ІНСТИТУТ МАТЕМАТИКИ
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 шістнадцятої міжнародної

науково-технічної конференції

29 – 30 квітня 2026 року

Том 3: секції 3, 4

Баку – Харків – Жиліна – 2026

УДК 004/681.3 doi: https://doi.org/10.32620/ICT.26.t3

У збірнику подано тези доповідей шістнадцятої 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

Співголови оргкомітету

ГАШИМОВ Ельшан Гіяс огли (*д.н.б.&в.н., проф., ІМ АР, Баку, Азербайджан*);
КОВАЛЕНКО Андрій Анатолійович (*д.т.н., проф., ХНУРЕ, Харків, Україна*);
КУЧУК Георгій Анатолійович (*д.т.н., проф., НТУ «ХПІ», Харків, Україна*);
ЛЕВАШЕНКО Віталій (*к.т.н., проф., Ун-т міста Жиліна, Жиліна, Словаччина*);
ФЕДОРОВИЧ Олег Євгенович (*д.т.н., проф., НАУ «ХАІ», Харків, Україна*).

Члени оргкомітету

ГЛАВЧЕВ Максим Ігорович (*к.е.н., доц., НТУ «ХПІ», Харків, Україна*);
ГЛИВА Валентин Анатолійович (*д.т.н., проф., КНУБА, Київ, Україна*);
ДОРОНІН Євген Володимирович (*к.т.н., доц., НУ «КАІ», Київ, Україна*);
ЗАЙЦЕВА Єлєна (*к.т.н., проф., Ун-т міста Жиліна, Жиліна, Словаччина*);
КАЛІНІН Євгеній Іванович (*д.т.н., проф., НУ БрПкУ, Київ, Україна*);
КАРПІНСЬКІ Міколай (*д.н., проф., Університет Бельсько-Бяла, Польща*);
КОЛОМІЙЦЕВ Олексій Володимирович (*д.т.н., проф., НТУ «ХПІ», Харків, Україна*);
КОСЕНКО Віктор Васильович (*д.т.н., проф., НУ «ПП», Полтава, Україна*);
ЛЕВЧЕНКО Лариса Олексіївна (*д.т.н., проф., НТУУ «КПІ», Київ, Україна*);
ЛЕЩЕНКО Олександр Борисович (*к.т.н., проф., НАУ «ХАІ». Харків, Україна*);
МОЖАЄВ Олександр Олександрович (*д.т.н., проф., ХНУВС, Харків, Україна*);
ПОДОРОЖНЯК Андрій Олексійович (*к.т.н., доц., НТУ «ХПІ», Харків, Україна*);
РОМАНЕНКОВ Юрій Олександрович (*д.т.н., проф., ХНУРЕ, Харків, Україна*);
РУБАН Ігор Вікторович (*д.т.н., проф., ХНУРЕ, Харків, Україна*);
СЄВЄРІНОВ Олександр Васильович (*к.т.н., доц., ХНУРЕ, Харків, Україна*);
СЕМЕНОВ Сергій Геннадійович (*д.т.н., проф.,УКНО, Краків, Польща*);
СМІРНОВ Олександр Анатолйович (*д.т.н., проф., ЦНТУ, Кропивницький, Україна*);
ТРЕТЬЯКОВ Олег Вальтерович (*д.т.н., проф., НУ «КАІ», Київ, Україна*);
ШЕФЕР Олександр Віталійович (*д.т.н., проф., НУ «ПП», Полтава, Україна*).

Секретаріат оргкомітету

КУЧУК Ніна Георгіївна (*д.т.н., проф., НТУ «ХПІ», Харків, Україна*);
ЛЯШЕНКО Олексій Сергійович (*к.т.н., доц., ХНУРЕ, Харків, Україна*).

© ІМ АР, НТУ "ХПІ", ХНУРЕ, НАУ «ХАІ», УмЖ, 2026

INSTITUTE OF MATHEMATICS
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 IN THE DEVELOPMENT OF INFORMATION AND COMMUNICATION TECHNOLOGIES AND CONTROL TOOLS

Proceedings of 16-th International

Scientific and Technical Conference

April 29 – 30, 2026

Volume 3: sections 3, 4

Baku – Kharkiv – Žilina – 2026

UDC 004/681.3 doi: https://doi.org/10.32620/ICT.26.t3

Abstracts of reports of the 16-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.

ORGANIZING COMMITTEE

Co-chairs of the organizing committee:

Elshan Giyas oglu HASHIMOV (Dr. Nat. security and mil. sc., Baku, Azerbaijan);
Andriy KOVALENKO (Dr. Sc. (Tech.), Prof., Kharkiv, Ukraine);
Heorhii KUCHUK (Dr. Sc. (Tech.), Prof., Kharkiv, Ukraine);
Vitaly LEVASHENKO (Dr. (Comp. Eng.), Prof., Zilina, Slovakia);
Oleg FEDOROVICH (Dr. Sc. (Tech.), Prof., Kharkiv, Ukraine).

Members of the organizing committee:

Maksym HLAVCHEV (PhD (Ycon.), Ass. Prof., Kharkiv, Ukraine);
Valentyn GLYVA (Dr. Sc. (Tech.), Prof., Kyiv, Ukraine)
Yevhen DORONIN (*PhD (Tech.), Ass. Prof., Kyiv, Ukraine*);
Elena ZAITSEVA (Dr. (Comp. Eng.), Prof., Zilina, Slovakia);
Yevhen KALININ (Dr. Sc. (Tech.), Prof., Kyiv, Ukraine);
Mikolay KARPINSKI (Dr. Sc. (Tech.), Prof., Bielsko-Biala, Poland);
Oleksii KOLOMIITSEV (Dr. Sc. (Tech.), Prof., Kharkiv, Ukraine);
Viktor KOSENKO (Dr. Sc. (Tech.), Prof., Poltava, Ukraine)
Larysa LEVCHENKO (Dr. Sc. (Tech.), Ass. Prof., Kyiv, Ukraine);
Oleksandr LESHCHENKO (PhD (Tech.), Prof., Kharkiv, Ukraine);
Oleksandr MOZHAIEV (Dr. Sc. (Tech.), Prof., Kharkiv, Ukraine);
Andrii PODOROZHNIAK (PhD (Tech.), Ass. Prof., Kharkiv, Ukraine);
Yuri ROMANENKOV (Dr. Sc. (Tech.), Prof., Kharkiv, Ukraine);
Igor RUBAN (Dr. Sc. (Tech.), Prof., Kharkiv, Ukraine);
Oleksandr SIEVIERINOV (PhD (Tech.), Ass. Prof., Kharkiv, Ukraine);
Serhii SEMENOV (Dr. Sc. (Tech.), Prof., Krakow, Poland);
Oleksii SMIRNOV (Dr. Sc. (Tech.), Prof., Kropyvnytskyi, Ukraine);
Oleg TRETYAKOV (*Dr. Sc. (Tech.), Prof., Kyiv, Ukraine*);
Oleksandr SHEFER (Dr. Sc. (Tech.), Prof., Poltava, Ukraine).

Secretariat of the organizing committee:

Nina KUCHUK (Dr. Sc. (Tech.), Prof., Kharkiv, Ukraine);
Oleksii LIASHENKO (PhD (Tech.), Ass. Prof., Kharkiv, Ukraine).

Шістнадцята міжнародна науково-технічна конференція “Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління” проводиться 29 та 30 квітня 2026 року в режимі ONLINE. Тези доповідей доступні в INTERNET.

