema, J., Hannuksela, M. M., Vadakital, V. K. M., & Aksu, E. B. HEVC Still Image Coding and High Efficiency Image File Format. *In Proceedings of the 2016 IEEE International Conference on Image Processing (ICIP)*, Phoenix, AZ, USA, 2016, pp. 71–75. DOI: 10.1109/ICIP.2016.7532321.

4. Kovalenko, B., & Lukin, V. BPG-based compression of Poisson noisy images, *Proceedings of DESSERT'2023*, Athens, Greece, 2023. 7 p. DOI: 10.1109/DESSERT61349.2023.10416544.

5. Dabov, K., Foi, A., Katkovnik, V., & Egiazarian, K. Image Denoising by Sparse 3-D Transform-Domain Collaborative Filtering. *IEEE Trans. on Image Process*, 2007, vol. 16, pp. 2080–2095. DOI: 10.1109/TIP.2007.901238.

# OBJECT LOCALIZATION AND RECOGNITION IN UAV-BASED NOISY IMAGES

Tsekhmystro R.V., Lukin V.V.
National Aerospace University
"Kharkiv Aviation Institute", Kharkiv, Ukraine

Images are known to be a source of useful information in many application areas [1]. A lot of images are nowadays acquired by sensors installed on-board of unmanned aerial vehicles (UAV) and drones [2, 3]. However, not all acquired images are of excellent quality since low quality of used sensors and bad weather conditions can lead to quite intensive noise and other degradations. In turn, they might lead to performance reduction of algorithms and tools applied for object localization and recognition in obtained images [1]. Recall that these tasks are nowadays usually carried out by trained convolutional neural networks (CNNs) [2]. Then, questions that arise are the following:

1) What are CNNs more robust to noise than others?

2) What is noise intensity leading to radical reduction of CNN performance?

3) Is it possible to improve the performance by image pre-processing, i.e. image denoising?

A part of these questions have been already answered in our paper [2]. In particular, it has been shown that, according to such metrics as Intersection over Union (IoU) and F1 score, most CNNs perform in a quite stable way until standard deviation (STD) of additive white Gaussian noise is smaller than 20 (for 8-bit data in each image component), i.e. if input peak signal-to-noise ratio exceeds 23 dB. Different CNNs have different insensitivity to the noise (see data in Fig.1). In particular, YOLO family CNNs are quite sensitive to the noise.

The **goal** of our study was to check whether or not the image pre-filtering is able to improve the performance.

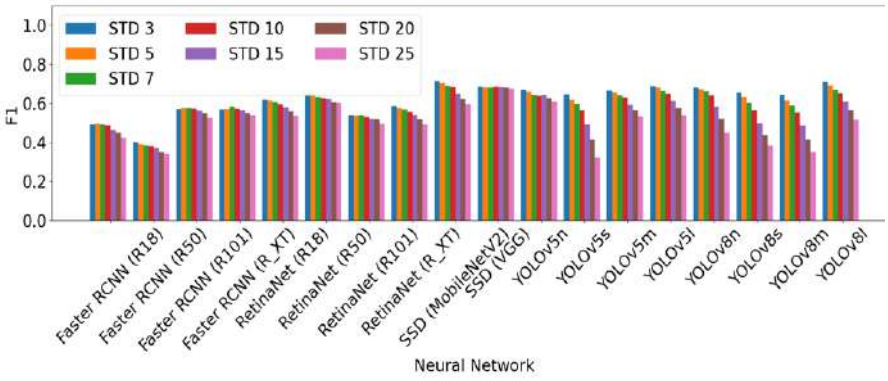


Fig. 1. F1 score for different CNNs depending on noise STD

A BM3D filter [4] has been applied for this purpose where we have supposed the noise characteristics known in advance or pre-estimated accurately enough [5]. Analysis of F1 score data presented in Fig. 2 show that the results for large STD values have improved for all considered CNNs and become stable (almost independent on the noise STD). The best results have been provided by the RetinaNet and YOLOv8 CNNs.

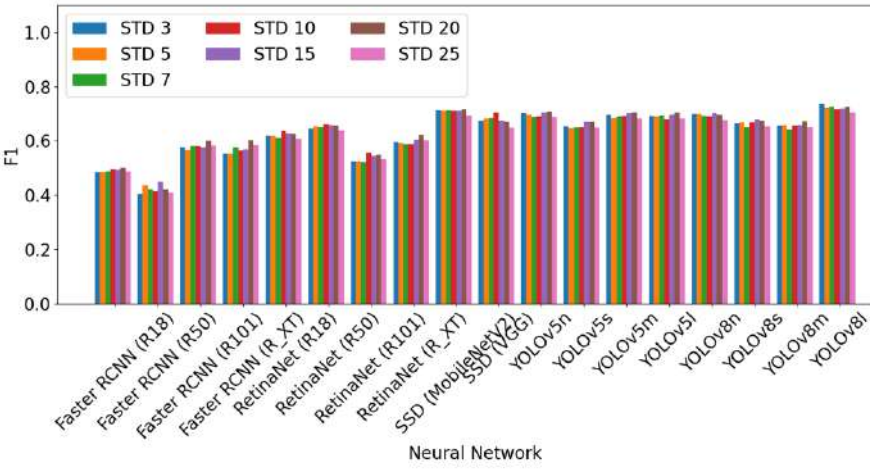


Fig. 2. F1 score for different CNNs depending on noise STD
for pre-filtered color images

**References**

1. Gonzalez R. C., Woods R. E. Digital image processing, 4th ed. Pearson: New York, NY, USA, 2018.

2. Tsekhmystro R., Rubel O., Prysiazhniuk O., Lukin V. Impact of distortions in UAV images on quality and accuracy of object localization. *Radioelectronic and computer systems*, no. 4, pp. 59-67, 2024. DOI: 10.32620/reks.2024.4.05.

3. Mishchuk V., Fesenko H., Kharchenko V. Deep learning models for detection of explosive ordnance using autonomous robotic systems: trade-off between accuracy and real-time processing speed. *Radioelectronic and computer systems*, no. 4, pp. 99-111, 2024. DOI: 10.32620/reks.2024.4.09.

4. Katkovnik V., Foi A., Egiazarian K. From Local Kernel to Nonlocal Multiple-Model Image Denoising. *International Journal of Computer Vision*, vol. 86, pp. 1-32, 2010. DOI: 10.1007/s11263-009-0272-7.

5. Vozel B., Chehdi K., Klaine L., Lukin V. V., Abramov S. K. Noise Identification and Estimation of its Statistical Parameters by Using Unsupervised Variational Classification. *2006 IEEE International Conference on Acoustics Speech and Signal Processing Proceedings*, Toulouse, France, 2006. DOI: 10.1109/ICASSP.2006.1660474.

# РОЗРОБКА ВЕБЗАСТОСУНКУ ДЛЯ ОНЛАЙН-ЗАПИСУ ТА УПРАВЛІННЯ БІЗНЕС- ПОСЛУГАМИ

Тимошенко Д.О., Канцір Р.Б.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному світі цифрових технологій автоматизація бізнес-процесів має особливий пріоритет. Розробка ефективного вебзастосунку для автоматизації процесу запису клієнтів є надзвичайно актуальним завданням, оскільки це сприяє покращенню комунікації з клієнтами та підвищенню рівня їхньої задоволеності [1].

Багато малих підприємств та ФОП досі не мають сучасних систем управління записом клієнтів, продовжуючи використовувати застарілі методи, такі як паперові журнали або телефонні дзвінки. Це спричиняє неефективність та підвищує ризик помилок, що може негативно вплинути на репутацію бізнесу [2].

Розробка системи запису клієнтів забезпечує швидкий доступ до послуг, знижує навантаження на робітників і дозволяє бізнесу зосередитися на підвищенні якості обслуговування, що є ключовим фактором успіху в умовах жорсткої конкуренції.

**Метою доповіді** є розробка вебзастосунку для автоматизації процесу запису клієнтів.

Система передбачає три ролі користувачів. Неавторизований користувач зможе обирати необхідні послуги, переглядати список доступних майстрів і записуватися в зручний для нього день та час. Адміністратор матиме змогу керувати записами, налаштовувати графік роботи майстрів та перелік послуг, додавати, видаляти чи приховувати майстрів, а також бачити усі записи стосовно своєї компанії. Майстер зможе редагувати час роботи та інформацію про себе, також матиме можливість переглядати записи та керувати ними.

**В доповіді** розглянуто технічні рішення, що забезпечують реалізацію вебзастосунку. Зокрема, використано фреймворк Next.js, що забезпечує гібридні методи рендерингу та ефективну роботу з даними. В якості системи управління базами даних використовується Pocketbase. Стилізація інтерфейсу користувача реалізована за допомогою Tailwind CSS. Адміністративна частина веб-застосунку реалізована за допомогою вбудованих можливостей Pocketbase та кастомних компонентів у Next.js.

**Список літератури**

1. Wamba, S. F., & Akter, S. (2019). The Role of Information and Communication Technology in Business Process Automation: A Review of Literature. Journal of Enterprise Information Management, 32(1), 107-129. DOI: https://doi.org/10.1007/978-3-642-45100-3_18

2. Lacity, M. C., & Willcocks, L. P. (2017). Robotic Process Automation: The Next Transformation Lever for Business. Journal of Information Technology Teaching, 18(2), 110-128. DOI: https://doi.org/10.1057/s41266-016-0016-9

# МЕТОДИ ОПТИМІЗАЦІЇ ІГРОВИХ ЗАСТОСУНКІВ

Холєв В.О., Медвєдєв М.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Індустрія відеоігор перетворилася із невеликого ринку для ентузіастів у найбільш зростаючу сферу розваг у XXI столітті. Пандемія COVID-19 руйнівно вплинула на усі галузі відпочинку, в той час як ігрова лише збільшувала обсяги доходів. У 2020 році вона навіть обійшла за прибутком кіноіндустрію [1], що стало безпрецедентною подією та спричинило серію великих інвестицій у ігрові студії.

Попри зростання фінансових потоків у цій сфері, комерційні аспекти поступово витісняють творчий потенціал. Сучасні ігрові релізи сповнені багів та умовностей і в той же час насичені мікротрансакціями та рекламою. Для розробників питання оптимізації стало другорядним, хоча для гравців це є визначаючим фактором при виборі продукту.

**Метою доповіді** є дослідження методів оптимізації ігрових застосунків задля покращення загальної продуктивності та, як результат, збільшення кількості потенційних гравців.

У рамках дослідження розглянуто методи зниження навантаження на графічний процесор шляхом використання моделей меншої деталізації при віддаленні від гравця [2]. Також проведено аналіз сучасних відеокарт для виявлення факторів, що обмежують їх продуктивність. Одним з таких визначено обсяг відеопам'яті. Варіантом вирішення проблеми було запропоновано використання текстурних атласів [3] та потокового завантаження рівня [4].

За результатами дослідження наводиться оцінка ефективності методів оптимізації на прикладі тестового ігрового застосунку. Кількість кадрів за секунду збільшилася на 30-40%, в той час як використання відеопам'яті зменшилося в середньому на 10-20%.

**Список літератури**

1. Gilbert B. Video-game industry revenues grew so much during the pandemic that they reportedly exceeded sports and film combined. *Business Insider*. URL: https://www.businessinsider.com/video-game-industry-revenues-exceed-sports-and-film-combined-idc-2020-12 (date of access: 24.03.2025).
2. GPU based dynamic geometry LOD – RasterGrid. *RasterGrid*. URL: https://www.rastergrid.com/blog/2010/10/gpu-based-dynamic-geometry-lod/ (date of access: 24.03.2025).
3. Ivanov I.-A. Practical texture atlases. *Game Developer | Game Industry News, Deep Dives, and Developer Blogs*. URL: https://www.gamedeveloper.com/programming/practical-texture-atlases (date of access: 24.03.2025).
4. Level streaming overview. *dev.epicgames.com*. URL: https://dev.epicgames.com/documentation/en-us/unreal-engine/level-streaming-overview-in-unreal-engine (date of access: 24.03.2025).

# ТЕЛЕГРАМ-БОТ ДЛЯ АВТОМАТИЗАЦІЇ ІНФОРМАЦІЙНОГО ОБСЛУГОВУВАННЯ СТУДЕНТІВ

Шевелєв В.Р., Гаврашенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У рамках даної доповіді буде виконано дослідження з розробки та впровадження телеграм-бота, покликаного автоматизувати процеси інформаційного обслуговування студентів університету. Проект спрямований на розв'язання проблем, пов’язаних із підвищенням ефективності комунікацій та студентами, зменшенням рутинного навантаження на працівників університету та оптимізацією доступу до інформації (розклад занять, часті запитання тощо). У сучасних умовах цифрової трансформації використання таких технологічних рішень є не лише актуальним, а й необхідним для створення гнучкої та інтерактивної освітньої екосистеми.

Дослідження охопить аналіз вимог студентів до отримання інформації, такої як розклад занять, організаційну інформацію тощо. Очікується, що телеграм-бот дозволить оперативно задовольняти інформаційні потреби.

Метою доповіді є створення рішення, яке буде здатне ефективно надавати інформацію студентам зменшуючи навантаження завдяки зменшенню рутинних задач для старост, кураторів тощо. Для досягнення поставленої мети буде виконано низку завдань, зокрема проаналізовано сучасні бібліотеки та технології для створення телеграм-ботів, розроблено модель взаємодії бота з базами даних та проведено тестування створеної системи.

За результатами роботи планується створення телеграм-бота, який стане інструментом для швидкої і автоматизованої взаємодії між студентами та університетом.

У реальних умовах використання бота передбачається значне зменшення часу обробки запитів на отримання повсякденної та потрібної інформації, підвищення загального рівня організації процесів в університеті.

У перспективі можливий розвиток функціоналу бота, зокрема його розширення для підтримки додаткових сервісів та створення різних нових функцій на основі попиту серед студентів.

**Список літератури**

1. Ruben Bermudez “Java library to create bots using Telegram Bots API” https://github.com/rubenlagus/TelegramBots

2. Prasol I., Dovnar O., Yeroshenko O. Method of Diagnostic Parameters Analysis and Software Features. 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek). 2022. Pp. 716–719.

3. Spring і Spring Boot: основні відмінності та особливості використання // https://foxminded.ua/ru/razlichiya-mezhdu-spring-i-spring-boot/ Режим доступу 30.10.24

# ОЦІНКА ВПЛИВУ МЕТОДІВ ПРЕПРОЦЕСІНГУ НА ТОЧНІСТЬ ПОШУКУ ОБЄКТІВ НА ЗОБРАЖЕННЯХ МІСЬКОГО СЕРЕДОВИЩА

Аврунін О.О., Барковська О.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

Актуальність дослідження зумовлена широким застосуванням технологій комп'ютерного зору в таких галузях, як безпека, міська інфраструктура, транспорт, медицина [1] та військова справа. Зростаючі обсяги візуальної інформації та необхідність точного автоматизованого виявлення об'єктів на зображеннях міського середовища зумовлюють потребу в підвищенні достовірності і надійності методів комп'ютерного зору за рахунок удосконалення методів попередньої обробки зображень [2].

**Метою роботи** є оцінка впливу методів препроцесінгу на точність пошуку об'єктів на зображеннях міського середовища на основі нейронних мереж.

У роботі розглядаються особливості застосування медіанного фільтру, налаштування яскравості та контрастності зображень перед їх подачею до нейромережевих моделей [3]. Дослідження проводилося на основі зображень міського середовища, що були завантажені із відкритої мережі та зроблені у різних погодних умовах, що дозволяє зробити оцінку максимально наближеною до практичного використання.

Результати показали, що збільшення кількості успішно виявлених об'єктів після попередньої обробки на основі медіанної фільтрації підтверджує доцільність включення етапу препроцесінгу в загальну конвеєрну обробку зображень.

Проте, навіть при високій точності (96–97%) систем розпізнавання, кількість помилок у реальних масштабах може бути критичною для систем, що працюють в автоматизованому середовищі.

Причиною є складність архітектури сучасних нейронних мереж, яка призводить до ефекту «чорної скриньки», що ускладнює пояснення результатів і внесення цілеспрямованих коректив. Подальші дослідження доцільно орієнтувати на збільшення обсягів тренувальної вибірки та розширення спектра сценаріїв зображень.

**Список літератури**

1. Application of SOFA framework for physics-based simulation of deformable human anatomy of nasal cavity / Maksym Tymkovych et. al// IFMBE Proceedings (2021). DOI: 10.1007/978-3-030-64610-3_14

2. Hoft, N., Schulz, H., Behnke, S.: Fast semantic segmentation of RGB-D scenes with GPU accelerated deep neural networks. In: 2014 37th German Conference Advances Artificial Intelligence, pp. 80–85 (2014)

3. Gupta G. et al. Algorithm for image processing using improved median filter and comparison of mean, median and improved median filter //International Journal of Soft Computing and Engineering (IJSCE). – 2011. – Т. 1. – №. 5. – С. 304-311.

# ІНТЕЛЕКТУАЛЬНА СИСТЕМА ВНУТРІШНЬОЇ НАВІГАЦІЇ ДЛЯ ЛЮДЕЙ ІЗ ВАДАМИ ЗОРУ

Буряк В.А., Головченко О.С., Барковська О.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

У роботі розглядається інтелектуальна система внутрішньої навігації, що орієнтована на підтримку людей із порушеннями зору при переміщенні у складних закритих просторах, зокрема в торгових центрах, медичних установах, складських приміщеннях тощо [1].

**Метою дослідження** є розробка підсистеми локальної навігації в межах технологічного рішення, що забезпечує голосову взаємодію з користувачем, орієнтацію в просторі, виявлення перешкод та побудову безпечного маршруту до заданої точки всередині приміщення.

Завданнями дослідження є розробка функціональних блоків підсистеми для обробки голосових команд, визначення вихідного положення користувача, побудова маршруту з врахуванням зовнішніх перешкод.

У дослідженні використано підхід, що поєднує технології BLE для точного позиціонування, мікрокомп'ютери Raspberry Pi для локальної обробки даних, переднавчені нейромережеві моделі для розпізнавання мови, інтерактивні карти з точками інтересу, а також алгоритми побудови маршрутів (Dijkstra, SLAM).

В результаті роботи розроблено функціональну архітектуру системи, виконано її декомпозицію на підсистеми (голосовий інтерфейс, локалізація, навігація, виявлення перешкод). Створено інтерактивну карту приміщення та протестовано BLE-маячки для покриття зон інтересу [2]. Реалізовано прототип мобільного додатку з голосовими підказками. Отримані результати демонструють високу точність позиціонування в межах тестового середовища.

Таким чином, запропонована система внутрішньої навігації забезпечує інклюзивність та безпеку пересування людей із вадами зору в закритих просторах. Інтеграція BLE, мови, комп'ютерного зору та маршрутизації в єдину платформу демонструє значний потенціал для подальшого впровадження в суспільно значущі інфраструктури.

**Список літератури**

1. Barkovska, Olesia, and Vitalii Serdechnyi. 'Intelligent Assistance System for People with Visual Impairments'. INNOVATIVE TECHNOLOGIES AND SCIENTIFIC SOLUTIONS FOR INDUSTRIES, no. 2(28), June 2024, pp. 6–16, https://doi.org/10.30837/2522-9818.2024.28.006.

2. Miñambres, María D., et al. Distance Estimation to BLE Beacons Using Raspberry Pi 3 Boards for Indoor Positioning and Social Tracking Applications. May 2024, https://doi.org/10.5281/ZENODO.11213335.

# ІНТЕЛЕКТУАЛЬНА СИСТЕМА АДАПТИВНОГО ЗАТЕМНЕННЯ ЛОБОВОГО СКЛА АВТОМОБІЛЯ

Костін А.О., Барковська О.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

У роботі розглядається розробка інтелектуальної програмно-апаратної системи для підвищення безпеки дорожнього руху шляхом автоматичного локального затемнення лобового скла автомобіля. Предметом дослідження є алгоритмічні та апаратні засоби, які дозволяють визначати напрямок погляду водія, проаналізувати інтенсивність зустрічного світла та динамічно відрегулювати прозорість рідкокристалічної плівки на склі. Це рішення орієнтоване на попередження тимчасового осліплення водіїв, спричиненого світлом фар зустрічного транспорту, що є поширеною причиною дорожньо-транспортних пригод, особливо за умов нічного керування [1].

**Метою дослідження** є створення системи, здатної адаптивно локалізувати затемнення на склі саме в тій області, де напрямок погляду водія перетинається з джерелом надлишкового освітлення.

В роботі запропоноване технологічне рішення, яке складається з трьох основних модулів: блоку відстеження погляду, системи фільтрації інтенсивного світлового потоку та контролера, що здійснює керування прозорістю активної LC-плівки [2]. Для аналізу напрямку погляду застосовано інфрачервону камеру з внутрішнього боку салону, яка працює в поєднанні з моделлю розпізнавання ключових точок обличчя (наприклад, MediaPipe FaceMesh або DeepGaze). Обчислення критичної області здійснюється з урахуванням фізіологічних особливостей водіїв та параметрів транспортного засобу. Рішення щодо активації локального затемнення приймається на основі комбінованого аналізу напрямку погляду та показників освітлення з урахуванням порогових значень, заданих адаптивним алгоритмом.

Запропоноване рішення має інноваційний характер та потенційне застосування не лише в автомобільній сфері. Порівняно з традиційними методами затемнення, розробка дозволяє динамічне та зоноване регулювання прозорості в залежності від ситуації на дорозі, що підвищує безпечність і комфорт керування.

**Список літератури**

1. L. Ewecker et al., "Detecting Oncoming Vehicles at Night in Urban Scenarios - An Annotation Proof-Of-Concept," 2024 IEEE Intelligent Vehicles Symposium (IV), Jeju Island, Korea, Republic of, 2024, pp. 2117-2124, doi: 10.1109/IV55156.2024.10588522.

2. Zhou, Le, et al. ‘Advancements and Applications of Liquid Crystal/Polymer Composite Films’. ACS Materials Letters, vol. 5, no. 10, Oct. 2023, pp. 2760–75. DOI.org (Crossref), https://doi.org/10.1021/acsmaterialslett.3c00665.

# 3D-ГЕНЕРАЦІЯ З ВИКОРИСТАННЯМ ОПИСОВИХ І ЧИСЛОВИХ ЗАПИТІВ

Бухарова Л.Д, Барковська О.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

Генеративні моделі глибинного навчання, призначені для синтезу тривимірних об'єктів на основі текстових або візуальних підказок, із подальшим застосуванням у сфері індивідуального протезування.

**Метою дослідження є** розробка підходу до генерації персоналізованої 3D-моделі накладки на протез з урахуванням індивідуальних параметрів користувача на основі сучасних генеративних нейронних мереж.

Завдання роботи полягає у дослідженні сучасних генеративних архітектур, що дозволяють створювати 3D-моделі з заданими характеристиками; а також у проведенні порівняльного аналізу якості, часу генерації та відповідності об'єкта до персональних параметрів [1].

Використаними для проведення дослідження є наступні класи моделей тривимірної генерації: трансформери та дифузійні моделі (TRELLIS, MicroDreamer, SDFusion, Hunyuan3D 2.0), що реалізовані на базі PyTorch із метриками R-presision, CLIP-S, FID та CD для оцінки відповідності згенерованої форми вхідному тексту [2]. Розроблено тестове середовище та виконано експерименти на GPU (Tesla T4). Серед протестованих моделей SDFusion показала найкращий баланс просторової відповідності та швидкості генерації, але точність розмірів та генерація гладкої геометрії обмежені, що обумовлено початковою вибіркою навчання. Модель Hunyuan3D 2.0 синтезує якісні сітки геометрії, але не відстежує всі деталі вхідної текстової умови та потребує більше часу на генерування. MicroDreamer забезпечує високоякісні текстури, але геометрія об'єктів потребує подальшої оптимізації. Було сформовано висновок щодо переваги моделей, які допускають інтеграцію 3D-апріорів різної деталізації, як-от GSGEN та CLAY, для створення заздалегідь відомих форм із варіативними параметрами. Таким чином, аналіз показав, що сучасні генеративні моделі здатні синтезувати 3D-об'єкти високої якості, але точна відповідність параметрам можливе лише при впровадженні додаткових обмежень у процес генерації. Для задачі створення персоналізованих протезних накладок доцільно комбінувати підходи генерації з тексту з переданими параметрами форми. Отримані результати можуть бути основою для розробки адаптивного сервісу генерації функціональних 3D-моделей на замовлення.

**Список літератури**

1. Бухарова Л.Д., Барковська О.Ю. Технологічне рішення для захисту модульних протезів // Проблеми інформатизації : XII міжнародна науково-технічна конференція. - 21-22 листопада 2024. –с.76. doi: https://doi.org/10.32620/PI.24.t2

2. Friedrich P., Frisch Y., Cattin P. C. Deep generative models for 3d medical image synthesis //Generative Machine Learning Models in Medical Image Computing. – Cham : Springer Nature Switzerland, 2024. – С. 255-278. https://doi.org/10.48550/arXiv.2410.17664.

# ГНУЧКА НАУКОВА ПЛАТФОРМА ДЛЯ ПІДТРИМКИ ДОСЛІДЖЕНЬ В ОБЛАСТІ КОМП'ЮТЕРНОГО ЗОРУ

Барковська О.Ю., Сердечний В.С.
Харківський національний університет радіоелектроніки, Харків, Україна

У дослідженні представлено інтелектуальну клієнт-серверну систему, призначену для підтримки науковців, які працюють з задачами комп'ютерного зору в складних умовах зйомки, зокрема для адаптації систем орієнтації слабозорих користувачів [1, 2]. Предметом дослідження є автоматизація побудови якісних тренувальних вибірок та подальшого аналізу якості розпізнавання об'єктів.

Метою розробки стало створення інструменту, що дозволяє швидко здійснювати розмітку відео з реальних умов, автоматично ініційовану моделлю YOLOv11, з подальшим ручним корегуванням і можливістю оцінки якості роботи широкого набору моделей (YOLOv8-11, MaskRCNN, DETR та ін.).

Завдання дослідження охоплювали створення зручного інтерфейсу для перегляду та корекції Bounding Box, підключення моделей розпізнавання, аналізу продуктивності моделей за метриками F1-score, mAP, IoU, Precision, Recall та FPS, а також візуалізацію результатів для порівняння точності.

Використаний технологічний стек включає бібліотеку Flask для побудови веб-інтерфейсу [3],

OpenCV — для попередньої обробки відео, PyTorch та Ulralytics — для запуску моделей. Реалізовано підтримку інтерактивної аналітики результатів.

Результатами роботи розробленого застосунку для підтримки досліджень в області комп'ютерного зору стало проведене тестування понад 15 моделей, результати яких відображаються у графічному вигляді.

Як висновок зазначимо, що запропонована система значно спрощує процес створення адаптивних тренувальних вибірок, дозволяє гнучко адаптувати та перевіряти моделі для умов, не представлених у класичних датасетах.

Це відкриває перспективи як для задач безпеки слабозорих, так і для автономного транспорту.

**Список літератури**

1. Serdechnyi V. et al. Knowledge systematization about the characteristics of existing technological means for assisting people with visual impairments //Advanced Information Systems. – 2025. – Т. 9. – №. 1. – С. 13-23.

2. Барковська О., Сердечний В. Intelligent assistance system for people with visual impairments //СУЧАСНИЙ СТАН НАУКОВИХ ДОСЛІДЖЕНЬ ТА ТЕХНОЛОГІЙ В ПРОМИСЛОВОСТІ. – 2024. – №. 2 (28). – С. 6-16.

3. Grinberg M. Flask web development. – " O'Reilly Media, Inc.", 2018.

# ПІДСИСТЕМА НАВІГАЦІЇ У МАПОВАНОМУ СЕРДОВИЩІ НА ОСНОВІ ТЕХНОЛОГІЙ NLP ТА BLE-МІТОК

Барковська О.Ю., Сторчай Д.Г.
Харківський національний університет радіоелектроніки, Харків, Україна

В умовах активного розвитку інформаційних технологій та медицини, можливості підтримки людей з інвалідністю у повсякденних справах стають все ширшими, а можливості сучасних вбудованих систем дозволяють створювати легкі у використанні та впровадженні пристрої. У той же час, в умовах воєнного та потенційного післявоєнного стану, важливим стає питання підтримки людей з інвалідністю у повсякденному житті [1]. Таким чином, актуальним стає питання дослідження потреб людей із вадами зору, а також проектування методів та систем для задовільнення таких потреб. Прикладом подібної інноваційної розробки є система внутрішньої навігації (indoor navigation system) у громадських місцях або будівлях, запропонована в даній роботі. Реалізація даної задачі вимагає комплексного підходу, що включає розробку механізмів, здатних ефективно працювати у динамічних складних умовах, як то визначення місцезнаходження користувача в певний момент часу та динамічне прокладання маршруту до точки призначення.

**Метою доповіді** є проектування системи навігації у мапованому середовищі на основі технологій NLP та BLE-міток, що могла б бути використана у громадських місцях.

В доповіді наводяться результати експериментальних досліджень працездатності елементів проектованої системи та точності її роботи. Наведені дані показуються вплив на роботу системи таких зовнішніх факторів, як відстань до користувача, рівень фонових шумів, чіткість мовлення, гучність мовлення. Результати виражені у показниках затримки відповіді та відсотку помилки.

У роботі запропонована підсистема, яка складається з апаратної та програмної частин і забезпечує спрямоване сприйняття звукових сигналів, їх обробку, трансформацію в корисну інформацію та реалізацію навігації на основі BLE-міток [2].

Окрему увагу приділено перспективам удосконалення системи шляхом застосування нейронних мереж для інтерпретації акустичних даних.

**Список літератури**

1. Serdechnyi V. et al. Knowledge systematization about the characteristics of existing technological means for assisting people with visual impairments //Advanced Information Systems. – 2025. – Т. 9. – №. 1. – С. 13-23. https://doi.org/10.20998/2522-9052.2025.1.02.

2. Plikynas, D., Žvironas, A., Budrionis, A., & Gudauskis, M. (2020). Indoor Navigation Systems for Visually Impaired Persons: Mapping the Features of Existing Technologies to User Needs. *Sensors, 20*(3), 636. https://doi.org/10.3390/s20030636

# РОЗРАХУНОК ВІДСТАНІ ДО ОБ'ЄКТА З ПОДАЛЬШОЮ НОРМАЛІЗАЦІЄЮ

Шапіро А.С., Сердечний В.С.
Харківський національний університет радіоелектроніки, Харків, Україна

У роботі розглядається задача визначення відстані до об'єкта за допомогою веб-камери на основі монокулярної геометрії та попередньо відомих масштабів об'єкта. Предметом дослідження є методи комп'ютерного зору, які дозволяють проводити оцінку відстані без використання стереозображень або додаткових сенсорів.

**Метою роботи** є аналіз точності методу FaceMesh з OpenCV для оцінки відстані до об'єкта за допомогою однієї камери в умовах змінних зовнішніх факторів.

У межах дослідження було поставлено завдання проаналізувати вплив роздільної здатності камери, освітленості, кута нахилу голови на точність розрахунку відстані. Для цього було створено тестове середовище, у якому фіксувалася реальна відстань, запускалися алгоритми з різними параметрами та фіксувалися похибки. Також було вивчено вплив багатопоточності на швидкодію програми.

Алгоритм ґрунтувався на детекції контрольних точок обличчя з подальшим застосуванням простих геометричних перетворень з урахуванням відомої фізичної відстані між очима.

Методика дозволяє ефективно працювати на слабкому апаратному забезпеченні без залучення глибоких нейромереж. Отримані результати показали, що точність оцінки значною мірою залежить від роздільної здатності камери: найкращі показники досягаються при Full HD, особливо для малих відстаней.

Зниження освітленості суттєво погіршує якість детекції ключових точок. Нахили голови понад 15° значно впливають на симетрію обличчя, що знижує точність вимірювання.

Метод FaceMesh з OpenCV може бути використаний як базовий модуль у розумних інтерфейсах для відстеження положення користувача [1]. У перспективі дослідження буде розширено шляхом порівняння з нейромережевими методами визначення глибини (наприклад, Monodepth, DPT), а також реалізовано адаптивне перемикання алгоритмів в залежності від умов.

**Список літератури**

1. Nazarkevych M. et al. Methods of Face Recognition in Video Sequences and Performance Studies //CEUR Workshop Proceedings. – 2023. – Т. 3421. – С. 246-253.

# АНАЛІЗ ВПЛИВУ ТІНЕЙ НА ПРОДУКТИВНІСТЬ 3D-ЗАСТОСУНКУ

Скороход М.М., Дуднік Д.О., Сердечний В.С.
Харківський національний університет радіоелектроніки, Харків, Україна

У наш час тривимірна графіка широко використовується в різних сферах, зокрема у відеоіграх, медицині, віртуальній реальності, симуляціях і наукових візуалізаціях. Особливу увагу привертає рендеринг у реальному часі, де кожен кадр має генеруватися за мінімально можливий проміжок часу для забезпечення плавного ігрового процесу або інтерактивного досвіду. Одним із ключових аспектів реалістичного рендерингу є система освітлення, яка включає динамічні тіні, що не тільки покращують візуальне сприйняття сцени, але й можуть значно впливати на продуктивність.

**Метою дослідження** є аналіз ефективності використання динамічних тіней у 3D-графіці, визначення впливу шейдерів на продуктивність графічного застосунку та розробка оптимізованого підходу до рендерингу тіней.

У роботі досліджено вплив тіней на продуктивність тривимірних застосунків у реальному часі шляхом реалізації алгоритму shadow mapping з використанням вершинного, фрагментного та вертексного шейдерів в середовищі OpenGL і мові програмування C++ [1-2]. Для оцінки ефективності було створено тестове середовище, яке дозволяє порівнювати продуктивність системи зі шейдерами та без них, з проведенням бенчмарків для вимірювання навантаження на CPU, GPU та використання оперативної пам’яті.

В результаті проведення досліджень встановлено, що шейдери істотно впливають на навантаження системи, але при цьому забезпечують значне підвищення візуального реалізму. Показано, що за рахунок поєднання геометричних і фрагментних шейдерів можливо досягти балансу між якістю тіней і обчислювальною ефективністю.

Таким чином, дослідження підтвердило, що грамотне застосування шейдерів дає змогу забезпечити стабільну роботу графічного застосунку навіть в умовах складної сцени. У подальшому планується дослідження масштабованості розробленого підходу на різних апаратних платформах.

**Список літератури**

1. Guha S. Computer Graphics Through OpenGL®: from theory to experiments. – CRC press, 2022.

2. Konnurmath G., Chickerur S. GPU Shader Analysis and Power Optimization Model //Engineering, Technology & Applied Science Research. – 2024. – Т. 14. – №. 1. – С. 12925-12930. https://doi.org/10.48084/etasr.6695.

# ПРОГРАМНІ ЗАСОБИ РОЗРОБКИ ЦИФРОВОЇ СЕРВІСНОЇ КНИЖКИ АВТОМОБІЛЯ

Олефір М.О., Єрошенко О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Цифрова трансформація в автомобільній індустрії актуалізує потребу у створенні новітніх засобів для ведення обліку технічного обслуговування транспортних засобів. Паперові сервісні книжки часто мають низку недоліків: схильність до втрати або пошкодження, складність доступу до історії обслуговування, відсутність зручного інтерфейсу користувача.

Метою доповіді є розробка мобільного додатка для ведення електронної сервісної книжки автомобіля. Програмне рішення реалізоване у вигляді Android-застосунку з використанням мови програмування Kotlin та сучасного фреймворку Jetpack Compose [1-5].

Додаток забезпечує зручне збереження та перегляд технічної інформації про обслуговування автомобіля, підтримує додавання текстових і фото нотаток, сповіщення про планові ТО, а також інтегрується з хмарними сервісами для синхронізації між пристроями.

У роботі представлено архітектуру додатка, описано реалізацію основних функціональних модулів та наведено попередній аналіз зручності використання. Порівняльна оцінка підтверджує доцільність застосування Kotlin для розробки сервісно-орієнтованих мобільних рішень у сфері технічного обслуговування автомобілів.

Подальші етапи розробки включають розширення функціоналу додатка шляхом додавання можливостей для взаємодії із СТО, підтримки обліку кількох автомобілів та реалізації резервного копіювання даних у зашифрованому вигляді.

**Список літератури**

1. Jemerov D., Isakova S. Kotlin in Action. Manning Publications, 2017.
2. Fedorchenko V., Yeroshenko O., Shmatko O., Kolomiitsev O., Omarov M. Password hashing methods and algorithms on the .NET platform. *Advanced Information Systems*. 2024. Vol. 8(4). P. 82–92. doi: https://doi.org/10.20998/2522-9052.2024.4.11
3. Олефір М.О., Єрошенко О.А. Цифрова сервісна книжка для автомобіля. *Проблеми інформатизації*: тези доповідей 12-тої міжнародної науково-технічної конференції. Т.2. 2024. С. 124.
4. Ткачов В.М., Гальченко К.Р., Коваленко А.А., Єрошенко О.А. Критерії вибору стандарту безпровідної передачі даних у високомобільних комп'ютерних мережах. Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2021. Т. 4 (66). С. 63-68. doi: https://doi.org/10.26906/SUNZ.2021.4.063
5. Щолкін М.М., Єрошенко О.А. Автоматизація управлінських рішень на основі BIG DATA та машинного навчання. Проблеми інформатизації: тези доповідей 12-тої міжнародної науково-технічної конференції. Т.2. 2024. С. 85.

# ПРОЄКТУВАННЯ ТА РОЗГОРТАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ДЛЯ ДАТА-ЦЕНТРУ

Гур'єва К.В., Ляшенко Г.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

Швидке розширення інформаційного простору змушує створювати дедалі масштабніші платформи для збереження даних.

Задачу накопичення та зберігання інформації успішно розв'язують дата-центри, які забезпечують та необхідні ресурси та автоматизують будь-яку бізнес-діяльність [1].

Сучасні технології хмарних обчислень значно впливають на процеси проєктування та розгортання мережевої інфраструктури для дата-центрів. Сьогодні хмарні технології пропонують великий об'єм ресурсів для бізнесу при вартості, яка є значно меншою в порівнянні з капітальними інвестиціями у власну інфраструктуру [2].

**Метою доповіді** є дослідження і розробка оптимальних підходів до проєктування та розгортання мережевої інфраструктури, яка відповідатиме сучасним вимогам продуктивності, надійності, гнучкості та безпеки. Для цього розглядаються методи побудови мереж, вибір топології, використання віртуалізації та хмарних технологій для підвищення ефективності роботи дата-центрів.

Консолідація обчислювальних ресурсів і засобів зберігання даних в дата-центрах дозволяє скоротити сукупну вартість володіння IT-інфраструктурою за рахунок можливості ефективного використання технічних засобів, наприклад, перерозподілу навантажень, а також за рахунок скорочення витрат на адміністрування [3].

У доповіді представлено результати аналізу сучасних тенденцій у розвитку мережних технологій для дата-центрів, а також рекомендації щодо їх впровадження з урахуванням потреб бізнесу та технічних обмежень. Зокрема, розглянуто питання масштабованості мереж, управління трафіком та забезпечення безперервності роботи дата-центру.

**Список літератури**

1. Коваль О. С. Модель захищеного дата-центру на базі технології cloud computing / О. С. Коваль, С. С. Бондаровець, С. О. Гнатюк // Захист інформації. 2016. Т. 18, № 2. С. 133–142.

2. Копійка О. В. Архітектура мережі в сучасних дата-центах / О. В. Копійка // Наукові записки Українського науково-дослідного інституту зв'язку. 2014. № 2. С. 34–41.

3. Теоретичні особливості використання центрів обробки даних в приватних хмарах: вимоги побудови, види, переваги та недоліки, надійність / О. Андрощук та ін. // Молодий вчений. 2021. № 7 (95). С. 1–5.

# АВТОМАТИЗАЦІЯ РОЗГОРТАННЯ СЕРВЕРНОЇ ІНФРАСТРУКТУРИ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ ЗА ДОПОМОГОЮ ANSIBLE

Кривонос П.Р., Ляшенко Г.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

Ansible являє собою практично незамінний інструмент автоматизації, за допомогою якого можна автоматизувати встановлення та налаштування широкого спектру програм та файлів конфігурації на практично будь-якій операційній системі. Одним з частих випадків використання даного інструменту є автоматизація налаштування мережевого обладнання, так як це дозволяє витрачати значно менше часу при необхідності налаштування нових пристроїв, особливо при їх великій кількості [1].

**Метою доповіді** розгляд існуючих модулів Ansible для розуміння можливих лімітів, таких як сумісність пристроїв з модулями Ansible та кроки, що передують безпосередньо процесу автоматизації, тобто кроки, які автоматизувати немає сенсу чи неможливо за певними причинами.