Том 1 (Volume 1)

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

Section 1. Theoretical and Applied Aspects of Decision-Making, Optimization, and Systems and Process Management

Секція 5. Сучасні інформаційно-вимірювальні системи

Section 5. Modern Information and Measurement Systems

Том 2 (Volume 2)

Секція 2. Комп’ютерні методи і засоби інформаційно-комунікаційних технологій та управління

Section 2. Computer Methods and Tools of Information and Communication Technologies and Management

Том 3 (Volume 3)

Секція 3. Методи швидкої та достовірної обробки даних в комп’ютерних системах та мережах

Section 3. Methods for Rapid and Reliable Data Processing in Computer Systems and Networks

Секція 4. Безпека функціонування комп’ютерних систем та мереж

Section 4. Security of Computer Systems and Networks Operation

Том 4 (Volume 4)

Секція 6. Інформаційні технології у цивільній безпеці

Section 6. Information Technologies in Civil Security

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

COMPARISON OF DAC AND PDCTC: VISUALLY LOSSLESS COMPRESSION OF JPEG IMAGES

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

Digital images have numerous applications [1, 2]. They are widely used in remote sensing, medicine, precise agriculture, ecology monitoring, autonomous and security systems, etc. There are many image compression algorithms. JPEG is de facto a standard for digital photos.

In our current research, we consider the problem of visually lossless compression of JPEG images. We investigate the performance of two algorithms: discrete atomic compression (DAC) [3] and progressive discrete cosine transform coder (PDCTC) [4]. **Our aim is** to show that visually lossless compression of JPEG images can be achieved using these methods.

In this talk, we present a comparison of DAC and PDCTC on the ImageNet ILSVRC validation set [5]. The total number of samples is 50,000. Each source image is stored in JPEG format.

We evaluate the following metrics:
- maximum absolute deviation (MAD),
- root mean square error (RMS),
- peak signal-to-noise ratio (PSNR),
- compression ratio relative to BMP - CR(BMP),
- compression ratio relative to JPEG - CR(JPEG).

Additionally, we analyze the correlation between MAD and RMS to evaluate the predictability of distortion for each algorithm. We compute Pearson and Spearman coefficients, as well as R^2-scores.

Tables 1-3 show the aggregated results.

In Fig. 1 and 2, the MAD vs. RMS correlation is shown. Finally, Fig. 3 displays overall algorithm profiles.

Table 1. MAD vs RMS Correlation

Algorithm	Pearson R	R^2-score	Spearman ρ
DAC	0.6534	0.4270	0.6792
PDCTC	0.4292	0.1842	0.5314

Table 2. Quality metrics for DAC and PDCTC

Metric	Algorithm	Min	Max	Mean	Median	Std. dev
MAD	DAC	12.00	56.00	**29.04**	29.00	4.93
	PDCTC	7.00	191.00	**39.89**	39.00	14.17
RMS	DAC	0.84	5.93	**3.96**	3.97	0.84
	PDCTC	0.81	8.07	**3.84**	3.79	1.23
PSNR, dB	DAC	32.67	49.63	**36.38**	36.16	1.96
	PDCTC	30.00	49.95	**36.92**	36.57	3.00

Table 3. Compression ratios for DAC and PDCTC

Metric	Algorithm	Min	Max	Mean	Median	Std. dev
CR(BMP)	DAC	1.25	206.75	**10.92**	8.71	8.14
	PDCTC	1.20	70.92	**8.20**	7.41	3.59
CR(JPEG)	DAC	0.14	19.38	**1.92**	1.86	0.68
	PDCTC	0.10	11.96	**1.58**	1.65	0.45

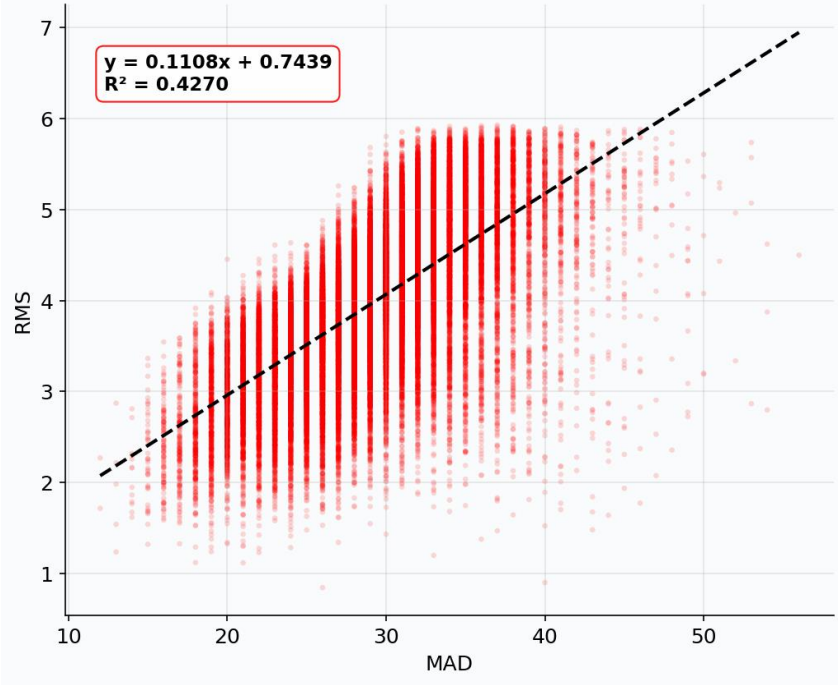


Fig. 1. MAD vs RMS correlation: the algorithm DAC

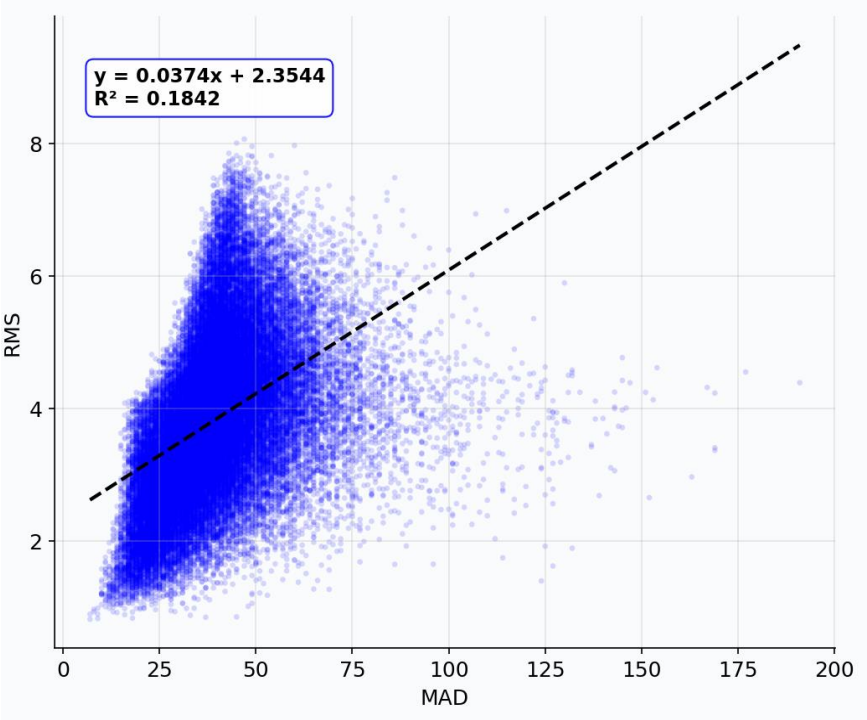


Fig. 2. MAD vs RMS correlation: the algorithm PDCTC

It follows that, on average, PSNR exceeds 35 dB for both algorithms. This means that loss of quality is invisible to a human eye.

Next, DAC outperforms PDCTC in five out of six key metrics. DAC achieves a 27.2% lower mean MAD (29.04 vs. 39.89), which indicates fewer visible artifacts in worst-case pixels.

The compression ratio relative to JPEG is 21.8% higher for DAC (1.92 vs. 1.58), resulting in a total compressed size of 3.50 GB compared to 4.04 GB for PDCTC - a 13.5% storage saving.

Moreover, the coefficient of determination between MAD and RMS is substantially higher for DAC (R^2 = 0.427 vs. 0.184), which means that distortion behavior is more predictable and controllable. PDCTC shows a marginal advantage in mean PSNR (36.92 vs. 36.38 dB); however, it has a notably higher variance (std. dev = 3.00 vs. 1.96 dB), making this advantage inconsistent across the dataset.

Thus, the DAC algorithm demonstrates superior compression efficiency, lower peak distortion, and more predictable quality control compared to the DCT-based PDCTC on a large-scale image dataset.

This makes DAC a more promising tool for visually lossless compression of JPEG images than PDCTC.

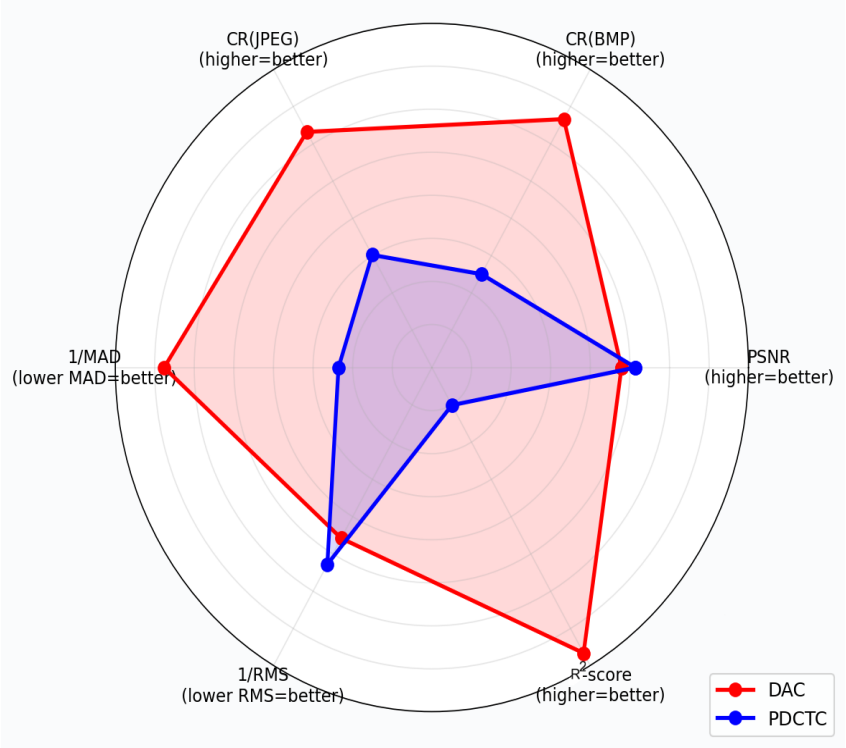


Fig. 3. Overall algorithm profiles

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. Lukin V., Brysina I., Makarichev V. Discrete Atomic Compression of Digital Images: A Way to Reduce Memory Expenses. In: Nechyporuk M., Pavlikov V., Kritskiy D. (eds) *Integrated Computer Technologies in Mechanical Engineering. Advances in Intelligent Systems and Computing*. 2020. Vol. 1113. Springer, Cham, P. 492-502. DOI: https://doi.org/10.1007/978-3-030-37618-5_42.

4. Makarichev V., Lukin V., Brysina I. Progressive DCT-based coder and its comparison to atomic function based image lossy compression. *Proceedings of the 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications, and Computer Engineering (TCSET).* 2022. Lviv-Slavske, Ukraine, February 22 - 26, 2022. P. 75-80. DOI: https://doi.org/10.1109/TCSET55632.2022.9766871.

5. Russakovsky O., Deng J., Su H. et al. ImageNet Large Scale Visual Recognition Challenge. *International Journal of Computer Vision*. 2015. Vol. 115. P. 211–252. DOI: https://doi.org/10.1007/s11263-015-0816-y.

APPLICATION OF FEATURE MAPS OF DIFFERENT SPATIAL RESOLUTION TO IMRPOVE ACCURACY IN VIDEO OBJECT DETECTION SYSTEM

Sadovnykov B.I.
National Aerospace University «Kharkiv Aviation Institute»

One of the biggest object detection challenges is detection of small objects. There is no single valid strategy to resolve this issue. It might be adaptation [1] of the detection algorithm to input data, so it expects all possible object sizes, genetic algorithms usage to perform this calibration or different convolutional neural networks modifications. Example of such an architecture is a Feature Pyramid Networks (FPN) [2]. The main idea is that a deep CNN already produces a natural hierarchy of feature maps: early layers have high spatial resolution but weak semantic meaning, while deeper layers have stronger semantic information but much lower resolution.

High-level deep features, which are passed though many convolutions provide more accurate data about exact object on the image, but lacks details like edges, corners and exact location of this object on the image.

Meanwhile features from earlier layers has much higher resolution i.e. passed less convolution and downsampling steps, so it preserves more spatial details like edges, corners, fine structure and the exact position on the picture.

But it has weaker semantic meaning, so it might not accurate define the object on the image.

Feature Pyramid Network upsamples and merged deep features with features from earlier, higher-resolution layers. As a result, each level of the pyramid gains stronger semantic content while preserving fine spatial detail. This produces feature maps at several scales that can all be used for detection, instead of relying only on the deepest layer. In object detection, this improves robustness to scale variation and is especially helpful for small objects, which often disappear or become poorly represented in very coarse feature maps.

The primary issue with FPN is that it consumes extra computation resources and memory on top-down pathway to perform upscaling operations. Plus, the feature-fusion algorithm itself is inefficient from both performance and accuracy perspective.

YOLOv3 [3] model applied concept proposed by a Feature Pyramid Networks, but in more efficient way: model can use limited amount of detection scales at predefined resolutions. It simplifies feature fusion process and reduce reduces computation cost.

So YOLOv3 model first extracts features using Darknet-53. Then it predicts on the deepest feature map, which has the lowest spatial resolution and the strongest semantic abstraction.

After that, it upsamples features and combines them with earlier, higher-resolution backbone features, then makes another prediction. This process is repeated once more to produce the third detection scale.

As a result, there are 3 prediction maps with different resolutions: deep one with large receptive field, providing strong semantic and good for large objects recognition, map in between the surface and deep layers, which is compromise between semantic richness and spatial details, working the best with medium size objects and the surface level layer with the most precise spatial details, good for small objects.

YOLO models utilizes division of the original image feature map on cells to detect the object and its position, so small object can appear only on a small portion of a cell or loose important details during convolutions, what prevents them from detection. With denser grids provided by the surface level map, small object detection becomes more reliable.

A similar optimization can also be applied to custom detection methods, especially in systems that must operate under scale variation or detect small objects in complex scenes.

Incorporating multi-scale prediction or pyramid-based feature fusion allows such models to use both semantically rich deep features and higher-resolution spatial information, which can improve localization quality and robustness without requiring a complete redesign of the detector. For this reason, the idea is valuable not only for standard YOLO-like architectures, but also for specialized domain-specific detectors in areas such as surveillance, industrial inspection, medical imaging, and autonomous systems.

In conclusion, multi-scale feature extraction has become one of the key ideas in modern object detection, since real-world images usually contain objects of very different sizes.