В доповіді наводяться результати дослідження офіційної документації та модулів, створених спільнотою. Результати показують, що офіційно Ansible підтримує ряд мережевих пристроїв, зокрема пристроїв компанії Cisco та пристроїв, що працюють на операційній системі ISO XR [2]. Окрім цього, існують колекції модулів, створені спільнотою, наприклад Community Network Collection, що містить в собі модулі для налаштування мережевих пристроїв Lenovo, Huawei та інших [3]. Проведено огляд підготовки до роботи з Ansible та основних моментів, на які треба звернути увагу при роботі з даним інструментом [4]. Отримані в результаті аналізу дані допомагають передбачити більшість помилок, що можуть виникнути при створенні скриптів для автоматичного налаштування та/або розгортання серверної інфраструктури.

**Список літератури**

1. Choi B., Medina E. Introduction to Ansible Network Automation. Berkeley, CA : Apress, 2023. URL: https://doi.org/10.1007/978-1-4842-9624-0 (date of access: 29.03.2025).
2. Collections in the Cisco Namespace. URL: https://docs.ansible.com/ansible/latest/collections/cisco/iosxr/index.html .
3. Community Network Collection. URL: https://galaxy.ansible.com/ui/repo/published/community/network/docs/ .
4. Okasha K. Network Automation Cookbook: Proven and Actionable Recipes to Automate and Manage Network Devices Using Ansible. Packt Publishing, Limited, 2020. 944 p.

# ПЛАНУВАННЯ БЕЗДРОТОВОЇ МЕРЕЖІ ДЛЯ РОЗУМНОГО БУДИНКУ

Левчук Д.Д., Ляшенко Г.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

Технологія Wi-Fi, заснована на стандарті IEEE 802.11, кардинально змінила звичайне життя, забезпечивши бездротовий доступ до інтернету для мільярдів пристроїв[1]. Це призвело до розробки стандартів бездротових технологій, які згодом набули попит у використанні бездротових сенсорних мереж.

Бездротові технології відіграють ключову роль у забезпеченні зв'язку між датчиками та серверами, що є необхідним для роботи будь-якого відповідного програмного забезпечення. Для цього існують три основні архітектури бездротового доступу, які базуються на різних бездротових технологіях, включаючи IEEE 802.15.3/4 для персональних мереж, IEEE 802.11g/n для локальних мереж, та HSDPA/LTE для глобальних мереж [2].

Прикладом може бути використання в розумних будинках автоматичного освітлення, яке працює на основі датчиків руху. Такі рішення дозволяють вмикати та вимикати світло відповідно до присутності людини в приміщенні, що не тільки підвищує зручність, а й сприяє енергозбереженню.

Оскільки бездротові сенсорні мережі часто працюють у важкодоступних місцях, або в умовах сильних перешкод, необхідно приділити велику увагу їх захисту, для запобігання мережевим атакам, підвищення безпеки та комфорту[3].

Метою доповіді є дослідження та розробка ефективної сенсорної мережі для систем розумних будинків, з особливим акцентом на підвищення рівня безпеки, комфорту та енергоефективності. Для забезпечення надійної та ефективної роботи сенсорної мережі використано оптимальну топологію, різні методи побудови мереж для бездротового зв'язку.

У роботі розроблено бездротову мережу, що є ключовим елементом для систем розумних будинків. Мережа складається з датчиків, координатора та використовується стандарт IEEE 802.11 для передачі даних. Також сенсори застосовуються і в системах безпеки, які поєднують датчики руху з комунікаційними механізмами та засобами оповіщення.

**Список літератури**

1. A. Belghith, M.S Obaidat. Smart Cities and Homes. 2016.

2. Kaveh Pahlavan, Prashant Krishnamurthy. Evolution and Impact of Wi-Fi Technology and Applications: A Historical Perspective. International Journal of Wireless Information Networks. 2020.

3. Zhang Huanan, Xing Suping, Wang Jiannan. Security and application of wireless sensor network. 2021.

# МОДЕЛЬ ПРОГНОЗУВАННЯ ВИТРАТ ЕНЕРГІЇ НА ПЕРЕДАЧУ ДАНИХ В РОЗПОДІЛЕНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМАХ НА ОСНОВІ МОБІЛЬНИХ ПРИСТРОЇВ

Мамчич О.О., Волк М.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Одним із вагомих внесків в енергетичну ефективність розподілених обчислювальних систем є витрати енергії на передачу даних між обчислювальними вузлами.

У попередніх наукових роботах було вивчено ефективність саме обчислювальної за допомогою мобільних пристроїв, а витрати на передачу даних було замінено на найпростішу лінійну модель.

Мобільні пристрої традиційно можуть працювати як з бездротовими мережами передачі даних (наприклад, Wi-Fi, Bluetooth, 5G) так і з проводними (наприклад, USB, Ethernet через адаптер). Слід врахувати що передача даних між мобільними пристроями супроводжується витратами енергії, які суттєво залежать від типу використовуваного зв'язку — бездротового або проводового.

Тому для більш точного врахування витрат енергії на передачу даних при обчисленні створена математична модель.

Метою доповіді є обґрунтування математичної моделі. Суть математичної моделі полягає у тому, що загальні витрати енергії залежать від потужності, яку споживає пристрій в різних режимах роботи, та тривалості роботи у кожному режимі.

Потужність, у свою чергу, складається з базового енергоспоживання у режимі очікування та додаткової складової, яка певним чином залежить від швидкості передачі даних. Оскільки тривалість передачі також прямо пов'язана з обсягом даних та швидкістю, формула дозволяє врахувати як технічні характеристики пристрою, так і особливості типу середовища передачі даних.

Наприклад, якщо сигнал нестабільний і потребує повторної передачі частини даних, це зменшує ефективність і збільшує витрати енергії [1]. Бездротовий зв'язок має суттєву перевагу у зручності — він забезпечує мобільність, відсутність кабелів і можливість передавати дані між кількома пристроями одночасно. Однак ця технологія характеризується вищим енергоспоживанням, особливо при передачі на великі відстані або за наявності перешкод, а також меншою стабільністю сигналу. Крім того, вона потребує додаткових заходів безпеки для захисту каналу обміну даними.

Проводове з'єднання, навпаки, забезпечує стабільну та швидку передачу даних з мінімальними втратами енергії. Воно значно ефективніше в плані енергоспоживання та менш залежне від зовнішніх факторів [2]. Утім, така передача обмежує мобільність користувача, вимагає фізичного підключення та менш зручна в умовах швидкого переміщення або великої кількості пристроїв.

Таким чином, математична модель дозволяє кількісно оцінити, які енергетичні витрати очікуються при використанні певного типа з'єднання.

В майбутньому дана модель буде узагальнена та об'єднана з існуючою уніфікованою моделлю прогнозування витрат енергії при обчисленні [3].

**Список літератури**

1. Masafumi Hashimoto, Go Hasegawa, Masayuki Murata Energy efficiency analysis of TCP with burst transmission over a wireless LAN, Communications and Information Technologies (ISCIT), 2011 11th International Symposium, Hangzhou, China, DOI:10.1109/ISCIT.2011.6089751

2. Bartosz Kopras, Filip Idzikowski, Hanna Bogucka A Survey on Reduction of Energy Consumption in Fog Networks—Communications and Computations, Faculty of Computing and Telecommunications, Poznan University of Technology, 2024, Poznan, Poland, DOI:10.3390/s24186064

3. Mamchych O., Volk M. A unified model and method for forecasting energy consumption in distributed computing systems based on stationary and mobile devices, RADIOELECTRONIC AND COMPUTER SYSTEMS, vol 2024, N 2, NAU KhAI, cc. 120-135, 2024, Kharkiv, Ukraine

## ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ ОБРОБКИ ДАНИХ У СИСТЕМІ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ

Філіппенко І.В., Кривицький А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток вбудованих систем і, як наслідок, підвищення ступеня технологічної складності створює нові типи викликів які мають бути вирішені під час розробки. Одним з найскладніших викликів є діагностика та верифікація.

Етап верифікації та діагностики є ключовим для критичних систем, наприклад таких як авіоніка, автомобільні системи безпеки, медичне обладнання, тощо.

Сучасні стандарти вимагають впровадження надійних методів діагностики та верифікації на всіх етапах розробки. Hardware-in-the-Loop (HIL) верифікація є ефективним підходом, що дозволяє здійснювати діагностику та верифікацію діагностованого пристрою в умовах, максимально наближених до реальних, ще до створення фізичного прототипу системи [1].

**Метою доповіді** є розробка програмно-апаратної реалізації інтерфейсу взаємодії між математичною моделлю та діагностованим пристроєм.

У контексті HIL-верифікації критичних пристроїв обробка даних в апаратній частині інтерфейсу взаємодії виконує роль ключової ланки між симуляційною математичною моделлю та фізичним об'єктом, що діагностується.

Основне завдання даного етапу полягає в перетворенні абстрактних числових результатів моделювання у реальні фізичні сигнали або протоколи, які розпізнаються цільовим пристроєм.

Апаратна частина інтерфейсу (зазвичай мікроконтролер або ПЛІС) виконує такі функції [2]:

– дискретно-аналогове або цифрове перетворення сигналів (DAC/PWM/GPIO): для формування сигналів, що емулюють фізичні впливи (наприклад, зміна напруги датчика);

– форматування та масштабування даних: значення з математичної моделі трансформуються до діапазону і точності, що відповідає вимогам пристрою (наприклад, перетворення значення температури 36.6°C у 12-бітове значення ADC)»

– буферизація та синхронізація: забезпечується рівномірна передача пакетів у режимі реального часу з фіксованою затримкою, що критично важливо для відтворення динаміки системи без спотворень;

– формування протоколів взаємодії (SPI, I2C, CAN, UART тощо): в залежності від типу інтерфейсу діагностованого пристрою, передача здійснюється згідно з відповідними часовими і логічними вимогами.

В доповіді наводиться приклад імплементації інтерфейсу між математичною моделлю IMU (Inertial Measurement Unit) та діагностованим об’єктом що зчитує з нього дані відповідно до документації що постачається разом з вимірювальним пристроєм.

Особливу увагу приділено забезпеченню достовірності обміну. Кожен пакет даних що передається від математичної моделі супроводжується службовою інформацією (контрольна сума, номер пакета, мітка часу), що дозволяє виявляти пошкоджені або втрачено-переставлені фрагменти. У разі виявлення похибки інтерфейс здатен здійснити запит на повторну передачу або перейти в безпечний режим, зберігаючи цілісність симуляції. Для досягнення високої швидкодії застосовано методи циклічного DMA-передавання, використання апаратних таймерів для точного тактування, та розділення обробки по пріоритетах (наприклад, переривання високого пріоритету надаються шинам, критичним до затримок). Таким чином, апаратна обробка даних не тільки виконує роль моста між симуляційною і фізичною частинами HIL-системи, але й забезпечує ключові характеристики: низькі затримки, високу достовірність передачі та врахування фізичних обмежень пристрою.

**Список літератури**

1. Advanced hardware-in-the-loop testing chain for investigating interactions between smart grid components during transients / A. Paspatis et al. ScienceDirect. URL: https://www.sciencedirect.com/science/article/abs/pii/S0378779623008787 (date of access: 01.04.2025).

2. Mihalič F., Truntič M., Hren A. Hardware-in-the-Loop simulations: a historical overview of engineering challenges. MDPI. URL: https://www.mdpi.com/2079-9292/11/15/2462 (date of access: 01.04.2025).

# СИСТЕМА УПРАВЛІННЯ ЗАВДАННЯМИ ДЛЯ IT-ВІДДІЛІВ НА ОСНОВІ ВЕБІНТЕРФЕЙСУ

Булгаков Р.І., Ляшенко Г.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

Система управління завданнями в IT-відділах є важливим та актуальним аспектом у сучасному світі, що обумовлено стрімким розвитком технологій. Успішне виконання завдання залежить від правильно контакту між командою розробників, співпраці та повного розуміння того, на якому етапі знаходиться розробка.

Під час реалізації проєктів важливим є використання інтуїтивно зрозумілого інтерфейсу, встановлення дедлайнів, можливість бачити активність команди та актуальний статус завдання. Тому з'являється необхідність створення такої системи, яка допомагає вирішити ці питання.

**Метою доповіді** є побудова веб-інтерфейсу, який допомагає покращити комунікацію під час виконання робочих завдань та розгортання проєктів. Створення такого додатку знижує ризики виникнення технічних помилок, через які може бути пошкоджена репутація IT-відділу. Це дозволяє зменшити час, необхідний на виконання проєкту [1].

В доповіді наводиться аналіз вже існуючих аналогів веб-інтерфейсів, їх порівняльна характеристика.

Описано розробку проєкту, у якому реалізовано наступні функції: авторизація, можливість додавання файлів та робота із запитами, завантаження фото та відео. Розробка системи управління завданнями складається зі створення інтерфейсу користувача на стороні клієнта з дотриманням стандартів WCAG 2.2[2] та серверної складової програми, яка реалізує обчислення, обробку даних, взаємодію з базами даних та виконання бізнес логіки [3].

Проєкт реалізовано з використанням таких технологій, як: Figma, HTML, CSS, NestJS, TypeScript та MongoDB. Для реалізації авторизації використано Passport.JS та JWT.

**Список літератури**

1. Mayank Mittal, "The art of building great products: Combine your intuition with the best proven methodologies to build digital products everyone will love", Mayank Mittal, 2022, 350 p.

2. Web Content Accessibility Guidelines (WCAG) 2.1 [Електронний ресурс]. – URL: https://www.w3.org/TR/WCAG21 (дата звернення: 02. 04.2025).

3. Back-End Developer: What It Is, and How to Become One [Електронний ресурс]. – URL: https://www.coursera.org/articles/back-end-developer (дата звернення: 02.04.2025).

# АРХІТЕКТУРНА МОДЕЛЬ АПАРАТНОГО ОБЧИСЛЮВАЧА ІРРАЦІОНАЛЬНИХ ФУНКЦІЙ З БІТ-ПОТОКОВИМ КОДУВАННЯМ

Ларченко Л.В., Красіля М.М.
Харківський національний університет радіоелектроніки, Харків, Україна

В даний час спостерігається зростання складності завдань щодо організації обчислень у сенсорних системах, робототехніці, системах управління. Одним із напрямків, пов'язаних із створенням нових базових компонентів для побудови названих систем є розробка пристроїв, що виконують функціональне перетворення інформаційних сигналів, представлених бітовими потоками, що отримують від сенсорів з частотним виходом [1]. При функціональному перетворенні бітових потоків реалізується потоковий спосіб обчислень, який передбачає бітово-кодову розгортку, при якій здійснюється паралельно-послідовне виконання перетворень над бітами потоку у відповідності до необхідної функції.

**Метою доповіді** є побудова архітектурної моделі обчислювача ірраціональних функції з використанням узагальненої архітектури біт-потокового обчислювача.

В доповіді наводяться результати синтезу деталізованої архітектури ірраціонального обчислювача на основі двож архітектур: архітектури біт-потокового обчислювача лінійних функції, що включений в прямий зв’язок архітектури, та пристрою добування кореня n-го степеня, що включений у зворотний зв’язок архітектури і представляє собою конвеєрну структуру. Спільним компонентом деталізованої архітектури ірраціонального обчислювача є суматор зі зворотним зв’язком, в якому здійснюється порівняння приростів двох одночасно відтворюваних висхідних ступінчастих функцій [2]. Вхідним та вихідним інформаційними сигналами є бітові потоки. Створена архітектура є основою архітектури пристрою добування квадратного кореня та розробленої на її базі HDL-моделі пристрою. В процесі дослідження Було здійснено верифікацію поведінкової моделі обчислювача, яка підтвердила правильність побудови архітектури та теоретичні розрахунки для проведення експериментів.

**Список літератури**

1. A.S. Shkil, L.V. Larchenko and B.D. Larchenko Bit-Stream Power Function Online Computer, *2020 IEEE East-West Design & Test Symposium (EWDTS)*, Varna, Bulgaria, 2020, pp. 1-6, , DOI: http://doi.org/10.1109/ewdts50664.2020.9224764.

2. L.V. Larchenko, A.V. Parkhomenko, B.D. Larchenko, V.R Korniienko. Design Models of Bit-Stream Online-Computers for Sensor Components, in *Radio Electronics, Computer Science ,Control*, 2024, vol.1(68), pp. 48-61. DOI: https://ric.zntu.edu.ua/article/view/300944.

# ОЦІНКА ТОЧНОСТІ ОБЧИСЛЕННЯ КУТА НАДХОДЖЕННЯ СИГНАЛУ МЕТОДАМИ МАТЕМАТИЧНОЇ СТАТИСТИКИ

Васильєв О.Ю., Філіппенко О.І.
Харківський національний університет радіоелектроніки, Харків, Україна

В сучасних радіотехнічних системах важливим завданням є швидке й точне визначення різниці фаз між сигналами, що використовується для визначення напрямку на джерело радіовипромінювання. Одним з методів широкосмугового аналізу кутів декількох сигналів що надходять одночасно є обчислення різниці фаз за допомогою швидкого перетворення Фур'є (ШПФ), що забезпечує високу точність і низьку затримку. **Метою дослідження** є оцінка точності роботи запропонованого алгоритму обчислення кута на джерело випромінювання за допомогою ШПФ методами математичної статистики.

Для визначення кута напрямку на джерело випромінювання зазвичай використовуються антенні масиви. Антенний масив – це група антенних елементів, розташованих на відомій відстані один від одного. Коли сигнал від джерела випромінювання досягає цього масиву, він надходить до кожного елемента з певним часовим зсувом, що залежить від напрямку на джерело. Напрямок на джерело можна визначити, оцінивши ці фазові зсуви.

Швидке перетворення Фур'є (ШПФ) застосовує спектральний аналіз для визначення частотних та фазових характеристик сигналу [1]. В даній роботі розглядаються сигнали, що знаходяться в обраній смузі частот. Для визначення кута на джерело за допомогою ШПФ необхідно порівняти фазові характеристики сигналів, що надходять на різні антени. Фазова різниця між компонентами сигналів, дозволяє визначити напрямок на їх джерело. Затримка надходження сигналу $\Delta t$ визначає різницю шляху, який проходить сигнал до кожної з антен. Відстань між антенами є відомою, що дає змогу розрахувати кут напрямку $\theta$ в залежності від часу та частоти:

$$\theta = \arcsin\left(\frac{p}{d}\right) = \arcsin\left(\frac{\Delta t \cdot c}{d}\right) = \arcsin\left(\frac{\Delta \varphi \cdot c}{2\pi d f}\right)$$

де d - відстань між антенами, c - швидкість світла, f - частота сигналу, $\Delta\varphi$ - різниця фаз сигналу [2].

На початковій стадії розробки вигідно здійснювати моделювання та тестування алгоритмів цифрової обробки сигналів на програмному рівні. Попереднє моделювання дозволяє оцінити ефективність і оптимізувати алгоритми перед їх впровадженням на платформу системи на кристалі. Для таких завдань мова програмування Python є дуже зручним інструментом завдяки широкому вибору відкритих бібліотек для швидких і точних математичних обчислень.

В доповіді наведено результати імітаційного моделювання приймання сигналу двома антенами із затримками, відповідними заданому куту на джерело випромінювання. Для імітації сигналів, що надходять з різних напрямків моделюється синусоїда з частотою, що відповідає першій зоні Найквіста, а для

наближення умов до реальних, сигнал модулюється та додаються шуми, амплітуда яких не перевищує максимальну амплітуду сигналу. Крім того, додається сигнал-завада з фіксованим кутом та частотою, амплітуда якого вдвічі перевищує амплітуду досліджуваного сигналу.

На основі зазначених характеристик було реалізовано Python-модель, яка випадковим чином задає частоту досліджуваного сигналу, частоту модуляції та заданий кут надходження сигналу, та формує сигнали на основі цих параметрів. Для згенерованих сигналів виконується розрахунок ШПФ, пошук піку амплітуди для визначення частотного каналу, якому відповідає досліджуваний сигнал. Для цього частотного каналу розраховується фазовий зсув за результатами кожного ШПФ, що і визначає кут надходження сигналу. Розрахований кут порівнюється із заданим, і обчислюється похибка або відхилення розрахунку. Для подальшого аналізу розрахунки багаторазово повторюються для формування статистичної вибірки даних з метою оцінки точності та залежності точності від різних параметрів.

Було проведено розвідувальний аналіз даних, який продемонстрував і дозволив відфільтрувати локальні викиди, що були викликані наближенням значення кута чи частоти до граничного або наближення частоти досліджуваного сигналу до сигналу-завади.

Також було проведено перевірку статистичної гіпотези і підтверджено, що результуюча вибірка відхилення розрахованого кута від заданого кута має нормальний розподіл.

Виконано кореляційний аналіз за Пірсоном змінних моделі. При цьому, значення кореляції можуть приймати значення від -1 до +1, де +1 означає повну залежність параметрів, а -1 повну зворотну залежність [3]. В результаті розрахунку отримані значення кореляції близькі до нуля, що свідчить про відсутність значущої лінійної залежності між точністю результату розрахунку та обраними вхідними параметрами.

Аналіз показав, що метод обчислення кута надходження сигналу шляхом визначення фазового зсуву з використанням ШПФ має низьку лінійну кореляцію похибки відносно вхідних параметрів.

Сформульовані обмеження, що викликають викиди не є завадою для використання методу, а метод є надійним та точним.

**Список літератури**

1. Lyons, R. G. Understanding digital signal processing. 3rd ed., Pearson, 2022. 998 p. ISBN 9780137582228.

2. Zuo, L., Pan, J. Accurate 2-D AOA estimation and ambiguity resolution for a single source under fixed uniform circular arrays. International Journal of Antennas and Propagation, 2017, Article ID 9489318, 6 p. DOI: https://doi.org/10.1155/2017/9489318.

3. Мельников, О. С. Інтелектуальний аналіз даних: монографія. Харків: Вид-во НТУ «ХПІ», 2023. 196 с.

# МАТЕМАТИЧНА МОДЕЛЬ ФУНКЦІОНАЛЬНОГО ПЕРЕТВОРЮВАЧА ІМПУЛЬСНИХ ПОТОКІВ НА ОСНОВІ СТЕПЕНЕВОГО МОДУЛЯ

Ларченко Л.В., Олефір А.В.
Харківський національний університет радіоелектроніки, Харків, Україна

В системах реального часу, таких як системи управління, сенсорні та роботехнічні системи, отримала розвиток концепція присенсорних обчислень, що передбачає переміщення обробки даних ближче до сенсорних компонентів [1]. Реалізація присенсорних обчислень потребує розробки спеціалізованих пристроїв, що виконують функціональне перетворення сигналів у тому ж форматі даних, які генеруються на виході сенсора. Широке застосування знаходять сенсори з частотним вихідним сигналом у вигляді імпульсного (бітового) потоку.

**Метою доповіді** є розробка удосконаленої математичної моделі апаратного обчислювача степеневих функцій з бітпотоковим кодуванням, що забезпечує мінімальну похибку обчислень, що складає половину одиниці молодшого біту аргументу.

В доповіді розглянуто підхід до розробки математичної моделі пристрою з використанням методу відтворення висхідних ступінчастих функції на основі зворотних функцій [2]. Досліджуваний пристрій працює в режимі вибірки певних бітів з вхідної імпульсної послідовності. Вибіркові значення бітів визначаються з використанням основної нерівності, що реалізується у пристрою.

Математична модель досліджуваного пристрою являє собою систему різницевих нерівностей, в яких прирости функції аргументу порівнюються з приростами рівнів вузлів апроксимації відтворюваної функції. При реалізації кожної нерівності математичної моделі на виході пристрою формується вихідний біт, що відповідає черговому рівню вузла апроксимації ступінчастої функції.

**Список літератури**

1. Korniienko V., Larchenko. L., Parkhomenko A., Larchenko B. Design Models of Bit-Stream Online-Computers of Elementary Mathematical Functions, *12th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Sep. 2023, Dortmund, Germany, pp. 585-589. DOI: https://doi.org/10.20998/2522-9052.2018.1.04.

2. L.V. Larchenko, A.V. Parkhomenko, B.D. Larchenko, V.R Korniienko. Design Models of Bit-Stream Online-Computers for Sensor Components, in *Radio Electronics, Computer Science ,Control*, 2024, vol.1(68), pp. 48-61. DOI: https://ric.zntu.edu.ua/article/view/300944.

# АДАПТИВНА СИСТЕМА КОРЕКЦІЇ ПОМИЛОК З УРАХУВАННЯМ АНАЛІЗУ СТАНУ КАНАЛУ ЗВ'ЯЗКУ У КОНТЕКСТІ ЦІЛЕЙ СТАЛОГО РОЗВИТКУ

Сергієнко В.І., Філіппенко І.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Зростання обсягів переданих даних та кількості пристроїв, підключених до цифрових мереж, потребує більш ефективних механізмів захисту інформації від помилок. Особливо це актуально в умовах мобільного та бездротового зв'язку, де вплив завад, зміни умов середовища й енергетичні обмеження значно впливають на якість зв'язку. У таких системах завелика фіксована надмірність може призводити до зайвого споживання енергії або затримок, тоді як її нестача — до великої кількості повторних передач [1].

У роботі запропоновано адаптивну модель корекції помилок, що динамічно змінює параметри кодування залежно від поточних умов передачі. Модель включає моніторинг каналу та QoS-параметрів (рівень шуму, SNR, швидкість руху користувача, рівень заряду батареї тощо), модуль оцінки стану каналу на основі евристичних або машинних алгоритмів, блок прийняття рішень, адаптивний перемикач кодів (LDPC, Turbo, Hamming), а також канали кодування та декодування. Важливим є також модуль зворотного зв'язку, який дозволяє адаптації навчатися або уточнювати стратегію вибору коду з часом [2].

Запропонована система реалізована мовою програмування Python і дозволяє проводити моделювання різних сценаріїв комунікації з урахуванням енергоспоживання, затримки та рівня помилок. Принцип дії системи полягає у попередньому зборі параметрів середовища, їх аналізі, оцінці якості каналу та прийнятті рішення щодо типу кодування. Таким чином, у сприятливих умовах система переходить до менш навантажених кодів, що знижує енергоспоживання, а при погіршенні каналу — активує більш надійні, але затратні методи захисту.

Такий підхід забезпечує не лише гнучкість, але й масштабованість рішення у різних середовищах передачі.

Результати моделювання показали, що запропонована система дозволяє зменшити кількість повторних передач, а середнє енергоспоживання на передачу одного біта — на 5–15% у порівнянні з неадаптивними методами. Також досягнуто покращення затримки в середньому на 10% при збереженні цільового рівня ймовірності помилки (BER) [3]. У перспективі планується розширення системи для роботи в умовах багатокористувацького доступу та мультиканальних сценаріїв зв'язку. Крім того, розглядається інтеграція з модулями передбачення навантаження на мережу для ще точнішої адаптації.

Модель відповідає низці цілей сталого розвитку, передусім:

– ЦСР 7 «Чиста енергія» — через зменшення енергоспоживання пристроїв зв'язку,

– ЦСР 9 «Інфраструктура та інновації» — через розвиток інтелектуальних адаптивних мереж,

– ЦСР 10 «Зменшення нерівності» — через забезпечення стабільного зв'язку навіть у складних умовах та з енергетично обмежених пристроїв.

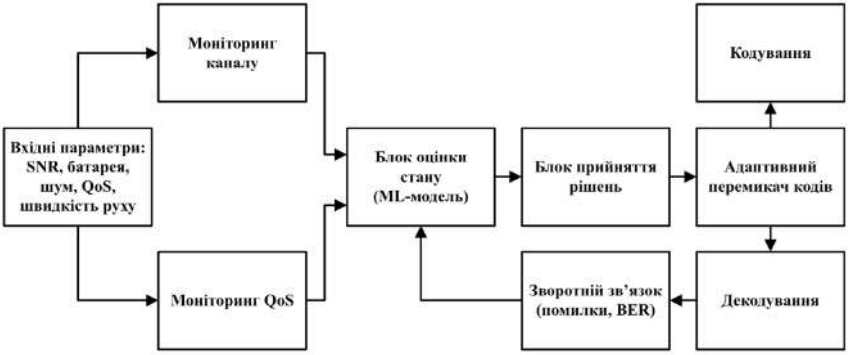


Рисунок 1 – Блок схема системи

Блок-схема моделі наведена на рис. 1. Завдяки модульній структурі модель є придатною до масштабування, адаптації під різні типи комунікаційних систем та потенційної реалізації в апаратному вигляді (наприклад, у вигляді IP-блоків для FPGA/SoC).

Окрему увагу приділено аналізу обмежень, які часто ігноруються в існуючих підходах до адаптивної корекції помилок. Зокрема, багато моделей не враховують часові обмеження на прийняття рішень у режимі реального часу, а також обчислювальні можливості кінцевих пристроїв. У контексті цілей сталого розвитку це особливо важливо для побудови технологій, здатних ефективно функціонувати в складних умовах — зокрема, в регіонах з обмеженим доступом до енергоресурсів або з підвищеними вимогами до стабільності цифрової інфраструктури.

**Список літератури**

1. Li S., Kim J.G., Han D.H., Lee K.S. A Survey of Energy-Efficient Communication Protocols with QoS Guarantees in Wireless Multimedia Sensor Networks // Sensors. – 2019. – Vol. 19, No. 1. – Article No. 199. – DOI: https://doi.org/10.3390/s19010199.

2. Lin D., Wang Q., Min W., Xu J., Zhang Z. A Survey on Energy-Efficient Strategies in Static Wireless Sensor Networks // ACM Transactions on Sensor Networks. – 2020. – Vol. 16, No. 1. – P. 1–37. – DOI: https://doi.org/10.1145/3386364.

3. Філіппенко І. В. Система завадостійкого кодування даних на ПЛІС / І. В. Філіппенко, Е. М. Кулак, В. І. Сергієнко.// Radioelectronics & Informatics – 2019. – №4. – С. 38–45.

# МЕТОД ОЦІНЮВАННЯ ПРОСТОРОВОЇ ГЛИБИНИ ЗА КОНТРОЛЬНИМИ ТОЧКАМИ ОБЛИЧЧЯ В РЕАЛЬНОМУ ЧАСІ

Постельняк Ю.П., Барковська О.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному технологічному світі точне визначення відстані до об'єктів набуває все більшого значення у широкому спектрі застосувань – від автономного транспорту та робототехніки до медичних систем і розумних середовищ [1].

Особливо актуальним це питання є у контексті створення легковагих, адаптивних рішень, здатних працювати на недорогому обладнанні та в умовах змінного зовнішнього середовища. Сучасні методи визначення відстані стикаються з численними викликами, пов'язаними з впливом освітлення, атмосферних умов, роздільної здатності та динаміки сцени, що знижує їх точність та надійність.

**Метою дослідження** є розробка та експериментальна перевірка геометричного методу оцінки відстані до об'єктів з використанням комп'ютерного зору, стійкого до змін зовнішніх факторів і придатного для впровадження на пристроях із обмеженими обчислювальними ресурсами.

В основі дослідження – застосування алгоритмів FaceMesh у поєднанні з методами перспективної геометрії для обчислення відстані до об'єкта на основі масштабу відомих контрольних точок [2].

Для моделювання було використано бібліотеку OpenCV, а точність оцінювалася в експериментальних умовах за різних параметрів сцени – освітлення, кута огляду, положення голови та роздільної здатності зображення.

Запропонований підхід показав достатню точність в умовах змінного середовища, з можливістю роботи в реальному часі без використання ресурсомістких нейромереж.

Встановлено вплив ключових зовнішніх факторів на результати, зокрема підтверджено ефективність попередньої обробки зображення, зокрема нормалізації контрасту.

Проведено порівняння результатів для indoor та outdoor умов, що дало змогу визначити області ефективного застосування.

**Список літератури**

1. Guo, Y., Wang, H., Wang, L., Lei, Y., Liu, L., & Bennamoun, M. (2023). 3D face recognition: Two decades of progress and prospects. *ACM Computing Surveys*, *56*(3), 1-39.

2. Amir A. H. A., Nemer Z. N. Inclusive Review on Advances in Masked Human Face Recognition Technologies //Iraqi Journal of Intelligent Computing and Informatics (IJICI). – 2025. – Т. 4. – №. 1. – С. 1-17.

# СТВОРЕННЯ WEB-ПЛАТФОРМИ, ЯК УЗАГАЛЬНЕНОГО РІШЕННЯ ДЛЯ ОРГАНІЗАЦІЇ КОЛЕКТИВНОЇ ДІЯЛЬНОСТІ

Топорець Д.О., Барковська О.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному світі, особливо в IT-сфері, спостерігається стрімке зростання кількості цифрових інструментів, призначених для організації командної роботи, управління проєктами та взаємодії між учасниками освітнього або виробничого процесу. Зростає і складність, пов'язана з необхідністю освоєння численних сервісів, що дублюють або частково перекривають функціональність один одного. Така фрагментація цифрових середовищ негативно впливає на ефективність командної співпраці та суперечить 17-й цілі сталого розвитку — «Партнерство заради сталого розвитку», яка акцентує увагу на необхідності консолідації зусиль задля досягнення спільних цілей.

Аналіз існуючих рішень, таких як Jira, Trello, Asana, Notion, DL.NURE, VSCode Live Share тощо, демонструє високий ступінь перетину функціоналу, однак відсутність єдиного адаптивного інтерфейсу ускладнює їх інтеграцію у єдине робоче середовище [1]. Це створює бар'єри для співпраці, особливо в умовах проєктно-орієнтованого навчання та IT-підприємництва.

**Метою роботи** є розробка уніфікованої веб-платформи для організації колективної діяльності, яка дозволить поєднати функціональність наявних цифрових інструментів у єдиному динамічно налаштовуваному інтерфейсі, що зберігає інтуїтивність і доступність для кінцевого користувача.

У межах дослідження реалізовано бета-версію веб-платформи з базовими можливостями керування робочими та навчальними процесами [2]. Система надає можливість гнучкого налаштування інтерфейсу, а також редагування локального серверного середовища користувачем, що відкриває перспективи персоналізованого використання платформи.

Подальший розвиток проєкту передбачає розширення функціоналу за рахунок впровадження шаблонів подій та інтеграції з API сторонніх сервісів, підтримку мультимовності. Впровадження платформи може стати внеском у розвиток цифрової інфраструктури освітніх установ та IT-компаній, забезпечивши ефективну, адаптивну та масштабовану взаємодію учасників.

**Список літератури**

1. Kamila, Jihan Syafa, and Muhammad Falah Marzuq. 'Asana and Trello: A Comparative Assessment of Project Management Capabilities'. *JOIV : International Journal on Informatics Visualization*, vol. 8, no. 1, Mar. 2024, p. 207., https://doi.org/10.62527/joiv.8.1.2595.

2. Bugl, Daniel. *Modern Full-Stack React Projects: Build, Maintain, and Deploy Modern Web Apps Using MongoDB, Express, React, and Node.Js*. 1st ed., Packt Publishing Limited, 2024.

# ВИКОРИСТАННЯ КВАНТОВИХ ОБЧИСЛЕНЬ ДЛЯ ШВИДКОЇ ОБРОБКИ ІНФОРМАЦІЇ

Келеберда П.О., Мороз А.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Зі зростанням обсягів даних та ускладненням обчислювальних задач традиційні підходи до обробки інформації стають недостатньо ефективними. Квантові обчислення відкривають нові можливості для швидкої обробки великих масивів даних, використовуючи принципи квантової суперпозиції та заплутаності. Завдяки цим властивостям квантові комп'ютери здатні розв'язувати складні задачі в рази швидше за класичні обчислювальні системи.[1]

Одним із найважливіших застосувань квантових обчислень є обробка інформації у сфері криптографії, оптимізації, машинного навчання та моделювання складних фізичних процесів.

Наприклад, алгоритм Шора дозволяє ефективно розкладати великі числа на прості множники, що має критичне значення для криптографічних систем.

Алгоритм Гровера, у свою чергу, значно прискорює пошук у невпорядкованих базах даних, що робить його корисним для аналітики та великих баз знань. [2]

Ще одним важливим напрямом є використання квантових алгоритмів у сфері штучного інтелекту. Поєднання квантових методів з класичним машинним навчанням дозволяє суттєво прискорити тренування моделей та покращити якість аналізу великих обсягів даних.

Наприклад, квантові нейромережі демонструють високий потенціал у сфері розпізнавання образів, фінансового прогнозування та біоінформатики. Водночас виклики, пов'язані зі стабільністю квантових обчислень та необхідністю розробки нових архітектур, залишаються актуальними. [3]

**Метою доповіді** є аналіз перспектив застосування квантових обчислень для швидкої обробки інформації, огляд сучасних квантових алгоритмів та їх впливу на ключові галузі науки й техніки.

**Список літератури**

1. Петренко В.О. Квантові обчислення: теоретичні основи та практичні аспекти. – Київ: Наукова думка, 2020. – 312 с.

2. Коваленко М.П. Алгоритми квантових обчислень: від теорії до застосування. – Львів: Технологічний університет, 2021. – 278 с.

3. Іванченко Г.С. Квантовий штучний інтелект: перспективи та виклики. – Харків: Видавничий дім, 2022. – 256 с.

# ІОТ-ПРИСТРОЇ: ОСНОВНІ СИСТЕМИ УПРАВЛІННЯ

Крикливець В.В., Тимошенко Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Зі зростанням обсягів даних та складності сучасних обчислювальних систем питання надійності даних у розподілених системах стає критично важливим. Розподілені системи працюють у середовищі, де можлива втрата вузлів, мережеві збої та пошкодження даних, що вимагає застосування спеціальних методів для забезпечення їхньої цілісності та доступності. [1]

Одним із ключових методів підвищення надійності даних є реплікація, яка передбачає зберігання копій даних на кількох вузлах системи. Це дозволяє зменшити ризик втрати інформації в разі відмови окремих серверів або мережевих елементів. Популярні алгоритми, такі як Raft і Paxos, забезпечують узгодженість реплік у розподілених базах даних та файлових системах. [2]

Іншим підходом є використання алгоритмів виправлення помилок, зокрема кодування з перевіркою на парність (erasure coding), що дозволяє відновлювати втрачені фрагменти даних за допомогою спеціальних контрольних блоків. Це широко застосовується в хмарних сховищах, таких як Amazon S3 та Google Cloud Storage. Окрім цього, механізми розподілених журналів транзакцій гарантують, що жодна важлива операція не буде втрачена навіть у разі відмови окремих вузлів системи. [3]

Ще одним напрямом підвищення надійності є використання технологій блокчейну для створення незмінних записів, що забезпечує додатковий рівень захисту даних від модифікації та втрат. Крім того, застосування самовідновлюваних мережевих топологій та інтелектуальних балансувальників навантаження дозволяє покращити загальну стабільність системи.

**Метою доповіді** є аналіз сучасних методів підвищення надійності даних у розподілених системах, включаючи реплікацію, кодування з виправленням помилок та блокчейн-технології, а також оцінка їх ефективності в реальних умовах експлуатації.

**Список літератури**

1. Петренко В.О. Надійність розподілених обчислювальних систем. – Київ: Наукова думка, 2021. – 312 с.

2. Коваленко М.П. Алгоритми реплікації та узгодженості даних у розподілених середовищах. – Львів: Технологічний університет, 2022. – 278 с.

3. Іванченко Г.С. Методи виправлення помилок і збереження даних у хмарних технологіях. – Харків: Видавничий дім, 2023. – 256 с.

# МУЛЬТИАГЕНТНІ СИСТЕМИ ТА ЇХ ЗАСТОСУВАННЯ В ЛОГІСТИЦІ ТА ЕКОНОМІЦІ

Жигалка М.І., Сітніков В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних наукових дослідженнях обсяг даних, що генеруються в процесі експериментів і спостережень, постійно зростає. Це ускладнює їхню обробку та аналіз за допомогою традиційних методів, що вимагає застосування автоматизованих підходів.

Використання технологій машинного навчання, штучного інтелекту та розподілених обчислень дозволяє значно прискорити аналіз великих наукових даних, підвищуючи точність і ефективність отриманих результатів. [1]

Одним із ключових напрямів автоматизації є використання алгоритмів штучного інтелекту для обробки великих масивів даних у таких галузях, як біоінформатика, фізика високих енергій та астрономія. Наприклад, глибокі нейронні мережі застосовуються для аналізу геномних послідовностей, класифікації астрономічних об’єктів та моделювання кліматичних змін. Такі підходи дозволяють автоматично виявляти закономірності та знаходити нові наукові знання. [2]

Ще одним важливим аспектом є використання розподілених обчислювальних платформ, таких як Apache Hadoop та Spark, для обробки даних у реальному часі. Це дозволяє ефективно аналізувати великі обсяги інформації, що надходять із датчиків, телескопів та експериментальних установок.