The use of pyramid-based representations makes it possible to combine high-level semantic information with finer spatial detail, which significantly improves the detector's ability to localize both large and small objects.

In this context, Feature Pyramid Networks and related approaches provide an effective foundation for building robust detection systems.

References

1. Sadovnykov, B., & Lysechko, V. Adaptive behavior tuning of a neural network-based method for moving object recognition in video streams// Computer-integrated technologies: education, science, production/ Lutsk National Technical University. – Lutsk. – 2025. (№60), P.P. 53-62, https://doi.org/10.36910/6775-2524-0560-2025-60-05.

2. Lin T., Dollár P., Girshick R. Feature Pyramid Networks for Object Detection, Online: ArXiv 1612.03144v2, DOI: https://doi.org/10.48550/arXiv.1612.03144

3. Redmon J., Farhadi A. YOLOv3: An Incremental Improvement. Online: ArXiv 1804.02767v1. Available from: https://arxiv.org/pdf/1804.02767.

4. Sadovnykov B.I., Lysechko V.P., Komar O.M., Zhuchenko O.S. A research of the latest approaches to visual image recognition and classification. 2024, National University «Zaporizhzhia Polytechnic». Radio Electronics, Computer Science, Control, 1(68), P. 140-147 DOI 10.15588/1607-3274-2024-1-13 (Web Of Science – 2024).

APPLICATION OF NEURAL NETWORKS TO THE PROBLEMS OF RADON EMISSIONS AND PREDICTING EARTHQUAKES

Bayramov A.A.
Republican Seismic Survey Center, Baku, Azerbaijan

Studying the emission of radioactive radon ^{222}Rn from the Earth's interior is important not only for environmental issues but also for earthquake prediction [1-5]. This problem is extremely complex and remains unanswered. This is because dozens of different external factors must be considered when solving these problems, and the answer is often ambiguous. Various mathematical methods are used in these problems. One promising approach is Artificial Intelligence [6], particularly neural networks (NNs). Correlation analysis of two data sets using NNs is used when the relationship between variables is nonlinear, complex, or dependent on multiple factors. Unlike classical correlation (for example, Pearson's coefficient), neural networks can detect hidden and nonlinear relationships. Let's assume we have two data sets: $X = \{x_1, x_2, \ldots, x_n\}$ and $Y = \{y_1, y_2, \ldots, y_n\}$. For example:

- (X) are seismic parameters (b-value, energy, event rate)
- (Y) are geochemical data (radon concentration, CO_2, etc.)

It is required to determine the presence and nature of the relationship between X and Y. The neural network is trained to predict Y from X. If the network predicts well: $Y = f(X)$, then there is a strong correlation between the sets. The measure of correlation becomes the prediction error: $MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2$ or the coefficient of determination: $R^2 = 1 - \sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \Big/ \sum_{i=1}^{n}(y_i - \bar{y}_i)^2$.

The purpose of the report is to use the Neural Network method to study the correlation between radon emissions and seismic processes on the territory of the Azerbaijan Republic.

References

1. Hashimov, E. G. Detection unobserved moving armored vehicles by seismic method // - Baku: National Security and Military Sciences. – 2015. – T. 1. – №. 1. – C. 128-132.

2. Bayramov A. Seismic location station for detection of unobserved moving military machineries //Journal of Management and Information Science. 2016. T.4. №. 2. 61-66.

3.Kartashov O.S. et al.Hybrid acoustic seismic approach for the identification of moving targets. *In* Problems of informatization. Proceedings of Thirteenth International Scientific and Technical Conference. Vol. 2., section 3,7. - Baku – Kharkiv – Bielsko-Biala: november 27 – 28**,** -2025, -p.p.118-119

4.Hashimov E. G., Bayramov A. A. Application of GIS and seismic location method for detection of invisible military objects. Monograph //Baku: Military publishing house. – 2017.

5. Hashimov E. G., Bayramov A. A., Khalilov B. M. Operative detection of ground enemy objects //Herbi Bilik,(1). – 2015. – C. 33-47.

6. Bayramov A. et al. AI-Based Complex for Measurement and Control Using the Machine Learning Method. Journal of Electrical Engineering. vol.10 (12). 2025. p. 116-128.

The work was carried out under a grant from AEF-BQM-BRFTF-4-2024-5(53).

ВИМОГИ ДО ВВЕДЕНОЇ ІНФОРМАЦІЙНОЇ НАДМІРНОСТІ В КРИПТОГРАФІЧНІ СИСТЕМИ

Рудницький В.М., Лада Н.В.,
Колесник С.М., Рудницький С.В.
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна

Дослідження та розробка методів і алгоритмів підвищення надійності, стійкості, достовірності та відповідно і захищеності інформаційних процесів шифрування - актуальна науково-технічна проблема. Одним із шляхів вирішення даної проблеми може бути введення інформаційної надмірності на основі застосування надмірних кодів та надмірних систем числення.

Придатність для практичного використання системи числення визначається низкою факторів: можливістю представлення будь-якого числа в заданому діапазоні; однозначністю представлення; простотою та компактністю запису чисел; легкістю освоєння системи, простотою та зручністю оперування нею.

За умови підвищених вимог до надійності, відмовостійкості та швидкості роботи обираються системи числення з активною інформаційною надмірністю, при цьому враховується наступне:

надмірність системи числення повинна забезпечувати прості алгоритми виконання арифметичних і логічних операцій та низьку складність пристроїв, що їх реалізують;

однозначність подання інформації забезпечує максимальні можливості контролю системи числення;

простота пристроїв збору, контролю, корекції та обробки інформації;

неоднозначність представлення повинна забезпечити виключення перенесень між групами розрядів коду;

простота прямого та зворотного перекладу між системами числення, у разі необхідності спільного використання систем числення.

Введена інформаційна надмірність має забезпечити:

можливість виконання арифметичних операцій будь-якого ступеня складності з точки зору реалізації; виконання логічних операцій та їх логічний взаємозв’язок із традиційними логічними операціями булевої алгебри;

високу швидкість виконання арифметико-логічних операцій за рахунок зменшення кількості перенесень між групами розрядів та низької складності пристроїв; простоту синтезу кодових комбінацій, а також пряме та зворотне перетворення безнадлишкового коду в надлишковий;

простоту алгоритмів виявлення та корекції помилок при низькій складності пристроїв їх реалізації, високій швидкості контролю та корекції;

умови для зменшення ймовірності виникнення помилок за рахунок підвищення захищеності від перешкод.

МУЛЬТИВАРІАНТНЕ ПРЕДСТАВЛЕННЯ СЕТ-ОПЕРАЦІЙ НА ОСНОВІ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ ОПЕРАЦІЙ, КЕРОВАНИХ ІНФОРМАЦІЄЮ

Підласий Д.А.
Черкаський державний технологічний університет, Черкаси, Україна

Використання моделей СЕТ-операцій побудованих на основі елементарних функцій операцій керованих інформацією дозволяє будувати мало ресурсні системи потокового шифрування з подвійним управлінням процесом криптографічного перетворення [1]. Проте моделювання даних СЕТ-операцій має свої особливості.