Автоматизація аналізу таких даних дає змогу дослідникам швидше отримувати результати та приймати обґрунтовані наукові рішення. [3]

**Метою доповіді** є аналіз сучасних методів автоматизації аналізу великих даних у наукових дослідженнях, зокрема застосування штучного інтелекту, розподілених обчислень та алгоритмів візуалізації даних.

**Список літератури**

1. Ковальчук В.О. Штучний інтелект у наукових дослідженнях: алгоритми та застосування. – Київ: Наукова думка, 2021. – 280 с.

2. Павленко Д.М. Великі дані у біоінформатиці: методи та перспективи. – Львів: Технологічний університет, 2022. – 320 с.

3. Сидоренко Г.С. Розподілені обчислення для аналізу наукових даних. – Харків: Видавничий дім, 2023. – 265 с.

# ПРОЄКТУВАННЯ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ БУДІВЕЛЬНОГО ПІДПРИЄМСТВА

Мірза Д.С., Ляшенко Г.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

Проєктування інфокомунікаційної мережі підприємства є актуальним завданням для забезпечення безперебійного зв'язку між структурними підрозділами, оптимізації обміну інформацією та підвищення рівня кібербезпеки корпоративних даних.

У доповіді розглядаються сучасні підходи до аналізу вимог до мережевої інфраструктури, оптимізація топологічних рішень, а також впровадження технологій VLAN, динамічних протоколів маршрутизації та механізмів захисту (ACL, VPN, firewall) [1].

Метою роботи є розробка комплексної інфокомунікаційної мережі, що дозволяє забезпечити ефективну інтеграцію локальної мережі підприємства з глобальними інформаційними системами та високу стійкість до збоїв.

Для візуалізації та перевірки працездатності розробленої інфраструктури використовувався програмний засіб Cisco Packet Tracer, який дозволяє моделювати реальні мережеві середовища з використанням віртуального мережевого обладнання. За його допомогою було створено повноцінну модель мережі, налаштування маршрутизаторів, комутаторів та реалізацією політики безпеки.

Протестовано пропускну здатність каналів та оцінено поведінку мережі при зміні навантаження. Це дозволило підвищити надійність проекту та забезпечити можливість попереднього аналізу перед фізичним впровадженням.

У ході дослідження було проведено порівняльний аналіз традиційних та сучасних мережевих технологій з урахуванням специфіки діяльності будівельного підприємства. Практичне застосування розробленої методології сприятиме зниженню експлуатаційних витрат і підвищенню загальної ефективності роботи підприємства. Запропоноване рішення може бути адаптовано для інших компаній схожого профілю, що підтверджує універсальність обраного підходу [3].

**Список літератури**

1. Cisco Systems. Основи мережевих технологій. – URL: https://www.cisco.com/ (дата звернення: 10.03.2025).

2. Cisco Packet Tracer: посібник користувача. – М.: Cisco Networking Academy, 2023.

3. Антонюк А. О., Жора В. В. Теоретичні основи моделювання та аналізу систем захисту інформації: [монографія] / А. О. Антонюк, В. В. Жора. - Ірпінь Національний університет ДПС України, 2010. - 310 с.

# АНАЛІЗ МЕТОДІВ ГЕНЕРАЦІЇ СИНТЕТИЧНИХ ДАНИХ З ВИКОРИСТАННЯМ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ

Бабаніна А.О., Коваленко А.А., Ситник О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Постійне зростання досліджень, зосереджених на створенні синтетичних даних із великих мовних моделей (LLM), особливо для сценаріїв з обмеженою доступністю даних, впроваджує помітні зміни в генеративному штучному інтелекті (ШІ). Здатність використовувати ці дані на рівні з реальними даними робить цей підхід переконливим рішенням для проблем із низьким ресурсом. У цьому досліджені було розгляуто передові технології, які використовують ці гігантські LLM для генерації навчальних даних для конкретних завдань.

Метою цієї роботи є аналіз методології, методів оцінювання та практичного застосування. В роботі проаналізовано поточні обмеження та запропоновано потенційні шляхи для майбутніх досліджень.

Поява Transformer [1], а потім новаторські LLM, такі як GPT від OpenAI і BERT від Google, створили початок нової ери в розумінні та генерації мови. Нещодавно генеративні LLM розвинули цю еволюцію до нових висот, плавно поєднуючись із Generative AI і провіщаючи нову еру в сфері генерації синтетичних даних [2]. Початок Generative AI можна простежити до основних моделей, таких як Generative Adversarial Networks і Variation Autoencoders, які продемонстрували здатність створювати реалістичні зображення та сигнали. Однак справжній розвиток Generative AI почав лише з появою LLM в останні роки. Ці моделі, які навчалися на величезних наборах даних, продемонстрували безпрецедентну здатність створювати зв'язний і контекстуально релевантний текст, розсуваючи межі того, чого ШІ може досягти в завданнях, пов'язаних із мовою. Синтез Generative AI і LLM у сфері створення синтетичних даних є не просто технологічним прогресом, але й глибокою зміною парадигми в нашому підході до створення даних і навчання моделей ШІ.

В доповіді представлено деякі методи практичного навчання для навчання подальших моделей на основі синтетичних даних, припускаючи, що якість даних є невідповідною.

**Список літератури**

1. A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, L. Kaiser, and I. Polosukhin, "Attention is all you need," 2023

2. Rudenko O., Bezsonov O., Vashchenko K., Rutska S. Synthetic Dataset Generation for Efficient Neural Network Training. Proceedings of the 7th International Conference on Computational Linguistics and Intelligent Systems. 2023. Т. 3387. С. 146–159.

# СТВОРЕННЯ ВЕБЗАСТОСУНКУ ДЛЯ МОНІТОРИНГУ ПРИСТРОЇВ РОЗУМНОГО БУДИНКУ

Грінь Д.В., Ляшенко Г.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасний розвиток технологій Інтернету речей (IoT) відкриває нові перспективи для автоматизації керування пристроями розумного будинку [1]. Одним із ключових завдань у цьому процесі є забезпечення можливості моніторингу їхнього стану в режимі реального часу, що сприяє підвищенню загальної ефективності системи та дозволяє оперативно реагувати на зміни. Для досягнення цієї мети необхідне створення функціональних веб-інтерфейсів, які дадуть змогу користувачам не лише отримувати актуальну інформацію, а й керувати пристроями з максимальним комфортом.

Метою цього дослідження є розробка веб-додатку для моніторингу пристроїв розумного будинку. В роботі проведено аналіз існуючих технологій, які можна використати для створення веб-додатку та забезпечення взаємодії з пристроями. Розглядаються способи реалізації безпечного та стабільного зв'язку між сервером і пристроями, що дає змогу забезпечити надійну роботу системи та захист від потенційних загроз.

**У доповіді** розглянуто технології для створення веб-додатків, зокрема використання HTML5, CSS3, React.js для розробки клієнтської частини, використання бази даних MySQL для зберігання даних [2].

У ході роботи проаналізовано актуальні дослідження та технічну документацію, що дозволило вивчити актуальні підходи до створення веб-додатків для моніторингу пристроїв розумного будинку. Крім того, використовуються сучасні технології веб-розробки, які забезпечують ефективну взаємодію системи з пристроями та її подальшу оптимізацію.

Основні результати включають створення прототипу веб-додатку, що дозволяє ефективно взаємодіяти з пристроями розумного будинку, відстежувати їх стан та аналізувати отримані дані. Особливу увагу приділено застосуванню принципів WCAG 2.2 [3]. Моделювання роботи датчиків виконано з використанням платформи Tinkercad. Проведене тестування підтвердило ефективність запропонованого підходу.

**Список літератури**

1. IoT Applications for Smart Buildings: Use Cases and Benefits [Електронний ресурс] // Digi International. – Режим доступу: https://www.digi.com/blog/post/iot-applications-for-smart-buildings-use-cases-and

2. "Веб-технології та веб-дизайн: навчальний посібник" / О. Г. Трофіменко, О. Б. Козін, О. В. Задерейко, О. Є. Плачінда. – Одеса: Фенікс, 2019. – 284 с.

3. Understanding WCAG 2.2 [Електронний ресурс] // W3C Web Accessibility Initiative. – Режим доступу: https://www.w3.org/WAI/WCAG22/Understanding/intro

# АНАЛІЗ МЕТОДІВ ЗБІЛЬШЕННЯ ДАНИХ ДЛЯ ПОКРАЩЕННЯ КОНТРОЛЬОВАНОГО НАВЧАННЯ ПРИ ВИЯВЛЕНІ КІБЕРАТАК

Баєв І.С., Знайдюк В.Г., Волощук О.Б.
Харківський національний університет радіоелектроніки, Харків, Україна

Зростаюча складність кібератак вимагає розробки передових систем виявлення, здатних точно ідентифікувати та пом'якшувати потенційні загрози [1]. Це дослідження вирішує критичну проблему виявлення кібератак за допомогою комплексного підходу, який включає створення реалістичного, але незбалансованого набору даних, що моделює різні типи кібератак

Метою цього дослідження було дослідити та оцінити різні методи доповнення даних для підвищення ефективності моделей навчання під наглядом у виявленні кібератак. По-перше, запропоновано створити детальний набір даних, який відображає реальні умови мережевих вторгнень, імітуючи низку типів кібератак, гарантуючи, що він втілює типові дисбаланси, які спостерігаються під час справжніх загроз кібербезпеці. По-друге застосовано декілька методів розширення даних, зокрема SMOTE та ADASYN, щоб усунути перекос у розподілі класів, забезпечивши таким чином більш збалансований набір даних для навчання моделей машинного навчання з наглядом.

Застосування SMOTE та ADASYN було особливо ефективним у збільшенні кількості екземплярів у менших класах до тих, що знаходяться в більшості класів, підкреслюючи їхню здатність посилювати дисперсію всередині класу за допомогою генерації синтетичних зразків на основі подібності простору ознак між існуючими меншими зразками [2]. Подібним чином Borderline-SMOTE, зосереджуючись на зразках поблизу кордонів класів, рівномірно збільшив кількість класів меншин, потенційно сприяючи точності моделі в прикордонних випадках. Оцінка цих методів у різних моделях, таких як випадкові ліси та нейронні мережі, демонструє значні покращення можливостей виявлення. Крім того, аналіз також поширюється на дослідження важливості ознак, надаючи критичне розуміння того, які атрибути найбільш суттєво впливають на прогнозні результати моделей. Це не тільки покращує інтерпретативність моделей, але й допомагає уточнювати процеси розробки функцій і вибору для оптимізації продуктивності.

**Список літератури**

1. Ляшенко О.С., Великодний І.А., Знайдюк В.Г., Журило О.Д. (2024). Модель та методи виявлення широкомасштабної атакив середовищі IoT. Системи управління, навігації та зв'язку. 2024. No 1 (75). С 127-132 https://doi.org/10.26906/SUNZ.2024.1.127

2. Rudenko O., Bezsonov O., Vashchenko K., Rutska S. Synthetic Dataset Generation for Efficient Neural Network Training. Proceedings of the 7th International Conference on Computational Linguistics and Intelligent Systems. 2023. Т. 3387. С. 146–159.

# ОСНОВНІ ПІДХОДИ ДО ВИРІШЕННЯ ЗАВДАНЬ РОЗПІЗНАВАННЯ ТА АВТОПУНКТУАЦІЇ ТЕКСТУ

Потапов Р.О., Федорченко В.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Розпізнавання тексту включає кілька етапів: попередню обробку, сегментацію, класифікацію символів і постобробку. Традиційні методи засновані на алгоритмах обробки зображень, таких як бінаризація, видалення шуму, виділення контурів та сегментація символів, методи порівняння шаблонів дозволяють розпізнавати символи, але погано працюють з рукописним текстом та різними шрифтами. Методи машинного навчання включають класичні алгоритми (SVM, Random Forest) які використовуються для класифікації окремих символів, глибокі нейромережі (CNN, RNN), що дозволяють аналізувати зображення тексту як цілісний об'єкт. В теперішній час активно розвиваються сучасні нейромережові підходи, а саме: CRNN (поєднання згорткових та рекурентних мереж) – успішно застосовується в сучасних OCR-системах; Transformer-моделі, такі як TrOCR, що дозволяють розпізнавати текст у складних умовах (розмитість, спотворення) [1].

Автоматичне розміщення розділових знаків вимагає розуміння контексту, структури речення та мовних закономірностей [2]. Для визначення правила та лінгвістичних моделей застосовується аналіз морфології та синтаксису, що дозволяє виявляти місця, де можливі коми, крапки та інші знаки. Використовуються парсери та POS-тегери – для визначення структури речення. Для визначення структури та мовних закономірностей застосовують статистичні методи та моделі: N-грамні моделі – аналізують послідовності слів та обчислюють ймовірність постановки знака; байєсовські методи використовують ймовірнісні оцінки на основі великих текстових корпусів. Нейромережові підходи, а саме RNN, LSTM, GRU застосовуються для передбачення пунктуації на основі аналізу послідовностей. Transformer-моделі (BERT, T5, GPT) забезпечують високу точність, враховуючи контекст цілого документа. Sequence-to-sequence моделі вирішують завдання у форматі машинного перекладу. Сучасні системи часто поєднують традиційні методи з нейромережами. Наприклад, спочатку проводиться попередня розмітка тексту за допомогою правил, потім застосовується нейромережева модель для уточнення результатів.

**Список літератури**

1. Basic Principles of OCR with Image Processing Techniques. URL: https://algi.ai/basic-principles-of-ocr-with-image-processing-techniques/ – 01.02.2025.

2. Enhancing handwritten text recognition accuracy with gated mechanisms. URL: https://www.nature.com/articles/s41598-024-67738-8 – 10.03.2025.

# МЕТОДИ ВИКОРИСТАННЯ SPRING BOOT У ХМАРНИХ ОБЧИСЛЕННЯХ

Дмитренко В., Федорченко В.М.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасну епоху хмарних обчислень широко використовується повностековий застосунок – розробка як фронтенда (клієнтської частини), так і бекенда (серверної частини) веб-додатка. У таких додатках бекенд являє собою серце і суть програми. Без масштабованого рішення додаток не може бути розширено для задоволення сучасних потреб середовища хмарних обчислень.

Тому реалізація та системний дизайн бекенд-додатку мають бути ретельно продумані. Spring Boot - це надбудова над Spring, яка спрощує конфігурацію та розгортання додатків.

Основним його завданням є автоматизація процесу конфігурації, що дає змогу мінімізувати ручні налаштування та прискорити процес створення застосунку.

Тобто він надає готові шаблони для створення мікросервісів і веб-додатків, що робить його чудовим вибором для старту нових проєктів [1, 2].

Коли ми маємо справу з постійними змінами та проблемами, використання корисних інструментів є життєво важливим для створення безпечних та масштабованих серверних систем. Це дослідження зосереджується на використанні Spring Boot.

Spring Boot – це механізм для багатьох швидких розробок додатків, що складаються з різноманітних мікросервісних архітектур та різноманітних корпоративних систем.

Великими перевагами Spring Boot є мінімізація готової конфігурації та інтеграція з усім стеком Spring. Іншою користю є сильна підтримка сучасних способів упакування (наприклад, Docker) разом з управлінням (наприклад, Kubernetes), а також певний відомий набір інструментів (як-от Spring Security та Spring Data JPA).

Основною проблемою в розробці хмарних застосунків є велика складність коду, а саме великий обсяг стандартного коду, який з'являється при автоматизації багатьох процесів.

Звичайно ж використання декількох засобів таких як JPA (це Java Persistence API) разом із Spring Data для налагодження взаємодії з різними базами даних (зокрема PostgreSQL), значно покращує процес розробки.

Але це може привести до великого, майже безмежного росту думок на рівні доступу до даних, у такому вигляді науковий аналіз однозначно вказує на те, що коли автоматизація дещо зменшується, зокрема, обмежується використання створення запитів у Spring Data, створюються умови для помітного підвищення адаптивності та безпеки кожної спеціальної системи [3].

Ще однією важливою перевагою Spring Boot для розробки хмарних застосунків є управління залежностями.

У чистому Spring розробникам доводиться вручну додавати та керувати версіями залежностей, що може призвести до конфліктів.

Spring Boot вирішує цю проблему, надаючи попередньо налаштовані стартові залежності, які гарантують сумісність усіх бібліотек.

Наприклад, якщо взяти до уваги Spring Security, можна просто додати Spring Security Starter Dependency до вашого проекту та забезпечити захист від таких атак, як фіксація сеансу, клікджекінг, підробка міжсайтових запитів тощо, а також розширювану підтримку як для автентифікації, так і для авторизації та керування сеансами [4].

Spring Boot у поєднанні з Spring Security, Docker та Kubernetes стає сильним інструментом для створення великих та безпечних додатків.

Завдяки автоматичній налаштуванні розробники можуть швидко запускати моделі і відмінно впроваджувати структуру мікросервісів.

Проте надмірна залежність від шаблонного коду може ускладнити проект, так що збалансований підхід до автоматизації – наприклад обмеження використання авто-сгенерованих запитів в Spring Data – допомагає зберегти контроль над кодовою базою.

Використання наскрізного шифрування E2EE й інтегрованих механізмів Spring Security таких як OAuth2 та JWT забезпечує надійний захист даних і API , зберігаючи при цьому гнучкість в розробці.

Ще одна перевага Spring Boot є його здатність управляти залежностями що робить процес створення і підтримки додатків більш стабільними.

**Список літератури**

1. Спілке Лауренціу, “Spring Security in Action” | https://surl.li/uoyhsk . – 2024. – С. 480.
2. Spring і Spring Boot: основні відмінності та особливості використання // [Електроний ресурс] https://foxminded.ua/ru/razlichiya-mezhdu-spring-i-spring-boot/ Режим доступу 30.10.24
3. Greg L. Turnquist, “Learning Spring Boot 3.0: Simplify the development of production-grade applications using Java and Spring, 3rd Edition” | https://github.com/PacktPublishing/Learning-Spring-Boot-3.0-Third-Edition , 2022.
4. Moises Macero Garcia, Tarun Telang, “ Learn Microservices with Spring Boot 3: A Practical Approach Using Event-Driven | https://github.com/Book-Microservices-v3

# АНАЛІЗ МЕТОДІВ ГЛИБОКОГО НАВЧАННЯ ПРИ ОБРОБЦІ МЕДИЧНИХ ДАНИХ

Велікан В.О., Ляшенко О.С., Волощук О.Б.
Харківський національний університет радіоелектроніки, Харків, Україна

В рамках дослідженні запропонована інтеграція хмарних обчислень і технологій глибокого навчання для аналізу медичних даних, зосереджуючись на їх спільному впливі на надання медичної допомоги та інформації для пацієнтів. Завдяки аналізу прикладів впровадження в різних закладах охорони здоров'я можна зробити висновки, наскільки добре ці технології керують різноманітними джерелами медичних даних, такими як дані про переносні пристрої, дані медичних зображень та електронні медичні записи.

**Метою доповіді є** аналіз методів глибокого навчання при обробки медичних даних. Сучасні медичні процедури дедалі більше керуються аналітикою даних, обробкою великих обсягів інформації з різноманітних джерел [1]. Складність і експоненціальне збільшення даних охорони здоров'я виходять за рамки традиційних статистичних інструментів і вимагають складних обчислювальних методів, керованих інфраструктурою хмарних обчислень і глибоким навчанням. Глибоке навчання (DL), одна з підгалузей машинного навчання, змінило інтерпретацію медичних даних шляхом створення складних нейронних мереж, здатних обробляти й аналізувати великі обсяги даних. Інтеграція DL із хмарними обчисленнями ще більше розширила ці можливості, уможлививши обробку великомасштабних медичних даних у реальному часі та сприяючи більш доступним аналітичним рішенням у сфері охорони здоров'я [2].

Проведене дослідження демонструє значне покращення діагностичної точності (збільшення в середньому на 15–20%) та ефективності роботи (скорочення часу обробки на 60%) при використанні хмарних систем глибокого навчання. Це дослідження також виявило критичні проблеми: 40% реалізацій стикаються з проблемами інтеграції даних, а 5% — з порушеннями безпеки. Завдяки емпіричному аналізу в доповіді пропонуємо структуровану структуру реалізації, яка вирішує ці проблеми, зберігаючи високі стандарти продуктивності.

**Список літератури**

1. Ляшенко О.С., Велікан О.В., Волк Д.М. Проєктування моделі інформаційної системи для обробки великих даних в медичних установах. Проблеми інформатизації: дванадцята міжнародна науково-технічна конференція. 21–22 листопада 2024 р. – Баку–Харків–Бельсько-Бяла, 2024. – Т. 2. – С. 99.

2. Vyshnivskyi Daniil Система оцінка пози людини з використанням алгоритмів глибокого навчання / Daniil Vyshnivskyi, Oleksii Liashenko, Nataliia Yeromina // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2023. – Т. 2 (72). – С. 75-79. – doi:https://doi.org/10.26906/SUNZ.2023.2.075.

# АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО ОПТИМІЗАЦІЇ УПРАВЛІННЯ ЕНЕРГІЄЮ В МІКРОМЕРЕЖАХ З УРАХУВАННЯМ НЕВИЗНАЧЕНОСТЕЙ

Демиденко Д.В., Колтун Ю.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Із зростанням ролі відновлюваних джерел енергії та необхідністю децентралізованого управління споживанням енергії, мікромережі стали об'єктом активного дослідження. Проте основним викликом для ефективного управління мікромережею залишається наявність невизначеності — у прогнозах генерації, поведінці споживачів, цінах на електроенергію, стані здоров'я обладнання. В [1] пропонується системний огляд технік, які дозволяють інтегрувати ці невизначеності в системи енергоменеджменту.

**Мета доповіді** є систематизація сучасних підходів до моделювання невизначеності та аналіз відповідних оптимізаційних алгоритмів в умовах реального часу для підвищення ефективності мікромереж.

Провівши літературний аналіз, можна зазначити, що підхід охоплює широке коло аспектів, пов'язаних із невизначеністю в енергетичних системах. Потрібно приділити особливу увагу класифікації джерел невизначеності та відповідним методам їх формалізації. Зокрема в роботі, акцент зроблено на необхідності точного відображення статистичних і динамічних характеристик, притаманних об'єктам енергетичної інфраструктури. Це включає як природні фактори (сонячна радіація, швидкість вітру, температура), так і поведінкові аспекти (споживчий попит, графіки використання електромобілів), що потребують застосування різнорідних моделей – від імовірнісних до нечітких або детермінованих.

Значну увагу в доповіді приділяється методологічному підґрунтю побудови моделей – як в умовах наявності великих обсягів історичних даних, так і в ситуаціях обмеженої інформації. Такий підхід дозволяє не лише підвищити точність прогнозів, а й забезпечити стійкість роботи мікромереж у реальному часі.

Запропоновані техніки оптимізації – стохастичне програмування, робастна оптимізація, модельно-прогнозне управління, мультипараметричне програмування та методи машинного навчання, які адаптуються до різних контекстів застосування, зокрема до оперативного управління або стратегічного планування.

**Список літератури**

1. Cabrera-Tobar, A.; Massi Pavan, A.; Petrone, G.; Spagnuolo, G. A Review of the Optimization and Control Techniques in the Presence of Uncertainties for the Energy Management of Microgrids. Energies 2022, 15, 9114. https://doi.org/10.3390/en15239114

# СИСТЕМА КЛАСИФІКАЦІЇ ОБ'ЄКТІВ НА ЗОБРАЖЕННЯХ З ВИКОРИСТАННЯМ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ

Климова І.М., Стукота О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні інформаційні системи дедалі частіше функціонують в умовах інтенсивного зростання обсягів візуальних даних, які надходять із численних джерел: камер спостереження, медичних приладів, безпілотних систем, супутникових платформ тощо. Одним із фундаментальних завдань у таких умовах є автоматична класифікація об’єктів на зображеннях. Це зумовлює потребу в дослідженні алгоритмічних рішень, що здатні забезпечити високу точність і адаптивність обробки візуального контенту. Задача класифікації зображень передбачає розпізнавання об’єктів у середовищі, для цього існує багато інструментів. Серед таких рішень ключову роль відіграють штучні нейронні мережі [1], насамперед згорткові.

**Метою доповіді** є аналіз архітектур нейронних мереж, які забезпечують адаптивну класифікацію об'єктів на зображеннях із урахуванням особливостей реальних задач, таких як обмеженість обчислювальних ресурсів, необхідність обробки в реальному часі та наявність перекривань між класами.

У доповіді наведено результати експериментального навчання нейронних моделей на відкритих наборах зображень (були використані CIFAR-10, ImageNet). Аналіз показує, що на якість класифікації істотно впливають тип архітектури, розмір вибірки, спосіб аугментації, а також параметри регуляризації. Встановлено, що особливо важливим є дотримання балансу між глибиною мережі та обсягом навчальних даних. Використання процедури спостереження за динамікою змін у процесі навчання моделі свідчить про нелінійний і нестаціонарний характер цього процесу.

Таким чином, система класифікації об’єктів на зображеннях, побудована на основі штучних нейронних мереж, є складною динамічною структурою, функціонування якої визначається великою кількістю внутрішніх параметрів і взаємодією між рівнями поступового перетворення «сирих» піксельних даних на зображенні у більш абстрактні та інформативні ознаки. Вивчення таких систем потребує поєднання математичного моделювання, глибокого експериментального аналізу та постійного удосконалення навчальних методів у контексті новітніх досліджень в галузі штучного інтелекту.

**Список літератури**

1. Flach P. A. Machine Learning: The Art and Science of Algoritms that Makes Sense of Data. Cambridge: Cambridge University Press. 2012. 291 p. https://doi.org/10.1017/CBO97805119730002.

# СИСТЕМА ЗБЕРІГАННЯ ТА АНАЛІЗУ ДАНИХ

Климова І.М., Шмарін М.Д.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних умовах стрімкого зростання обсягів цифрової інформації критичною задачею стає ефективне зберігання та обробка великих обсягів даних, що надходять з різноманітних джерел: сенсорних мереж, інформаційних систем підприємств, онлайн-сервісів тощо [1]. Здатність своєчасно накопичувати, структуровано зберігати й аналітично опрацьовувати ці дані визначає конкурентоспроможність організацій та якість прийнятих управлінських рішень. У зв'язку з цим побудова комп'ютерних систем, здатних забезпечити надійне зберігання й високопродуктивний аналіз даних, є важливою науково-технічною проблемою.

**Метою доповіді** є висвітлення архітектурних принципів побудови комп'ютерної системи, призначеної для тривалого зберігання та обробки великих обсягів даних [2]. Зокрема, досліджені методи організації розподіленого зберігання, балансування навантаження та застосування інструментів аналізу з використанням паралельних обчислень.

У доповіді наведено результати впровадження гібридного сховища даних на базі HDFS та обчислювального кластеру Spark, що використовується для обробки логів клієнтських запитів і фінансових транзакцій. Аналіз показав, що використання схеми розподілу даних із попередньою фільтрацією суттєво знижує затримку при виконанні аналітичних запитів і дозволяє досягти масштабування системи без істотного зниження продуктивності.

Важливим компонентом є впровадження механізмів резервного копіювання та індексації, що гарантують як відмовостійкість системи, так і прискорене виконання складних запитів. Зокрема, у випадку використання Elasticsearch для аналізу логів за часовими мітками забезпечено продуктивність до 100 тис. запитів/хв на одному вузлі.

Таким чином, сучасна комп'ютерна система для зберігання та аналізу даних виступає як інтегрована платформа, що поєднує засоби горизонтального масштабування, адаптивного кешування, обробки даних у реальному часі й можливості когнітивного аналізу.

**Список літератури**

1. Marz, N., Warren J. Big Data: Principles and best practices of scalable real-time data systems. Manning Publications, 2021. P. 328.

2. Guller M. Big Data Analytics with Spark: A Practitioner's Guide to Using Spark for Large Scale Data Analysis. Apress, 2020. P. 235.

# ПРОГРАМНІ ЗАСОБИ МОНІТОРИНГУ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Климова І.М., Колобаєв Н.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Інформаційні системи сучасного покоління характеризуються високим ступенем динамізму, розподіленою архітектурою та великою кількістю взаємодіючих компонентів, що функціонують в умовах непередбачуваних змін навантаження. У таких умовах підвищується ймовірність виникнення критичних збоїв або аномалій у роботі окремих елементів системи. Тому дослідження засобів моніторингу стану інформаційної системи, а також розробка ефективних механізмів виявлення та аналізу відхилень у її роботі є актуальною науково-практичною проблемою [1]. Із зростанням складності програмних і апаратних компонентів системи виникає потреба у створенні високоточних інструментів контролю. Застосування таких програмних засобів дозволяє здійснювати превентивне реагування.

**Метою доповіді** є дослідження механізмів реалізації інструментів моніторингу інформаційної системи, зокрема з урахуванням властивостей багаторівневої архітектури та розподіленої обробки подій. Аналіз охоплює як традиційні підходи (логування, збирання метрик), так і сучасні концепції, пов’язані з застосуванням агентських систем, машинного навчання та когнітивного аналізу поведінкових моделей [2]. У доповіді наведено результати застосування таких програмних систем, як Zabbix, Nagios, Prometheus та ELK Stack, для моніторингу навантаження на сервери, аналізу пропускної здатності мереж, відстеження стану віртуальних машин і контейнеризованих середовищ. Показано, що ефективність виявлення аномалій істотно залежить від частоти збору даних, способу їх агрегування та застосованих методів кореляційного аналізу.

Таким чином, програмні засоби моніторингу не лише забезпечують видимість внутрішніх процесів інформаційної системи, але й створюють базу для прийняття рішень щодо її оптимізації, масштабування та підвищення стійкості до збоїв.

**Список літератури**

1. Ling Gao-yuan and Zhu Lin, 2016. Design and Implementation of the Internet Traffic Monitoring and Control Software. COMPUTER ENGINEERING&SOFTWARE. 37, 7 (Jan. 2016), 48-52.

2. Khandani A. E., Kim A. J., Lo A. W. Consumer credit-risk models via machine-learning algorithms. Journal of Banking & Finance, Elsevier, Vol. 35(11), 2019. p. 2767–2787.

# СЕКЦІЯ 4
# БЕЗПЕКА ФУНКЦІОНУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

**Керівник секції**: д.т.н., проф. О. А. Смірнов, ЦНТУ, Кропивницький
**Секретар секції**: к.т.н., доц. О. В. Сєвєрінов, ХНУРЕ, Харків

## THE ROLE OF MATHEMATICAL MODELLING IN INFORMATION SECURITY

Agayeva U.H.
Military İnstitute named after H. Aliyev, Baku, Azerbaijan,
Haqverdiyeva Z.H.
Fugro Gb (North) Marıne Lımıted, Aberdeen, Scotland

Mathematical modeling of information security involves the application of various mathematical approaches and algorithms to ensure the protection of information system security. In the field of information security, the development of a mathematical model of information security is one of the main stages in order to protect the confidentiality, integrity and other various security risks and vulnerabilities of the system [1].

Mathematical modelling, which describes and analyzes systems and processes with mathematical formulas, helps to better understand information security from a theoretical and practical perspective and to find and develop the most optimal security solutions [5-9]. Protecting the state's information resources from natural and man-made threats is one of the important priorities of national security. The importance of information security was felt more clearly during the second Karabakh war [10]. The enemy, taking advantage of the opportunity to change public opinion in the international community in its favor by using information technologies, was drawing attention to itself and presenting itself as the wronged party. According to the famous strategist and military analyst John Boyd, who coined the phrase "He who has the best information wins," the side that obtains the best information and uses it quickly and effectively gains an advantage in wars and strategic struggles. The Tavush bot operation conducted by Azerbaijan against information warfare interfered with the enemy's information sources through social media bots and supported the provision of authentic information to the Armenian side [11].

Mathematical models are applied to investigate and improve the most effective methods for optimizing the performance of bots [5]. For example, if the interactions in networks where bots communicate are represented using graph theory and Markov chains, probability theory is applied to estimate the likelihood of the bot achieving the best result and its repetition. Markov chains or hierarchical models are applied to natural language processing (NLP) technologies in modeling

bot interactions with users. Mathematical models that determine how effectively bots work are implemented using decision theory. Machine Learning algorithms are used to improve decision-making ability and optimize their performance [2].

Michael E. Whitman and Herbert J. Mattord, renowned US experts in the field of information and cybersecurity, discussed the mathematical models used to identify and protect against bots in their book "Principles of information security."

To detect the simplest anomalies, t-test, k-nearest neighbors algorithm [4], machine learning, CAPTCHA model (Completely Automated Public Turing test to tell Computers and Humans Apart) [3] , which presents mathematical or logical tasks to distinguish humans from bots. CAPTCHA mathematical model is generally based on the principles of distortion and image manipulation, simple mathematical operations, image and object recognition, and voice commands.

Naive Bayes algorithm helps to distinguish between bot and human activities based on probabilities. This algorithm is particularly used to detect spam emails and other malicious behavior. In the Naive Bayes model, the probability of which class an object belongs to is calculated based on Bayes' theorem. Analysis of various mathematical models allows to increase the effectiveness of bots, prevent them or redirect them in a positive way. Also, combining these models helps to identify threats more effectively and protect against them. Although the applied model shows satisfactory results, higher efficiency can be achieved by searching for new optimal options. Research on mathematical models that provide risk reduction, more optimal resource management, and increased system reliability is ongoing.

**References**

1. Aghayeva U.H. Hacker attacks and their consequences. // -Baku: “Proceedings of scientific works”, 2015, №1(24), 35-38.

2. David W. Aha, Dennis Kibler, and Marc K. Albert. 1991. Instance-based learning algorithms. Mach. Learn. 6, 1 (1991), 37-66.

3. Darko Brodic, Alessia Amelio.The CAPTCHA: perspectives and challenges in artificial intelligence, 2019, 128, 123 p.

4. Padraig C., Sarah J. D. k-Nearest Neighbour Classifiers.ACM Computing Surveys, Volume 54, Issue 6, Article No.: 128, Pages 1 – 25, 2021.

5. Hashimov, E.G., Talibov, A.M., Gasanov, A.Q. Mathematical modeling of military systems. Textbook. -Baku: Military publishing house, -2018. -266 p.

6. Piriyev H. K. et al. Modelling of the battle operations //Monograph. Baku: Military publishing house. – 2016. – 256 p.

7. Nasibov Y. A. et al. Modelling of the rationally deployment of observing systems // Сучасні інформаційні системи. – 2019. – №. 3, № 2. – С. 10-13.

8. Piriyev H.K. et al. Some issues of pedagogical staff training for special-purpose higher education institutions // Military knowledge, 2014, No. 4, p. 3-9.

9.Agayev S.O. et al. Modern pedagogical technologies in military education. Textbook. Part I. // - Baku: Military Publishing House, 2016, 152 p.

10. Piriyev, H.K., Hashimov, E.G. The Second Karabakh War: military-political and military-technical aspects // - Baku: Proceedings of the Military Institute named after Heydar Aliyev, - 2023. No. 1 (40). - p. 7-16.

11. https://hit.az/az/olke/216070/prezident-mukafatcisi-ferid-perdesunas-kimdir/

# APPLICATIONS OF GENERATIVE AI AND LARGE LANGUAGE MODELS IN NETWORK AND CLOUD SECURITY

Nadtochyi M.M., Balagura D.S.
Kharkiv National University of Radioelectronics, Kharkiv, Ukraine

The cybersecurity landscape is undergoing a significant transformation with the emergence of generative artificial intelligence (AI) and Large Language Models (LLMs). These technologies present a dual-edged sword, offering unprecedented opportunities to enhance network and cloud security while simultaneously introducing new and sophisticated threats. Scientific research indicates that generative AI can bolster defenses through advanced intrusion and anomaly detection, proactive vulnerability testing, and the simulation of complex attack scenarios [1]. LLMs, with their proficiency in natural language processing, are proving invaluable in areas such as phishing detection, malware analysis, and automated threat intelligence gathering [2]. The commercial sector is rapidly integrating these AI innovations into security products, promising enhanced threat detection, automated response capabilities, and more intuitive security operations.

**The aim of the paper** is to analyze theory and practice of GenAI and LLM applications in network and cloud security.

The scientific exploration of generative AI in network security consistently reveals its dual potential. While it significantly enhances defensive capabilities, it also presents a powerful tool that can be leveraged by attackers. This creates a continuous cycle of innovation, often referred to as a cybersecurity "arms race", where advancements in defensive AI are met by increasingly sophisticated AI-driven attacks

Generative AI, using models like Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs), enhances intrusion detection by simulating attacks and identifying anomalies. LLMs are used in detecting phishing attempts, analyzing malware, and automating threat intelligence. They offer sophisticated analysis and automate responses, improving security posture. In cloud environments, generative AI automates security controls and enhances threat detection.

The future of cybersecurity will be shaped by the ongoing interplay between AI-powered threats and defenses, and organizations that embrace a forward-thinking and adaptive security strategy will be best positioned to thrive in this dynamic environment.

**References**

1. Generative AI in cybersecurity, Capgemini Research Institute (2024) https://www.capgemini.com/insights/research-library/generative-ai-in-cybersecurity/

2. Kasri, W., Himeur, Y., Alkhazaleh, H. A., Tarapiah, S., Atalla, S., Mansoor, W., Al-Ahmad, H. (2025) From Vulnerability to Defense: The Role of Large Language Models in Enhancing Cybersecurity DOI: https://doi.org/10.3390/computation13020030

# COMPARATIVE CHARACTERISTICS OF WAVE AND RYDE IN THE TERMS OF SECURITY AND PERFORMANCE

Telnova A.A., Hrinenko T.O.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

The development of quantum computers threatens modern cryptographic algorithms. Post-quantum digital signature (PQDS) algorithms have been developed to provide cryptographic security in the face of quantum computers that can break traditional cryptographic algorithms. In 2022, the National Institute of Standards and Technology launched an additional selection stage for PQDS standardization, choosing 40 candidates. This paper discusses algorithms based on common classes of PQDS problems, including code-based cryptosystems and multi-party computing (MPC) protocols.

**The purpose of this paper** is to study and compare code-based and MPC signatures on the example of WAVE and RYDE digital signatures, which will serve as a basis for further analysis of these digital signature mechanisms.

**The paper presents** the results of a comparative analysis of the WAVE and RYDE algorithms in terms of their foundations, performance and data size, and algorithmic resistance to attacks. In particular, it was found that the WAVE algorithm is based on lattice theory and uses a noise coding method to protect against attacks [1], while the RYDE algorithm is based on error-corrected codes [2] and offers a compromise between security and performance. The performance of both algorithms was also investigated in the context of key generation and signature creation and verification, where RYDE had smaller key and signature sizes and faster key generation compared to WAVE, but WAVE provided a higher level of security. Both algorithms demonstrated high resistance to classical and quantum attacks. However, WAVE is better protected against denial-of-service (DoS) attacks, while RYDE is optimized for running on devices with limited resources.

The results of the study show that WAVE is a promising solution for highly secure systems such as government and military applications. RYDE, in turn, is more optimal for commercial applications that require speed and efficient use of resources.

**References**

1. Gustavo Banegas, Kévin Carrier, André Chailloux, Alain Couvreur, Thomas Debris-Alazard, Philippe Gaborit, Pierre Karpman, Johanna Loyer, Ruben Niederhagen, Nicolas Sendrier, Benjamin Smith, Jean-Pierre Tillich. WAVE Specification Document. 2023. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/wave-spec-web.pdf.

2. Nicolas Aragon, Magali Bardet, Loïc Bidoux, Jesús-Javier Chi-Domínguez, Victor Dyseryn, Thibauld Feneuil, Philippe Gaborit, Antoine Joux, Matthieu Rivain, Jean-Pierre Tillich, Adrien Vinçotte. RYDE Specification Document. 2023. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/ryde-spec-web.pdf

# АНАЛІЗ ВЛАСТИВОСТЕЙ ДЕТЕРМІНОВАНОГО ЦИФРОВОГО ПІДПИСУ В ГРУПАХ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ ІЗ ОНОВЛЕНОГО СТАНДАРТУ

Мельникова О.А., Грасмік С.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Серед суттєвих змін в оновленому стандарті ЦП (цифрового підпису) [1] — нові механізми формування детермінованого варіанту підпису, а також можливість використання еліптичних кривих Едвардса, які досить давно використовуються у відомих бібліотеках та додатках [2].

**Метою доповіді** є аналіз властивостей та особливостей реалізації детермінованого варіанту цифрового підпису. **В доповіді** розглянуто переваги та недоліки використання детермінованого підпису, у порівнянні з недетермінованим варіантом, а також особливості його ефективної програмної реалізації. Попередні версії стандарту визначали тільки недетермінований ЦП, однією з переваг якого є можливість використання передпідписів $\{k_i^{-1} \bmod n, r_i\}$. Що потенційно дозволяє реалізовувати розширений варіант передпідписів $\{k_i^{-1} \bmod n, r_i, \ d \cdot r_i \bmod n\}$ для зменшення обчислювальної складність основного етапу формування ЦП [3], що важливо при використанні в режимі реального часу.

Детермінований ЦП не передбачає використання передпідписів через те, що формування конфіденційного сеансового значення $k_i$ залежить від особистого конфіденційного ключа $d$ автора підпису та від геш-значення $H(M)$ інформації $M$, що підписується. Тоді як в недетермінованому варіанті $k_i$ формується на основі генерування унікальної випадкової / псевдовипадкової послідовності бітів. Таким чином, перевагою детермінованого алгоритму є те, що його реалізація не потребує використання сертифікованого криптографічно сильного генератору випадкових / псевдовипадкових послідовностей бітів. Якісна реалізація якого, в ідеалі, має включати не тільки сертифіковані варіанти алгоритмів, а й апаратну підтримку (для створення саме випадкових, а не псевдовипадкових послідовностей). Завдяки тому, що конфіденційне сеансове значення $k_i$ є функцією від інформації, що підписується, та особистого конфіденційного ключа $d$ автора підпису, маємо детерміноване відображення інформації, що підписується, в цифрові підписи. При цьому відпадає необхідність контролювати унікальність та якість статистичних властивостей значень $k_i$ для забезпечення стійкості ЦП до криптографічних атак, які можуть використовувати недостатню випадковість $k_i$ для підробки ЦП або навіть розкриття особистого ключа $d$ автора підпису (як згадується в самому стандарті).

Для детермінованого ЦП передбачається формування $k_i$ на основі алгоритму HMAC_DRBG [4, 5]. При цьому, в якості внутрішньої допоміжної геш-функції для HMAC_DRBG, рекомендовано використовувати в точності той самий варіант сертифікованого криптографічно стійкого алгоритму гешування (FIPS 202, FIPS 180-4), що й в основному алгоритмі формування

ЦП. Початкові значення для HMAC_DRBG формуються на основі конкатенації значень $d$ та $H(M)$, представлених рядками у вісімковий системі подання. Крім того, за основним алгоритмом формування підпису, діапазон значень $k_i$ обмежується простим порядком $n$ базової точки, що може викликати повторні ітерації основного циклу алгоритму HMAC_DRBG для створення значень-кандидатів $k_i$ у випадках $k_i \notin [1, n-1]$.

За варіантом [5] алгоритму HMAC_DRBG дозволяється застосовувати повторні ітерації ще й при отриманні на основі поточного $k_i$ першого компоненту підпису $r_i = 0$. Тобто до циклу формування значень-кандидатів $k_i$ включаються ще й розрахунки першого компонента $r_i$ підпису: визначення афінної координати $x_R$ точки $R = [k_i]G = (x_R, y_R)$, перетворення $x_R$ на елемент базового поля $r_i$ та перевірку $r_i \neq 0$. Проблемним моментом є те, що детермінованість значення $k_i$ для певної інформації $M$, що підписується, теоретично може привести до формування другого компоненту цифрового підпису $s_i = 0$. Статистично така ситуація є вкрай малоймовірною. Але, за її виникнення, алгоритм формування підпису повертає помилку. Теоретично, цієї ситуації можна уникнути при включенні перевірки $s_i = 0$ в умови повторних ітерацій формування значень-кандидатів $k_i$., але в стандарті такий варіант не розглядається.

Згідно до своїх властивостей, детермінований алгоритм підпису може надати перевагу при реалізації ЦП для пристроїв, які не дозволяють підтримувати криптографічно стійкий генератор випадкових послідованостей з певних технічних обмежень або через високу вартість розробки.

**Список літератури**

1. National Institute of Standards and Technology (2023) Digital Signature Standard (DSS). (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 186-5. DOI: https://doi.org/10.6028/NIST.FIPS.186-5

2. Мельникова О. А., Джурик О. В., Маслєннікова А. О. Еліптичні криві Едвардса. Порівняння криптографічних бібліотек // Радіотехніка. — 2018. — №. 195. — С. 41 - 45. DOI: https://doi.org/10.30837/rt.2018.4.195.05

3. Мельникова О.А., Польовий О.А. Аналіз обчислювальної складності варіантів передпідписів за стандартами ЦП в групах точок ЕК [Текст] // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тези доп. 14-ї міжнар. наук.-техн. конф., 25-26 квітня 2024 р., Баку–Харків–Жиліна : [у 2 т.]. Т. 2 : секція 3-6 / Нац. ун-т оборони Азербайджанської Республіки [та ін.]. — Харків : Impress., 2024. — С. 50. DOI: https://doi.org/10.32620/ICT.24.t2

4. Barker EB, Kelsey JM (2015) Recommendation for Random Number Generation Using Deterministic Random Bit Generators. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-90A, Rev. 1. DOI: https://doi.org/10.6028/NIST.SP.800-90Ar1

5. Pornin T (2013) Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA). (Internet Engineering Task Force (IETF)), IETF , Request for Comments (RFC) 6979. DOI: https://doi.org/10.17487/RFC6979

# ОСОБЛИВОСТІ ВИКОРИСТАННЯ ЕЛІПТИЧНИХ КРИВИХ ЕДВАРДСА В ОНОВЛЕНОМУ СТАНДАРТІ ЦИФРОВОГО ПІДПИСУ

Мельникова О.А., Олійник Е.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Еліптичні криві (ЕК) Едвардса, які до оновленого стандарту цифрового підпису (ЦП) [1] було додано лише в 2023 році, досить давно використовуються у багатьох відомих криптографічних бібліотеках [2, 3], а також у популярних додатках (зокрема, для реалізації автентифікації користувачів).

**Метою доповіді** є аналіз властивостей, переваг, а також особливостей програмної реалізації алгоритмів ЦП із використанням ЕК Едвардса. **В доповіді** також розглянуто зв'язок специфіки реалізації базових операцій з точками ЕК Едвардса та стійкістю алгоритмів (зокрема, до атак за побічними каналами). В алгоритмах ЦП на еліптичних кривих Едвардса використовуються скручені криві Едвардса з параметрами Ed25519 та Ed448 [4], які забезпечують рівні криптографічної стійкості приблизно еквівалентні 128-бітовому та 224-бітовому значенням, відповідно.

Поточна версія стандарту пропонує лише детерміновані варіанти ЦП із використанням ЕК Едвардса, хоча є припущення щодо можливого подальшого доповнення недетермінованою версією підпису. Під детермінованістю мається на увазі, що при формування підпису використовується унікальне значення, сформоване з ґеш-значення від особистого конфіденційного ключа автора підпису та самої інформації, що підписується. Порівнюються два детерміновані варіанти ЦП: HashEdDSA (підписується ґеш-значення від інформації) та EdDSA (підписується безпосередньо сама інформація). Перший варіант, як вважається, є більш вразливим до можливих колізій ґеш-значень.

**Список літератури**

1. National Institute of Standards and Technology (2023) Digital Signature Standard (DSS). (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 186-5. DOI: https://doi.org/10.6028/NIST.FIPS.186-5

2. Мельникова О. А., Джурик О. В., Маслєннікова А. О. Еліптичні криві Едвардса. Порівняння криптографічних бібліотек // Радіотехніка. — 2018. — №. 195. — С. 41 - 45. DOI: https://doi.org/10.30837/rt.2018.4.195.05

3. Мельникова О. А., Джурик О. В., Масленникова А. О. Аналіз криптографічних бібліотек, які підтримують еліптичні криві Едвардса [Текст] // Проблеми інформатизації: тези доп. 6-ї міжнар. наук.-техн. конф. / Черк. держ. технолог. ун-т [та ін.]. — Харків : Петров В. В., 2018. — С. 14-15. URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/41370

4. Chen L, Moody D, Regenscheid A, Robinson A, Randall K (2023) Recommendations for Discrete-Logarithm Based Cryptography: Elliptic Curve Domain Parameters. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-186. https://doi.org/10.6028/NIST.SP.800-186

# ПРОБЛЕМАТИКА ЗАХИСТУ ІНФОРМАЦІЇ У ВЕБ-СЕРВІСАХ

Малярова Д.М., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна
Нарєжній О.П.
Харківський національний університет імені В. Н. Каразіна, Харків, Україна

Веб-сервіси стали ключовими інструментами обміну даними, організації бізнес-процесів і комунікації. Разом із цим зростає кількість кіберзагроз, що спрямовані на несанкціонований доступ до інформації, її модифікацію чи знищення. Надійний захист даних у веб-сервісах є критично важливим аспектом кібербезпеки.

Сучасні веб-сервіси обробляють значний обсяг персональних, фінансових та корпоративних даних, що робить їх привабливою мішенню для кіберзлочинців. Найпоширенішими атаками залишаються SQL-ін'єкції, міжсайтовий скриптинг (XSS), підробка міжсайтових запитів (CSRF), MITM, атаки грубої сили, DDoS-атаки, а також Broken Authentication [1, 2].

Основними причинами існування вразливостей є нехтування принципами безпечної розробки, відсутність тестування, застарілі бібліотеки, слабке шифрування та контроль доступу.

Враховуючи вищесказане, для безпеки веб-сервісів необхідно [3]:

– застосовувати тестування SAST, DAST і Fuzzing;

– впроваджувати багатофакторну автентифікацію, TLS, HMAC;

– перевіряти налаштування серверів та середовища, регулярно оновлювати ПЗ, використовувати сканери (Burp Suite, OWASP ZAP);

– використовувати контроль доступу (RBAC), WAF;

– навчати персонал цифровій безпеці та реагуванню на інциденти.

Через еволюцію загроз, адаптування зловмисників та вдосконалення методів атак, ефективний захист веб-додатка вимагає комплексного підходу. В доповіді надані результати аналізу та оцінки ефективності існуючих захисних механізмів, рекомендації щодо поліпшення безпеки веб-сервісів.

У підсумку, безпека веб-сервісів – це технічне і організаційне питання, де поєднуються технології управління ризиками, освітні практики та постійний моніторинг нових загроз. Такий підхід забезпечує безпеку веб-сервісів, зменшує ризик кіберзагроз та підвищує довіру користувачів.

**Список літератури**

1. Васильченко Д.І., Лавровський І.М. Огляд типових уразливостей web-сайтів організацій у 2019-2020 році. Сучасний захист інформації. 2021. №1(45). С. 41-46.

2. Lysakov V., Sievierinov O., Taran I. Security of Web Applications Using AWS Cloud Provider // Computer and Information Systems and Technologies (2021).

3. Кравчук Н. В., Коробейнікова Т.І. Огляд проблематики захищеного доступу до вебсерверів. Вісник Львівського державного університету безпеки життєдіяльності. 2024. № 30. С. 78-89.

# АВТОМАТИЗОВАНИЙ ЗАСІБ АНАЛІЗУ ПРОТОКОЛІВ AVISPA

Рой Є.О., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному світі інформаційна безпека постає як один з ключових викликів, з якими стикаються організації, державні структури та звичайні користувачі. Для гарантування необхідного рівня захисту інформації надзвичайно важливим є аналіз криптографічних та комунікаційних протоколів на предмет слабких місць і потенційних атак. Однією з найефективніших систем автоматизованого аналізу безпеки протоколів є AVISPA (Automated Validation of Internet Security Protocols and Applications).

AVISPA – це інструмент, призначений для автоматизованого аудиту захищеності криптографічних та комунікаційних протоколів. Він використовує формальні методи для моделювання та подальшого аналізу протоколів. Це дозволяє виявляти потенційні вразливості ще на стадії розробки, що суттєво зменшує ймовірність їхнього експлуатування в реальних системах. Процес використання AVISPA складається з кількох етапів: від специфікації протоколу, використовуючи мову HLPSL, до застосування одного з вбудованих аналізаторів задля перевірки безпеки [1, 2].

Ключовими перевагами AVISPA є автоматизація аудиту безпеки, висока швидкість аналізу та здатність виявляти різноманітні атаки. З іншого боку, є й певні недоліки, наприклад, труднощі з моделюванням надто складних протоколів, чи нездатність оцінити всі потенційні загрози у деяких сценаріях.

В доповіді надані результати аналізу та дослідження потенціалу та специфіки використання AVISPA для аналізу криптографічних та комунікаційних протоколів, і як приклад застосування AVISPA, надані результати аналізу безпеки протоколу TLS.

Отже, AVISPA є потужним інструментом для автоматизованого аналізу безпеки криптографічних та комунікаційних протоколів. Його функціонал дає змогу зменшувати вірогідність появи вразливих протоколів у реальних інформаційно-комунікаційних системах, що вкрай важливо для сьогоденної інформаційної безпеки. Завдяки використанню формальних методів та багатьох аналізаторів, зокрема на основі моделювання, обмежень логіки, AVISPA може стати незамінним помічником при розробці та тестуванні нових мережевих протоколів.

**Список літератури**

1. AVISPA v1.0 User Manual. AVISPA Team. 2006. URL: https://people.rennes.inria.fr/Thomas.Genet/Crypt/AVISPA_manual.pdf.

2. F. Kammuller. Verification with AVISPA to Engineer Network Security Protocols. *International Journal on Advances in Security*. 2012. No. 3,4. P. 112-120. URL:https://personales.upv.es/thinkmind/dl/journals/sec/sec_v5_n34_2012/sec_v5_n34_2012_4.pdf

# ВІДПОВІДНІСТЬ SIEM ELASTIC ВИМОГАМ ISO/IEC 27001, ISO/IEC 27002 та ISO/IEC 27035

Туз М.О., Гріненко Т.О.
Харківський національний університет радіоелектроніки, Харків, Україна

SIEM-рішення (Security Information and Event Management) дозволяють об'єднати в єдину платформу збір, кореляцію, аналіз та зберігання даних про події в мережі, допомагаючи виявляти потенційні загрози та ефективно реагувати на них. Вони є ключовим компонентом сучасних стратегій кібербезпеки, надаючи можливість не лише запобігати атакам, але й зменшувати їхній вплив [1, 2].

Elastic, один із популярних інструментів SIEM, пропонує комплексне рішення для моніторингу та аналізу даних, забезпечуючи масштабованість, високу продуктивність і функціональність. Завдяки можливості автоматизації збору, аналізу, збереження логів та моніторингу подій безпеки, SIEM Elastic сприяє виявленню загроз, реагуванню на інциденти та забезпеченню збереження доказів [3].

**Метою доповіді** є аналіз особливостей роботи SIEM-рішень, зокрема Elastic, оцінка їхніх можливостей у виявленні загроз та атак, а також визначення їх відповідності вимогам міжнародних стандартів інформаційної безпеки, таких як ISO/IEC 27001, ISO/IEC 27002 та ISO/IEC 27035 [4]. В доповіді надані результати аналізу та дослідження основних можливостей та функціоналу платформи Elastic, принципів її роботи та застосування.

Основний функціонал Elastic забезпечує гнучкий підхід до збору, обробки, аналізу та візуалізації даних, що робить цю платформу універсальним інструментом для моніторингу та забезпечення безпеки. Максимальна ефективність цього інструменту залежить від кваліфікації та досвіду персоналу. Успіх у реагуванні на інциденти та виявленні потенційної загрози чи спроби несанкціонованого доступу значною мірою визначається рівнем обізнаності користувачів, їх здатністю правильно налаштовувати правила та інтерпретувати отриману інформацію. Впровадження SIEM-рішення Elastic дозволить організаціям ефективно реалізовувати вимоги міжнародних стандартів ISO/IEC 27001, ISO/IEC 27002 та ISO/IEC 27035, забезпечуючи належний рівень управління інформаційною безпекою.

**Список літератури**

1. Овчаренко М.Ю., Сєвєрінов О.В. Аналіз сучасних систем управління інформаційною безпекою та інцидентами безпеки. ЧДТУ, НТУ" ХПІ", ВА ЗС АР, УТіГН, ДП" ПД ПКНДІ АП", 2019.

2. Сєвєрінов О.В., Ушатов В.В. Управління інцидентами інформаційної безпеки на основі використання SIEM систем. (2019).

3. Marco Mancini. Security analytics with Elastic. openaccess.uoc.edu:веб-сайт. URL: http://surl.li/hfdbus.

4. Сєвєрінов О.В., Черниш В.І., Молчанова М.Є. Управління інформаційною безпекою згідно міжнародних стандартів // Системи управління, навігації та зв'язку.– К: ДП «ЦНДІ НіУ».-2011.–Вип 4.20 (2011): 250-253.

# ДОСЛІДЖЕННЯ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ЕЛЕКТРОМАГНІТНІ ПЕРЕВИПРОМІНЮВАННЯ ДОПОМІЖНИХ ТЕХНІЧНИХ ЗАСОБІВ І СИСТЕМ

Кустов А.К., Заболотний В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Забезпечення інформаційної безпеки засобів електронно-обчислювальної техніки (ЕОТ) є важливим завданням комплексів технічного захисту інформаційних систем. Особливої уваги потребують технічні канали витоку інформації (ТКВІ), зокрема канали побічних електромагнітних випромінювань (ПЕМВ), які становлять значну загрозу інформації з обмеженим доступом (ІзОД) [1].

**Метою доповіді** є побудова математичних моделей, які дозволять враховувати особливості ТКВІ всіх варіантів перевипромінень випадковими антенами (ВА) створеними допоміжними технічними засобами і системи (ДТЗС), що розташовані в в зоні 1 навколо основних технічних засобів (ОТЗ) [2]. Дослідження охоплює як якісні, так і кількісні підходи до моделювання процесів витоку інформації, що формуються в зоні, безпосередньо навколо ОТЗ.

**В доповіді** наводяться необхідні для аналізу можливі варіанти створення пар перевипромінювачів: рамка-рамка по магнітному полю, рамка-диполь по електричному полю, диполь-диполь по електричному полю, диполь-рамка по магнітному полю [3]. Розміри зони 2 перевипромінень – мета, яка дозволяє надалі планувати і реалізовувати заходи комплексу технічного захисту інформації.

Оскільки ПЕМВ відеотракту ЕОТ є найбільш небезпечними, то ці сигнали і являються предметом першочергового дослідження. Запропоновані підходи для розрахунку збільшення зони 2 за рахунок впливу означених перевіпромінювань.

Отримані результати сприятимуть впровадженню ефективних методів захисту інформації, що є надзвичайно актуальним у сучасних умовах розвитку цифрових технологій [1–3].

**Список літератури**

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

2. Заболотний В. І., Олейніков А. М., Заболотний Д. М., Кустов А. К. Технічний канал витоку інформації побічними електромагнітними перевипромінюваннями допоміжних технічних засобів і систем. Радіотехніка, 2024. Т. 3, № 218. DOI: https://doi.org/10.30837/rt.2024.3.218.04.

3. Шокало В. М., Правда В. І., Усін В. А., Вунтесмері В. С., Грецьких Д. В. Електродинаміка та поширення радіохвиль. Частина 1. Харків: ХНУРЕ, Колегіум, 2009.

# МАТЕМАТИЧНА МОДЕЛЬ КОЕФІЦІЄНТА ПЕРЕДАЧІ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ ВІДЕОТРАКТУ ЗАСОБІВ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ ДЛЯ ШИРОКИХ ДІАПАЗОНІВ ЧАСТОТ І ВІДСТАНЕЙ

Гапіченко А.М., Заболотний В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному світі інформаційні технології є невід'ємною складовою більшості сфер діяльності людини. Широке використання персональних комп'ютерів та інших пристроїв для обробки, зчитування, зберігання й відтворення даних призводить до зростання обсягу інформації, що циркулює у засобах обчислювальної техніки. Водночас ці компоненти генерують електромагнітне випромінювання, яке може містити інформацію з обмеженим доступом. У зв'язку з потенційною загрозою витоку інформації такий технічний канал витоку інформації (ТКВІ) [1] потребує детального аналізу з метою розробки та впровадження ефективних заходів захисту небезпечної інформації.

Метою цієї доповіді є розробка та дослідження моделей прояву впливу магнітної та електричної складових побічних електромагнітних випромінювань (ПЕМВ) для створення комплексів технічного захисту інформації. У доповіді представлено розроблені моделі складових поля у типових діапазонах частот та відстаней, включаючи ближню, проміжну і дальню зони відповідних полів у формі коефіцієнтів передачі.

Для оцінки параметрів ПЕМВ під час вимірювань показників захисту використовуються рівняння Максвелла, які описують зв'язок між електричним і магнітним полями [2]. У процесі дослідження отримано результати, що дозволяють оцінити рівень загрози ТКВІ та розробити заходи для їх мінімізації. Визначено коефіцієнти передачі випромінювання для різних частотних діапазонів спектрів ПЕМВ, що є важливим при проектуванні комплексів технічного захисту інформації.

Таким чином, результати дослідження можуть бути використані для подальшого вдосконалення заходів захисту інформації від витоку через ПЕМВ і наведення.

**Список літератури**

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. / С.О. Іванченко, О.В. Гавриленко , О.А. Липський, А.С. Шевцов – Київ : НТУУ «КПІ», 2016. – 101 с.

2. Заболотний, В. І. Дослідження зміни форми сигналу у каналі побічних електромагнітних випромінювань монітору / В. І. Заболотний, Є. В. Герасименко, В. І. Перепадя // Радіотехніка: Всеукр. межвід. наук.-техн. зб. – Харків, 2014. – Вип. 176. – С. 116– 121

# АНОНІМІЗАЦІЯ ВИБОРЦІВ В СИСТЕМІ Е-ГОЛОСУВАННЯ З ВИКОРИСТАННЯМ КОРПОРАТИВНИХ ЗАСОБІВ

Левандовський О.С., Заболотний В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

В воєнному стані держави не припиняються важливі демократичні процеси. До них можна віднести проведення виборів на посади керівників деяких органів управління установ, профспілок тощо. Традиційний процес голосування бюлетенями може обмежуватися вимогами безпеки пересування і концентрації людей на певних територіях і на певний час. Існує можливість організації і проведення електронного голосування (е-голосування) за допомогою автоматизованої інформаційно-телекомунікаційної системи [1, 2]. Участь у електронному голосуванні можуть брати як уповноважені виборці, так і стовідсотковий контингент установи, які пройшли ідентифікацію за допомогою корпоративних автентифікаційних даних, зокрема корпоративного номера телефону або електронної пошти. Особливі вимоги по проведннню голосування реалізує відповідна комплексна система захисту інформації (КСЗІ), яка створюється, впроваджується і функціонує згідно національної законодавчої бази в галузі інформаційної безпеки.

**Метою доповіді є** розкриття особливостей системи е-голосування, яка реалізує політику багаторівневого контролю доступу, що включає принцип найменших привілеїв (Least Privilege Principle), розподіл обов'язків для запобігання монополізації контролю над системою (Separation of Duties) та модель нульової довіри (Zero Trust), яка виключає довіру до будь-якого учасника за замовчуванням [1, 3].

**В доповіді** розриваються питання перевірки автентичності голосу кожного виборця, яка здійснюється за допомогою технології сліпого підпису (Blind Signature). Після проходження верифікації особи виборець отримує унікальний токен зі сліпим підписом, що дозволяє йому подати голос без можливості ідентифікації з боку сервера голосування. Це гарантує анонімність виборчого процесу та виключає прив'язку голосу до особистих даних виборця.

Після завершення голосування система підраховує голоси за кожного кандидата та формує остаточний результат. Дані голосування зберігаються до офіційного оголошення результатів, після чого виборча база підлягає знищенню відповідно до регламентованих процедур.

**Список літератури**

1. Шаннуссо Т., Іашвілі Г. Кібербезпека на виборах в Україні Аналіз та рекомендації. червень 2022. URI: https://www.ifesukraine.org/wp-content/uploads/2024/01/

2. Токар-Остапенко О.В. Електронне голосування: перспективи впровадження в Україні. 2021. URI: https://niss.gov.ua/sites/default/files/2021-02/tokar-1.pdf.

3. Moskvin K., Sievierinov O. Zero Trust Architecture in Corporate Cybersecurity Systems. ХНУРЕ, 2025.

# ЗАХИСТ ІНФОРМАЦІЇ, ЩО ОЗВУЧУЄТЬСЯ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ВІД ВИТОКУ КАНАЛАМИ ЛАЗЕРНИХ ЗАСОБІВ АКУСТИЧНОЇ РОЗВІДКИ

Заболотний В.І., Холєв Н.О., Свиридов Г.І.
Харківський національний університет радіоелектроніки, Харків, Україна

У сфері захисту інформації, на об'єктах інформаційної діяльності існує загроза використання лазерних засобів акустичної розвідки (ЛЗАР). Як протидія цьому існують і застосовуються певні комплекси заходів і засобів захисту від технічних каналів витоку інформації (ТКВІ) цієї природи [1, 2, 3].

**Метою доповіді є** аналіз існуючого стану заходів захисту від ЛЗАР, розробка кількісних моделей елементів ЛЗАР та пропозицій з покращення захисту від них.

До заходів захисту інформації, що озвучується на ОІД, відносяться організаційні та (або) технічні: пасивні й активні. Останні поділяються на методи з використанням акустичних та вібраційних пристроїв.

До організаційних методів захисту мовної інформації від можливого витоку належить комплекс організаційних заходів, спрямованих на забезпечення мінімального ризику витоку мовної інформації з ОІД. До цих заходів відноситься [1]. вибір відповідного приміщення для ведення конфіденційних перемовин, забезпечення функціонування на службовій території відповідної охоронної служби, зачинення вікон під час ведення конфіденційної розмови з метою запобігання розвідки бесіди за допомогою акустичних спрямованих мікрофонів тощо.

До пасивних методів захисту мовної інформації відноситься, наклеювання на шибку спеціальної плівки [2], що забезпечує неможливість отримання ЛЗАР відбитого від віконної шибки сигналу.

Активний метод захисту мовної інформації із використанням акустичних і вібраційних пристроїв, що передбачає створення акустичного шуму та вібрацій в приміщенні та віконних рам що, понижує комфортність ведення перемов [3]. В доповіді наведено окремі моделі цього ТКВІ. Сформульовано пропозиції до розвитку підходів до «безшумного» захисту інформації, що озвучується у ВП.

**Список літератури**

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. / С.О. Іванченко, О.В. Гавриленко , О.А. Липський, А.С. Шевцов – Київ : НТУУ «КПІ», 2016. – 101 с.

2. Дудикевич В. Б., Пасивний захист інформації від лазерного зондування / В. Б. Дудикевич, І. С. Собчук, В. О. Ракобовчук // Вісник Національного університету "Львівська політехніка". Сер. : Автоматика, вимірювання та керування. -2013. - № 753. - С. 118-123. - Режим доступу: http://nbuv.gov.ua/UJRN/VNULP_2013_753_20.

3. В.І. Заболотний, Ю.О. Ковальчук. "Безшумний" захист від "Лазерних мікрофонів". Прикладная радиоэлектроника, 2009, Том 8, № 3. С. 377-381.

# ЗАХИСТ ВЕБЗАСТОСУНКІВ ВІД XSS ТА CSRF АТАК НА ПРИКЛАДІ СУЧАСНОГО FRONT-END ФРЕЙМВОРКУ

Синиціна В.С., Балагура Д.С.,
Харківський національний університет радіоелектроніки, Харків, Україна
Сухотеплий В.М.
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна

З розвитком вебтехнологій зростає кількість атак на клієнтську частину веб-додатків. Особливу загрозу становлять атаки типу Cross-Site Scripting (XSS) та Cross-Site Request Forgery (CSRF), що можуть призвести до компрометації конфіденційних даних користувачів [1, 2]. У сучасних front-end фреймворках, таких як React, реалізовані певні механізми захисту, але їх недостатньо для повного усунення цих загроз.

XSS-атаки базуються на виконанні шкідливого коду в контексті веб-додатка, що дозволяє зловмисникам красти дані або здійснювати маніпуляції з контентом [3]. Основними методами захисту є: використання dangerouslySetInnerHTML лише в обґрунтованих випадках; екранування вхідних даних через бібліотеки, такі як DOMPurify; впровадження Content Security Policy (CSP) для обмеження виконання скриптів. CSRF-атаки експлуатують відсутність перевірки джерела запитів та дозволяють здійснювати несанкціоновані дії від імені користувача [4]. Методи запобігання включають: використання CSRF-токенів у POST-запитах; перевірку заголовка SameSite для cookies; обмеження дозволених методів запитів на сервері.

**Метою доповіді є** аналіз загроз, пов'язаних із XSS та CSRF-атаками у сучасних вебзастосунках, а також розгляд ефективних методів їх запобігання у front-end фреймворках, зокрема React. Особливу увагу приділено інтеграції механізмів безпеки на клієнтському рівні та необхідності комплексного підходу до захисту веб-додатків [5]. Дослідження демонструє, що застосування перелічених методів у React-додатках значно підвищує рівень їхньої безпеки. Проте, комплексний захист передбачає інтеграцію різних підходів на рівні як клієнтської, так і серверної частини.

**Список літератури**

1. Д'якова Н.Є., Сєвєрінов О.В. Тестування вразливостей сучасних вебресурсів, НТУ «ХПІ»,. – 2022.
2. Сєвєрінов О.В., Шевцов В.О., Сокол-Кутиловська А.С. Аналіз сучасних методів атак на електронні ресурси органів управління // Системи озброєння і військова техніка 1 (2017): 65-68.
3. OWASP Foundation. "Cross-Site Scripting (XSS)." OWASP Cheat Sheet Series, 2023.
4. OWASP Foundation. "Cross-Site Request Forgery (CSRF)." OWASP Cheat Sheet Series, 2023.
5. Grossman, J. "Web Application Security: XSS and CSRF Attacks," Security Journal, vol. 15, no. 2, pp. 45-67, 2022.

# БЕЗПЕКА HTTP ЗАГОЛОВКІВ

Синицін Я.С., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком веб-технологій питання безпеки веб-додатків стає все більш актуальним [1]. HTTP-заголовки відіграють ключову роль у захисті комунікацій між сервером і клієнтом. Неправильна конфігурація цих заголовків може призвести до серйозних загроз, таких як XSS, Clickjacking, MIME-Sniffing та Man-in-the-Middle атаки [2]. Для забезпечення високого рівня безпеки веб-додатків в процесі розробки додатків та їх експлуатації необхідно здійснювати постійний аналіз та контроль щодо відсутності основних вразливостей, до яких можна віднести: відсутність або неправильне використання HTTP-заголовків безпеки, що може призвести до атак XSS, Clickjacking та MIME-Sniffing; надлишкова інформація у заголовках (наприклад, X-Powered-By), що сприяє роботі зловмисників; неправильна конфігурація політик безпеки, зокрема Content Security Policy (CSP).

**Метою доповіді є** аналіз основних загроз, пов'язаних із некоректним налаштуванням HTTP-заголовків, оцінка існуючих механізмів безпеки та розгляд ефективних методів захисту.

Серед основних механізмів безпеки можна відзначити елементи заголовків:

- Strict-Transport-Security (HSTS) - примусове використання HTTPS;
- Content-Security-Policy (CSP) - обмеження джерел виконуваного коду;
- X-Frame-Options - захист від Clickjacking;
- X-Content-Type-Options - запобігання MIME-Sniffing;
- Referrer-Policy - контроль передачі реферер-заголовків;
- Permissions-Policy - управління доступом до браузерних API.

Аналіз зазначених механізмів дозволив розробити практичні рекомендації.

1. Використання HTTPS та примусове шифрування через HSTS є обов'язковим та має використовуватись постійно.
2. Впровадження CSP для обмеження виконуваного JavaScript-коду.
3. Автоматичне визначення MIME-типів має бути вимкнено.
4. Сайт не має завантажуватися у фреймі, функціонал має бути недоступний.
5. Політики доступу до API має бути проаналізована та верифікована. Необхідно підтримувати мінімальний рівень, що реалізує потрібний функціонал.
6. Має регулярно проводитись аудит безпеки заголовків.

Дотримання наведених рекомендацій дозволяє суттєво зменшити ризики атак та підвищити рівень безпеки веб-додатків.

**Список літератури**

1. Д'якова Н.Є., Сєвєрінов О.В. Тестування вразливостей сучасних вебресурсів, НТУ «ХПІ»,. – 2022.
2. OWASP Foundation. "HTTP Security Headers." OWASP Cheat Sheet Series, 2023.

# РОЗРОБКА СИСТЕМИ МОНІТОРИНГУ МЕРЕЖЕВОЇ АКТИВНОСТІ З ВИКОРИСТАННЯМ ELK STACK

Шмагун В.І., Балагура Д.С., Смірнов А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Моніторинг мережевої активності відіграє ключову роль у забезпеченні інформаційної безпеки та ефективному управлінні мережевими ресурсами. У сучасних інформаційних системах, де постійно збільшується обсяг переданих і оброблюваних даних, необхідно використовувати потужні інструменти для збору, аналізу та візуалізації інформації. Одним із найбільш ефективних рішень для таких задач є стек ELK (Elasticsearch, Logstash, Kibana) [1]. Його використання дає змогу централізовано збирати журнали подій з різних джерел, обробляти їх у реальному часі, а також аналізувати отримані дані для виявлення загроз і аномалій. Гнучка архітектура дозволяє адаптувати систему під конкретні потреби організації та масштабувати її відповідно до зростання навантаження. Використання ELK Stack вимагає імплементації та впровадження певного процесу, який забезпечить всі етапи моніторингу мережевої активності. Так, на першому етапі розгортання ELK Stack необхідно налаштувати збір даних. Для цього використовуються агенти, такі як Filebeat або Winlogbeat, які дозволяють отримувати логи з серверів, мережевого обладнання та інших джерел. Наступним етапом після збору даних є їх обробку за допомогою Logstash або Ingest Pipelines в Elasticsearch. На цьому етапі застосовуються фільтри для нормалізації, розбору та збагачення логів додатковою інформацією. На третьому етапі відбувається аналіз отриманих даних. Аналіз здійснюється в Elasticsearch, який дозволяє виконувати швидкий пошук та виявляти закономірності в мережевій активності. Використання Kibana дає змогу створювати інтерактивні дашборди для візуалізації ключових показників безпеки. Це дозволяє адміністраторам швидко виявляти підозрілі дії та оперативно реагувати на потенційні загрози.

Ефективність моніторингу можна підвищити за рахунок використання машинного навчання для виявлення аномалій у поведінці користувачів та мережевого трафіку. Вбудовані можливості Machine Learning в Elasticsearch дозволяють автоматично визначати відхилення від нормальної поведінки та генерувати сповіщення у разі виявлення підозрілих активностей.

**Метою доповіді** є аналіз особливостей впровадження ELK Stack у корпоративне середовище, визначення типових викликів, що пов’язані з обробкою великих обсягів логів, їх аналізом, проблемами візуалізації результатів задля ефективного реагування з боку адміністраторів, та надання пропозицій щодо підходів для оптимізації та підвищення ефективності на кожному етапі роботи системи моніторингу.

**Список літератури**

1. Brown T., Wilson P. Advanced log analysis techniques in Elasticsearch. Network Security Review. 2021. Vol. 6, No. 2. P. 89–95.

# МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАХИСТУ ЦИФРОВИХ АКТИВІВ ВЕБЗАСТОСУНКІВ В УМОВАХ DDOS-АТАКИ

Шестопал Д.О., Балагура Д.С., Смірнов А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

В умовах сучасного цифрового світу, веб-додатки є основними платформами для надання послуг та взаємодії з користувачами. Проте зростання їхньої популярності супроводжується зростанням кількості кіберзагроз, серед яких особливе місце займають DDoS-атаки (Distributed Deny of Service): різновид атак, які відрізняються збільшеною складністю у виявлені та відбитті у порівнянні з класичними DoS-атаками [1, 2]. Ці атаки спрямовані на перевантаження серверів і призводять до недоступності послуг, втрати прибутку та репутаційних ризиків.

У даній доповіді розглянуто сучасні методи та технології захисту цифрових активів веб-додатків від DDoS-атак. Разом з цим було проаналізовано варіанти простих атак з використанням сучасних видів захисту.

**Метою доповіді** є моделювання DDoS атаки, аналіз існуючих рішень, надання рекомендацій та впровадження ефективних захисних механізмів та заходів для забезпечення стабільної роботи веб-додатків, що атакуються, безпосередньо під час DDoS атаки.

В доповіді проведено огляд та класифікацію DDoS-атак, розглянуто основні механізми їх реалізації та існуючі методи захисту. Крім того проаналізовано архітектурні рішення та мережеві технології, що можуть бути використані для мінімізації впливу DdoS-атак, а також зроблено висновки щодо їх ефективності.

В практичній частині роботи створено тестовий полігон та проведено аналіз вразливостей веб-додатку, впроваджено захисні заходи та проведено моніторинг їх ефективності. Результати дослідження можуть бути використані для покращення захисту веб-додатків від DDoS-атак.

Для захисту від DDoS-атак перспективним напрямом є використання машинного навчання.

Ці технології дозволяють виявляти аномалії в мережевому трафіку на ранніх етапах та класифікувати типи атак із високою точністю.

**Список літератури**

1. Бірюков А.А. Інформаційна безпека: захист та напад. – видавництво ДМК-ПРЕСС. – 2016. – 434 с.

2. Сєвєрінов О.В., Шевцов В.О., Сокол-Кутиловська А.С. Аналіз сучасних методів атак на електронні ресурси органів управління // Системи озброєння і військова техніка 1 (2017): 65-68.

3. Kavetskyi M.S., Sievierinov O.V., Gvozdov R.Y., Smirnov A.O. (2024). Використання машинного навчання для класифікації атак типу DOS/DDOS. *Radiotekhnika*, (217), 55-63.

# ОСОБЛИВОСТІ ОЦІНКИ РИЗИКІВ БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ IDIS2GO

Уманська А.О., Смірнов А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Управління ризиками безпеки програмного забезпечення - це процес виявлення, оцінки та мінімізації ризиків, пов'язаних із розробкою, впровадженням та використанням програмного забезпечення. Його мета - зменшити ймовірність виникнення проблем (наприклад, збоїв, помилок, загроз безпеці) та їхній вплив, забезпечуючи стабільність, якість і безпеку роботи програмного забезпечення. Сучасні інформаційні технології відіграють ключову роль у розвитку медицини, забезпечуючи ефективне управління пацієнтськими даними, автоматизацію діагностики та моніторинг стану здоров'я. Програмне забезпечення, що використовується в медичній сфері, вимагає особливо високих стандартів безпеки та надійності, оскільки від його роботи залежить не лише якість медичних послуг, а й життя пацієнтів [1]. Оцінка ризиків безпеки є критичним етапом у розробці та впровадженні медичних програмних продуктів. Вона дозволяє виявити потенційні загрози, що можуть вплинути на конфіденційність, цілісність і доступність медичних даних, а також уникнути збоїв у роботі систем, які можуть призвести до критичних наслідків. Загрози безпеці програмного забезпечення можуть включати як технічні аспекти, такі як помилки програмного коду чи кібератаки, так і організаційні фактори, наприклад, недоліки у використанні програмного забезпечення або неналежне управління доступами [2, 3].

Метою доповіді є розробка стратегії безпеки оцінки ризиків програмного забезпечення IDIS2GO в сучасних медичних сервісних системах. В доповіді наводиться, що управління ризиками в програмному забезпеченні IDIS2GO є ключовим етапом для забезпечення його стабільної, безпечної та ефективної роботи. Враховуючи, що система працює з медичними даними, особливу увагу потрібно приділити конфіденційності, цілісності та доступності інформації, а також безперервності її функціонування. Виявлені загрози у процесі аналізу визначено, що найбільші ризики для IDIS2GO пов'язані з технічними аспектами (помилки коду, збої в алгоритмах, вразливості безпеки, можливі кіберзагрози), організаційними чинниками (недостатня підготовка користувачів, некоректне управління доступами, ризики втрати даних), операційною безпекою (відсутність механізмів резервного копіювання, відмовостійкості, планів відновлення після збоїв). Для мінімізації потенційних загроз запропоновані були наступні заходи: технічні рішення: регулярне оновлення програмного забезпечення, впровадження механізмів шифрування та автентифікації, автоматизоване тестування на помилки та вразливості; організаційні заходи: навчання медичного персоналу щодо безпечного використання системи, визначення ролей і рівнів доступу для користувачів, розробка політики реагування на інциденти та планів відновлення; моніторинг

і контроль: використання систем логування та аналізу безпеки (SIEM). Не менш важливим аспектом є механізми самодіагностики та моніторингу: вбудована система перевірки коректності зібраних даних, виявлення аномалій та автоматичне сповіщення адміністратора, логування всіх критичних подій у системі. Організаційні заходи: навчання персоналу: регулярні тренінги для лікарів та технічного персоналу щодо використання IDIS2GO, ознайомлення з протоколами кібербезпеки, симуляційні навчання щодо дій у разі збоїв системи [2, 4].