Метою доповіді є дослідження особливостей моделювання СЕТ-операцій побудованих на основі елементарних функцій операцій керованих інформацією та розробка рекомендацій по мінімізації складності пристроїв криптографічного перетворення. Основна особливість елементарних функцій операцій керованих інформацією полягає в можливості представлення їх трьома варіантами дискретно-казуальних моделей:

$$f_{43} = (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) = (x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3) = (x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3);$$

$$f_{77} = (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) = (x_1 \vee x_3)(x_2)(x_1 \cdot x_3) = (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2).$$

Виходячи з цього дискретно-казуальна модель СЕТ-операції, яка поєднує в собі три різні елементарні функції може бути представлена за допомогою 27 дискретно-казуальних моделей:

$$C(x) = \begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (x_2 \vee x_3)(x_1)(x_2 \cdot x_3) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \end{bmatrix} = \begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (x_2 \vee x_3)(x_1)(x_2 \cdot x_3) \\ (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \end{bmatrix} = \begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (x_2 \vee x_3)(x_1)(x_2 \cdot x_3) \\ (x_1 \cdot x_2)(x_3)(x_1 \vee x_2) \end{bmatrix} = \ldots\ldots.$$

Будо досліджено два підходи до вибору дискретно-казуальних моделей СЕТ-операцій. Перший підхід полягає в побудові моделей СЕТ-операцій на основі елементарних функцій побудованих на основі однієї і тієї ж керуючої функції. Другий підхід полягає в побудові моделей СЕТ-операцій на основі елементарних функцій порядковий номер керуючої функції якої співпадає з порядковим номером самої елементарної функції в операції. Обидва підходи забезпечують побудову моделей однакової складності. Проте перший підхід дозволяє спростити правила побудови моделей багатоопераднних СЕТ-операцій. Другий підхід дозволяє інтегрувати правила побудови базових груп СЕТ-операцій на основі елементарних функцій операцій керованих інформацією в загальну концепцію побудови базових груп СЕТ-операцій. Тому на практиці доцільно використовувати другий підхід.

Список літератури

1. Архітектура СЕТ-операцій і технології потокового шифрування. Architecture of CET-operations and stream encryption technologies: монографія / В. М. Рудницький, Н. В. Лада, Г. А. Кучук, Д. А. Підласий. – Черкаси: видавець Пономаренко Р.В., 2024. – 374 с. https://dndivsovt.com/index.php/monograph/issue/view/22/22

СУЧАСНІ ТЕХНОЛОГІЇ В УДАРНИХ БЕЗЕКІПАЖНИХ НАЗЕМНИХ КОМПЛЕКСАХ ПІДТРИМКИ ПІХОТИ

Головняк Д.В., Заїка В.М., Мокринський О.В.
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна

В збройних конфліктах велика роль відводиться наземним операціям, у зв'язку з цим питання створення, модернізацій та розвитку ударних безекіпажних наземних комплексів (БеНК) є актуальним. Ніша ударних БеНК продовжує швидко заповнюватись, використовуючи досвід активних бойових дій. Наявність безекіпажних комплексів, які мають достатнє озброєння для подавлення та ураження вогневих засобів противника, значно підвищить ефективність бойової спроможності піхотинця на полі бою та скоротить втрати живої сили підрозділів. Особливість ударних БеНК полягає у тому, що на наземний апарат встановлюється бойовий модуль (турель) з сучасним озброєнням, який, з високою інтенсивністю здатен вражати як живу силу, так і легкоброньовані об'єкти та техніку в умовах вогневого контакту з противником. В якості озброєння використовують стрілецьку зброю, автоматичні гранатомети та вогнемети. Прицільними пристроями служать блоки з денними, тепловізійними та інфрачервоними камерами, які дозволяють оператору використовувати ударні БеНК у денний та нічний час доби, в переважній більшості не залежно від погодних умов. Для визначення відстані до цілей, можуть використовуватись лазерні далекоміри або балістичні сітки. Важливу роль в створенні зразків ударних БеНК грає прохідність.

Використання різних типів зв'язку дозволяє застосовувати БеНК в умовах впливу засобів радіоелектронної боротьби. Існує практика постійної модернізації БеНК. Встановлення стабілізуючих пристроїв дозволить якісно використовувати БеНК не тільки при стрільбі з місця та коротких зупинок але і при стрільбі в динаміці, що значно підвищить ефективність його використання. Наявність "backtracking" – слідування у зворотному напрямку, дозволяє в разі втрати зв'язку з БеНК, повертатись за попереднім маршрутом, до точки відновлення зв'язку. Система штучного інтелекту дозволяє блокам прицілювання виявляти та супроводжувати цілі передаючи сигнал відкриття вогню.

Налаштування автоматичного режиму ведення вогню, виконує БеНК самостійно. Важливим фактом являється те, що модулі (турелі) можуть бути замінені на інші без виконання додаткових робіт по його кріпленню (уніфікація). Аналіз застосування ударних БеНК показав, що найбільш перспективним тактичним прийомом є вогнева засідка, а підрозділи продовжують здобувати досвід і розробляти ефективну тактику ведення бойових дій.

СУКУПНИЙ МЕТОД ВИМІРЮВАННЯ ФАЗОВОГО ЗСУВУ З ВИКОРИСТАННЯМ ФУНКЦІЇ ОТРИМАНОЇ ДВОХ ГАРМОНІЙНИХ СИГНАЛІВ, ПІСЛЯ ПРОВЕДЕННЯ ЇХ ДВОНАПІВПЕРІОДНОГО ПЕРЕТВОРЕННЯ ТА ПІДСУМУВАННЯ

Тишко С.О., Макаренко Р.Г., Трофименко С.І.
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна

Запропонований спосіб визначення фазового зсуву двох гармонічних сигналів, в основі якого лежить сукупний метод визначення з використанням сигналу отриманого шляхом підсумування двох гармонічних сигналів після проведення їх двохнапівперіодного перетворення.

Під час синтезу запропонованого способу вимірювання проведено вирішення часткової задачі визначення множини миттєвих значень вектору досліджуваного сигналу, що знаходяться на часовому інтервалі першого та другого напівсигналів.

Проведена ліанілізація функцій, що описують сигнал отриманий шляхом підсумування двох гармонічних сигналів після проведення їх двохнапівперіодного перетворення та проведено вирішення надвизначених систем рівнянь методом найменших квадратів.

Синтезовані аналітичні співвідношення з використанням яких можливо провести визначення фазового зсуву.

Застосування цього методу порівняно з відомими методами, в основі яких лежить аналого-цифрове амплітудно-часове перетворення дозволяє:

- зменшити складову похибки, обумовлену фазовою асиметрією каналів передачі сигналу, за рахунок зменшення їх довжини;
- суттєво знизити вимоги до якості виконання операції автоматичного регулювання рівня вхідних сигналів;
- синтезувати один канал аналого-цифрового перетворення сигналу, що аналізується, замість двох, що, в свою чергу, робить непотрібною синхронізацію аналого-цифрового перетворення для кожного каналу обробки сигналів.

Використання запропонованого принципу визначення фазового зсуву значно зменшить складність вимірювальних систем за рахунок спрощення схемотехнічних рішень, а це у свою чергу, дасть можливість заощадити матеріальні ресурси для контролю технічних характеристик безпілотних систем спеціального призначення та їх складових (близько 10%) під час випробувань на етапах розробки та виготовлення зразка без зниження якості контролю.

HDL-МОДЕЛЮВАННЯ ТА ОЦІНКА ПРОДУКТИВНОСТІ СПЕЦІАЛІЗОВАНИХ ОБЧИСЛЮВАЧІВ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

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

Сучасні вимоги до швидкодії спеціалізованих комп'ютерних засобів обробки інформації (СКЗОІ) обумовлюють пошук нових архітектурних рішень.

Система залишкових класів (СЗК) завдяки паралелізму на рівні залишків є перспективною для побудови обчислювачів [1, 2].

Проте ефективне впровадження систем залишкових класів у реальні пристрої потребує переходу до методів моделювання на основі MBSE для забезпечення цілісності архітектури [3] та використання сучасних засобів апаратного опису (HDL) [4].