Впровадження розробленої стратегії дозволить зменшити ймовірність збоїв і атак завдяки вдосконаленій архітектурі безпеки та підвищити якість та надійність програмного забезпечення шляхом покращення тестування та контролю, а також забезпечити відповідність нормативним вимогам медичної сфери та законодавства у сфері захисту даних. Ці заходи допоможуть знизити фінансові та репутаційні ризики для медичних установ, що використовують IDIS2GO.

На основі зазначених ризиків можна виділити декілька рекомендацій щодо вдосконалення, таке як: резервування, безперервне навчання персоналу, тестування, впровадження SIEM (використовувати системи моніторингу подій безпеки для швидкого виявлення загроз) та регулярний аудит (проводити технічні й безпекові аудити, оцінюючи ризики на основі оновлених даних). Управління ризиками є критично важливим етапом у процесі розробки програмного забезпечення (ПЗ), що дозволяє мінімізувати можливі негативні наслідки, пов'язані з невизначеністю, що може вплинути на якість, безпеку, бюджет та строки виконання проєкту [5].

Отже, розробка та впровадження ефективної системи управління ризиками для IDIS2GO забезпечить високий рівень безпеки, надійності та стабільності роботи програмного забезпечення. Це дозволить розширити сфери його використання, покращити довіру серед лікарів та пацієнтів, а також сприятиме успішній інтеграції системи в сучасну медичну інфраструктуру.

**Список літератури**

1. PQCrypto 2017. Netherlands, 26--28 June 2017. [Електронний ресурс] – Режим доступа: https://2017.pqcrypto.org/conference/ - 02.06.2018.

2. Tkachov, A., Hapon, A., Balagura, D., Sievierinov, O., Bukatych, I., & Havrylova, A. (2024, November). Analysis of the Software Security Protection. In 2024 8th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-8). IEEE.

3. Сєвєрінов, О.В., Переметчик О.В.. Комбінований метод аналізу ризиків інформаційної безпеки. Diss. НТУ «ХПІ», 2020.

4. Овчаренко М.Ю., Сєвєрінов О.В. Аналіз сучасних систем управління інформаційною безпекою та інцидентами безпеки. ЧДТУ, НТУ" ХПІ", ВА ЗС АР, УТіГН, ДП" ПД ПКНДІ АП", 2019.

5. Krishnan M. Soumya Software Development Risk Aspects and Success Frequency on Spiral and Agile Model. InternationalJournal of Innovative Research in Computer and Communication Engineering. 2015. № 3(1). P. 301-310.

# СУЧАСНІ ЗАСОБИ ЗАХИСТУ МЕРЕЖ WI-FI

Блінна В.С., В'юхін Д.О., Шулік П.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Бездротові мережі стали не тільки частиною життя, але й мішенню для кібератак. Використання комплексного захисту значно зменшує ризики злому.

**Метою доповіді** є розгляд та порівняння сучасних засобів захисту Wi-Fi. Розглядаються основні типи захисту.

1) Використання надійного пароля. Пароль повинен мати щонайменше 10-12 символів з використанням цифр, розділових знаків і службових символів ($, @ і %), без простих послідовностей, щоб уникнути атаки грубою силою.

2) Приховання SSID (ідентифікатор набору послуг) [1] зменшує ризик несанкціонованого доступу та атак, таких як War Driving і Evil Twin. Після ручних налаштувань Wi-Fi більше не буде видимим при скануванні сусідніх мереж, ці точки можливо знайти лише при використанні додаткових засобів.

3) Увімкнення бездротового шифрування також є важливим для захисту даних. Сьогодні найбільш захищеним є протокол WPA3 [2]. WPA3 пропонує більш гнучке шифрування за допомогою AES-CCMP/AES-GCMP, дозволяє використовувати 128- і 256-бітові сеансові ключі [3].

4) Вимкнення віддаленого доступу до Wi-Fi, оскільки зловмисники, особливо у публічних мережах, можуть отримати контроль над маршрутизатором через атаки Brute Force, Man-in-the-Middle та DNS Spoofing.

5) VPN також має важливе значення для захисту інформації, він відправляє трафік користувача через зашифрований «тунель», що ускладнює його розшифрування та перехоплення, і маскує IP-адресу [4].

Таким чином, складні паролі, VPN, протокол WPA3 та приховування мережі забезпечують надійний рівень захисту для Wi-Fi. Нажаль, іноді неможливо застосувати всі засоби, тому приховування SSID може бути менш важливим, особливо коли ввімкнено WPA3, яке забезпечує більш надійне шифрування та захист від грубої сили. У такому випадку навіть якщо хтось побачить SSID, зламати мережу без знання пароля буде вкрай складно.

**Список літератури**

1. Hack proofing your wireless network / ed. by B. Christian, O. Neal. Rockland, Mass: Syngress Pub., 2002. 483 c.

2. Золотарьов В., Фодченко А. ШИФРУВАННЯ WI-FI 6-МЕРЕЖ. *Радіоелектроніка та молодь у XXI столітті. Т. 4: Конференція "Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій"*. Харків, Україна, 2024. DOI: https://doi.org/10.30837/iyf.pdicimt.2024.168.

3. Wireless Network Security: WEP, WPA, WPA2 & WPA3 Explained. eSecurity Planet. URL: https://www.esecurityplanet.com/trends/the-best-security-for-wireless-networks.

4. Сердюков Д.В., Сєвєрінов О.В., Сидоренко З.М. Безпечне підключення мобільних пристроїв до корпоративної мережі з використанням тунелю VPN. 2023.

# ЗАХИСТ ВІД ФІШИНГ АТАКИ «ФІШИНГ-КЛОН»

Іващенко І.В., В'юхін Д.О., Смірнов А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

«Фішинг-клон» (Clone Phishing) - це різновид фішингу, коли зловмисники копіюють справжній електронний лист, змінюючи посилання на підроблений сайт. Такий лист виглядає легітимним і може обманом змусити користувача надати конфіденційну інформацію. Часто націлений на відомих осіб, особливо у політиці та бізнесі, для отримання фінансових даних. Від звичайного фішингу відрізняється тим, що всі вихідні дані залишаються недоторканими, але вони дублюються [1]. Фішинговий електронний лист-клон часто містить дивні формулювання, створює відчуття терміновості та підштовхує до швидких дій, таких як натискання посилання або розкриття конфіденційної інформації [2]. **Метою доповіді** є розгляд та аналіз фішингової атаки типу «Фішинг-клон». Проведений аналіз показав, що для запобіганню Clone Phishing атаці потрібно здійснити наступні кроки.

1. Перевірка посилань – потрібно не переходити за посиланням без перевірки їхньої автентичності та джерела.

2. Аналіз вкладень – потрібно сканувати файли на віруси перед відкриттям.

3. Перевірка відправника – потрібно знайти адресу в пошукових системах для підтвердження її справжності.

4. Використання спам-фільтрів – необхідно автоматично блокувати підозрілі листи.

5. Перевірка на помилки – необхідно знаходити помилки, які можуть змусити повірити, що вони не є на 100% законними. Клоновані електронні листи можуть добре емулювати справжні, але трапляються помилки.

6. Завжди необхідно використовувати шифрування електронної пошти, надсилаючи найбільш конфіденційну інформацію [3, 4].

Фішингові афери-клони, на жаль, є одним з найпростіших видів шахрайства. Оскільки вони використовують вже існуючий бренд, а не створюють новий, вони зазвичай виглядають більш переконливо. Потрібно виконувати розглянуті кроки, щоб захистити себе від фішингових афер-клонів.

**Список літератури**

1. Lady Liberty. What is clone phishing? HackYourMom. URL: https://hackyourmom.com/en/kibervijna/shho-take-fishyng-kloniv/.

2. What Is Clone Phishing? ProofPoint. URL: https://www.proofpoint.com/us/threat-reference/clone-phishing.

3. Аноха Рудра. Що таке фішинг клонів? Power DMARC. URL: https://powerdmarc.com/ru/what-is-clone-phishing/.

4. Giulian Garruba. Introduction to Clone Phishing: How Can It Be Prevented? Mimecast. URL: https://www.mimecast.com/blog/introduction-to-clone-phishing-how-can-it-be-prevented/.

# WEB-ДОДАТОК З ВІДСТЕЖЕННЯ ТА БЛОКУВАННЯ DDoS-АТАК

Коломицев А.Р., Наконечний М.В., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У наш час веб-додатки та сайти стали ключовим інструментом для бізнесу, комунікацій та обслуговування клієнтів. Однак розвиток цифрових технологій також супроводжується збільшенням кіберзагроз.

**Метою доповіді** є розгляд однієї з найпоширеніших атак – атаки на відмову в обслуговуванні (Distributed Denial of Service, DDoS). Її метою є перевантаження серверів і обмеження доступу до ресурсу легітимним користувачам. Захист веб-додатків від таких загроз є критично важливим завданням [1]. DDoS-атаки полягають у масовому надсиланні запитів до сервера з різних джерел, що призводить до перевантаження мережі та відмови у її функціонуванні. Різновиди таких атак включають UDP-флудинг, SYN-флудинг, HTTP-флудинг та інші.

У доповіді розглядається створення веб-додатку, що дозволяє відстежувати та блокувати DDoS-атаки на веб-сайті. Основними функціями такого додатку є моніторинг трафіку, виявлення підозрілих активностей та оперативна реакція на можливі загрози шляхом блокування атакуючих IP-адрес або інших заходів [2].

Основні етапи створення веб-додатку з функціями захисту від DDoS-атак:

1. Моніторинг мережевого трафіку. Збір даних про запити до сервера в реальному часі. Це включає відстеження таких параметрів, як частота запитів, обсяги трафіку та географічне розташування джерел запитів.
2. Виявлення аномалій. Використання алгоритмів аналізу для визначення нетипової активності.
3. Реалізація механізмів блокування. Забезпечення можливості блокування підозрілих IP-адрес або обмеження доступу на певний проміжок часу. Реалізація функції автоматичного блокування на основі налаштованих правил.
4. Інтеграція системи оповіщення. Додаток повинен забезпечувати своєчасне інформування адміністраторів про можливі загрози через електронну пошту, повідомлення або інші засоби комунікації.
5. Візуалізація даних. Надання візуальної інформації для зручного аналізу роботи системи та виявлення тенденцій у мережевому трафіку.

Результатом реалізації такого веб-додатку є зменшення ризиків збоїв у роботі сайту через DDoS-атаки, підвищення надійності інформаційної системи та захист даних користувачів.

**Список літератури**

1. Cloudflare. DDoS Protection. URL: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

2. Д'якова Н.Є., Сєвєрінов О.В. Тестування вразливостей сучасних веб-ресурсів, НТУ «ХПІ»,. – 2022.

# АНАЛІЗ АТАК ПО КЛОНУВАННЮ МАРШРУТИЗАТОРА

Якимчук М.Д., Наконечний М.В., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасний світ наразі не може існувати без Інтернету та мережі. Маршрутизатор відіграє в ній ключову роль, забезпечуючи передавання даних між сегментами. **Метою доповіді** є проведення аналізу атаки по клонуванню маршрутизатора.

Однією з можливих атак як зловмисників так і "білих"-хакерів є атаки типу «людина посередині» (MITM), а саме атака клонуванням маршрутизатора. Вона передбачає створення ідентичної копії маршрутизатора перехоплення або модифікації трафіку.

Під час атаки «злий двійник» зловмисник створює підроблену Wi-Fi-мережу, яка імітує легітимну точку доступу, щоб обманом змусити жертву підключитися до неї та викрасти конфіденційну інформацію. Основний принцип цієї атаки полягає у розгортанні фальшивої бездротової мережі з тим самим SSID, що й у справжньої точки доступу, яку необхідно скомпрометувати. Ця атака можлива лише якщо більшість пристроїв, таких як смартфони та ноутбуки тощо, при виборі Wi-Fi-з'єднання орієнтуються лише на ідентифікатор SSID, не маючи механізмів для розрізнення автентичних і підроблених мереж з однаковою назвою та типом шифрування. Користувачі, не підозрюючи небезпеки, автоматично підключаються до мережі з найсильнішим сигналом, що часто виявляється шкідливою копією [1].

Одним із найпоширеніших сценаріїв реалізації атаки є використання механізму Captive Portal. Ця система, зазвичай застосовувана у громадських Wi-Fi-мережах, змушує користувача пройти авторизацію перед отриманням доступу в інтернет. Зловмисник може створити підроблену сторінку входу, схожу на офіційний портал авторизації, і тим самим змусити жертву ввести облікові дані або іншу конфіденційну інформацію. Отримані дані можуть використовуватися для подальших атак, перехоплення трафіку або компрометації корпоративних і особистих акаунтів. Успішне клонування маршрутизатора може призвести до перехоплення конфіденційної інформації, здійснення атак MITM, впровадження шкідливого програмного забезпечення та порушення стабільності роботи мережі. Протистояти атаці такого виду можливо за допомогою аналізу аномалій у трафіку, перевірці цифрових сертифікатів пристроїв та фізичної ідентифікації обладнання. Для захисту мережі необхідно використовувати захищені протоколи зв'язку, сегментувати мережу, контролювати доступ і відстежувати зміни в інфраструктурі.

**Список літератури**

1. Reddy B. I., Srikanth V. Review on Wireless Security Protocols (WEP, WPA, WPA2 and WPA3) // International Journal of Scientific Research in Computer Science, Engineering and Information Technology. — 2019.

# АНАЛІЗ СПУФІНГ АТАК НА BLUETOOTH-ПРИСТРОЇ

Штангей В.О., Наконечний М.В., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасний світ наповнений Bluetooth-пристроями, від мобільних пристрїв, IoT-систем, медичних приладів та промислового обладнання. Однак відкритий характер технології створює значні ризики для користувачів, зокрема вразливість до спуфінг-атак, що дозволяють зловмисникам підміняти ідентифікаційні дані пристроїв для отримання несанкціонованого доступу або їх відмови [1].

**Метою доповіді** є розгляд методу атаки на Bluetooth-пристрої з використанням атаки через l2ping, яка дозволяє надсилати пакети заданого розміру на цільовий пристрій, викликаючи його нестабільність або навіть тимчасовий вихід з ладу. Такий спосіб впливу порушує нормальне функціонування Bluetooth-модуля жертви, що може призвести до зниження продуктивності або розриву бездротового з'єднання.

Атака передбачає підміну ідентифікаційних даних Bluetooth-пристрою, зокрема MAC-адреси або імені, щоб змусити інші пристрої вважати зловмисника довіреним партнером. Вона може бути реалізована за допомогою спеціального програмного забезпечення, що імітує роботу справжнього пристрою, або методів перехоплення й модифікації трафіку.

Головна особливість цієї атаки полягає в її простоті. Виконання команди l2ping не потребує складних налаштувань і може бути здійснене всього одним запуском, що робить її швидкою та ефективною. Атакуючий може заздалегідь підготувати файл із параметрами і просто виконати його, запустивши атаку без додаткових дій. Команда ініціює відправлення пакетів зазначеного розміру до пристрою з вказаною MAC-адресою. У процесі атаки час відповіді цільового пристрою почне поступово збільшуватися, а його Bluetooth-модуль може вийти з ладу або тимчасово відключитися.

Ефективне виявлення спуфінг-атак передбачає аналіз поведінки Bluetooth-з'єднань, виявлення аномалій у процесі підключення та застосування криптографічних методів для перевірки автентичності пристроїв. Для підвищення безпеки використовуються механізми шифрування переданих даних, що ускладнюють можливість їхнього перехоплення або модифікації [2, 3].

**Список літератури**

1. Д'якова, Н.Є., Сєвєрінов О.В. Аналіз загроз безпеки у системах розумного будинку. ВА ЗС АР; НТУ" ХПІ"; НАУ, ДП "ПДПРОНДІАВІАПРОМ"; УмЖ, 2021.

2. Польська Б. Ю. Методи захисту інформації в IoT – https://openarchive.nure.ua/entities/publication/89c3cc5e-8b01-43d5-be13-8fc837ad0ae4.

3. Matheus E. Garbelini, Sudipta Chattopadhyay, Vaibhav Bedi, Sumei Sun, Ernest Kurniawan (2021), Braktooth: Causing Havoc on Bluetooth Link Manager.

# АНАЛІЗ АТАК ЧЕРЕЗ ЗАГРОЗУ ШИФРУВАННЯ ДАНИХ ЗА ДОПОМОГОЮ СХЕМИ ЕЛЬ-ГАМАЛЯ

Яхно С.С., В'юхін Д.О., Шулік П.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Атаки на шифрування за схемою Ель-Гамаля можуть становити серйозну загрозу для конфіденційності інформації, якщо не дотримано належного рівня криптографічної обережності.

В доповіді розглянуто докладний аналіз потенційних атак, що можуть бути застосовані проти схеми шифрування Ель-Гамаля, а також шляхи їх запобігання.

**Метою доповіді** є аналіз загроз, пов'язаних з використанням схеми Ель-Гамаля, зокрема, у контексті фішингових атак. Дослідження фокусується на фішингових атаках, які здійснюються через електронну пошту, оскільки цей вектор атаки є одним з найчастіше використовуваних [1].

Незважаючи на складну математичну основу, сучасні криптографічні бібліотеки роблять реалізацію схеми Ель-Гамаля відносно простою, що відкриває доступ до неї зловмисникам з різними технічними навичками. У долповіді зроблений порівняльний аналіз обраної схеми з іншими найбільш популярними алгоритмами.

Виходячи з проведеного аналізу схема Ель-Гамаля стає потенційним вибором зловмисника для атаки на електронну пошту з кількох причин. Її відносна простота реалізації, поєднана з високим рівнем безпеки при належному використанні, робить її привабливою для тих, хто прагне забезпечити конфіденційність своїх дій.

Шифрування за схемою Ель-Гамаля може бути надійним за умови правильного використання. Основні вразливості пов'язані з реалізацією, особливо з генерацією випадкових чисел, повторним використанням параметрів, та відсутністю CCA-захисту.

Для підвищення безпеки рекомендується:

- використовувати гібридні криптосистеми;
- захищати канали обміну ключами;
- застосовувати сучасні модифікації на основі еліптичних кривих.

**Список літератури**

1. Методики розслідування фішингових атак: [Електронний ресурс]. URL: https://openarchive.nure.ua/server/api/core/bitstreams/63036cab-5814-4191-ab31-5cf94f4da284/content».

2. Сєвєрінов О.В., Шевцов В.О., Сокол-Кутиловська А.С.. Аналіз сучасних методів атак на електронні ресурси органів управління. *Системи озброєння і військова техніка* 1 (2017): 65-68.

3. ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. // IEEE Transactions on Information Theory. [1] — 1985. — Т. 31, № 4. — С. 469—472. [Електронний ресурс]. URL: https://bibliotekanauki.pl/articles/305780.

# АНАЛІЗ ВІДЕОДАНИХ ЯК СТЕГАНОГРАФІЧНОГО КОНТЕЙНЕРА ДЛЯ ПРОВЕДЕННЯ АТАК

Літвін О.О., Наконечний М.В., В'юхін Д.О.
Харківський Національний університет радіоелектроніки, Харків, Україна

Стеганографія відеофайлів також як і стеганографія зображень стає одним із ключових інструментів у сучасних кібератаках, оскільки дозволяє зловмисникам ефективно приховувати шкідливий код або конфіденційну інформацію, мінімізуючи ймовірність виявлення [1].

**Метою доповіді** є аналіз можливості використання відео як стеганографічного контейнера для проведення різноманітних атак.

Використовуючи методи стеганографії, хакери можуть передавати віруси, трояни чи інші шкідливі програми без явних ознак у вигляді традиційних підозрілих файлів [2]. Це дозволяє їм обминати системи безпеки, такі як антивірусне програмне забезпечення, і здійснювати атаки, не привертаючи уваги. Враховуючи ці загрози, розробка високотехнологічних методів для виявлення прихованих шкідливих кодів у відеофайлах є надзвичайно важливою для боротьби з кіберзлочинністю та захисту інформаційних систем.

Було проведено дослідження методів аналізу стеганографії у відео даних. Основними є методи: статистичний аналіз, спектральний аналіз, методи машинного навчання, зворотний аналіз.

Виходячи з отриманих даних найбільш перспективним є гібридний метод, що поєднує машинне навчання та спектральний аналіз. Машинне навчання ефективно виявляє приховані закономірності, а спектральний аналіз дозволяє виявляти зміни в частотній ділянці, характерні для стеганографії. Таке поєднання підвищує точність та надійність виявлення прихованої інформації, особливо у стислих відеоформатах.

Розглянуті деякі методи захисту сучасних систем від атак з використанням відеофайлів.

Захист від атак через відеофайли потребує багаторівневого підходу, що включає: технологічні обмеження (sandbox, контроль MIME); інструменти для аналізу прихованих даних; безперервне оновлення ПЗ, аналітику й моніторинг поведінки файлів.

**Список літератури**

1. Гриньов, Р.С., Сєвєрінов, О.В. (2019). Аналіз небезпеки впровадження вірусного програмного забезпечення в зображення // Комп'ютерні та інформаційні системи і технології.

2. Гриньов, Р., & Сєвєрінов, О. (2019). Метод подолання засобів захисту з використанням вразливостей графічних файлів формату BMP. Радіотехніка, 3(198), 192–202.

# СИСТЕМИ ВИЯВЛЕННЯ АТАК

Хая А.О., В'юхін Д.О., Смірнов А.О.
Харківський національний університет радіоелектроніки Харків, Україна

**Метою доповіді** є розгляд систем виявлення атак IDS (Intrusion Detection System). Це технологія, що виявляє неправомірні або шкідливі активності в комп'ютерних системах чи мережах [1]. Її основна мета - моніторинг загроз і сповіщення адміністратора про потенційні ризики. IDS може бути програмним забезпеченням або апаратним пристроєм, інтегрованим у систему чи мережу, а дані про підозрілу активність зазвичай передаються адміністратору або системам управління інформацією та подіями (SIEM).

Одним із найпоширеніших методів розвідки перед здійсненням атаки є сканування портів. Це техніка, яку використовують зловмисники для виявлення відкритих портів і доступних сервісів на цільовій системі.

Система IDS, розгорнута в мережі, аналізує трафік і може виявити ознаки сканування портів на основі таких факторів [2]:

– незвичайно висока кількість підключень до різних портів від одного джерела за короткий час;

– наявність специфічних шаблонів запитів, характерних для сканування (наприклад, послідовне надсилання SYN-пакетів без завершення з'єднання);

– використання нестандартних комбінацій прапорців TCP (наприклад, FIN- або XMAS-сканування, що використовується для обходу фільтрації).

Якщо IDS виявляє подібну активність, вона може діяти кількома способами. По-перше, система може вести логування та надсилати сповіщення адміністратору безпеки, що дозволяє оперативно реагувати та блокувати потенційного зловмисника. По-друге, якщо використовується інтегрована система виявлення та запобігання вторгнень (IPS), вона може автоматично блокувати IP-адресу атакуючого через брандмауер або інші засоби захисту. Також IDS може ініціювати зміну параметрів безпеки, наприклад, додавання нових правил у файрвол або обмеження доступу для підозрілих IP-адрес.

Система IDS дозволяє адміністраторам своєчасно реагувати на потенційні загрози. У разі використання інтегрованої IPS, можливе автоматичне блокування атакуючого, що значно знижує ризик подальшого проникнення [3]. Однак для підвищення рівня безпеки важливо також використовувати файрволи, обмеження доступу та оновлення політик безпеки, щоб запобігти несанкціонованому доступу до критично важливих сервісів.

**Список літератури**

1. Сєвєрінов, О.В., Хрєнов А.Г.. Аналіз сучасних систем виявлення вторгнень. *Системи обробки інформації* 6 (2014): 122-124.

2. Cyberset. IDS (Intrusion Detection System): Захист. 2024. URL: https://cyberset.com.ua/network/what-is-ids-intrusion-detection-system-zakhyst/

3. Barracuda. Intrusion Detection System. URL: https://www.barracuda.com/support/glossary/intrusion-detection-system

# ПРИНЦИП РОБОТИ АТАКИ SNAILLOAD

Ніконенко Д.В., В'юхін Д.О., Голобородько Ю.М.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному цифровому світі питання кібербезпеки набувають все більшої актуальності, адже, попри постійне оновлення антивірусів та захисного програмного забезпечення, кіберзлочинці не стоять на місці й постійно знаходять нові способи обходу існуючих механізмів захисту.

**Метою доповіді** є розгляд SnailLoad - нового типу атаки побічного каналу, що дозволяє віддаленому зловмиснику визначати активність користувача в інтернеті, зокрема, які вебсайти він відвідує або які відео переглядає, навіть без безпосереднього доступу до його мережевого трафіку.

Основна ідея SnailLoad полягає у використанні варіацій затримки (latency) в мережевому з'єднанні жертви для отримання інформації про її онлайн-активність [1]. Зловмисник спочатку створює контрольований сервер і спонукає жертву завантажити з нього невеликий нешкідливий файл, наприклад, зображення або стилістичний файл CSS. Це може статися під час відвідування жертвою певного вебсайту або перегляду реклами, де вбудовано посилання на сервер зловмисника. Важливо, що цей файл не містить шкідливого коду, тому антивірусні програми не виявляють загрози.

Під час завантаження файлу сервер зловмисника навмисно передає дані дуже повільно, що дозволяє йому постійно відстежувати зміни в затримці мережевого з'єднання жертви. Ці зміни можуть бути викликані іншою активністю користувача, наприклад, переглядом відео або відвідуванням інших вебсайтів. Кожен тип контенту має унікальний "відбиток" — специфічний патерн змін затримки, обумовлений розміром і частотою передачі пакетів даних. Аналізуючи ці патерни, зловмисник може визначити, який саме контент споживає жертва.

Атака типу SnailLoad становить серйозну загрозу для конфіденційності користувачів, оскільки дозволяє зловмиснику виступати в ролі "людини посередині" (man-in-the-middle) без фактичного перехоплення чи дешифрування трафіку [2]. Завдяки особливостям побічного каналу, атакуючий може повністю приховано спостерігати за онлайн-активністю жертви - наприклад, які відео вона переглядає або які сайти відвідує. При цьому весь трафік залишається зашифрованим і ніщо не викликає підозри в користувача, що робить виявлення атаки вкрай складним.

Подальші дослідження допоможуть розробити ефективні стратегії протидії таким загрозам та забезпечити більшу конфіденційність і безпеку в Інтернеті.

**Список літератури**

1. Gast S., Czerny R., Juffinger J., Rauscher F., Franza S., Gruss D. "SnailLoad: Exploiting Remote Network Latency Measurements without JavaScript". Graz University of Technology, 2024. URL: https://www.snailload.com/snailload.pdf.

2. "SnailLoad: Exploiting Remote Network Latency Measurements Leak User Activity". SnailLoad Official Website, 2024. URL: https://www.snailload.com/.

# БЕЗПЕКА З ВИКОРИСТАННЯМ SESSION-BASED AUTHENTICATION

Ляшко М.С., В'юхін Д.О., Голобородько Ю.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Традиційний підхід до автентифікації, заснований на використанні сесій, залишається популярним завдяки своїй безпеці та ефективному контролю над станом користувача.

**Метою доповіді** є розгляд контролю безпеки та можливостей масштабування за допомогою Session-based Authentication.

У цьому підході сервер зберігає унікальний ідентифікатор сесії, а браузер користувача отримує відповідний cookie. Завдяки цьому сервер може легко керувати доступом користувачів, відкликати сесії у реальному часі та реалізовувати строгі політики автентифікації.

Головна перевага Session-based Authentication полягає у можливості миттєвого відкликання доступу, що усуває проблему повторного використання викрадених токенів. У разі несанкціонованого доступу адміністратор може негайно завершити активні сесії користувача, що неможливо зробити у випадку з JWT без додаткових механізмів. Крім того, використання session cookies дозволяє захистити автентифікацію за допомогою атрибутів Secure, HttpOnly та SameSite, що значно зменшує ризик атак XSS та CSRF.

Однак Session-based Authentication має і свої недоліки, зокрема у контексті продуктивності та масштабованості. Оскільки сервер повинен зберігати інформацію про всі активні сесії, це створює додаткове навантаження на базу даних або зовнішнє сховище, таке як Redis чи Memcached. Це може призвести до проблем із продуктивністю у випадку великих навантажень або розподіленої архітектури, де необхідно підтримувати синхронізацію між декількома серверами. Крім того, якщо сховище сесій виходить з ладу, всі користувачі можуть втратити доступ до системи, що створює додатковий рівень ризику.

Попри це, Session-based Authentication залишається надійним вибором для додатків, де критично важливим є контроль доступу в реальному часі. Для вирішення проблем масштабованості можна використовувати кластери того ж Redis або розподілені бази даних, що дозволяють зберігати сесії у надійному та доступному форматі.

**Список літератури**

1. Session Management - OWASP Cheat Sheet Series. Introduction - OWASP Cheat Sheet Series. URL: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html.

2. Authgear. What Is Session Management: Threats and Best Practices - Authgear. Simplified Identity & Access Management, Built for Dev with Security - Authgear. URL: https://www.authgear.com/post/session-management.

3. Session-Based Authentication: A Detailed Guide [2024]. SuperTokens, Open Source User Authentication. URL: https://supertokens.com/blog/session-based-authentication.

# ШИФРУВАННЯ ДАНИХ У ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ

Новік Т.О., В'юхін Д.О., Фроленко В.О.
Харківський Національний університет радіоелектроніки, Харків, Україна

Сучасний світ характеризується зростаючою залежністю від цифрових технологій, що робить питання захисту даних у централізованих системах надзвичайно актуальним.

**Метою доповіді** є проведення порівняльного аналізу методів шифрування в централізованих системах.

Централізовані системи зберігають великі обсяги конфіденційної інформації, що робить їх привабливою ціллю для зловмисників. У зв'язку з цим, дослідження та впровадження ефективних методів шифрування є критично важливим завданням.

У першій половині 2024 року в блокчейні зафіксовано 185 значних інцидентів безпеки, які призвели до збитків у розмірі до 920 мільйонів доларів. Однак порівняно з першим півріччям 2022 року, коли збитки сягнули близько 2 мільярдів доларів, цей показник знизився на 54% [1]. Інцидент зі зломом DMM Bitcoin підкреслює фундаментальну важливість захисту даних у децентралізованих системах шляхом використання передових методів шифрування [2].

Вразливість, що виникла внаслідок соціальної інженерії, дозволила хакерам отримати доступ до приватних ключів і контролювати транзакції в блокчейні.

Втрата доступу до приватного ключа в децентралізованій мережі фактично означає втрату активів, адже криптовалюта в таких системах зберігається не фізично, а через криптографічний захист записів у ланцюзі блоків.

У цьому контексті шифрування виконує такі ключові функції.

1. Захист приватних ключів: використання апаратних криптогаманців із мультипідписами або шифрування ключів у корпоративних сховищах може запобігти подібним атакам.

2. Мультифакторна автентифікація (MFA): складне шифрування даних автентифікації та додатковий рівень безпеки у вигляді біометрії чи динамічних ключів унеможливили б доступ до системи лише на основі викрадених облікових даних.

3. Децентралізовані ідентифікаційні системи (DID): це ще один перспективний напрямок, де криптографічні ключі забезпечують безпеку автентифікації в децентралізованих мережах і блокують доступ для шахраїв, що діють через соціальну інженерію.

Одним з перспективних напрямків у сфері захисту даних є використання децентралізованих технологій, таких як блокчейн, Internet Computer Protocol (ICP) та смарт-протоколи. Ці технології пропонують ряд переваг щодо безпеки даних.

Серед основних переваг блокчейну виділяють децентралізацію, яка мінімізує ризик атак на центральний сервер; незмінність інформації, що ускладнює її підробку чи видалення без згоди більшості учасників мережі; прозорість транзакцій, які доступні для публічної перевірки; та підвищену стійкість до атак завдяки розподіленому зберіганню даних [3]. Водночас блокчейн має і певні обмеження: високу потребу в обчислювальних ресурсах, недостатню масштабованість для систем із високим навантаженням та значні витрати на впровадження [4].

У доповіді представлений порівняльний аналіз методів шифрування децентралізованих систем.

Основні методи шифрування в децентралізованих системах:

- асиметричне шифрування (Public-key crypto) (RSA, ECC (Elliptic Curve Cryptography), ElGamal);
- симетричне шифрування (AES, ChaCha20);
- гомоморфне шифрування (Homomorphic Encryption) [5];
- атрибутивне шифрування (Attribute-Based Encryption, ABE);
- порогове шифрування / секретне діління (Shamir's Secret Sharing);
- Zero-Knowledge Proofs (ZKP).

З огляду на все складніші схеми кібератак, подібні методи шифрування та розподіленої автентифікації мають стати стандартом у криптовалютному секторі та інших децентралізованих системах.

Комбінування методів шифрування є основною стратегією шифрування у децентралізованих системах. Перспективними напрямами залишаються: гомоморфне шифрування та ZKP, попри їхню складність.

Використання технологій блокчейну, ICP та смарт-протоколів забезпечує значне підвищення рівня безпеки та зменшує ризик зловживань.

Попри виклики, пов’язані з їх впровадженням, ці технології мають значний потенціал для розвитку та вдосконалення систем кібербезпеки у майбутньому.

**Список літератури**

1. Марія Огнівчук. Прогноз проблем безпеки для технологій блокчейн у 2024 році [електронний документ] URL: https://www.h-x.technology/ua/blog-ua/top-blockchain-security-threats-in-2024-ua.
2. Slowmist. Blockchain Security and AML Annual Report. 2024.
3. Зражевець, К. П. Дослідження рішень щодо збереження безпеки ключів у блокчейн-технологіях. Харків, 2023 URL: https://openarchive.nure.ua/handle/document/24113
4. Терещенко, Г. Ю. Дослідження та оцінка ефективності алгоритмів шифрування, що використовуються в технології Блокчей Харків, 2020, URL:http://openarchive.nure.ua/handle/document/14878.
5. Khalimov, Gennady, et al. "Encryption Based on the Group of the Hermitian Function Field and Homomorphic Encryption." 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T). IEEE, 2021.

# КРИПТОГРАФІЧНІ МЕХАНІЗМИ ЗАХИСТУ СМАРТ-КОНТРАКТІВ

Мокрій В.С., В'юхін Д.О., Власов А.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Смарт-контракти є елементом технології блокчейн, здатним автоматично виконувати угоди між сторонами без залучення третіх осіб. Їхня безпека базується на застосуванні криптографічних методів, де геш-функції відіграють центральну роль. Геш-функція являє собою математичний алгоритм, який перетворює вхідні дані на вихідне значення (геш) фіксованої довжини.

**Метою доповіді** є аналіз криптографічних механізмів, що застосовуються для захисту смарт-контрактів, зокрема алгоритмів гешування, їх стійкості до атак і практичного застосування у блокчейн-системах.

Геш-функції застосовуються у смарт-контрактах для забезпечення захисту конфіденційної інформації, формування цифрових підписів та механізмів довіри.

Вони також слугують для створення унікальних ідентифікаторів транзакцій і користувачів. У фінансових блокчейн-додатках ці функції є основою для доказів нульового розголошення, що дозволяє особам підтверджувати знання певних даних, не розкриваючи їх [1].

Проте використання геш-функцій у смарт-контрактах не позбавлене ризиків. Наприклад, можливі атаки методом грубої сили, використання веселкових таблиць та криптоаналітичні атаки. Зокрема, атаки на день народження можуть бути використані для виявлення колізій, а атаки розширення довжини - для маніпулювання хешем. Згідно з дослідженням, застарілі алгоритми, такі як MD5 і SHA-1, були зламані, отже, їх не можна використовувати у смарт-контрактах.

Окрім вибору надійного алгоритму, важливим є його правильне втілення у код смарт-контракту. Навіть найміцніші геш-функції можуть виявитися марними, якщо реалізація містить логічні похибки або слабкі місця. Частими помилками є повторне використання одних і тих же даних для гешування, неправильне формування повідомлень чи ігнорування принципів криптографічної ентропії. Отже, надзвичайно важливо не тільки обрати сучасні алгоритми, але й дотримуватися найкращих практик програмування та пройти аудит безпеки.

Для підвищення рівня безпеки необхідно застосовувати надійні криптографічні алгоритми, такі як SHA-256 та Keccak-256, які використовуються в блокчейнах Bitcoin і Ethereum. Додатково, рекомендується використовувати алгоритми гешування з сіллю, що ускладнює генерацію гешів за допомогою таблиць, а також алгоритми з регульованою складністю, такі як Argon2, які підвищують витрати ресурсів на злом [3].

Також важливо впровадити механізми, які забезпечують стійкість до квантових обчислень, оскільки розвиток квантових комп'ютерів може зробити традиційні геш-функції вразливими. Наприклад, алгоритм SHA-3 (Keccak) вважається більш стійким до потенційних квантових атак у майбутньому [4].

Аналіз показав, що геш-функції MD5 і SHA-1 більше не відповідають сучасним вимогам безпеки через їх низьку стійкість до колізій та наявність успішних атак. SHA-256 та Keccak-256 забезпечують високий рівень криптографічної надійності, що робить їх основними алгоритмами безпеки для блокчейнів, таких як Bitcoin і Ethereum. Якщо замінити SHA-1 на SHA-3, то системи стануть більш стійкими до потенційних атак, зокрема загроз з боку квантових комп'ютерів, завдяки вдосконаленій архітектурі та високій криптографічній стійкості.

Окрім технічних нюансів, значущу роль у безпеці смарт-контрактів відіграє грамотне керування ключами. Втрата секретного ключа може призвести до повного контролю над контрактом з боку третіх осіб. З цією метою застосовуються апаратні гаманці, захищені середовища виконання (TEE), а також методи децентралізованого зберігання ключів, які мінімізують ймовірність компрометації. Надійне керування ключами є основоположним елементом загальної стратегії кібербезпеки в екосистемі блокчейн.

Захист смарт-контрактів вимагає не лише використання надійних геш-функцій. Також необхідний комплексний підхід, що включає застосування додаткових механізмів захисту, таких як багатофакторна автентифікація, оновлення алгоритмів та аудит безпеки. Крім того, для зменшення ризику атак рекомендується використовувати багаторівневий підхід до безпеки, що поєднує кілька методів шифрування. Використання сучасних криптографічних методів може допомогти зменшити ризик атаки та підвищити довіру до блокчейн-програм.

**Список літератури**

1. Вимоги до безпеки смарт-контрактів у фінансових застосунках: ключові аспекти та рекомендації. URL: https://cryptoznannya.com.ua/vimogi-do-bezpeki-smart-kontraktiv-u-finansovix-zastosunkax/.

2. Аналіз і обґрунтування використання наявних блокчейн-рішень для захисту цифрових активів. URL:https://openarchive.nure.ua/entities/publication/64a5900f-8de4-4582-ad1b-7cf88140bf85.

3. 8 найкращих практик для забезпечення безпеки блокчейну. URL: https://www.h-x.technology/ua/blog-ua/8-best-practices-for-blockchain-security-ua.

4. Зражевський К.П. Дослідження рішень щодо збереження безпеки ключів у блокчейн-технологіях: кваліфікаційна робота (магістерська). ХНУРЕ, 2023.URL:https://openarchive.nure.ua/server/api/core/bitstreams/8622fcbb-630b-4c03-ba51-89cfc4a77bc8/content.

# ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ КРИПТОАНАЛІЗУ

Леонова А.О., В'юхін Д.О., Лук`яненко М.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Криптоаналіз - це процес виявлення вразливостей у криптографічних алгоритмах з метою дешифрування інформації без доступу до ключа. З появою штучного інтелекту (ШІ), криптоаналіз отримав інструменти для автоматизації, зокрема методи машинного та глибокого навчання, - тим самим зменшуючи час, підвищуючи точність і дозволяючи аналізувати навіть складні шифри.

**Метою роботи** є розглядання переваг використання інструментів ШІ у сучасному криптоаналізі.

Основну увагу варто приділити практичним перевагам автоматизованого криптоаналізу з використанням ШІ. Це значне скорочення часу, необхідного на аналіз складних криптографічних структур, зменшення людського фактору та можливість обробки великих обсягів даних у реальному часі. Наприклад, системи, що використовують нейронні мережі, можуть автоматично розпізнавати зашифровані повідомлення, аналізувати їх на предмет шаблонів, а також оцінювати ефективність захисту. У режимі «чорного ящика» ШІ здатен розпізнавати приховані закономірності в зашифрованих даних, здійснювати статистичний аналіз і вивчати поведінку криптографічних протоколів [1]. Це дозволяє автоматизувати атаки, які раніше виконувалися вручну, наприклад, атаки з відкритим текстом або диференціальний криптоаналіз.

ШІ може імітувати поведінку шифру та поступово навчатися обходити його, що дає можливість здійснювати автоматизований криптоаналіз без явного декодування алгоритму [2].

ШІ також застосовується в контексті квантової криптографії, де традиційні засоби криптоаналізу часто безсилі. Алгоритми машинного навчання можуть допомагати в аналізі квантових каналів, виявленні вразливостей протоколів квантового обміну ключами та симуляції квантових атак [3]. Поєднання ШІ та квантових обчислень створює новий клас інструментів криптоаналізу, здатних адаптуватися до систем, які досі вважалися незламними. Але масове впровадження ШІ в криптоаналіз створює нові ризики. Технології, які використовуються для захисту, можуть бути адаптовані і для атак.

Загалом, використання штучного інтелекту для автоматизації криптоаналізу є потужним інструментом, що дозволяє значно підвищити ефективність інформаційної безпеки.

**Список літератури**

1. AI in Cryptography. (електронний ресурс): URL: https://insights2techinfo.com/ai-in-cryptography.

2. Neural Cryptography: (електронний ресурс): URL: https://en.wikipedia.org/wiki/Neural_cryptography.

3. Artificial Intelligence and Quantum Cryptography.: (електронний ресурс): URL: https://jast-journal.springeropen.com/articles/10.1186/s40543-024-00416-6.

# ОРГАНІЗАЦІЯ ДОВІРЕННОГО СЕРЕДОВИЩА ВИКОНАННЯ З ВИКОРИСТАННЯМ QEMU ТА TRUST DOMAIN EXTENSIONS ВІД INTEL

Шулік П.В., Федюшин О.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Для ефективного захисту і обробки інформації у сучасних комп'ютерних системах використовується архітектура з розподілом на два світа: звичайний (non secure world) – де працює звичайне програмне забезпечення та захищений світ (secure world), в якому ведеться робота з конфіденційною інформацією. Для організації такого розподілу необхідна підтримка як з боку програмного так і з боку апаратного забезпечення. Як приклад програмної підтримки такого підходу можна привести опен соурс фреймфорк OP-TEE [1].

OP-TEE фреймфорк орієнтований на платформу ARM та технологію ARM TrustZone де периферія теж поділяється для роботи з захищеною та звичайною інформацією. Підтримка OP-TEE з боку Intel-x86 платформ є проблематичною, тому що Intel не має подібних рішень. Але Intel-x86 має розвинену апаратну підтримку віртуалізацій, де для secure world може використовуватися емулятор QEMU/KVM, на якому і виконується secure world.

**Метою даного дослідження** є розгляд одного із підходів інтеграції OP-TEE фреймворка з Intel-X86 платформами із використанням технологій віртуалізації. **Предметом дослідження** є програмні засоби інтеграції OP-TEE фреймворка с Intel-X86 з використанням QEMU/KVM [2].

Суть інтеграції OP-TEE складається в заміщенні технології TrustZone віртуальними машинами QEMU/KVM та технологією Intel Trust Domain Extensions (Intel TDX). Intel TDX вводить нові архітектурні елементи, які допоможуть розгорнути апаратно ізольовані віртуальні машини під назвою Trust Domains (TDs) на основі Intel® Total Memory Encryption - Multi-Key (Intel TME) і режим виконання процесора під назвою Secure-Arbitration Mode (SEAM). У цьому випадку основна операційна система і гіпервізор KVM (а також емулятор QEMU, де виконується робота з конфіденційною інформацією) ізолюються одна від одного.

Таким чином, практично технологія Intel TDX виконує дуже схожу функціональність з ARM TrustZone, може використовуватися сумісно з OP-TEE фрейворком.

**Список літератури**

1. GlobalPlatform, Inc.: TEE System Architecture Version 1.2 (Nov 2018), GPD SPE 009

2. Arshad Nehal, Priyanka Ahlawat Securing IoT applications with OP-TEE from hardware level OS: 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA) 10.1109/ICECA.2019.8822040

# ВИКОРИСТАННЯ ВІРТУАЛЬНИХ МАШИН ДЛЯ ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ НА ПЛАТФОРМАХ INTEL

Шулік П.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Вже понад більш ніж 10 років в операційних системах для захисту інформації існує підхід з використанням двох операційних систем, де система поділяється на два світи: звичайний (non secure world) – де працює звичайне програмне забезпечення, та захищений світ (secure world), в якому ведеться робота з секретною інформацією. Як приклад програмної підтримки такого підходу можна привести опен соурс фреймфорк OP-TEE [1]. Також для такого розподілу необхідна і апаратна підтримка, де периферія теж поділяється для роботи з захищеною та звичайною інформацією. Така підтримка існує з боку ARM систем і називається ARM TrustZone. В ARM TrustZone вводиться захищений режим роботи ARM ядра –у якому виконується робота з секретною інформацією, яка не повинна бути доступною для основної операційної системи та її додатків. Підтримка такого підходу з боку Intel-x86 платформ є проблематичною, тому що Intel не має подібних рішень. Але Intel-x86 має розвинену апаратну підтримку віртуалізацій, де для організації secure world може використовуватися окрема віртуальна машина.

**Метою даного дослідження** є розгляд одного із підходів інтеграції OP-TEE фреймворка з Intel-X86 платформами із використанням технологій віртуалізації. **Предметом дослідження** є програмні засоби інтеграції OP-TEE фреймворка с Intel-X86.

Суть інтеграції OP-TEE складається в заміщенні технології TrustZone віртуальними машинами та технологіями процесорів Intel-x86 VT-d/VT-x, де апаратні ресурси розподіляються між віртуальними операційними системами, і забезпечують ізоляцію ресурсів та інформації між операційними системами. У якості арбітра, який керує переключенням роботи процесора та доступу до ресурсів може виступати гіпервізор першого типу. У якості такого гіпервізора в запропонованому рішенні виступає гіпервізор компанії Intel Kernel Guard Technology (iKGT). Основний підхід закладений в iKGT називається Intel Supervisor Mode Execution Prevention (SMEP) - запобігання виконання коду в режимі супервізора. Технологія полягає в запобіганні виконання коду, розташованого на сторінці користувача (тобто звичайний світ, який не повинен мати доступу до захищеної інформації), при поточному рівні привілеїв рівному 0 (рівень доступу до захищеної інформації).

Таким чином, практично технологія Intel SMEP виконує дуже схожу функціональність з ARM TrustZone може використовуватися сумісно з OP-TEE фреймворком.

**Список літератури**

1. GlobalPlatform, Inc.: TEE System Architecture Version 1.2 (Nov 2018), GPD SPE 009.

# АВТЕНТИФІКАЦІЇ ТА БЕЗПЕКА IOT-ПРИСТРОЇВ У КОНТЕКСТІ АРХІТЕКТУРИ НУЛЬОВОЇ ДОВІРИ

Нєдєльніцев І.В., Антіпов І.Є.
Харківський національний університет радіоелектроніки Харків, Україна

**Метою доповіді** є аналіз особливостей інтеграції принципів архітектури нульової довіри (ZTA) з пристроями Інтернету речей (IoT) для підвищення рівня їх безпеки без суттєвого зниження зручності та збільшення витрат.

**В доповіді** наводяться рішення для подолання основних викликів, пов'язаних із впровадженням ZTA в IoT-середовищах, зокрема: використання додаткових факторів автентифікації для зменшення незручностей для користувача, кешування автентифікаційних даних, застосування існуючих бібліотек/технологій для оптимізації витрат на розробку ПЗ, перенесення ресурсомістких обчислювальних операцій у хмарні сервіси задля покращення продуктивності систем та автономності роботи пристроїв.

Надмірна автентифікація в IoT може бути незручною через обмежені інтерфейси пристроїв. Як рішення пропонується використання геолокації, що дозволяє автоматично перевіряти розташування пристроїв і виявляти аномальний доступ [1]. Інший підхід – біометрична автентифікація, яка забезпечує високий рівень безпеки і є зручнішою за паролі [2]. Додатково можна кешувати токени автентифікації для зменшення ручних дій, зберігаючи принципи Zero Trust.

Впровадження складних методів автентифікації збільшує витрати часу і коштів на розробку. Оптимальним є використання готових бібліотек (TLS/SSL, OAuth 2.0, біометрії), що економить ресурси і підвищує надійність [3]. Економічно вигідним рішенням також є використання хмарних сервісів автентифікації від платформ (AWS IoT, Azure IoT), які відповідають сучасним вимогам безпеки.

IoT-пристрої часто обмежені ресурсами і батареєю, що ускладнює постійну автентифікацію. Рішенням є кешування автентифікаційних даних для зменшення навантаження, а також використання легковагих алгоритмів. Інший підхід – винос складних обчислень у хмару, де обчислювальні ресурси необмежені. Пристрій лише надсилає дані і отримує результат, економлячи ресурси та енергію.

Впровадження ZTA в IoT підвищує безпеку, балансуючи між зручністю, витратами на розробку та ресурсними обмеженнями пристроїв. Комбінація підходів дозволяє покращити безпеку IoT без зниження продуктивності чи зручності.

**Список літератури**

1. Can Zero Trust Work with the IoT? Red River: вебсайт. URL: https://redriver.com/cybersecurity/zero-trust-iot.

2. Importance of Biometric in IoT Application. M2SYS Blog, 2019: вебсайт. URL: https://www.m2sys.com/blog/guest-blog-posts/importance-of-biometric-in-iot-application/.

3. Morrow S. The Dangers of "Rolling Your Own" Encryption. – Infosec Institute, 28.03.2019: вебсайт. URL: https://www.infosecinstitute.com/resources/cryptography/the-dangers-of-rolling-your-own-encryption/.

# МЕТОДИ ОЦІНКИ СТІЙКОСТІ ЛЕГКОВАГИХ СИМЕТРИЧНИХ ШИФРІВ ДО ДИФЕРЕНЦІЙНО-ЛІНІЙНИХ АТАК

Цемма Д.О., Руженцев В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Легковагова криптографія є головним інструментом, що забезпечує безпеку пристроїв з обмеженими обчислювальними ресурсами. Але, не дивлячись на її ефективність, такі шифри можуть бути вразливими до диференційно-лінійного криптоаналізу (DL-криптоаналізу), що поєднує методи лінійного та диференційного аналізу [1].

**Метою доповіді** є аналіз методів оцінки стійкості легковагових симетричних шифрів до диференційно-лінійного криптоаналізу та виявлення основних факторів, що впливають на їхню безпеку.

DL-криптоаналіз використовує статистичні закономірності між зашифрованими та відкритими текстами щоб зменшити простір ключів.

Аналіз стійкості легковагових шифрів, таких як Ascon, PRESENT та LED, показує, що їхня безпека залежить від структури S-Box та кількості раундів [2].

Для підвищення стійкості пропонується збільшення кількості раундів, модифікація нелінійних компонентів та використання адаптивних алгоритмів зміни ключів [3].

Рекомендовані заходи підвищення стійкості:

– використовувати S-Box з високою нелінійністю та низькою диференційною/лінійною ймовірністю;
– збільшення кількості раундів (без значної втрати продуктивності);
– проєктування раундових функцій із мінімізацією лінійних кореляцій.

Методи оцінки стійкості до диференційно-лінійних атак є важливою складовою криптографічної експертизи легковагих шифрів. Їх застосування дозволяє:

– виявити потенційні слабкі місця в дизайні;
– визначити необхідну кількість раундів для забезпечення безпеки;
– порівняти ефективність різних шифрів.

Таким чином, розробка та оцінка стійкості легковагових шифрів до DL-криптоаналізу є критично важливими для забезпечення безпеки IoT-систем та вбудованих пристроїв.

**Список літератури**

1. Бірюков А., Дункельман О., Келлер Н. Диференційно-лінійний криптоаналіз Serpent. Journal of Cryptographic Engineering, 2017.

2. Мендель Ф., Над Т., Шлеффер М. Диференційно-лінійний криптоаналіз спрощеного PRESENT. Fast Software Encryption, 2019.

3. Столлінгс В. Криптографія та безпека мереж: принципи та практика. Pearson, 2020.

# СИСТЕМИ ОБФУСКАЦІЇ ТРАФІКУ ДЛЯ ЗАХИСТУ ВІД ГЛИБОКОЇ ІНСПЕКЦІЇ ПАКЕТІВ

Пліщенко В.С., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Обфускація мережевого трафіку є методом захисту від перехоплення і аналізу вмісту трафіку в інформаційно-комунікаційних системах, завдяки чому цей метод широко застосовується для уникнення блокування мережевих протоколів DPI-системами і мережевими фільтрами [1].

Сучасні системи глибокої інспекції трафіку набули значного розвитку і активно застосовують методи машинного навчання, які дозволяють виявляти протоколи обфускації по статистичних характеристиках, ентропії, часових інтервалах між пакетами та по інших паттернах трафіку. У зв'язку з цим актуальним є пошук адаптивних комбінованих рішень [2, 3], які забезпечують високий рівень стійкості до атак та до аналізу обфускованого трафіку при збереженні продуктивності мережі.

**Метою доповіді** є розгляд сучасних підходів до обфускації трафіку, методів розрізнення обфускованого трафіку, а також визначення критеріїв та порівняння за ними сучасних систем, що реалізують різні підходи до обфускації трафіку.

В доповіді наводяться результати практичного порівняння систем обфускації трафіку Shadowsocks, V2Ray, obfs4 та Rosen за наступними критеріями: стійкість до DPI, стійкість до атак (активного втручання в протокол обфускації) та статистичного аналізу, а також ефективність, продуктивність і ресурсоємність обфускації. Наведені дані показують, що кожна з розглянутих систем має свої переваги та недоліки, і тому найбільш ефективним підходом є комбіноване застосування одночасно декількох рішень, зокрема стеку систем обфускації трафіку Shadowsocks + V2Ray + Cloudflare CDN [4].

**Список літератури**

1. Wu, M., Sippe, J., Sivakumar, D., Burg, J., Anderson, P., Wang, X., ... & Wustrow, E. How the Great Firewall of China Detects and Blocks Fully Encrypted Traffic. In 32nd USENIX Security Symposium (USENIX Security 23). 2023. С. 2653-2670. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/wu-mingshi.

2. Alwhbi, I. A., Zou, C. C., & Alharbi, R. N. Encrypted Network Traffic Analysis and Classification Utilizing Machine Learning. Sensors. 2024. 24. №11:3509. DOI: https://doi.org/10.3390/s24113509.

3. Zhou, J.; Fu, W.; Hu, W.; Sun, Z.; He, T.; Zhang, Z. Challenges and Advances in Analyzing TLS 1.3-Encrypted Traffic: A Comprehensive Survey. Electronics. 2024. 13. №20:4000. DOI: https://doi.org/10.3390/electronics13204000.

4. Umar, A. Obfuscating Network Traffic to Circumvent Censorship. 2021. URL: https://sy.st/archive/Paper/obfuscating-network-traffic.pdf.

# МЕТОДИ ЗАХИСТУ ВІД ФІШИНГОВИХ АТАК

Філатова А.С., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Фішинг – це одна з найпопулярніших та найнебезпечніших атак з використанням методів соціальної інженерії, оскільки дозволяє отримати несанкціонований доступ до інформаційно-телекомунікаційних систем через фактор людської помилки користувачів, які можуть довіритись фішинговим email/sms повідомленням, що містять зловмисне програмне забезпечення та/або посилання на зловмисні ресурси.

Згідно з сучасними дослідженнями [1, 2] фінансові наслідки фішингових атак зросли, оскільки компанії переходять на віддалену та гібридну роботу. Такі атаки завдають великим компаніям збитків майже на 15 мільйонів доларів щорічно. Дослідження в Інституті Понемону [1] також продемонстрували, що добре навчений персонал здатен зменшити ефективність фішингових атак на 50%. Це означає, що окрім технічних методів протидії фішингу важливим чинником економічної та інформаційної безпеки компаній є обізнаність та навченість працівників щодо дій при отриманні фішингових повідомлень.

**Метою доповіді** є дослідження та моделювання сучасних методів захисту від фішингових атак для визначення та порівняння їхньої ефективності.

**В доповіді** наводяться результати моделювання наступних найпоширеніших методів фільтрації фішингових повідомлень [2]: автентифікація домену відправника; перевірка IP-адреси відправника та наявних у повідомленні URL-адрес за актуальними чорними списками; розпізнання фішингових повідомлень за їхнім вмістом та за структурою наявних у повідомленні URL-адрес методами машинного навчання.

Наведені дані показують, що найбільш високу ймовірність розрізнення фішингових повідомлень (для подальшого їх блокування) забезпечує комплексне застосування зазначених методів. Втім, завжди присутня в роботі таких методів ймовірність помилок першого та другого роду (що підтверджується іншими дослідженнями [2]) зумовлює те, що добре навчений персонал є важливою «останньою лінією захисту» від фішингових атак.

**Список літератури**

1. The Ponemon 2021 Cost of Phishing Study. URL: https://www.bankinfosecurity.com/whitepapers/-w-8959

2. Сєвєрінов О.В., Шевцов В.О., Сокол-Кутиловська А.С.. Аналіз сучасних методів атак на електронні ресурси органів управління // Системи озброєння і військова техніка 1. – 2017, С. 65-68.

3. Takashi Koide, Naoki Fukushi, Hiroki Nakano, Daiki Chiba. ChatSpamDetector: Leveraging Large Language Models for Effective Phishing Email Detection. DOI: https://doi.org/10.48550/arXiv.2402.18093

# АНАЛІЗ ВРАЗЛИВОСТЕЙ БІОМЕТРИЧНИХ СИСТЕМ АВТЕНТИФІКАЦІЇ ЗА ВІДБИТКАМИ ПАЛЬЦІВ ДО АТАК ІЗ ЗАСТОСУВАННЯМ ГЕНЕРАТИВНО-ЗМАГАЛЬНИХ МЕРЕЖ

Олешко І.В., Луценко В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Біометричні системи автентифікації використовують унікальні фізіологічні або поведінкові характеристики людини такі, як відбитки пальців, обличчя чи голос для ідентифікації особи.

Системи біометричної автентифікації порівнюють біометричні дані користувача з даними, що зберігаються в базі шаблонів і, якщо зразки збігаються, автентифікація вважається успішною і доступ надається [1].

Прогрес у сфері штучного інтелекту створює принципово нові загрози для біометричних систем автентифікації.

Генеративні змагальні мережі синтезують біометричні зразки даних, здатні обходити захисні механізми [2].

Генеративно-змагальні мережі є архітектурою глибокого навчання, яка включає дві нейромережі.

Генеративна мережа створює нові зразки, схожі на реальні дані. Дискримінаторна мережа вчиться відрізняти справжні дані від синтезованих. Під час спільного навчання дискримінатор забезпечує генеративну мережу зворотним зв'язком, що допомагає удосконалювати якість створених зразків [3].

Одним з найпоширеніших методів біометричної автентифікації наразі є автентифікація за відбитком пальця. Штучне відтворення відбитків пальців має на меті відтворити розташування та розподіл дрібних деталей оригінального відбитку.

Сучасні схеми штучного відтворення складаються з двох етапів: спочатку реконструюється поле орієнтації на основі дрібних деталей, а потім відтворюється папілярний візерунок за допомогою реконструйованого поля орієнтації [3].

$$o(z) = \left[ o_\infty + \frac{1}{2} \times \left( \sum_{i=1}^{\mathrm{K}} \arg(z - z_{ci}) - \sum_{j=1}^{\mathrm{L}} \arg(z - z_{dj}) \right) \right] mod\ \pi \quad (1)$$

Поле орієнтації відтворюється з використанням моделі нуль-полюс. У цьому підході кожне ядро у відбитку пальця розглядається як нуль, а кожна дельта як полюс.

У наведеній формулі (1) $z_{ci}$ та $z_{dj}$ є відповідно і-та ядра та j-та дельти відбитка пальця, а $o_\infty$ є константним корекційним членом. У точці $z$ вплив ядра $z_{ci}$ дорівнює $\frac{1}{2} \times \arg(z - z_{ci})$, а вплив дельти $z_{dj}$ дорівнює $\frac{1}{2} \times \arg(z - z_{dj})$ [4].

Генеративно-змагальна мережа для штучного відтворення відбитків пальців включає три основні компоненти: генератор, що створює синтетичні

зображення, кодувальник, який реконструює відбитки на основі карт дрібних деталей для забезпечення точної структури, та редактор атрибутів, що модифікує візуальні характеристики.

Для оцінки ефективності запропонованого підходу було проведено штучне відтворення відбитків пальців з бази даних NIST SD4.

Для імітування автоматичного розпізнавання відбитків пальців у системах, використовувалось відкрите програмне забезпечення Bozorth3 [5].

Система біометричної автентифікації помилково прийняла як істинні 97 % зразків, створених генеративно-змагальною мережею.

**Метою доповіді** є аналіз вразливостей сучасних біометричних систем автентифікації за відбитками пальців до атак, які використовують методи та технології штучного інтелекту.

Розглянуто методи створення синтетичних зразків, що можуть імітувати реальні біометричні дані та проходити автентифікацію в системах захисту.

В доповіді наводяться результати вимірювань ефективності атак на біометричні системи автентифікації за відбитками пальців з використанням генеративних моделей штучного інтелекту.

Наведені дані показують, що системи автентифікації за відбитками пальців виявили вразливість до синтетичних шаблонів, створених за допомогою генеративно-змагальних мереж.

**Список літератури**

1. Shoroog Albalawi, Lama Alshahrani, Nouf Albalawi,Reem Kilabi, and A'aeshah Alhakamy. A comprehensive overview on biometric authentication systems using artificial intelligence techniques. International Journal of Advanced Computer Science and Applications, 13(4):1–11, 2022. DOI: http://dx.doi.org/10.14569/IJACSA.2022.0130491

2. Bontrager, P.; Roy, A.; Togelius, J.; Memon, N.D.; Ross, A. DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution. In Proceedings of the 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), Redondo Beach, CA, USA, 22–25 October 2018; pp. 1–9. DOI: http://dx.doi.org/10.1109/BTAS.2018.8698539

3. Bouzaglo, Rafael, and Yosi Keller. Synthesis and reconstruction of fingerprints using generative adversarial networks. arXiv preprint arXiv:2201.06164, 2022. DOI: https://doi.org/10.48550/arXiv.2201.06164

4. Fan, L.L.; Wang, S.G.; Wang, H.F.; Guo, T.D. Singular Points Detection Based on Zero-Pole Model in Fingerprint Images. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 30, no. 6, pp. 929-940, June 2008 . DOI: https://doi.org/10.1109/TPAMI.2008.31

5. NIST Biometric Image Software (NBIS). – 2010. – Режим доступу до ресурсу: https://www.nist.gov/services-resources/software/nist-biometric-image-software-nbis

# ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В DLP-СИСТЕМАХ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Єнальєва Г.С., Сєвєрінов О.В., Сидоренко З.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні загрози інформаційній безпеці постійно розвиваються, створюючи значні проблеми для захисту конфіденційних даних. Системи Data Loss Prevention (DLP) є ключовим інструментом у боротьбі з витоком інформації. Однак звичайні методи часто виявляються недостатньо ефективними в умовах зростаючої складності кіберзагроз [1]. Впровадження штучного інтелекту (ШІ) у DLP-системи дозволяє значно підвищити ефективність виявлення, класифікації та запобігання втратам даних. Це робить їх більш адаптивними та надає можливість реагувати на нові атаки [2]. Інтеграція ШІ у DLP-системи покращує автоматизоване виявлення загроз завдяки алгоритмам машинного навчання, які аналізують значні обсяги трафіку в реальному часі, виявляючи аномалії та підозрілу активність. Обробка природної мови (NLP) сприяє більш точному контекстуальному аналізу даних, що забезпечує кращу класифікацію конфіденційної інформації. Головною перевагою цих систем є здатність знижувати кількість хибних спрацьовувань, оскільки ШІ ефективно розрізняє справжні загрози від безпечних дій, що посилює заходи безпеки [3].

**Метою доповіді** є аналіз можливостей використання штучного інтелекту в DLP-системах для підвищення ефективності інформаційної безпеки, зокрема виявлення загроз, класифікації конфіденційних даних та мінімізації ризику їх витоку.

Інтеграція ШІ дозволяє DLP-системам не лише реагувати на порушення, але й прогнозувати ризики, аналізувати поведінку користувачів і розрізняти нормальні та підозрілі дії.

В доповіді наводяться результати дослідження впливу алгоритмів машинного навчання та прогнозної аналітики на функціональність DLP. Адаптивність і масштабованість є значними перевагами використання ШІ в DLP-системах, оскільки алгоритми постійно навчаються на основі нових даних, що дозволяє коригувати політики безпеки відповідно до нових загроз. Це особливо корисно для великих організацій із розгалуженою розподіленою інфраструктурою, де традиційні системи безпеки можуть не справлятися з обробкою значних обсягів інформації.

Використання ШІ в DLP-системах суттєво підвищує інтеграцію з SIEM та SOAR системами. Штучний інтелект автоматично передає дані про витоки (або потенційні витоки) з DLP до SIEM (систем управління інформаційною безпекою), які аналізують ці дані у загальному контексті безпеки: логіни, мережеві аномалії, привілейовані дії. Потім, у SOAR (платформах автоматизації відповідей), ШІ може ініціювати автоматичне блокування, сповіщення або розслідування.

Важливою складовою є також виявлення внутрішніх загроз. Системи, керовані ШІ, можуть аналізувати поведінку користувачів, створюючи профілі типових дій і виявляючи відхилення, які можуть свідчити про потенційні внутрішні загрози [4]. Крім того, використання прогнозної аналітики дає змогу передбачати можливі витоки даних шляхом аналізу історичних тенденцій, тим самим полегшуючи коригування політик безпеки. Цей комплексний підхід сприяє створенню безпечнішого та стійкішого інформаційного середовища [2].

Попри значні переваги, інтеграція ШІ у DLP-системи супроводжується певними викликами. Основна проблема полягає в забезпеченні конфіденційності даних, враховуючи, що для навчання моделей ШІ зазвичай потрібні великі набори даних. Крім того, постійна розробка та підтримка AI-рішень вимагає значних фінансових і кадрових ресурсів. Додатковий виклик є складність інтерпретації рішень, керованих ШІ, може створювати перешкоди, оскільки деякі моделі працюють як "чорний ящик". Ця непрозорість ускладнює здатність аналізувати основні фактори, що сприяють певним активаціям [3].

Також деяким проблемним питанням є те, що навчання моделей потребує якісних даних.

Останнім часом проблемним стає можливість обходу ШІ-перевірки шляхом обфускації даних. Подолання цієї проблеми можливо тільки у разі правильного навчання і використання комбінації технологій.

Впровадження DLP-систем на основі штучного інтелекту є значним прогресом у розвитку інформаційної безпеки.

Такі системи пропонують підвищену точність, масштабованість і гнучкість.

Хоча можуть виникнуть певні виклики, як захист конфіденційності даних та значні ресурси, вони можуть бути ефективно вирішені шляхом продуманого планування та впровадження сучасних технологічних рішень.

**Список літератури**

1. Ушатов В., Сєвєрінов О.В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки // Global Cyber Security Forum : матеріали Першого міжнародного науково-практичного форуму, 14 – 16 листопада 2019 р. – Харків : ХНУРЕ, 2019. – С. 104–105.

2. Dorcas Esther. AI in Data Loss Prevention: Safeguarding Sensitive Data Against Unauthorized Access and Leakage.

3. Kunle-Lawanson O. The Role of AI in Information Security Risk Management. World Journal of Advanced Engineering Technology and Sciences, vol. 7, no. 2, 2022, pp. 308–319.

4. Пасєка І., Сєвєрінов О.В. Проблеми впровадження системи аналітики поведінки користувачів та сутностей // Global Cyber Security Forum : матеріали Першого міжнародного науково-практичного форуму, 14 – 16 листопада 2019 р. – Харків: ХНУРЕ, 2019. – С. 82–83.

# МЕТОД ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ У СИСТЕМАХ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ

Євгеньєв А.М., Сидоренко З.М., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Промисловий Інтернет речей (Industrial Internet of Things, IIoT) - це технологія, що поєднує інтелектуальні датчики, пристрої та програмне забезпечення для автоматизації, моніторингу та управління промисловими процесами. Однією з ключових проблем IIoT є забезпечення цілісності даних, тобто гарантія того, що передані та збережені дані залишаються незмінними, точними та достовірними без несанкціонованих змін або пошкоджень [1].

Забезпечення цілісності даних у системах IIoT є критичним аспектом інформаційної безпеки, оскільки порушення цілісності може призвести до неправильного функціонування обладнання, аварій та втрати довіри до системи. У промисловому середовищі це питання набуває ще більшого значення, зважаючи на автоматизовані процеси та великі об'єми взаємодіючих пристроїв.

**Метою доповіді** є аналіз методів забезпечення цілісності даних у системах промислового Інтернету речей. Розгляд методу забезпечення цілісності на основі використання завадостійких кодів.

На даний час для забезпечення цілісності даних в IIoT використовуються різні методи [1]:

– криптографічні геш-функції на основі алгоритмів SHA-2, SHA-3 для формування контрольної суми (гешу);

– цифровий підпис на основі алгоритмів RSA, ECDSA, постквантових схем на решітках;

– протоколи безпечної передачі TLS, DTLS, MQTT-SN з шифруванням, що підтримує контроль цілісності (наприклад, HMAC);

– апаратні модулі захисту (HSM, TPM) перевірки автентичності даних на рівні пристроїв;

– запис даних від пристроїв у блокчейн або розподілений реєстр, в яких будь-яка зміна залишає цифровий слід.

Але на даний час ці методи не в повній мірі забезпечують цілісність даних. Існує багато загроз, яким традиційні системи не в повній мірі можуть протистояти. Також традиційні криптографічні методи (AES, RSA, ECC) не можуть виправляти помилки, спричинені шумами або апаратними збоями. Більшість з них не забезпечать стійкість у постквантовий період.

Саме тому перспективним рішенням є поєднання криптографії та завадостійкого кодування. Кодові криптосистеми (McEliece, Niederreiter) можуть забезпечити одночасно шифрування та перевірку на цілісність, що особливо актуально у постквантовий період [2-4].

Дані криптосистеми засновані на застосуванні одного з підкласів альтернативних кодів - кодів Гоппи, які мають найкращі характеристики в

класі лінійних блокових кодів. Характерною властивістю кодів Гоппи є той факт, що є велика кількість способів формування коду із заданими параметрами, що потенційно може вирішити задачу не тільки забезпечення високої стійкості до перешкод, але і цілісності даних в системах промислового Інтернету речей [5]. У завадостійких кодах як і в кодах автентифікації послідовності, що передаються, містять спеціальну надлишкову інформацію. Різниця полягає в тому, що якщо у звичайних завадостійких кодах є одне правило кодування, що відповідає фіксованому коду, то в кодах автентифікації є багато правил кодування, з яких передавач чи приймач може обирати для використання одне конкретне (таємне) правило. Саме тому звичайні завадостійкі коди не можуть бути використані для забезпечення цілісності даних. Одним із небагатьох класів лінійних блокових кодів, що мають безліч законів формування при фіксованих параметрах коду, є коди Гоппи, що явно стало причиною спроб створення на їх основі систем криптозахисту.

Коди Гоппи утворять великий клас, найважливішими підкласами якого є коди БЧХ, коди Срівестави, узагальнення Ченя-Чоя кодів БЧХ. Для даного класу доведене існування кодів, лежачих на границі Варшамова-Гілберта. Крім того, велике число багаточленів G(x), що визначають код з параметрами не гірше заданих, дозволяє використовувати дані коди для забезпечення цілісності даних, а можливість визначення всієї множини кодових слів за допомогою одного багаточлена дозволяє останній використовувати як ключ.

Стійкість схем, побудованих на кодах Гоппи заснована на складності рішення відомої в теорії завадостійкого кодування важко вирішуваної задачі декодування випадкового коду. Також дані системи мають достатньо високу швидкість (в порівнянні з криптосистемами RSA, ECC і ін.) перетворень. Крім того кодові криптосистеми залишаються стійкими навіть при використанні квантових обчислень [5]. Їх застосування дозволяє сумістити в один механізм процедури захисту інформації і завадостійкого кодування.

Таким чином, слід припустити, що використання для захисту від помилок кодів Гоппи дозволить додатково вирішувати такі завдання, як забезпечення цілісності та інформаційної скритності каналів передачі даних у системах IIoT.

**Список літератури**

1. Сирадоєв А.О., Можаєв О.О. (2024). Дослідження споживчого і промислового Інтернету речей.

2. Y. Melenti et al. Development of post-quantum cryptosystems based on the Rao-Nam scheme. (2025) Eastern-European Journal of Enterprise Technologies, 1 (9(133)), pp. 35-48.

3. Керничний В., Сєвєрінов О.В. Аналіз стійкості криптосистеми McEliece // Global Cyber Security Forum: матеріали Першого міжнародного науково-практичного форуму, 14 – 16 листопада 2019 р. – Харків: ХНУРЕ, 2019. – С. 55–56.

4. Шипілов Д.В., Халімов Г.З. Аналіз постквантової криптосистеми McEliece. // Комп'ютерні та інформаційні системи і технології, ХНУРЕ, 2019. - С. 83–84.

5. Bernstein, Daniel J., Buchmann, Johannes, and Dahmen, Erik. Post-Quantum Cryptography. – 2009, Springer-Verlag, Berlin-Heidleberg. – 245 p.

# МЕТОДИ АВТОМАТИЧНОГО ВИЯВЛЕННЯ НЕЗАКОННОГО ВІДЕОКОНТЕНТУ

Кібірєв Д.О., Федорченко В.М.
Харківський національний університет радіоелектроніки Харків, Україна

У сучасну цифрову епоху відеоконтент став одним із найбільш поширених способів передачі інформації. Однак з розвитком технологій стрімко зростає і кількість випадків незаконного розповсюдження відео - від порушення авторських прав до публікації заборонених або шкідливих матеріалів [1]. Це створює потребу у впровадженні автоматизованих методів виявлення незаконного контенту, які працюють в режимі реального часу, здатні аналізувати великі обсяги даних і інтегруватися в системи модерації та безпеки.

Під незаконним відеоконтентом розуміється будь-який відеоматеріал, розповсюдження або зберігання якого заборонене законом чи порушує інтелектуальні, етичні або безпекові норми.

**Метою доповіді** є аналіз сучасних методів автоматичного виявлення незаконного відеоконтенту.

Метод перцептивного гешування (Perceptual Hashing) дозволяє створити унікальний "відбиток" відео на основі його візуальних характеристик. Він ефективний навіть після стиснення або часткових змін відео. Найбільш відомі алгоритми pHash, aHash, dHash. Переваги даного методу: стійкість до редагування відео; висока швидкість обробки; простота інтеграції в існуючі системи. В якості недоліків можна виділити те, що не завжди метод точний при великих модифікаціях (наприклад, поворот, інверсія кольорів), потребує великої бази гешів для високої ефективності та може давати хибнопозитивні/хибнонегативні результати без оптимізації.

Інший метод оснований на аналізі цифрових водяних знаків (ЦВЗ). Суть його в тому, що правовласники вбудовують у відео непомітні цифрові позначення [2]. Системи автоматично виявляють такі знаки, ідентифікуючи джерело нелегального копіювання. Переваги використання ЦВЗ: висока стійкість до типових атак: масштабування, обтинання, стиснення; підтримка трасування витоків (відстеження по джерелу); можливість юридичного підтвердження прав на контент. Метод може застосовуватись в поєднанні з ШІ для масової автоматичної перевірки та дає змогу автоматично блокувати або сповіщати про незаконний контент. Недоліками є те, що не всі методи водяного знака є достатньо стійкими, вимагає впровадження на етапі створення або розповсюдження контенту, не завжди можливо виявити водяний знак, якщо відео зазнало глибокого перекодування, а також потребує спеціального програмного забезпечення для вбудовування/зчитування.

Метод машинного навчання (ML) і глибокого навчання (DL) є потужними інструментами для автоматичного виявлення незаконного відеоконтенту, особливо в умовах великого обсягу даних, які щоденно з'являються в Інтернеті. Глибоке навчання використовує нейронні мережі, які можуть

автоматично виділяти ознаки з відеоданих без ручної обробки. Ці підходи дозволяють будувати адаптивні системи, здатні навчатися з даних, виявляти складні шаблони, розпізнавати відео з порушенням авторських прав або неприйнятним вмістом. На даний час нейронні мережі навчаються класифікувати контент за допомогою аналізу зображення, звуку, тексту (субтитри) тощо. Застосовують мережі CNN для аналізу кадрів, RNN або Transformer для аналізу звуку/мовлення, Multimodal networks для аналізу одразу кількох типів даних. Переваги методів ML/DL: висока точність в умовах великої кількості відео, стійкість до обфускацій, змін формату, редагування, можливість навчати моделі під нові загрози, підтримка реального часу та масштабування. В якості недоліки можна вказати необхідність великих обсягів навчальних даних, високі обчислювальні витрати, чутливість до перенавчання або недостатнього навчання та ускладненість пояснення результатів DL-моделей (black-box).

Метод семантичного аналізу змісту оснований на використанні NLP та комп'ютерного зору для виявлення заборонених фраз, символіки, об'єктів (зброя, насильство) в кадрі.

Також можуть використовуватись системи розпізнавання обличчя на основі автоматичного виявлення конкретних осіб, які фігурують у заборонених матеріалах або порушують конфіденційність.

На даний час основними проблемами в застосуванні методів автоматичного виявлення незаконного відеоконтенту є:

– обфускація контенту, тобто змінення формату, фільтрів, розміру для обходу автоматичного виявлення;

– похибки класифікації, які призводять до хибного спрацьовування або пропуску шкідливого відео;

– морально-правова дилема, тобто необхідність знаходження балансу між контролем і свободою слова;

– обчислювальна складність методів, що потребує потужних ресурсів для обробки великих відеопотоків.

Пропонується використовувати гібрідний метод, заснований на аналізі цифрових водяних знаків () з використанням методів машинного (ML) і глибокого навчання (DL).

Методи автоматичного виявлення незаконного відеоконтенту є критично важливими для захисту цифрового простору. Поєднання штучного інтелекту, машинного навчання та цифрового маркування (ЦВЗ) дозволяє створити надійні механізми боротьби з нелегальним відео.

**Список літератури**

1. Кібірєв, Д.О., Федорченко В.М. Аналіз методів захисту відеоконтенту від несанкціонованого копіювання. ХНУРЕ, 2023.

2. Martovytskyi V., Ruban I., Bolohova N., Sievierinov O., Zhurylo O., Permiakov O., Nosyk A., Nepokrytov D., Krylenko I. (2021). Development of Methods for Generation of Digital Watermarks Resistant to Distortion. Eastern-European Journal of Enterprise Technologies, 6(2), 114.

# АНАЛІЗ КВАНТОВИХ АЛГОРИТМІВ CRYSTALS-KYBER І CRYSTALS-DILITHIUM

Хівренко Г.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Постквантова криптографія (PQC) стала центром досліджень, оскільки прориви в квантових обчисленнях загрожують безпеці класичних криптографічних систем. У роботі досліджені протоколи CRYSTALS-KYBER і CRYSTALS-Dilithium, призначені для захисту зв'язку від квантових противників [1, 2]. Використовуючи решіткові задачі, які вважаються стійкими до квантових атак, ці протоколи пропонують перспективне рішення для захисту конфіденційних даних від руйнівного потенціалу нових квантових технологій.

**Метою роботи** є оцінка теоретичних основ, які забезпечують безпеку алгоритмів CRYSTALS-KYBER і CRYSTALS-Dilithium від відомих квантово-здатних опонентів. Також проаналізовані їх характеристики продуктивності, такі як розмір ключа, затримка та накладні витрати на обчислення, під час розгортання на різних платформах, включаючи обмежені середовища, такі як пристрої IoT. Крім того досліджені стратегії безперебійного переходу від поточних стандартів (RSA та ECC) до квантово-стійких протоколів, що забезпечують безперервність захищених комунікацій без шкоди для ефективності та зручності використання.

Квантові комп'ютери можуть скомпрометувати існуючі криптографічні алгоритми протягом найближчих десятиліть. Завдяки систематичному вивченню CRYSTALS-KYBER і CRYSTALS-Dilithium - двох провідних кандидатів у постквантові стандарти NIST - надаються практичні ідеї для практиків безпеки і системних архітекторів, які готуються до майбутнього [3].

У доповіді розглянуті комплексна структура для розуміння та впровадження CRYSTALS-KYBER і CRYSTALS-Dilithium, підкреслюючи їхні криптографічні переваги, практичні міркування щодо розгортання та ширшу актуальність для захисту цифрових комунікацій [4].

Проведено аналіз формування ключових пар, створення цифрового підпису для CRYSTALS-Dilithium та шифрування для CRYSTALS-Dilithium. Проведений аналіз безпеки цих алгоритмів та була проведена оцінка швидкості та ефективність наведених алгоритмів.

**Список літератури**

1. Khalimov, G. and others. Towards three-parameter group encryption scheme for MST3 cryptosystem improvement Proceedings of the 2021 5th World Conference on Smart Trends in Systems Security and Sustainability, WorldS4 2021, 2021, P. 204–211.