Метою доповіді є підвищення швидкодії та ефективності функціонування СКЗОІ шляхом розробки та впровадження HDL-моделей, що реалізують обчислювальні процеси у системі залишкових класів на основі методу порозрядної табличної реалізації арифметичних операцій, що дозволяє забезпечити паралелізм на апаратному рівні та отримати об'єктивні кількісні показники продуктивності розроблених засобів.

У роботі дістала подальший розвиток HDL-модель спеціалізованого комп'ютерного засобу, яка базується на методі порозрядної табличної реалізації.

Використання унітарного коду результату дозволяє мінімізувати логічну глибину схем, що критично важливо при реалізації на FPGA [5].

Розроблена модель, на відміну від існуючих, має додаткову можливість опису функціонування СКЗОІ безпосередньо у системі залишкових класів, що дозволяє:

1. Описати архітектуру обчислювальних модулів на мовах Verilog/VHDL з урахуванням специфіки модулярної арифметики.

2. Провести функціональне моделювання та верифікацію коректності обчислень для великих наборів модулів.

3. Кількісно оцінити продуктивність, а саме визначити максимальну тактову частоту, часові затримки та витрати апаратних ресурсів (кількість логічних вентилів або LUT-секцій FPGA).

Проведене синтезування та часовий аналіз моделі показали, що таблична реалізація дозволяє підвищити швидкість виконання базових операцій у системі залишкових класів на 15–20% порівняно з класичними архітектурами за рахунок усунення ланцюгів поширення переносу та розпаралелювання на рівні бітових груп.

Запропонований підхід до HDL-моделювання дозволяє не лише автоматизувати процес проектування СКЗОІ у системb залишкових класів, а й

отримати точні кількісні характеристики, які підтверджують ефективність непозиційних систем числення для високопродуктивної обробки даних у реальному часі.

Список літератури

1. Янко А. С., Глушко А. Д., Крук О. І., Прокудін А. Ю. Підвищення ефективності процесу корекції даних у системі залишкових класів. *Системи управління, навігації та зв'язку*. 2024. № 4 (78). С. 169–175. DOI: https://doi.org/10.26906/SUNZ.2024.4.169

2. Янко А. С., Торбенко О. С. Табличний метод підвищення продуктивності комп'ютерних систем обробки цілочисельних даних на основі непозиційних кодових структур. *Таврійський науковий вісник. Серія: Технічні науки*. 2022. № 5. С. 21–26. DOI: https://doi.org/10.32851/tnv-tech.2022.5.3

3. Dambietz F. M., Rennpferdt C., Hanna M., Krause D. Using MBSE for the Enhancement of Consistency and Continuity in Modular Product-Service-System Architectures. *Systems*. 2021. Vol. 9, No. 3. 63. DOI: https://doi.org/10.3390/systems9030063

4. Purraji M., Zamiri E., de Castro A. Easy and Straightforward FPGA Implementation of Model Predictive Control Using HDL Coder. *Electronics*. 2025. Vol. 14, No. 3. 419. DOI: https://doi.org/10.3390/electronics14030419

5. Bassoli M., Bianchi V., De Munari I. A Model-Based Design Floating-Point Accumulator. Case of Study: FPGA Implementation of a Support Vector Machine Kernel Function. *Sensors*. 2020. Vol. 20, No. 5. 1362. DOI: https://doi.org/10.3390/s20051362

ОПТИМІЗАЦІЯ ПРОЦЕСІВ ДІАГНОСТУВАННЯ ДАНИХ У КОМП'ЮТЕРНИХ ЗАСОБАХ КОМУТАЦІЙНИХ ВУЗЛІВ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

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

Сучасні комутаційно-комунікаційні вузли (ККВ) телекомунікаційних систем вимагають безперервного підвищення показників надійності та швидкодії обробки інформації.

Використання непозиційних систем числення, зокрема класу лишків (КЛ), відкриває нові можливості для побудови відмовостійких архітектур завдяки властивостям паралелізму та контролепридатності кодових структур [1, 2].

Проте ефективна реалізація засобів виявлення та корекції помилок потребує вдосконалення алгоритмів контролю для мінімізації часових затримок [3].

Метою доповіді є підвищення оперативності та достовірності діагностування даних у комп'ютерних засобах обробки інформації ККВ шляхом розробки методів контролю, що базуються на ефективному використанні внутрішніх властивостей класу лишків.

Основна частина. У ході дослідження було удосконалено метод діагностики в класі лишків, заснований на визначенні частинних ортогональних базисів.

На відміну від традиційних підходів, запропоноване рішення базується на поєднанні у часі процесів аналізу проекцій діагностованого числа. Це дозволяє проводити перевірку коректності даних паралельно з основними обчислювальними циклами [4].

Застосування частинних ортогональних базисів у поєднанні з оптимізованими алгоритмами аналізу проекцій забезпечує суттєве скорочення часових витрат на виявлення помилок у кодових структурах класу лишків. Це досягається завдяки можливості паралельного обчислення контрольних ознак для кожної проекції числа окремо, що мінімізує загальну затримку в системі діагностування.

Такий підхід дозволяє досягти підвищення глибини діагностування пристроїв комутаційного вузла без суттєвого нарощування апаратних витрат [5].

Оскільки аналіз базується на внутрішніх властивостях системи залишкових класів, реалізація контрольних модулів потребує меншої кількості додаткових логічних елементів порівняно з класичними методами дублювання або введення значної кодової надмірності

Удосконалений метод діагностики створює теоретичне підґрунтя для реалізації стратегій оптимального резервування комп’ютерних засобів комутаційно-комунікаційнb[вузлsd, забезпечуючи заданий рівень безвідмовності телекомунікаційних мереж.

Список літератури

1. Yanko A. S., Krasnobayev V. A., Nikolsky S. B., Kruk O. O. Method for determining the bit grid overflow of a computer system operating in the system of residual classes. *Radio Electronics, Computer Science, Control*. 2024. № 1. С. 228–241. DOI: https://doi.org/10.15588/1607-3274-2024-1-21

2. Янко А. С., Крук О. О., Гончаренко С. О. Теоретичне обґрунтування математичної моделі безвідмовності системи обробки інформації автоматизованих робототехнічних платформ у системі залишкових класів. *Системи управління, навігації та зв’язку*. 2025. Т. 1, № 79. С. 72–76. DOI: https://doi.org/10.26906/SUNZ.2025.1.72-76

3. Boyko Y., Pyatin I. Features of code redundancy formation in information transmission channels. *Інфокомунікаційні та комп’ютерні технології*. 2022. Т. 2, № 04. С. 12–25. DOI: https://doi.org/10.36994/2788-5518-2022-02-04-01

4. Xiao H., Garg H. K., Hu J., Xiao G. New Error Control Algorithms for Residue Number System Codes. *ETRI Journal*. 2016. Vol. 38, No. 2. С. 326–336. DOI: https://doi.org/10.4218/etrij.16.0115.0575

5. Ananda Mohan P. V. Error Detection, Correction and Fault Tolerance in RNS-Based Designs. *Residue Number Systems*. 2016. С. 163–175. DOI: https://doi.org/10.1007/978-3-319-41385-3_7

ЗАСОБИ ПЛАТФОРМИ .NET ДЛЯ РЕАЛІЗАЦІЇ МІКРОСЕРВІСІВ У СИСТЕМАХ ОРКЕСТРАЦІЇ КОНТЕЙНЕРІВ

Слукін Д.І., Федорченко В.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасний розвиток програмних систем характеризується переходом до мікросервісної архітектури, яка забезпечує гнучкість, масштабованість і незалежність розгортання окремих компонентів. Використання контейнеризації та систем оркестрації контейнерів дозволяє ефективно управляти життєвим циклом мікросервісів, забезпечуючи автоматичне масштабування, балансування навантаження та стійкість до відмов. У цьому контексті особливого значення набувають засоби платформи .NET, які надають широкий набір інструментів для розробки, розгортання та супроводу мікросервісних додатків. Однак складність інтеграції різних компонентів системи, а також необхідність забезпечення ефективної взаємодії між сервісами зумовлюють актуальність дослідження можливостей платформи відносно реалізації мікросервісів у середовищах оркестрації контейнерів [1, 2].