2. Micciancio, D., & Regev, O. (2009). *Lattice-based Cryptography.* In D. J. Bernstein, J. Buchmann, & E. Dahmen (Eds.), Post-Quantum Cryptography (pp. 147–191). Springer.

3. NIST. (2022). Post-Quantum Cryptography Standardization Process: Round 3 Submissions. Retrieved from https://csrc.nist.gov/Projects/post-quantum-cryptography.

4**.** Chen, L., et al. (2016). *Report on Post-Quantum Cryptography*. NISTIR 8105.

# ПРОБЛЕМНІ ПИТАННЯ ЗАСТОСУВАННЯ БЛОКОВОЇ LSB СТЕГАНОГРАФІЇ ДЛЯ КВАНТОВИХ ЗОБРАЖЕНЬ

Головко Є.В., Федюшин О.І.
Харківський національний університет радіоелектроніки, Харків, Україна

LSB квантова стеганографія - це сучасний напрямок в області захисту інформації, що поєднує ідеї квантових обчислень і класичної стеганографії, зокрема техніки Least Significant Bit (LSB), при якому інформація вбудовується в найменш значущі біти (LSB) цифрових зображень, аудіо або відео для приховування даних [1, 2].

Така інтеграція забезпечує надвисокий рівень конфіденційності, стійкості до атак і ускладнює виявлення прихованої інформації.

На даний час відомі два види LSB квантової стеганографії: класична та блокова.

При блоковій стеганографії модифікується не окремий елемент, а цілий блок елементів або квантових станів для підвищення рівня секретності. Блочний підхід дозволяє підвищити стійкість і ефективність прихованого обміну повідомленнями у квантових або квантово-класичних системах [3, 4].

**Метою доповіді є** аналіз методу блокової LSB стеганографії квантових зображень, можливих сфер застосування та проблемних питань його використання.

При блоковому методі квантове представлення ділиться на блоки розміром m×n (наприклад, 8×8 кубітів). Це дозволяє локалізовано вбудовувати дані, що підвищує стійкість до атак і спрощує адаптивну обробку. У кожному блоці змінюються найменш значущі біти кубітів. Це робиться зміною станів кубітів без порушення суперпозиції. За допомогою квантових алгоритмів аналізу зображення вибираються ті блоки, які мають високий рівень складності (текстура, шум). Це ускладнює виявлення прихованої інформації навіть при стеганоаналізі.

Завдяки розподілу по блоках та використанню квантових ефектів зменшується ризик повного витоку даних. Також такі системи більш стійкі до стеганоаналізу, атак з підміною та шумів. Пропонується додатково застосовувати квантове шифрування повідомлення перед вбудовуванням.

Проведений аналіз показав, що основними сферами застосування блокової LSB стеганографії є:

– захист конфіденційної інформації шляхом приховування секретних повідомлень у квантових зображеннях;

– медична передача даних зі збереженням конфіденційності пацієнтів в телемедицині або медичній діагностиці;

– супутникова та аерокосмічна розвідка. Приховування аналітичних даних у зображеннях з дронів, супутників чи літаків;

– безпечний обмін даними в IoT системах;

– захист авторських прав через приховану ідентифікацію власника в цифрових зображеннях;

– квантова криміналістика та стеження. Збір доказів, що приховані в цифровому вигляді без можливості виявлення сторонніми особами;

– квантові системи безпеки в складних схемах передачі даних в умовах квантового каналу, де шифрування йде разом зі стеганографією.

Використання квантової блокової LSB-стеганографії дозволяє не просто "приховати дані", а й використовувати переваги квантової суперпозиції, паралельної обробки та заплутаності для безпечнішого приховування.

При цьому на даний час існує низька проблемних питань в застосуванні блокової LSB квантової стеганографії:

1. Недосконаліть квантових технологій у практиці. На сьогодні квантові пристрої ще не готові до широкого застосування, а більшість методів квантової стеганографії реалізуються лише в симуляторах.

2. Складність квантового представлення блоків. Кодування зображень або сигналів у NEQR, QRMW чи інших форматах потребує значних обчислювальних і квантових ресурсів. Проблема розбиття на блоки зберігає свою складність у квантовій системі, особливо при обробці великих обсягів даних.

3. Вразливість до квантового стеганоаналізу. Існує ризик створення квантових стеганоаналізаторів, що можуть виявляти закономірності навіть у квантових станах. Якщо шаблон вбудовування не є адаптивним або непередбачуваним, можливе виявлення змін у фазах або поляризації.

4. Проблеми синхронізації між сторонами. Для коректного декодування інформації потрібно: знати розбиття на блоки; параметри LSB-вбудовування; стани заплутаності, якщо вони використовувались. Будь-який збій у синхронізації робить повідомлення потенційно нерозшифрованим.

5. Невисока ємність приховування. Кількість інформації, яку можна вбудувати, обмежена: кількістю LSB-бітів у блоках; допустимим рівнем модифікації, щоб уникнути виявлення. У квантових системах додатково накладаються фізичні обмеження на кількість доступних кубітів.

**Список літератури**

1. Zhou, R. G., Luo, J., Liu, X., Zhu, C., Wei, L., & Zhang, X. (2018). A novel quantum image steganography scheme based on LSB. International Journal of Theoretical Physics, 57, 1848-1863.

2. Li, P., & Lu, A. (2018). LSB-based steganography using reflected gray code for color quantum images. International journal of theoretical physics, 57(5), 1516-1548.

3. A. AL-Salhi, Y. E., & Lu, S. (2016). Quantum image steganography and steganalysis based on LSQu-blocks image information concealing algorithm. International Journal of Theoretical Physics, 55, 3722-3736.

4. Zhou, R. G., Hu, W., & Fan, P. (2017). Quantum watermarking scheme through Arnold scrambling and LSB steganography. Quantum Information Processing, 16, 1-21.

# ПРОБЛЕМНІ ПИТАННЯ ЗАСТОСУВАННЯ ГОМОМОРФНОГО ШИФРУВАННЯ

Гущин Б.-Д.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Гомоморфне шифрування (Homomorphic Encryption, HE) - технологія, що дозволяє виконувати обчислення над зашифрованими даними без їх розшифрування [1-3]. Застосування гомоморфного шифрування відкриває великі можливості для обробки зашифрованих даних без їх розшифрування в багатьох сферах, де критично важливо зберігати конфіденційність інформації.. Однак, попри потенціал, існує низка проблемних питань, які стримують широке впровадження цієї технології в практичні системи безпеки та обробки даних.

**Метою доповіді** є аналіз проблемних питань при практичному застосуванні гомоморфного шифрування.

В роботі розглянуті ключові сучасні сфери застосування HE [1-3].

1. Хмарні обчислення (Cloud Computing), обробка зашифрованих даних на стороні постачальника хмарних послуг без розкриття вмісту.

2. В медицині та біоінформатиці захищене зберігання та аналіз медичних записів пацієнтів, генетичної інформації (DHK). Використання HE у дослідженнях із багатьма організаціями без обміну розшифрованими даними.

3. В фінансових сервісах конфіденційна аналітика для банків, страхових компаній, бірж. Обчислення кредитного рейтингу, оцінка ризиків без доступу до відкритих даних клієнта.

4. Електронне голосування (E-voting). Забезпечення анонімності та перевірності результатів голосування, так як дані не розкриваються, але можуть бути агреговані без розшифрування.

5. В Інтернеті речей (IoT) для обробки конфіденційних даних, зібраних з розумних пристроїв, безпосередньо на сервері або у хмарі. Використання в промисловому IoT (IIoT), медичних пристроях, Smart City.

6. Захист персональних даних у Big Data, аналітика зашифрованих великих масивів даних з соціальних мереж, телекомів, сервісів для обчислення трендів, поведінкових моделей, не розкриваючи особистості.

7. Машинне навчання над зашифрованими даними (Privacy-Preserving ML). Навчання або інференс моделей на даних, які ніколи не розшифровуються. Використання в конфіденційній медичній діагностиці, рекомендаційних системах, фінансах. Працює разом з Federated Learning, Secure Multi-Party Computation (SMPC).

8. В юридичних сервісах та державному управлінні для безпечної взаємодії між державними структурами при обробці реєстрів, митних даних, податкових баз, де важлива повна конфіденційність.

9. В системах кібербезпеки та цифрової ідентичності. Застосовується в антифрод-системах, аналізі поведінки користувачів без втрати їхньої конфіденційності. Підтримка Zero Knowledge Proofs та протоколів автентифікації.

В процесі проведеного аналізу виявлені проблемні питання, які стримують широке впровадження гомоморфного шифрування в практичні системи безпеки та обробки даних.

1. Обчислювальна складність та продуктивність. Базові арифметичні операції (додавання, множення) в HE можуть займати в сотні або тисячі разів більше часу, ніж у звичайних обчисленнях, тому гомоморфне шифрування є надзвичайно ресурсомістким.

2. Розмір зашифрованих даних в HE системах мають величезний розмір. Це створює проблему при збереженні, передаванні та обробці таких даних, особливо в хмарних середовищах та IoT-системах.

3. Обмежена функціональність у деяких реалізаціях. Частково гомоморфне шифрування (PHE) підтримує лише одну операцію (додавання або множення), складно реалізувати умовні оператори (if/else), порівняння або логічні операції, діє обмеження на глибину обчислень (multiplicative depth) у схемах FHE.

4. Інтеграція з існуючими системами. Потрібна адаптація програмного забезпечення, баз даних, аналітичних інструментів до роботи з HE.

5. Складність реалізації. Розробка систем із підтримкою HE вимагає висококваліфікованих спеціалістів. Висока вірогідність помилок внаслідок складної математичної бази (решітки, модулярна арифметика, шумові моделі).

6. Відсутність єдиного загальноприйнятого стандарту HE. Утруднене сумісне використання різних криптобібліотек (SEAL, HElib, TenSEAL). Складнощі з юридичними аспектами, якщо система повинна відповідати, наприклад, GDPR.

7. Обмежена підтримка в апаратному забезпеченні. Переважна більшість CPU/GPU не оптимізована для обчислень у HE. Високопродуктивні реалізації можливі лише з використанням спеціалізованого апаратного прискорення (FPGA, ASIC), що ще не є масовим.

8. Проблеми масштабування. Обробка великих обсягів зашифрованих даних вимагає величезних обчислювальних ресурсів, унеможливлюючи застосування в реальному часі для Big Data, IoT, Smart Grid.

10. Обмежене практичне використання. Реальних продуктів із повною підтримкою HE одиниці: proof-of-concept, обмежені демонстраційні системи.

Таким чином гомоморфне шифрування – це потужний інструмент для захисту конфіденційності, але висока обчислювальна складність, великі розміри даних, складність реалізації та відсутність стандартів гальмують широке впровадження цієї технології.

**Список літератури**

1. Halevi, S., & Shoup, V. (A Full Introduction to Homomorphic Encryption). 2013. IBM Research. 92 ps.

2. Yi, X., Paulet, R., Bertino, E., Yi, X., Paulet, R., & Bertino, E. (2014). Homomorphic encryption (pp. 27-46). Springer International Publishing

3. Coron, J.-S., Naccache, D., & Tibouchi, M. (Homomorphic Encryption). 2011. Springer. 142 p.

# ОЦІНКА ВПЛИВУ В СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ З ТОЧКИ ЗОРУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Риков Д.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Соціальні інтернет-сервіси стали невід'ємною частиною сучасного інформаційного простору. Вони активно використовуються як приватними особами, так і підприємствами для комунікації, обміну даними, реклами та поширення новин. Проте їх зростаюча популярність несе із собою низку викликів у сфері інформаційної безпеки.

**Метою доповіді** є розгляд впливу соціальних сервісів на інформаційну безпеку, основні ризики та методи оцінки таких впливів.

Соціальні інтернет-сервіси (Facebook, Instagram, TikTok, X (Twitter), YouTube, LinkedIn та інші) дозволяють користувачам створювати публічний чи приватний контент, спілкуватися, формувати мережі контактів. Вони збирають велику кількість персональних і поведінкових даних, що відкриває потенціал для аналізу та багатьох зловживань. З точки зору інформаційної безпеки можна виділити такі методи оцінки впливу.

1. Privacy Impact Assessment (PIA). Метод, який дозволяє виявити ризики обробки персональних даних у відкритому просторі.
2. Threat Modeling. Використання моделей атак для передбачення можливих векторів загроз.
3. OSINT-аналітика. Моніторинг публічних джерел задля виявлення витоків або проявів інформаційних атак.
4. Аналіз цифрового сліду. Оцінка обсягу персональних або корпоративних даних, доступних у публічному просторі.

В резкультаті проведеного аналізу пропонуються рекомендації для зменьшення впливу в соціальних інтернет-сервісах. По-перших, це розробка внутрішніх політик поведінки в соцмережах. По-друге, навчання персоналу цифровій гігієні. Також необхідне використання автоматизованих систем моніторингу активності в публічному просторі та мінімізація цифрового сліду користувачів і компаній. Соціальні Інтернет-сервіси створюють нові можливості, але й нові ризики. Для забезпечення інформаційної безпеки необхідно впроваджувати системний підхід до оцінки впливу соціальних платформ, контролю цифрової присутності та моніторингу аномальної активності. Без відповідних заходів організація або приватна особа може стати легкою мішенню для кібератак або маніпуляцій.

**Список літератури**

1. Матвійчук, Андрій Вікторович. "Метод виявлення інформаційної загрози за парсингом спільнот у соціальних інтернет-сервісах." (2023).
2. Молодецька-Гринчук, К. "Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах." Автоматизация технологических и бизнес-процессов 9, Iss. 2 (2017): 36-42.

# ВИКОРИСТАННЯ МЕТОДІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ АТАК НА БЛОКЧЕЙН СИСТЕМИ

Просолов В.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Блокчейн став всюдисущим поняттям, який охоплює соціальні перспективи та нову технологію[1].

Спочатку запропонований як рішення для системи ведення реєстрів криптовалюти Bitcoin, блокчейни тепер використовуються для зберігання записів для багатьох типів програм. Блокчейн асоціюється для більшості людей із чимось більшим, ніж просто світ криптовалют.

Обіцянка, яку багато хто асоціює з блокчейн-додатками, полягає в тому, що вони зруйнують централізовані системи. Використовуючи централізовані системи, люди повинні довіряти контрагенту, але самі не мають ресурсів, щоб зробити це самостійно [2].

Таким чином, простий спосіб визначити місце, де застосовується технологія блокчейн, - це пошук областей, у яких потрібен посередник для сприяння довірі.

Довіра має важливе значення для таких речей, як переказ грошей, голосування, земельні записи, права інтелектуальної власності та ідентифікація. Програмне забезпечення блокчейна використовується для того, щоб замінити посередників, ставши надійним гарантом для системи ведення записів [3].

**Мета доповіді** полягає в тому, щоб розглянути метод виявлення атак на блокчейн системи з використанням методів машинного навчання. Для цього розглядається та аналізується система блокчейна з точки зору її вразливості щодо шкідливого впливу.

У даній роботі представлено метрики оцінки для цього дослідження, порівняння результатів та обговорення нашого експерименту. Метрики оцінки є дуже важливою частиною виміру якості та продуктивності нашого рішення. Оцінки метрики були зроблені з використанням інтерфейсу розробки Python і відповідних бібліотек Python.

Ми використовували набір даних для 10000 записі. Потім цей набір даних з файлу .csv було поділено з використанням бібліотек Pandas і Numpy.

Окремо ми виділили бінарні змінні, не враховуючи цільову. Після цього проведено попередню обробку даних з метою класифікації, використовуючи алгоритм, розглянутий у попередньому розділі.

У бібліотеці scikit-learn є багато алгоритмів класифікації, які ми могли б використовувати для побудови моделі. У цьому прикладі ми використовуватимемо класифікатор на основі модернізованого методу k-NN, який легко інтерпретувати.

Побудова цієї запропонованої моделі полягає лише у запам'ятовуванні навчального набору. Для того, щоб зробити прогноз для нової точки даних,

алгоритм обирає точку в навчальному наборі, яка знаходиться найближче до нової точки. Потім він надає мітку, що належить цій точці навчального набору, новій точці даних.

У scikit-learn всі моделі машинного навчання реалізовані у власних класах, які називають класами Estimator.

Алгоритм класифікації на основі методу k-NN реалізований у класифікаторі KNeighborsClassifier модуля neighbors. Оскільки цей класифікатор працює за шістнадцятьма класами, то цілком доцільно вибрати змінну числа сусідів n_neighbor=5.

Був проведений ряд експериментів із розбиттям на тестовий та навчальний набір даних. Слід зазначити, що якість моделі, яка визначає правильність (accuracy), це сильно впливає. Зокрема, за всіх заданих умов accuracy не перевищувала 0.89, що фактично визначає вірогідність правильного прогнозу.

Подальший аналіз проведено з використанням методики роботи [4]. Алгоритми k-NN, Random Forest і Decision Tree порівнювали з використанням таких показників оцінки: accuracy, recall, precision та F1. Зокрема, для алгоритму k-NN результати accuracy для 10 000 даних дорівнюють 75.0%. Для поданої моделі - 75.0 %.

Оскільки запропонована модель була тестова, і призначена для відпрацювання методики двоетапного експерименту. Тим не менш, якщо ми цікавимося шкідливими атаками на систему блокований, то часто немає необхідності проводити повномасштабне дослідження даних. Тим більше, що ніхто не дозволить використовувати конфіденційну статистику. Якщо виділити бінарні змінні і за ними провести класифікацію, то остаточний результат такої урізаної моделі показує результат не гірше, ніж повномасштабне дослідження.

Методи аналізу даних широко використовувалися в галузі кібербезпеки та захисту інформації, а недавнє поширення передових методів машинного навчання дозволило точно ідентифікувати кібератаки та виявляти загрози як у режимі реального часу, так і під час аналізу після інциденту.

**Список літератури**

1. Laurence T. *Introduction to blockchain technology*. Amersfoort – NL: Van Haren Publishing, 2019. 250 p.

2. Ye, C., Li, G., Cai, H., Gu, Y., & Fukuda, A. (2018, September). Analysis of security in blockchain: Case study in 51%-attack detecting. In *2018 5th International conference on dependable systems and their applications (DSA)* IEEE, 2018. p. 15-24.

3. Khan S. N., Loukil F., Ghedira-Guegan C., Benkhelifa E., & Bani-Hani A. Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-peer Networking and Applications.* 2021. Vol.14. P. 2901-2925.

4. Sanda, O., Pavlidis, M., Seraj, S., & Polatidis, N. Long-Range attack detection on permissionless blockchains using Deep Learning. *Expert Systems with Applications.* 2023. Vol. 218. P. 119606.

# ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ РАДІОКАНАЛІВ УПРАВЛІННЯ БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ

Переметчик Д.О., Смірнов А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному світі безпілотні літальні апарати (БПЛА) набувають усе більшого поширення в різних галузях, включаючи військову справу, сільське господарство, наукові дослідження, моніторинг навколишнього середовища, логістику та охорону правопорядку [1]. Однак з розвитком технологій зростають і ризики, пов’язані з безпекою систем управління безпілотниками, особливо радіоканалів, через які здійснюється їхній контроль і керування.

**Метою доповіді** є аналіз

Одним із ключових аспектів безпеки БПЛА є забезпечення захищеності радіоканалів управління, які можуть бути вразливими до різних типів атак: перехоплення сигналу, втручання, глушіння або навіть захоплення управління апаратом [2]. Розвиток технологій БПЛА йде в ногу з розвитком засобів радіозв'язку, але разом з цим збільшуються ризики кібератак, зокрема перехоплення сигналу, спуфінг (підробка сигналу) і джемінг (глушіння сигналу). Особливу увагу викликають загрози, пов'язані з перехопленням даних, переданих через відкриті канали зв'язку, та можливістю зовнішнього втручання у роботу дронів. Зважаючи на підвищення кількості атак на радіоканали БПЛА, дослідження методів захисту стає вкрай актуальним. В роботі розглянуті сучасні методи шифрування та автентифікації, засоби захисту від глушіння та підміни сигналу, а також перспективи використання нових технологій для підвищення безпеки систем управління БПЛА. До найпоширеніших загроз належать:

– перехоплення сигналу БПЛА, що дозволить контролювати дії дрону або отримати важливу інформацію;

– спуфінг – коли зловмисник підробляє сигнал оператора, що може призвести до зміни маршруту польоту БПЛА або виконання небажаних команд;

– джемінг – глушіння радіоканалів, що може призвести до втрати управління дроном або його аварії;

– кібератаки на інфраструктуру – атаки на елементи системи управління, такі як наземні станції або сервери передачі даних.

Для захисту радіоканалів управління БПЛА пропонується низка методів і технологій, які забезпечують конфіденційність, цілісність та доступність сигналу.

**Список літератури**

1. Drone Development from Concept to Flight: Design, assemble, and discover the applications of unmanned aerial vehicles. Smit Sgarma C. 99–108.

2. Mykhatskyi, Oleksii. "Інформаційна безпека радіоканалів безпілотних авіаційних комплексів." *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»* 1.1 (2018): 56-62.

# ФОРМУВАННЯ ПРАВИЛ ЕКРАНУВАННЯ IP ТРАФІКУ НА ОСНОВІ АНАЛІЗУ МЕРЕЖЕВИХ ДІАГРАМ

Кулик Ю.О., Смідович Л.С.
Національний аерокосмічний університет
«Харківський авіаційний інститут», Харків, Україна

Одним із напрямків забезпечення безпеки корпоративної мережі виступає створення та підтримка міжмережевих екранів між сегментами корпоративної мережі. При цьому виникають задачі документування екранування трафіку, формування та узгодження правил для різних екранів, конфігурування обладнання, інспектування налаштованих правил та передачі трафіку в мережі на основі вхідних мережевих діаграм у форматі xml [1]. Важливим фактором виступає час модифікації налаштувань при змінах, що вносяться в процесі функціонуванні мережі. Такі зміни виникають в процесі розвитку систем, що призначені для надання інформаційних послуг користувачам та розміщуються в різних сегментах мережевих модулів корпоративної мереж.

**Метою доповіді** є розгляд підходу до автоматизації формування правил для міжмережевих екранів на основі аналізу мережених діаграм, експортованих з diagrams.net у файли формату XML /.drawio [2].

Мережеві діаграми повинні готуватись в diagrams.net з використанням правил іменування компонентів на основі словника та можуть містити множину пов’язаних компоненів.

Для формування набору правил для кожного міжмережного екрану, що міститься на діаграмі, пропонується виконати аналіз трас проходження зв’язків між компонентами. Перетин зв’язком компонента FIREWALL означає одне правило для відповідного екрану між кінцевими компонентами.

Для такого аналізу можна використати розроблений додаток, на вхід якого подається файл .drawio, а на виході отримаємо набір правил для кожного компонента FIREWALL діаграми у форматі CSV. Описаний підхід дозволяє скоротити час аналізу мережевих діаграм, що підвищує ефективність роботи системних адміністраторів, які конфігурують міжмережні екрани в корпоративній мережі.

В подальшому можливий розвиток додатку в напрямку кастомізації формату правил для їх завантаження на обладнання різних виробників.

**Список літератури**

1. Extensible Markup Language (XML). Official website, World Wide Web Consortium (W3C) [Електронний ресурс] – Режим доступу: https://www.w3.org/XML/

2. Flowchart maker and Online Diagram Software [Електронний ресурс] – Режим доступу: https://app.diagrams.net/

# СИСТЕМИ ЗБЕРІГАННЯ КРИПТОГРАФІЧНИХ КЛЮЧІВ

Щербакова Ю.А., Острижна Є.С.
Національний аерокосмічний університет
«Харківський авіаційний інститут», Харків, Україна

Зберігання криптографічних ключів є важливим аспектом забезпечення безпеки інформаційних систем на державному рівні [1, 2], у фінансовій сфері [3, 4] та у приватному спілкуванні.

Ризики, пов'язані з втратою, компрометацією або неправильним зберіганням ключів, мають значний вплив на цілісність і конфіденційність інформації, тому дослідження критеріїв оптимальності при створенні таких систем, а також вибір параметрів їх функціонування набувають значної актуальності

**Метою доповіді** є розробка системного підходу до аналізу, проектування та вдосконалення системи зберігання криптографічних ключів для забезпечення конфіденційності, цілісності та доступності даних, а також підвищення рівня захищеності інформації в сучасних інформаційних системах.

**Виклики, виявлені в дослідженнях:**

- Компрометація ключів,
- Баланс між безпекою та продуктивністю,
- Захист ключів у багатокористувацьких середовищах,
- Відповідність нормативним вимогам.

**Перспективи розвитку:**

- Інтеграція штучного інтелекту,
- Покращення алгоритмів шифрування,
- Автоматизація управління життєвим циклом ключів.

**Можливі критерії оптимізації.**

Оптимізація системи зберігання криптографічних ключів спрямована на підвищення її ефективності, безпеки та надійності. Критерії оптимізації поділяються на три основні категорії: продуктивність, захищеність і економічна ефективність.

**1. Продуктивність системи.**

Оптимізація продуктивності спрямована на зменшення затримок, підвищення швидкості роботи системи і забезпечення її масштабованості.

***Критерії***:

– Час доступу до ключів (мінімізація часу, необхідного для обробки запиту на отримання ключа),

– Швидкість генерації ключів (зменшення часу, потрібного для створення криптографічного ключа),

– Пропускна здатність системи,

– Масштабованість (можливість обробляти зростаючий обсяг даних).

**2. Захищеність системи**

Оптимізація захищеності спрямована на мінімізацію ризиків компрометації ключів, забезпечення стійкості системи до атак.

***Критерії***:

– Рівень безпеки зберігання ключів(гарантія, що ключі захищені від фізичного та логічного доступу неавторизованих користувачів),

– Контроль доступу до ключів (ефективність політик доступу, що регулюють права користувачів),

– Стійкість до компрометації ключів (мінімізація ризиків витоку ключів та впливу їх компрометації на систему),

– Відмовостійкість системи (здатність системи продовжувати роботу у разі збоїв або атак.).

–

**3. Економічна ефективність**

Оптимізація витрат на розробку, впровадження та обслуговування.

***Критерії***:

– Вартість розгортання системи (мінімізація витрат на встановлення обладнання та програмного забезпечення),

– Вартість обслуговування системи (зменшення витрат на підтримку та оновлення системи),

– Ефективність використання ресурсів (оптимізація використання обчислювальних ресурсів для роботи системи).

**Методи реалізації оптимізації**

– Автоматизація управління ключами: Ротація, архівація, створення та видалення ключів виконуються без участі адміністратора,

– Модульність: Поділ системи на окремі компоненти (зберігання, авторизація, резервне копіювання), які можна оптимізувати незалежно,

– Моніторинг продуктивності: Регулярний аналіз роботи системи для виявлення вузьких місць,

– Інтеграція штучного інтелекту

**Список літератури**

1. Інструкція про порядок генерації ключів програмного комплексу «Варта». https://uakey.com.ua/files/uploads/ba58cdbb8a1dcb8b96c7d426de177ab8.pdf

2. GDPR — Загальний регламент захисту даних (General Data Protection Regulation): https://eur-lex.europa.eu/legal

3. Порядок роботи з криптографічними ключами модулів безпеки Національної платіжної системи “Український платіжний простір” https://bank.gov.ua/admin_uploads/law/Decision_Prostir_28062024_57-13_Crypto_Keys_Procedure

4. PCI DSS — Стандарт безпеки даних індустрії платіжних карт: https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1

Посібник з SSL-сертифікату Exchange Server https://www.ssl.com/guide/exchange-server-ssl-certificate-guide/

# ІНТЕЛЕКТУАЛЬНИЙ МОДУЛЬ НАВІГАЦІЇ ДЛЯ РЕАБІЛІТАЦІЇ ОСІБ З ВАДАМИ ЗОРУ НА ЗУПИНКАХ ГРОМАДСЬКОГО ТРАНСПОРТУ

Нечітайло О.В., Гаврашенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сьогодні, на жаль, достатньо гостро стоїть питання реабілітації військових та громадян України з вадами зору. За даними дослідження Міністерства соціальної політики України у 2021 році нараховувалося 17 тис. осіб. Вже у 2023 ця кількість зросла до 19 тисяч [1]. Вказане дослідження також показало, що серед військових 19,1% поранень стосуються уражень голови, у тому числі й органів зору [2].

Наведена вище статистика свідчить, що питання реабілітації та адаптації людей із вадами зору до повноцінного життя в Україні потребує розробки та впровадження спеціальних технічних засобів, зокрема для доступності інфраструктури, а саме зупинок громадського транспорту.

Отже, **метою дослідження** є розробка програмно-апаратного модулю для допомоги особам з вадами зору, у самостійному орієнтуванні на зупинках громадського транспорту. Розробити та протестувати систему, яка розпізнає тип транспорту, його маршрутний номер та напрямок руху, а також надасть голосові підказки користувачу.

Для досягнення поставленої мети, необхідно розробити спеціальний модуль із застосуванням методів комп'ютерного зору (OpenCV, YOLO) для ідентифікації транспорту та визначення його параметрів руху, модуля голосового супроводу та синтезу мовлення на основі Google Text-to-Speech для голосових підказок у реальному часі, GPS та картографічними сервісами для визначення точного розташування користувача та його зупинки за допомогою Google Maps API. Останнім кроком є перевірка стабільності застосунку в польових умовах, зокрема адаптації до змін погоди, освітлення та роботи на енергоощадних пристроях типу Raspberry Pi.

Подальший розвиток проєкту полягає у розширенні функціоналу для роботи з розумними зупинками (IoT-інфраструктура), інтеграції з мобільним додатком для персоналізації налаштувань, використанні технологій штучного інтелекту для адаптації системи до різних користувачів.

**Список літератури**

1. Чорна, В., Заводяк, А., Плахотнюк, І., Липкань, В., Томашевський, А., Коломієць, В. Особливості поранень від різних типів зброї, місцезнаходження особи на момент вибуху. *Україна. Здоров'я нації*. 2024. №2. 113–121.

2. Живи без обмежень: 26 людей з вадами зору отримали реабілітацію за новою комплексною моделлю. URL: https://surl.li/cqhcgr (дата звернення: 28.03.2025).

# РОЗРОБКА КЛІЄНТ-СЕРВЕРНОГО ВЕБЗАСТОСУНКУ ДЛЯ СПІЛКУВАННЯ МІЖ КОРИСТУВАЧАМИ

Сочівкін В.М., Гаврашенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному цифровому світі ефективна комунікація є ключовим елементом як для особистого, так і для професійного розвитку. Тому актуальність розробки застосунку, який забезпечує спілкування між користувачами через текстовий, аудіо- та відеочати [1] в режимі реального часу, неможливо переоцінити.

Такий застосунок дозволяє користувачам обирати найбільш зручний спосіб взаємодії що підвищує ефективність обміну інформацією, не зважаючи на відстань між співрозмовниками в реальному житті. Крім того, онлайн-спілкування також знижує фактор фізичних перепонів, що можуть виникнути при спілкуванні вживу, як от наприклад, сторонні шуми з інших джерел.

Метою доповіді є місткий опис структури вебзастосунку [2] для спілкування між користувачами. Чималу увагу при створенні застосунку треба надати приємному на вигляд і інтуїтивно зрозумілому для всіх інтерфейсу користувача. Для розробки структури та дизайну інтерфейсу, що відповідає вказаним вимогам, буде використано стек програмування з мов розмітки HTML та CSS.

Функціонал застосунку буде реалізований за допомогою фреймворку React.js, який поєднує в собі простоту розробки, універсалізм і структурованість. Весь цей стек сформує клієнтську сторону застосунку.

В якості середовища для обробки і зберігання даних буде використано сервер, написаний за допомогою Node.js, який стабільно виконуватиме свою роботу у тандемі з WebSocket, що робить можливою обробку пакетів даних в реальному часі.

Для зберігання файлів на сервері, було обрано формат файлу JSON, який передбачає чудову вкладеність та легкість читання. Для передачі даних використовуватиметься End-to-End шифрування [3], що не дозволить отримати будь-які чутливі дані третім особам.

**Список літератури**

1. Zhang, L., & Wang, Y. (2021). Real-Time Video Conferencing Technologies: A Comparative Study. *Proceedings of the International Conference on Computer Communications and Networks*, 789-795.

2. Smith, J., & Doe, A. (2023). Development of Real-Time Communication Web Applications: Challenges and Solutions. *Journal of Web Engineering*, 22(4), 345-360.

3. Nguyen, T. K., & Patel, R. (2022). Secure Messaging Systems: Implementing End-to-End Encryption in Web Applications. *International Journal of Information Security*, 31(2), 123-135.

# ДЕЦЕНТРАЛІЗОВАНИЙ МАРКЕТПЛЕЙС ОБЧИСЛЮВАЛЬНИХ ПОТУЖНОСТЕЙ НА БЛОКЧЕЙНІ

Ботнар П.Д., Янковський О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

У роботі представлено підхід до розробки децентралізованої платформи для оренди та надання обчислювальних потужностей на базі технологій блокчейну [1]. Актуальність дослідження обумовлена стрімким зростанням потреб у високопродуктивних обчисленнях для задач машинного навчання, обробки великих даних, графічного рендерингу тощо. Існуючі централізовані сервіси мають низку обмежень, зокрема високу вартість, відсутність гнучкості та недостатній рівень прозорості. Запропонована модель поєднує поєднує переваги блокчейн архітектури та розподілених обчислень великих даних, дозволяючи формувати відкритий, саморегульований ринок обчислювальних ресурсів.

**Метою дослідження є** побудова децентралізованої системи управління обчислювальними ресурсами, в якій користувачі можуть надавати або орендувати ресурси за допомогою смарт-контрактів. Серед ключових компонентів системи – алгоритм розподілу задач з урахуванням репутації, навантаження та обчислювальної потужності вузлів, модуль перевірки коректності результатів з використанням контрольних задач та zero-knowledge proof, а також адаптивна модель зберігання даних у IPFS або Arweave. Основу реалізації складає блокчейн-рішення, що гарантує безпечність транзакцій, чесність розрахунків і прозорість роботи платформи.

Порівняльний аналіз з існуючими платформами, такими як Golem та Akash Network [2], виявив переваги запропонованої системи в частині автоматичного підбору виконавців, покращеної системи валідації обчислень та оптимізованої моделі оплати . Наукова новизна полягає у розробці гібридного механізму розподілу завдань, який поєднує класичні та інтелектуальні методи, а також у впровадженні гнучкого рівня перевірки достовірності результатів без розкриття вхідних даних.

Результати дослідження мають значний потенціал для впровадження в сферу децентралізованих обчислень, індустрії штучного інтелекту, а також у державних і наукових системах, що потребують прозорого управління ресурсами та надійної перевірки результатів обробки даних.

**Список літератури**

1. Tripathi G., Ahad M. A., Casalino G. A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges //Decision Analytics Journal. – 2023. – Т. 9. – С. 100344. https://doi.org/10.1016/j.dajour.2023.100344.

2. Marple T. Bigger than Bitcoin: A theoretical typology and research agenda for digital currencies //Business and Politics. – 2021. – Т. 23. – №. 4. – С. 439-455. https://doi.org/10.1017/bap.2021.12

# ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС ДЛЯ ДИСТАНЦІЙНОГО КЕРУВАННЯ МОБІЛЬНИМ РОБОТОМ

Єрошенко О.А., Щербак А.С.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному світі технологічного прогресу та автоматизації важливу роль відіграють розумні системи керування, що дозволяють дистанційно контролювати різноманітні пристрої. Особливо актуальним стає використання мікроконтролерних платформ для створення мобільних роботизованих моделей, які можуть бути застосовані як у навчальних цілях, так і для розробки більш складних автономних систем. Одним із найбільш популярних рішень для таких проєктів є платформа Arduino, що забезпечує доступність, простоту програмування та можливість розширення функціональності [1-2].

Метою даної роботи є розробка мобільної моделі, що керується за допомогою Bluetooth-з'єднання, використовуючи мікроконтролер Arduino та мобільний застосунок. Система побудована на основі плати Arduino UNO, яка отримує команди від Bluetooth-модуля і, відповідно до отриманих сигналів, керує рухом моделі через драйвер двигунів. Живлення пристрою забезпечується двома літій-іонними акумуляторами, з'єднаними послідовно. Конструкція включає чотири мотори, які підключені паралельно та працюють за принципом танкової схеми керування: при русі вперед усі двигуни обертаються в одному напрямку, під час повороту – двигуни однієї сторони змінюють напрямок обертання або зупиняються.

Для керування моделлю використовується мобільний застосунок, який надсилає команди. Bluetooth-модуль приймає сигнали, передає їх на контролер, де вони обробляються та перетворюються у відповідні дії для руху моделі. Такий підхід забезпечує зручне та інтуїтивно зрозуміле управління моделлю, що дозволяє користувачам легко взаємодіяти з пристроєм.

Завдяки використанню доступних компонентів і відкритих технологій, розроблена система є гнучкою та масштабованою, що дозволяє модифікувати її відповідно до потреб користувача.

Розроблена модель може бути використана в освітніх цілях для навчання основам робототехніки, електроніки та програмування мікроконтролерів. Вона також є корисною для дослідницьких проєктів, спрямованих на вивчення бездротових технологій керування.

**Список літератури**

1. Tanenbaum A. S., Bos H. Modern Operating Systems. 4th ed. Pearson, 2014. 1136 p.

2. Fedorchenko V., Yeroshenko O., Shmatko O., Kolomiitsev O., Omarov M. Password hashing methods and algorithms on the .NET platform. *Advanced Information Systems*. 2024. Vol. 8(4). P. 82–92. doi: https://doi.org/10.20998/2522-9052.2024.4.11

# АНАЛІЗ ВРАЗЛИВОСТЕЙ СУЧАСНИХ ВЕБ-САЙТІВ

Безродний Є.С., Ярошевич Р.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Безпека веб-застосунків є критично важливою у сучасному цифро-вому світі. Кожного дня з'являються нові сайти онлайн-магазини, курси, фо-руми, відеохостинг, тощо. Вразливості в безпеці можуть призвести до витоку даних, фінансових втрат і репутаційних ризиків. Ними користуються інтер-нет-шахраї та хакери, у цілях заволодіти особистими даними користувачів, в першу чергу даними акаунтів та платіжних карток.

**Метою доповіді** є ознайомлення з основними вразливостями сучасних веб-застосунків та методами їх усунення. Одним із прикладів поширених веб-загроз є міжсайтовий засіб підробки запитів – Cross-Site Request Forgery (CSRF) [1]. Це тип атаки, при якій зловмисник ініціює виконання певних дій від імені авторизованого користувача без його відома. Хоча зловмисник зазвичай не може безпосередньо отримати дані відповіді на підроблений запит, він здатний ініціювати небезпечні дії, такі як переказ коштів, зміна паролів або персональних даних користувача. Якщо атакована особа має адміністративні права, під загрозою може опинитися весь веб-сайт. Для запобігання таким атакам застосовують спеціальні CSRF-токени, які супроводжують кожен запит і перевіряються сервером, а також багатофакторну автентифікацію.

Ще однією важливою проблемою є витік даних через слабкі API. Коли API недостатньо захищені або не перевіряють права доступу, конфіденційні дані можуть потрапити до рук зловмисників [2]. Використання незахищених HTTP-запитів також може призвести до перехоплення важливої інформації. Для запобігання витоку через API необхідно, по-перше, використовувати захищені протоколи HTTPS або TLS, що забезпечують шифрування даних при передачі. По-друге, рекомендовано впроваджувати OAuth 2.0 та API-ключі, які дозволяють безпечно відкривати доступ до приватних даних іншому сервісу без розголошення паролів та логінів.

Загалом, безпека веб-застосунків вимагає комплексного підходу. Веб-розробникам та компаніям необхідно активно впроваджувати сучасні методи захисту, такі як параметризовані запити, шифрування даних, контроль доступу та багатофакторна автентифікація.

Регулярні тестування і моніторинг безпеки дозволяють оперативно виявляти загрози і суттєво знижувати ризики атак.

**Список літератури**

1. Е. Хоффман. Безпека веб-застосунків. Розвідка, захист, напад. Аналіз API. 2020. Т.1, №5, С. 114-123.

2. M. Monte. Network Attacks and Exploitation: A Framework. 2015. Т1, №3, С. 65-72

# ОГЛЯД СПЕЦІАЛІЗОВАНИХ БІБЛІОТЕК ЦИФРОВОЇ ОБРОБКИ СИГНАЛІВ ДЛЯ ПЛАТФОРМИ XILINX ZYNQ 7000

Філіппенко О.І., Корнієнко В.Р.
Харківський національний університет радіоелектроніки, Харків, Україна

Проблема оптимізації часу виконання алгоритмів цифрової обробки сигналів на вбудованих системах на базі SoC є актуальною на поточний момент. Однією з головних складових є вибір спеціалізованих бібліотек які надають необхідний функціонал та імплементацію алгоритмів для конкретної архітектури. Зокрема, актуальними напрямами досліджень є аналіз прискорення швидкого перетворення Фур'є як одного з базових алгоритмів цифрової обробки сигналів. Перетворення Фур'є є одним з блоків які використовуються під час побудови гібридних систем з використанням нейронних мереж для покращення мовлення у відеоконференційному зв'язку[1].

Одним з паралельних актуальних напрямів досліджень є проектування та реалізація ефективного апаратного прискорювача для обчислення швидкого перетворення Фур'є (FFT) в обробці сигналів FMCW-радарів. Основними проблеми автори роботи [2] виділяють баланс між споживанням апаратних ресурсів і швидкістю обчислень.

**Метою доповіді** є аналіз та дослідження спеціалізованих обчислювальних бібліотек реалізації перетворення Фур'є для оцінки можливостей прискорення виконання алгоритмів придушення шуму на базі згорткових нейронних мереж на платформі ZYNQ.

В доповіді наводяться результати вимірювань часу виконання та використання ресурсів системи на платформі ZYNQ на ARM частині SoC. Проводиться аналіз API бібліотек та оцінка можливостей інтеграції їх у проект RNNoise. Наведено аналіз результатів придушення шуму за допомогою об'єктивних метрик SIGMOS та NISQA з урахуванням параметрів noiseness та coloration. Наведені результати свідчать про потенціал використання спеціалізованих бібліотек обчислення перетворення Фур'є на платформі ZYNQ 7000.

Наступні етапи досліджень включають до себе аналіз та вивчення особливостей інтеграції багатоканальної обробки аудіо даних на SoC та реалізації алгоритмів обробки даних з мікрофонних матриць.

**Список літератури**

1. An Improved Real-Time Noise Suppression Method Based on RNN and Long-Term Speech Information / B. Cheng et al. International Symposium on Automation, Information and Computing, Beijing, China, China, 9–11 December 2022. 2022. URL: https://doi.org/10.5220/0012055400003612 (date of access: 19.06.2024).

2. FPGA Implementation of an Efficient FFT Processor for FMCW Radar Signal Processing / J.Heo et al. // Sensors. – 2021. – Vol. 21, no. 19. – P. 6443. URL: https://doi.org/10.3390/s21196443 (date of access: 22.03.2025).

# МЕТОД ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО СЕГМЕНТА КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ МОДЕЛІ ZERO TRUST

Любчик В.О., Чепурна І.С.
Харківський національний університет радіоелектроніки, Харків, Україна

В сучасних корпоративних мережах, як у державному, так і в приватному секторі, значно зростають ризики, пов'язані з кіберзагрозами, витоком конфіденційної інформації та несанкціонованим доступом до конфіденційних даних. Традиційні підходи базуються на концепції периметрового захисту, проте вони втрачають актуальність в умовах зростаючої складності атак і широкого використання хмарних технологій. Збільшення кількості віддалених підключень, мобільних користувачів та оверлейних архітектур потребують новітніх підходів до управління доступом та контролю над мережними ресурсами. Імплементація методів і технологій, заснованих на концепції моделі нульової довіри (Zero Trust), яка ґрунтується на принципі «нікому не довіряти, завжди перевіряти», забезпечує високий рівень інформаційної безпеки та захисту користувацьких даних, особливо в умовах віддаленого доступу до корпоративних ресурсів [1]. Концепція передбачає, що всі запити на доступ, з внутрішньої мережі або ззовні, підлягають суворій автентифікації, авторизації та постійному моніторингу з метою мінімізації ризиків несанкціонованого доступу та компрометації інформаційних систем [2].

**Метою роботи** є організація захищеного сегмента корпоративної мережі, яка забезпечує динамічний контроль доступу до ресурсів мережі, забезпечуючи високий рівень захисту даних, мінімізуючи ризики несанкціонованого доступу та витоку інформації.

Віртуальні приватні мережі (VPN) забезпечують захищений та шифрований канал зв'язку між віддаленими користувачами та корпоративними ресурсами [3]. Використання механізмів шифрування та протоколів тунелювання гарантують конфіденційність переданих даних та забезпечують цілісність інформації під час передачі інформації, що є ключовим аспектом реалізації моделі нульової довіри. Інтеграція VPN з механізмами автентифікації та контролю доступу сприяє впровадженню принципів Zero Trust Architecture (ZTA) в сучасних IT-екосистемах. В рамках цієї моделі усі запити на доступ перевіряються незалежно від їхнього походження, що дозволяє мінімізувати ризики компрометації даних та забезпечити високий рівень безпеки корпоративної інфраструктури.

В роботі досліджено основні принципи архітектури Zero Trust, методи сегментації мережі та механізми реалізації політик доступу, що сприяють мінімізації ризиків компрометації інформаційної системи. Запропонований підхід передбачає створення захищеного каналу зв'язку за допомогою VPN, централізоване управління автентифікацією, а також впровадження моделі рольового контролю доступу (RBAC), що забезпечує принцип мінімальних привілеїв при доступі до корпоративних ресурсів. Проведене моделювання

функціонування захищеного сегмента корпоративної мережі демонструє високий рівень конфіденційності, цілісності та доступності даних, а також ефективність автентифікації та контролю доступу на основі ролей і привілеїв користувачів. Подальші дослідження в цьому напрямі спрямовані на оптимізацію використання обчислювальних ресурсів в умовах підвищених вимог до безпеки та захисту даних, зменшення затримок при доступі до ресурсів, що сприяє підвищенню якості обслуговування користувачів та зниженню навантаження на корпоративну інфраструктуру.

**Список літератури**

1. New Microsoft guidance for the CISA Zero Trust Maturity Model | Microsoft Security Blog. Microsoft Security Blog. URL: https://www.microsoft.com/

2. Tsai M., Lee S., Shieh S. W. Strategy for implementing of zero trust architecture //IEEE Transactions on Reliability. – 2024. – Т. 73. – №. 1. – С. 93-100.

3. Ткачов В. М., Чепурна І. С., Фесенко Т. Г. Метод мультирівневого vpn-тунелювання для забезпечення віддаленого доступу до вузлів екстранет-мережі // Вісник Херсонського НТУ. – 2024. – №. 3 (90). – С. 299-308.

## МЕТОД ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ВЕБЗАСТОСУНКІВ З ВИКОРИСТАННЯМ WAF

Корякіна А.М., Чепурна І.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Активне впровадження вебдодатків сприяє розвитку бізнес-процесів та покращенню взаємодії з користувачами, забезпечуючи зручний доступ до послуг та інформаційних ресурсів. Водночас зі зростанням кількості вебресурсів пропорційно зростає масштаб і складність кібератак, спрямованих на несанкціонований доступ до даних користувачів та компрометацію інформаційних систем [1]. Для ефективного захисту вебдодатків та мінімізації ризиків компрометації даних використовуються вебекрани захисту додатків (WAF). Однією з основних переваг використання WAF є його здатність динамічно адаптуватися до змін у трафіку, забезпечуючи гнучкість у виявленні та блокуванні атак [2]. Однак, складність налаштування правил фільтрації трафіку може призвести до збільшення затримок при обробці запитів, що збільшує навантаження на вебсервери та сповільняє швидкість обробки запитів, особливо в умовах високого трафіку або складних правил фільтрації.

**Метою доповіді** є розробка методу підвищення продуктивності вебдодатків шляхом інтеграції WAF з механізмом балансування навантаження.

У доповіді представлено огляд методів і технологій оптимізації продуктивності вебдодатків, зокрема через використання проксі-серверів, організації кластерної інфраструктури для обслуговування запитів, в поєднанні з застосуванням правил фільтрації трафіку для зниження навантаження на основні сервери та оптимізації обробки даних.

**Список літератури**

1. Боскін, О. О. "Безпека веб-додатків та хакерські атаки", *Вісник Херсонського національного технічного університету,* 3 (86) (2023): 83-92.
2. Lakhno, V., Husiev, B., Smolii, V., Blozva, A., Kasatkin, D., & Osypova, T. (2021). WAF захист у внутрішніх сервісів у структурі ZERO TRUST. *Кібербезпека: освіта, наука, техніка»*, *1*(13), 81–91. https://doi.org/10.28925/2663-4023.2021.13.8191

## ВИКОРИСТАННЯ ПОСЛІДОВНОСТІ МЕТОДІВ ПОПЕРЕДНЬОЇ ОБРОБКИ В СИСТЕМАХ ГОЛОСОВОЇ ІДЕНТИФІКАЦІЇ

Бондаренко М.Е., Іващенко Г.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Створення універсальних систем голосової ідентифікації потребує ретельного аналізу голосових сигналів та їх акустичного середовища, враховуючи вплив фонового шуму, реверберації та інших викривлень [1]. Для підвищення точності аналізу аудіосигналів застосовується попередня обробка, що спрямована на мінімізацію впливу шумових завад. Методи обробки поділяються на статичні та динамічні, які застосовуються залежно від специфіки мовного сигналу та умов його запису [2]. Вибір відповідного методу є критичним, оскільки він безпосередньо впливає на якість сигналу та точність подальшого розпізнавання.

**Метою дослідження** є аналіз ефективності методів попередньої обробки мовних записів для покращення роботи систем голосової ідентифікації. Проведено аналіз впливу різних типів шумових завад та методів їх пригнічення, що дозволило визначити оптимальні підходи для зменшення впливу небажаних факторів. Особливу увагу приділено порівнянню алгоритмів обробки сталого та динамічного шуму, що є одними з основних джерел викривлення мовних сигналів.

Запропонований двоступеневий підхід до пригнічення шуму включає обробку як сталого, так і динамічного шуму, що дозволяє значно підвищити якість мовного сигналу та точність ідентифікації користувачів. Результати дослідження підтверджують високу ефективність запропонованого методу, подальші дослідження будуть спрямовані на оптимізацію алгоритмів обробки та їх адаптацію до реальних умов функціонування системи.

**Список літератури**

1. Бондаренко М.Е. Вплив рівня знання мови на надійність голосової ідентифікації / Максим Едуардович Бондаренко. // 11 МНТК «Проблеми інформатизації». – Баку – Харків, 2023 р. – С. 56. DOI: https://doi.org/10.32620/PI.24.t2.
2. Г.С. Іващенко. Методи рішення задачі комівояжера на основі обчислювального інтелекту / Г. С. Іващенко, О. І. Онищенко, М. Е. Бондаренко, Н. В. Здорик // Системи управління, навігації та зв'язку.– Полтава: ПНТУ, 2024. – Т. 2 (76). – С. 99-105. DOI: https://doi.org/10.26906/SUNZ.2024.2.099.

# ВИКОРИСТАННЯ ПАРАЛЕЛІЗАЦІЇ МЕТОДІВ ПОПЕРЕДНЬОЇ ОБРОБКИ В СИСТЕМАХ ГОЛОСОВОЇ ІДЕНТИФІКАЦІЇ

Бондаренко М.Е., Іващенко Г.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Паралелізація методів попередньої обробки мовних сигналів у системах голосової ідентифікації дозволяє не лише скоротити час обробки, а й підвищити точність розпізнавання [1]. Виконання декількох етапів обробки паралельно, зокрема пригнічення шуму, нормалізації та виділення ключових ознак мовлення, сприяє зменшенню затримок і покращенню стабільності роботи системи [2, 3]. Однак існуючі бібліотеки паралелізації, такі як Intel Threading Building Blocks та POSIX Threads, мають обмеження, що ускладнюють їх ефективне застосування в умовах реального часу.

**Метою дослідження** є розробка та аналіз ефективності власного підходу до паралелізації методів попередньої обробки аудіосигналів у системах голосової ідентифікації. Проведено аналіз продуктивності традиційних бібліотек паралелізації та запропонованої системи, а також вивчено вплив різних типів шумових завад на швидкість і точність обробки сигналів. Розроблений підхід оптимізує розподіл обчислювальних ресурсів і мінімізує затримки, що дозволяє скоротити час обробки мовного сигналу.

Запропонована система паралельної обробки демонструє вищу продуктивність порівняно з існуючими бібліотеками та дозволяє значно підвищити точність голосової ідентифікації. Отримані результати підтверджують ефективність використання адаптивної паралелізації, що сприяє кращому пригніченню шуму та збереженню інформативних характеристик мовного сигналу.

Подальші дослідження мають бути спрямовані на вдосконалення алгоритмів динамічного балансування навантаження системи.

**Список літератури**

1. Бондаренко М.Е. Вплив рівня знання мови на надійність голосової ідентифікації / Максим Едуардович Бондаренко. // Одинадцята міжнародна науково-технічна конференція «Проблеми інформатизації». – Баку – Харків – Бельсько-Бяла. – 2023 р. – С. 56. DOI: https://doi.org/10.32620/PI.24.t2.

2. Г.С. Іващенко. Методи рішення задачі комівояжера на основі обчислювального інтелекту / Г. С. Іващенко, О. І. Онищенко, М. Е. Бондаренко, Н. В. Здорик // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2024. – Т. 2 (76). – С. 99-105. DOI: https://doi.org/10.26906/SUNZ.2024.2.099.

3. Martovytskyi V., Sievierinov O., Liashenko O., Koltun Y., Liashenko S., Kis V., Sukhoteplyi V., Nosyk A., Konov D., Yevstrat D. (2022). Devising an approach to the identification of system users by their behavior using machine learning methods // EasternEuropean Journal of Enterprise Technologies, 3 (117), 2022, pp. 23–34. DOI: https://doi.org/10.15587/1729-4061.2022.259099.

# МЕТОД РОЗГОРТАННЯ ЗАХИЩЕНОГО СЕГМЕНТА КОМП'ЮТЕРНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ DOCKER

Резніков Д.О., Чепурна І.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні інформаційні системи потребують високого рівня захисту даних користувачів та мережних ресурсів. Віртуальні приватні мережі (VPN), завдяки створенню захищених каналів зв'язку, забезпечують конфіденційність переданих даних, знижують ризик несанкціонованого доступу до ресурсів і мінімізують ймовірність витоку інформації.

Однак, зі зростанням кількості кіберзагроз і підвищенням вимог до безпеки, традиційні методи побудови захищених з'єднань, зокрема апаратні VPN-шлюзи, виявляють обмеження в гнучкості, масштабованості та ефективності використання апаратних ресурсів [1].

Контейнеризація, зокрема в Docker, є сучасним підходом до розгортання мережних сервісів, зокрема засобів інформаційної безпеки, що забезпечує ізоляцію середовища виконання, ефективне використання апаратних ресурсів, високу масштабованість і підвищений рівень захисту даних [2].

**Метою роботи** є розробка методу розгортання захищеного сегмента комп'ютерної мережі на основі Docker-контейнера з OpenVPN для забезпечення безпечного та гнучкого доступу до ресурсів локальної інфраструктури.

У доповіді проведено аналіз існуючих протоколів тунелювання, зокрема OpenVPN, WireGuard та IPSec, а також підходів до їх застосування в контейнеризованих середовищах.

Наведені дані підтверджують, що контейнеризація на основі Docker забезпечує ефективний доступ до ресурсів локальної мережі навіть в умовах обмежених апаратних можливостей, мінімізує затримки під час передачі даних і підвищує стійкість до збоїв.

Водночас застосування OpenVPN в контейнеризованому середовищі є доцільним завдяки його високій сумісності з технологіями контейнеризації, підтримці різних операційних систем, а також низьким впливом на апаратні ресурси [3].

**Список літератури**

1. Верховський І., Ткачов В. Методи побудови віртуальних тунелів extranet–систем. Scientific review. 2023. Т. 4, № 89. С. 22. URL: https://doi.org/10.26886/2311–4517.4(89)2023.2.

2. Muzumdar, Prathamesh, et al. "Navigating the Docker Ecosystem: A Comprehensive Taxonomy and Survey." Asian J. Res. Com. Sci 17.1 (2024): 42-61.

3. Ткачов В. М., Чепурна І. С., Фесенко Т. Г. Метод мультирівневого vpn-тунелювання для забезпечення віддаленого доступу до вузлів екстранет-мережі //Вісник Херсонського національного технічного університету. – 2024. – №. 3 (90). – С. 299-308.

# ПОСТКВАНТОВА КРИПТОГРАФІЯ: ПЕРСПЕКТИВИ ТА ВИКЛИКИ

Зінов'єв А.В., Мороз А.В.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком квантових обчислень постає загроза компрометації традиційних криптографічних алгоритмів, зокрема RSA, ECC та інших методів, що ґрунтуються на складності факторизації великих чисел або дискретного логарифмування.

Алгоритм Шора, реалізований на потужному квантовому комп'ютері, здатний за поліноміальний час розкласти великі числа на множники, що зробить сучасні криптографічні протоколи вразливими. У зв'язку з цим виникає необхідність у розробці криптографічних методів, стійких до атак квантових комп'ютерів. [1]

Постквантова криптографія (PQC) спрямована на створення алгоритмів, які залишатимуться безпечними навіть за умови існування квантових комп'ютерів. Основні підходи включають криптографію на ґратках, кодову криптографію, мультилінійну алгебру, хеш-функції та ізогенії еліптичних кривих.

Зокрема, алгоритми, такі як NTRUEncrypt та Crystals-Kyber, демонструють високу стійкість до атак квантових обчислень та є кандидатами на стандартизацію Національним інститутом стандартів і технологій США (NIST). [2]

Попри значний прогрес у дослідженні постквантових алгоритмів, залишаються відкриті питання щодо їхньої ефективності, продуктивності та практичної реалізації.

Наприклад, криптосистеми на ґратках вимагають значних обчислювальних ресурсів, а кодова криптографія має великі ключі, що ускладнює їх впровадження в реальних системах. Крім того, актуальним залишається питання інтеграції PQC-алгоритмів у сучасні криптографічні протоколи, такі як TLS, IPsec і VPN. [3]

**Метою доповіді** є аналіз перспектив та викликів постквантової криптографії, огляд сучасних підходів до захисту інформації в умовах квантових загроз, а також обговорення можливих напрямів розвитку цієї галузі.

**Список літератури**

1. Гриценко П.В. Квантові загрози традиційним криптосистемам: аналіз та прогноз. – Київ: Наукова думка, 2021. – 278 с.

2. Лисенко О.М. Постквантова криптографія: алгоритми та стандартизація. – Львів: Технологічний університет, 2022. – 304 с.

3. Іванченко Г.С. Виклики та перспективи безпеки в еру квантових обчислень. – Харків: Видавничий дім, 2023. – 256 с.

# ВИКОРИСТАННЯ ZERO TRUST ПІДХОДУ В КОРПОРАТИВНІЙ КІБЕРБЕЗПЕЦІ

Буканов І.В., Сітніков В.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Зі зростанням кількості кіберзагроз та атак на корпоративні мережі традиційні методи безпеки, засновані на периметровому захисті, стають менш ефективними. Сучасні організації все частіше впроваджують концепцію Zero Trust (нульової довіри), яка передбачає перевірку кожного користувача та пристрою незалежно від їхнього місця розташування в мережі. Це дозволяє мінімізувати ризики внутрішніх загроз і підвищити загальний рівень кібербезпеки компанії. [1]

Основний принцип Zero Trust – "ніколи не довіряй, завжди перевіряй". У цьому підході контроль доступу базується на багатофакторній автентифікації (MFA), моніторингу активності користувачів у режимі реального часу та сегментації мережі для обмеження можливостей зловмисників. Крім того, використовуються сучасні методи аналітики поведінки (UBA), які допомагають виявляти аномальні дії та потенційні загрози. [2]

Важливим аспектом впровадження Zero Trust є принцип мінімальних привілеїв, що передбачає надання доступу лише до необхідних ресурсів. Це значно знижує ризик компрометації даних у разі витоку облікових даних або компрометації пристрою. Також широко застосовуються технології Endpoint Detection and Response (EDR) та Security Information and Event Management (SIEM) для збору та аналізу подій у системі безпеки. [3]

Практичне впровадження Zero Trust у корпоративних середовищах включає використання Software-Defined Perimeter (SDP), захищених шлюзів доступу (ZTNA), а також інтеграцію з хмарними сервісами для контролю доступу до ресурсів.

Такі рішення допомагають організаціям захистити свої критично важливі дані навіть у разі використання віддалених робочих місць або підключення до незахищених мереж.

**Метою доповіді** є аналіз концепції Zero Trust, основних механізмів її реалізації та розгляд практичних кейсів впровадження в корпоративній кібербезпеці.

**Список літератури**

1. Коваленко В.І. Zero Trust як нова парадигма кібербезпеки. – Київ: Видавничий дім, 2022. – 260 с.

2. Петренко О.М. Захист корпоративних мереж: впровадження підходу Zero Trust. – Львів: Технопринт, 2023. – 312 с.

3. Сидоренко Г.С. Інноваційні методи кіберзахисту: Zero Trust, AI та поведінковий аналіз. – Харків: Інформатика, 2021. – 280 с.

# ВЕБЗАСТОСУНОК ДЛЯ МЕДИТАЦІЇ

Москвіна О.Л., Єрошенко О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному світі, що характеризується високим темпом життя, інформаційним перевантаженням і зростанням рівня стресу, питання збереження психологічного здоров'я набуває особливої актуальності. Одним із ефективних способів підтримки ментального балансу є практика медитації, що з кожним роком стає все популярнішою серед користувачів цифрових технологій.

З огляду на це, розробка зручних інструментів для медитативної практики, зокрема веб-додатків, є доцільним і перспективним напрямом у сфері інформаційних технологій.

Веб-додаток для медитації — це програмне рішення, що надає користувачам доступ до різноманітних практик усвідомленості, дихальних вправ, звукових сесій тощо через браузер без необхідності встановлення програмного забезпечення. Такі додатки можуть бути адаптивними, мультиплатформеними й персоналізованими відповідно до потреб користувача.

**Мета дослідження** — обґрунтувати доцільність створення веб-додатку для медитації, визначити його основні функціональні характеристики та технології реалізації, а також розглянути приклади практичного застосування.

Згідно з дослідженнями психологів, регулярна практика медитації сприяє зниженню рівня тривожності, покращенню концентрації, підвищенню емоційної стабільності та загального рівня задоволеності життям. Разом із тим, не всі користувачі мають змогу відвідувати спеціалізовані курси або користуватись мобільними застосунками, що вимагають встановлення на пристрій.

Веб-додаток для медитації є ефективним інструментом для підтримки ментального здоров'я, особливо в умовах цифрового світу. Успішна реалізація такого продукту потребує міждисциплінарного підходу - залучення фахівців з IT, психології, дизайну та контент-менеджменту.

Перспективним напрямом є створення веб-додатків, адаптованих до культурних та мовних особливостей користувачів, із розширеним функціоналом і підтримкою офлайн-режиму.

**Список літератури**

1. Fedorchenko V., Yeroshenko O., Shmatko O., Kolomiitsev O., Omarov M. Password hashing methods and algorithms on the .NET platform. *Advanced Information Systems*. 2024. Vol. 8(4). P. 82–92. doi: https://doi.org/10.20998/2522-9052.2024.4.11

2. Щолкін М.М., Єрошенко О.А. Автоматизація управлінських рішень на основі BIG DATA та машинного навчання. *Проблеми інформатизації*: тези доповідей 12-тої міжнародної науково-технічної конференції. Т.2. 2024. С. 85.

# ЗАСТОСУНОК ДЛЯ ВІДСТЕЖЕННЯ ВИТРАТ ТА ДОХОДІВ

Єрошенко О.А., Балабанов Р.М.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному світі цифрові технології активно інтегруються у повсякденне життя людини, змінюючи способи взаємодії з фінансовими ресурсами. Управління особистими фінансами стало актуальним питанням, особливо в умовах економічної нестабільності. Одним із ефективних інструментів контролю та планування бюджету є мобільні та веб-застосунки для обліку доходів і витрат. Такі застосунки не лише автоматизують процес фінансового моніторингу, але й сприяють формуванню фінансової грамотності серед користувачів.

Метою цієї роботи є аналіз функціональних особливостей застосунку для відстеження доходів і витрат, а також розгляд підходів до його розробки з урахуванням потреб користувача та технічних вимог.

Застосунок для обліку фінансів виконує кілька ключових функцій. Реєстрація транзакцій, користувачі мають можливість вручну фіксувати витрати та доходи, класифікувати їх за категоріями. Один із найважливіших елементів – візуалізація даних. Планування бюджету, інструменти планування дозволяють встановлювати фінансові цілі, обмеження витрат у певних категоріях, автоматичні нагадування про платежі або перевищення бюджету. Синхронізація та збереження даних, застосунок має підтримувати резервне копіювання та синхронізацію даних між пристроями. Це забезпечує безперервність доступу до інформації. Безпека та конфіденційність, особиста фінансова інформація вимагає надійного захисту. Впровадження сучасних методів шифрування, автентифікації (наприклад, 2FA) та захисту баз даних є обов’язковим.

Технічно застосунок реалізується на основі сучасних фреймворків.

Створення застосунку для відстеження доходів і витрат є важливим кроком у напрямку підвищення фінансової грамотності користувачів. Такий інструмент сприяє формуванню усвідомленого ставлення до особистих фінансів, дозволяє контролювати бюджет та ефективно планувати витрати.

**Список літератури**

1. Fedorchenko V., Yeroshenko O., Shmatko O., Kolomiitsev O., Omarov M. Password hashing methods and algorithms on the .NET platform. *Advanced Information Systems*. 2024. Vol. 8(4). P. 82–92. doi: https://doi.org/10.20998/2522-9052.2024.4.11

2. Щолкін М.М., Єрошенко О.А. Автоматизація управлінських рішень на основі BIG DATA та машинного навчання. *Проблеми інформатизації*: тези доповідей 12-тої міжнародної науково-технічної конференції. Т.2. 2024. С. 85.

3. Yeroshenko O., Prasol I., Trubitsyn O., Rebezyuk L.Organization of a Wireless System for Individual Biomedical Data Collection. *International Journal of Innovative Technology and Exploring Engineering*. Vol. 9, no. 4. 2020, P. 2418-2421.

# ВПЛИВ UX/UI-ДИЗАЙНУ НА ЕФЕКТИВНІСТЬ АДАПТИВНИХ ВЕБЗАСТОСУНКІВ У СФЕРІ ЗАМОВЛЕННЯ ТА ДОСТАВКИ ПРОДУКТІВ ХАРЧУВАННЯ

Касянчук Д.І., Ярошевич Р.О.
Харківський національний університет радіоелектроніки, Харків, Україна

UX/UI-дизайн є визначальним фактором ефективності адаптивних веб-застосунків у сфері доставки їжі. Саме якісний дизайн інтерфейсу дозволяє користувачам швидко досягати своїх цілей, скорочуючи кількість необхідних дій для пошуку товарів, оформлення замовлень і вибору зручного часу доставки. Це мінімізує кількість помилкових дій, адже чіткі та зрозумілі підказки допомагають уникнути неправильних кроків.

**Метою доповіді є** аналіз впливу UX/UI-дизайну на ефективність використання адаптивних веб-застосунків для замовлення та доставки продуктів харчування, а також визначення ключових аспектів, що покращують користувацький досвід та загальну продуктивність сервісів.

Ключовим фактором успішності таких застосунків є їх адаптивність, яка передбачає зручну роботу на різних пристроях — смартфонах, планшетах і ноутбуках. Застосування підходу mobile-first дозволяє створити ефективний інтерфейс для мобільних пристроїв з подальшим масштабуванням для великих екранів, що відповідає актуальним тенденціям веб-розробки.

Важливим елементом є також грамотне використання кольорових рішень і типографіки. Кольори впливають на емоційний стан користувачів та формують відповідні асоціації з діями, наприклад, зелений для підтвердження або червоний для попереджень. Використання не більше двох-трьох шрифтів забезпечує легкість сприйняття інформації та стилістичну єдність інтерфейсу [1].

Також важливим аспектом UX/UI-дизайну є зручність використання, яка досягається через спрощення навігації, створення логічної структури та інтуїтивно зрозумілих елементів інтерфейсу. Мінімізація зусиль досягається завдяки правильному розташуванню кнопок, лаконічному тексту та відсутності зайвих елементів, що можуть заплутати користувачів [2]. Користувачам важливо забезпечити швидкий доступ до основних функцій, таких як пошук товарів, перегляд кошика, оформлення замовлення та перегляд історії покупок. Використання зрозумілих піктограм та логічна структура сторінок позитивно впливають на взаємодію користувачів, а зручне розміщення кнопки «Оформити замовлення» сприяє зменшенню кількості покинутих кошиків.

**Список літератури**

1. Tuhin Bhatt. Intelivita (2023). Role of UI/UX Design in Food Delivery App Development.

2. Company „Weavers Web Solutions Pvt. Ltd.” (2024). 6 Essential UI/UX Design Principles for Food Delivery Apps in 2025.

## УЧАСНИКИ КОНФЕРЕНЦІЇ (секції 3, 4)


Agayeva U.H. ..... 62
Balagura D.S. ..... 64
Brysina I.V. ..... 10
..... 14
Haqverdiyeva Z.H. .. 62
Hrinenko T.O. ..... 65
Lukin V.V. ..... 10
..... 14
..... 16
..... 18
Makarichev V.O. ..... 10
..... 14
Nadtochyi M.M. ..... 64
Ovdiyuk E. ..... 12
Rebrov V.S. ..... 16
Telnova A.A. ..... 65
Tsekhmystro R.V. .... 18
Аврунін О.О. ..... 23
Антіпов І.Є. ..... 99
Бабаніна А.О. ..... 51
Баєв І.С. ..... 53
Балабанов Р.М. ..... 137
Балагура Д.С. ..... 76
..... 77
..... 78
..... 79
Барковська О.Ю. .... 23
..... 24
..... 25
..... 26
..... 27
..... 28
..... 45
..... 46
Безродний Є.С. ..... 127
Блінна В.С. ..... 82
Бондаренко М.Е. .... 131
..... 132
Ботнар П.Д. ..... 125
Буканов І.В. ..... 135
Булгаков Р.І. ..... 38
Буряк В.А. ..... 24
Бухарова Л.Д ..... 26
В'юхін Д.О. ..... 82
..... 83
..... 84
..... 86
..... 87
..... 88
..... 89
..... 90
..... 91
В'юхін Д.О. ..... 92
..... 94
..... 96
Васильєв О.Ю. ..... 40
Велікан В.О. ..... 57
Власов А.В. ..... 94
Волк М.О. ..... 35
Волощук О.Б. ..... 53
..... 57
В'юхін Д.О. ..... 83
Гаврашенко А.О. ... 123
..... 124
..... 22
Гапіченко А.М. ..... 73
Голобородько Ю.М. 90
..... 91
Головко Є.В. ..... 112
Головченко О.С. .... 24
Горчаненко С.О. .... 6
Грасмік С.В. ..... 66
Гріненко Т.О. ..... 69
..... 70
..... 71
Грінь Д.В. ..... 52
Гур'єва К.В. ..... 32
Гущин Б.-Д.І. ..... 114

Демиденко Д.В. ..... 58
Дмитренко В. ..... 55
Дуднік Д.О. ..... 30
Євгеньєв А.М. ..... 107
Єнальєва Г.С. ..... 105
Єрошенко О.А. ..... 126
..... 136
..... 137
..... 31
Жигалка М.І. ..... 49
Заболотний В.І. ..... 72
..... 73
..... 74
..... 75
Зінов'єв А.В. ..... 134
Знайдюк В. Г. ..... 53
Іващенко Г.С. ..... 131
Іващенко Г.С. ..... 132
Іващенко І.В. ..... 83
Калмиков А.В. ..... 9
Калмикова К.А. ..... 9
Канцір Р.Б. ..... 20
Касянчук Д.І. ..... 138
Келеберда П.О. ..... 47
Кібірєв Д.О. ..... 109
Климова І.М. ..... 59
..... 60
..... 61
Коваленко А.А. ..... 51
Колобаєв Н.М. ..... 61
Коломицев А.Р. ..... 84
Колтун Ю.М. ..... 58
Корнієнко В.Р. ..... 128
Корякіна А. М. ..... 130
Костін А.О. ..... 25
Красіля М.М. ..... 39
Кривицький А.О. ... 36
Кривонос П.Р. ..... 33
Крикливець В.В. .... 48
Кулик Ю.О. ..... 120
Кустов А.К. ..... 72
Ларченко Л.В. ..... 39
..... 42
Левандовський О.С. 74
Левчук Д.Д. ..... 34
Леонова А.О. ..... 96
Літвін О.О. ..... 88
Лук`яненко М.С. .... 96
Луценко В.І. ..... 103
Любчик В.О. ..... 129
Ляшенко Г.Є. ..... 32
..... 33
..... 34
..... 38
..... 50
..... 52
Ляшенко О.С. ..... 57
Ляшко М.С. ..... 91
Малярова Д.М. ..... 69
Мамчич О.О. ..... 35
Медвєдєв М.І. ..... 21
Мельникова О.А. ... 66
..... 68
Мизюра М.С. ..... 7
Мірза Д.С. ..... 50
Мокрій В.С. ..... 94
Мороз А.В. ..... 134
..... 47
Москвіна О.Л. ..... 136
Наконечний М.В. ... 84
..... 85
..... 86
..... 88
Нарєжній О.П. ..... 69
Настенко А.О. ..... 101
..... 102
Нечітайло О.В. ..... 123
Нєдєльніцев І.В. ..... 99
Ніконенко Д.В. ..... 90
Новік Т.О. ..... 92
Олефір А.В. ..... 42
Олефір М.О. ..... 31
Олешко І.В. ..... 103
Олійник Е.В. ..... 68
Острижна Є.С. ..... 121
Переметчик Д.О. .... 119
Пліщенко В.С. ..... 101

Постельняк Ю.П. ... 45
Потапов Р.О. ..... 54
Просолов В.В. ..... 117
Рева О.А. ..... 9
Резніков Д.О. ..... 133
Риков Д.М. ..... 116
Рой Є.О. ..... 70
Руженцев В.І. ..... 100
Свиридов Г.І. ..... 75
Сергієнко В.І. ..... 43
Сердечний В.С. ..... 27
..... 29
..... 30
Сєвєрінов О.В. ..... 105
..... 107
Сидоренко З.М. ..... 105
..... 107
Синицін Я.С. ..... 77
Синиціна В.С. ..... 76
Ситник О.В. ..... 51
Сітніков В.І. ..... 135
..... 49
Скороход М.М. ..... 30
Смідович Л.С. ..... 120
Смірнов А.О. ..... 119
..... 78
Смірнов А.О. ..... 79
..... 80
..... 83
..... 89
Сочівкін В.М. ..... 124
Сторчай Д.Г. ..... 28
Стукота О.В. ..... 59
Сухотеплий В.М. ... 76
Тимошенко Д.О. .... 20
..... 48
Топорець Д.О. ..... 46
Туз М.О. ..... 71
Уманська А.О. ..... 80
Федорченко В.М. ... 109
..... 54
..... 55
Федюшин О.І. ..... 112
..... 97
Філатова А.С. ..... 102
Філіппенко І.В. ..... 36
..... 43
Філіппенко О.І. ..... 128
..... 40
Фроленко В.О. ..... 92
Хая А.О. ..... 89
Хівренко Г.О. ..... 111
Холєв В.О. ..... 21
Холєв Н.О. ..... 75
Цемма Д.О. ..... 100
Чепурна І. С. ..... 130
..... 129
..... 133
Шапіро А.С. ..... 29
Шевелєв В.Р. ..... 22
Шестопал Д.О. ..... 79
Шмагун В.І. ..... 78
Шмарін М.Д. ..... 60
Штангей В.О. ..... 86
Шулік П.В. ..... 82
..... 87
..... 97
..... 98
Щербак А.С. ..... 126
Щербакова Ю.А. .... 121
Якимчук М.Д. .....
Янко А.С. ..... 6
..... 7
Янковський О.А. .... 125
Ярошевич Р.О. ..... 127
..... 138
Яхно С.С. ..... 87

## ОРГАНІЗАЦІЇ, ЯКІ ПРИЙНЯЛИ УЧАСТЬ У КОНФЕРЕНЦІЇ

*Азербайджанський державний аграрний університет, Баку, Азербайджан*
*Азербайджанський державний економічний університет, Баку, Азербайджан*
*Азербайджанський державний педагогічний університет, Баку, Азербайджан*
*Азербайджанський технічний університет, Баку, Азербайджан*
*Азербайджанський технологічний університет, Баку, Азербайджан*
*Азербайджанський університет будівництва та архітектури, Баку, Азербайджан*
*Бакинський військовий коледж, Баку, Азербайджан*
*Бакинський державний університет, Баку, Азербайджан*
*Бакинський інженерний університет, Баку, Азербайджан*
*Військовий науково-дослідний інститут, Баку, Азербайджан*
*Військовий інститут імені Гейдара Алієва, Баку, Азербайджан*
*Військовий інститут танкових військ НТУ ХПІ, Харків, Україна*
*Державний біотехнологічний університет, Харків, Україна*
*Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна*
*Державний університет «Київський авіаційний інститут», Київ, Україна*
*Інститут військового управління, Баку, Азербайджан*
*Інститут нафтохімічних процесів імені акад. Ю.Г. Мамедалієва, Баку, Азербайджан*
*Інститут систем управління Азербайджанської Національної академії наук, Баку, Азербайджан*
*Київський національний університет будівництва і архітектури, Київ, Україна*
*Космічне агентство Азербайджанської Республіки, Баку, Азербайджан*
*Навчальний центр Азербайджанського агентства наземного транспорту, Баку, Азербайджан*
*Нахічеванський державний університет, Нахічевань, Азербайджан*
*Національна авіаційна академія, Баку, Азербайджан*
*Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, Львів, Україна*
*Національне аерокосмічне агентство, Баку, Азербайджан*
*Національний аерокосмічний університет "Харківський авіаційний інститут", Харків, Україна*

*Національний технічний університет "Харківський політехнічний інститут", Харків, Україна*
*Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна*
*Національний університет оборони Азербайджанської республіки, Баку, Азербайджан*
*Національний університет оборони України, Київ, Україна*
*Національний університет цивільного захисту України, Харків, Черкаси, Україна*
*Педагогічний університет імені Комісії Національної Освіти в Кракові, Краків, Польща*
*Представництво «Оракл Іст Сентрал Юроп Сервісис Б.В.», Київ, Україна*
*Придніпровська державна академія будівництва та архітектури» УДУНТ, Дніпро, Україна*
*Республіканський центр сейсморозвідки, Баку, Азербайджан*
*Університет міста Жиліна, Жиліна, Словаччина*
*Університет технології і гуманітарних наук, Бельсько-Бяла, Польща*
*Харківський національний автомобільно-дорожній університет, Харків, Україна*
*Харківський національний економічний університет імені Саймона Кузнеця, Харків, Україна*
*Харківський національний університет імені В.Н. Каразіна, Харків, Україна*
*Харківський національний університет міського господарства імені О.М. Бекетова, Харків, Україна*
*Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна*
*Харківський національний університет радіоелектроніки, Харків, Україна*
*Харківський радіотехнічний фаховий коледж, Харків, Україна*
*Fugro Gb (North) Marine Limited, Абердин, Шотландія, Великобританя*
*Черкаський державний технологічний університет, Черкаси, Україна*

## АФІЛЯЦІЯ УЧАСНИКІВ КОНФЕРЕНЦІЇ

## ЗМІСТ

**Том 1:** секції 1, 5

**Том 2:** секція 2

**Том 3:** секції 3, 4

**Секція 3** Методи швидкої та достовірної обробки даних в комп'ютерних системах та мережах ..... 6

**Секція 4** Безпека функціонування комп'ютерних систем та мереж ..... 62

**Учасники конференції** (секції 3, 4) ..... 139

**Організації, які прийняли участь у конференції** ..... 142

**Том 4:** секція 6

---

НАУКОВЕ ВИДАННЯ

**СУЧАСНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ**

**Тези доповідей**
**п'ятнадцятої міжнародної науково-технічної конференції**
**(24 – 25 квітня 2025 року)**
**Том 3: секції 3, 4**

Відповідальний за випуск *В. В. Косенко*
Технічний редактор *І. А. Лєбедева*
Коректор *В. В. Богомаз*
Комп'ютерне складання та верстання *Н. Г. Кучук*

Адреса оргкомітету: вул. Кирпичова, 2, Харків, 61002, Україна
Вечірній корпус, кімната 314
тел. +38 (057) 707 61 65

Підписано до друку 18.04.2025 Формат 60 × 84/16
Ум.-вид. арк. 9,0. Тираж 100 пр. Зам. 418/3-25

Віддруковано з готових оригінал-макетів у цифровій друкарні Impress
61002, м. Харків, вул. Пушкінська, 56, тел. **+ 38 (057) 714-52-11**
e-mail: **irina@impress.biz.ua**