Сучасні підходи до побудови мікросервісних систем передбачають використання контейнерних технологій, зокрема Docker, а також платформ оркестрації, таких як Kubernetes, які забезпечують автоматизацію процесів розгортання, масштабування та управління контейнерами [3]. Платформа .NET підтримує розробку мікросервісів із використанням ASP.NET Core, що дозволяє створювати високопродуктивні вебсервіси та API. Крім того, важливу роль відіграють інструменти для організації взаємодії між сервісами, такі як брокери повідомлень і механізми API Gateway, що забезпечують узгоджену роботу розподілених компонентів. Інтеграція .NET із сучасними інструментами оркестрації дозволяє створювати масштабовані та надійні системи, здатні працювати в умовах високих навантажень.

Метою доповіді є дослідження засобів платформи .NET для реалізації мікросервісів у системах оркестрації контейнерів, а також оцінка їх ефективності при побудові розподілених систем. У межах дослідження розглядаються основні компоненти мікросервісної архітектури, включаючи сервіси, механізми їх взаємодії, системи моніторингу та управління конфігураціями. Запропонований підхід передбачає використання контейнеризації для ізоляції сервісів, а також застосування платформ оркестрації для автоматизації процесів їх розгортання та масштабування. Особлива увага приділяється питанням забезпечення стійкості до відмов, балансування навантаження та безперервної доставки оновлень.

У доповіді наведено результати експериментального дослідження, виконаного на основі розробленого прототипу мікросервісної системи, реалізованої із використанням платформи .NET та системи оркестрації Kubernetes. Проведений аналіз показує, що використання сучасних інструментів контейнеризації та оркестрації дозволяє значно підвищити ефективність управління мікросервісами, скоротити час розгортання та

забезпечити гнучке масштабування системи. Встановлено, що продуктивність і надійність системи залежать від конфігурації кластеру, способу організації взаємодії між сервісами та використання механізмів кешування і балансування навантаження. Крім того, показано, що застосування засобів моніторингу та логування дозволяє оперативно виявляти проблеми та підвищувати якість функціонування системи. Отримані результати можуть бути використані при розробці сучасних корпоративних інформаційних систем, орієнтованих на використання мікросервісної архітектури та технологій контейнеризації.

Список літератури

1. Joao Paulo Karol Santos Nunes, Shiva Nejati, Mehrdad Sabetzadeh, and Elisa Yumi Nakagawa. Self-adaptive, Require-ments-driven Autoscaling of Microservices. In Proceedings of the 19th International Symposium on Software Engineer-ing for Adaptive and Self-Managing Systems (SEAMS '24). Association for Computing Machinery, New York, NY, USA, 2024. P. 168–174. https://doi.org/10.1145/3643915.3644094.
2. Nishal Gurung, Sushil Shrestha, Rajani Chulyadyo. Scalability in Microservices: A systematic literature review. Journal of Computer Science and Technology, 25(2), e.11, 2025. https://doi.org/10.24215/16666038.25.e11.
3. Sai Vaibhav Medavarapu, Sachin Samrat Medavarapu. Enhancing Scalability and Performance of .NET Microservices on Azure Kubernetes Service (AKS).Journal of Scientific and Engineering Research, 10(6), 2023, P. 133-139. https://doi.org/10.5281/zenodo.13597405.

МОДЕЛЬ ІНТЕГРАЦІЇ BIG DATA ДЛЯ СЕРВІСНИХ ТЕХНОЛОГІЙ АВТОМОБІЛЬНОЇ ГАЛУЗІ

Скляров І.І.
Харківський національний автомобільно-дорожній університет,
Харків, Україна

Інтенсивний розвиток цифрових технологій в автомобільній галузі, зокрема впровадження концепцій підключених транспортних засобів, телематики та інтелектуальних транспортних систем, зумовлює стрімке зростання обсягів даних, що генеруються різноманітними джерелами. До таких джерел належать бортові сенсори автомобілів, системи діагностики, мобільні застосунки користувачів, а також зовнішні інформаційні сервіси. Обробка таких даних потребує використання сучасних підходів Big Data, які дозволяють забезпечити їх ефективний збір, зберігання та аналіз у режимі, наближеному до реального часу. Водночас складність інтеграції різнорідних джерел даних і забезпечення їх узгодженості створює додаткові умови для побудови сервісних технологій в автомобільній галузі [1].

Сучасні сервіси в автомобільній сфері орієнтовані на підвищення безпеки, комфорту та ефективності експлуатації транспортних засобів. До них належать системи обслуговування за технічним станом з прогнозуванням, управління автопарками, навігаційні сервіси та системи аналізу поведінки

водія [2]. Реалізація таких сервісів потребує інтеграції великих обсягів даних із різних джерел, що характеризуються різною структурою, швидкістю надходження та рівнем достовірності. У цьому контексті особливого значення набувають моделі інтеграції Big Data, які забезпечують об'єднання даних у єдине інформаційне середовище з можливістю їх подальшої обробки та аналізу. Використання сучасних технологій потокової обробки даних і розподілених обчислень дозволяє забезпечити високу продуктивність і масштабованість таких систем [3].

Метою доповіді є розробка моделі інтеграції Big Data для сервісних технологій автомобільної галузі, яка забезпечує ефективне об'єднання, обробку та аналіз даних із різнорідних джерел. Запропонована модель базується на використанні багаторівневої архітектури, що включає рівні збору даних, їх попередньої обробки, зберігання та аналітики. У межах моделі передбачено використання механізмів потокової обробки для роботи з даними в реальному часі, а також застосування алгоритмів машинного навчання для виявлення закономірностей і прогнозування стану транспортних засобів. Особлива увага приділяється забезпеченню узгодженості даних і мінімізації затримок при їх обробці.

У доповіді наведено результати експериментального дослідження, спрямованого на оцінку ефективності запропонованої моделі в умовах надходження потоків даних. Отримані результати свідчать, що використання інтегрованих підходів до обробки Big Data дозволяє підвищити точність аналітики та ефективність сервісів у автомобільній галузі. Встановлено, що ключовими факторами, які впливають на ефективність моделі, є швидкість надходження даних, їх якість, а також обрана архітектура системи. Крім того, показано, що використання адаптивних алгоритмів обробки даних дозволяє підвищити стійкість системи до змін умов експлуатації та забезпечити більш точне прогнозування технічного стану транспортних засобів. Запропонована модель може бути використана при створенні інтелектуальних сервісів для автомобільної галузі, орієнтованих на підвищення безпеки, ефективності та якості обслуговування.

Список літератури

1. M. Jain, D. Vasdev, K. Pal, V. Sharma. Systematic literature review on predictive maintenance of vehicles and diagno-sis of vehicle's health using machine learning techniques. Computational Intelligence, 38. 2022. p. 1990–2008. https://doi.org/10.1111/coin.12553.

2. Andreas Theissler, Judith Pérez-Velázquez, Marcel Kettelgerdes, Gordon Elger. Predictive maintenance enabled by ma-chine learning: Use cases and challenges in the automotive industry. Reliability Engineering & System Safety. Volume 215. 2021. 23 p. https://doi.org/10.1016/j.ress.2021.107864.

3. Danilo Giordano, Flavio Giobergia, Eliana Pastor, Antonio La Macchia, Tania Cerquitelli, Elena Baralis, Marco Mellia, Davide Tricarico. Data-driven strategies for predictive maintenance: Lesson learned from an automotive use case. Com-puters in Industry.Volume 134.2022. https://doi.org/10.1016/j.compind.2021.103554.

МЕТОД ВИЯВЛЕННЯ МЕРЕЖНИХ АНОМАЛІЙ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

Свистельник А.О., Сорокін А.Р.
Харківський національний університет радіоелектроніки, Харків, Україна

Зростання складності сучасних комп'ютерних мереж, збільшення обсягів мережного трафіка та поширення кіберзагроз зумовлюють необхідність розробки ефективних методів виявлення мережних аномалій. Традиційні підходи до аналізу мережевого трафіка, що базуються на сигнатурних методах або фіксованих правилах, часто не здатні своєчасно виявляти нові або невідомі типи атак, а також складні аномальні шаблони поведінки. Крім того, висока динамічність мережних процесів, наявність великої кількості параметрів і шумів у даних ускладнюють використання класичних статистичних методів. У зв'язку з цим актуальною є задача розробки методів виявлення мережних аномалій із використанням машинного навчання, які дозволяють автоматично аналізувати великі обсяги даних і виявляти приховані закономірності [1, 2].

Сучасні підходи до виявлення аномалій базуються на використанні різних моделей машинного навчання, включаючи методи класифікації, кластеризації та аналізу часових рядів. Зокрема, значного поширення набули алгоритми глибокого навчання, такі як автоенкодери [3], рекурентні нейронні мережі та згорткові архітектури, які здатні ефективно виявляти складні нелінійні залежності у мережному трафіку.

Водночас важливу роль відіграють методи попередньої обробки даних, включаючи відбір ознак, нормалізацію та усунення шумів, що дозволяє підвищити точність і стабільність моделей. Крім того, інтеграція моделей машинного навчання з системами моніторингу мережі забезпечує можливість виявлення аномалій у реальному часі [4, 5].

Метою доповіді є розробка методу виявлення мережних аномалій із використанням машинного навчання, який забезпечує підвищення точності виявлення підозрілих подій і зниження кількості хибних спрацьовувань. Запропонований метод передбачає багаторівневу обробку даних, що включає збір параметрів мережі, їх попередню обробку та аналіз із використанням адаптивних моделей машинного навчання. У межах методу використовується комбінація алгоритмів, що дозволяють виявляти як відомі, так і нові типи аномалій, включаючи атаки відмови в обслуговуванні, сканування мережі та інші підозрілі активності. Особлива увага приділяється адаптації моделей до змін умов функціонування мережі.

У доповіді наведено результати експериментів, виконаних на основі відкритих наборів мережних даних, які демонструють ефективність запропонованого методу. Проведений аналіз показує, що якість виявлення аномалій залежить від вибору ознак, структури моделей і характеристик мережного трафіка. Встановлено, що використання комбінованих підходів, які поєднують методи глибокого навчання та класичні алгоритми аналізу даних, дозволяє підвищити точність виявлення аномалій і зменшити кількість

помилкових спрацьовувань. Крім того, показано, що застосування адаптивних моделей сприяє підвищенню стійкості системи до змін у поведінці трафіку в мережі та появи нових типів загроз. Отримані результати можуть бути використані при створенні інтелектуальних систем кібербезпеки, орієнтованих на захист сучасних комп'ютерних мереж.

Список літератури

1. Blazquez-Gartfa, A., Conde A., Mori U., Lozano J. A review on outlier/anomaly detection in time series data, ACM Comput. Surv. Vol. 54. No. 3. 2021. DOI: http://dx.doi.org/10.1145/3444690.

2. M. Ring, S. Wunderlich, D. Scheuring, D. Landes, A. Hotho. A survey of network-based intrusion detection data sets. Elsevier. ScinceDirect. Computers & Security, vol. 86, 2019. P. 147-167. https://doi.org/10.1016/j.cose.2019.06.005.

3. Y. Mirsky, T. Doitshman, Y.Elovici, A. Shabtai. Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. Cornell University. Computer Science, 2018. 15 p. https://doi.org/10.48550/arXiv.1802.09089.

4. R.Abu-Zaid, A.Hammad. Streamlining Data Processing Efficiency in Large-Scale Applications: Proven Strategies for Optimizing Performance, Scalability, and Resource Utilization in Distributed Architectures. International Journal of Machine Intelligence. International Journal of Machine Intelligence for Smart Applications, 14(8), 2024. P. 31-49. https://dljournals.com/index.php/IJMISA/article/view/27.

5. Vaishali Bhatia; Shabnam Choudhary; K.R Ramkumar. A Comparative Study on Various Intrusion Detection Techniques Using Machine Learning and Neural Network. 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2020. https://doi.org/10.1109/ICRITO48877.2020.9198008.

МЕТОД МОНІТОРИНГУ ДАНИХ В СЕНСОРНІЙ МЕРЕЖІ З ВИКОРИСТАННЯМ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ

Міхаль О.П., Савуляк В.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Інтенсивний розвиток безпровідних сенсорних мереж [1] сприяє їх широкому застосуванню у системах екологічного моніторингу, промислової автоматизації, транспортних системах та інфраструктурі розумних міст, що обумовлює необхідність ефективного контролю стану мережі та достовірності отриманих даних. Потоки даних, що генеруються сенсорними вузлами, характеризуються високою динамічністю, наявністю шумів, пропусків і можливими аномаліями, що ускладнює їх аналіз і знижує якість прийнятих рішень. Традиційні методи моніторингу, які базуються на фіксованих порогових значеннях і простих статистичних моделях, не забезпечують необхідного рівня точності та адаптивності в умовах змінного середовища функціонування мережі. У зв'язку з цим актуалізується задача розробки методів моніторингу даних у сенсорних мережах із використанням моделей машинного навчання, здатних виявляти складні закономірності та аномалії у потоках даних [2].

Сучасні підходи до моніторингу сенсорних мереж передбачають використання інтелектуальних моделей, які враховують як часові, так і просторові залежності між вимірюваннями. Застосування методів машинного навчання, зокрема алгоритмів класифікації, кластеризації та прогнозування, дозволяє підвищити точність виявлення відхилень і зменшити кількість хибних спрацьовувань. Особливу ефективність демонструють моделі глибокого навчання, такі як рекурентні нейронні мережі та автоенкодери, які здатні виявляти приховані структури в даних і адаптуватися до зміни їх статистичних характеристик. Крім того, інтеграція таких моделей із підходами розподіленої обробки даних дозволяє реалізувати моніторинг у реальному часі без значного збільшення навантаження на мережу [3].

Метою доповіді є розробка методу моніторингу даних у сенсорній мережі з використанням моделей машинного навчання, який забезпечує підвищення точності виявлення аномалій і оцінку стану мережі за рахунок адаптивного аналізу потоків даних. Запропонований метод базується на поєднанні процедур попередньої обробки даних, включаючи фільтрацію та нормалізацію, із використанням моделей машинного навчання для аналізу часових рядів. У межах методу передбачено використання алгоритмів, здатних виявляти як короткочасні відхилення, так і довготривалі зміни у поведінці системи, що дозволяє підвищити ефективність моніторингу.

У доповіді наведено результати експериментальних досліджень, виконаних на основі даних, отриманих із сенсорних мереж, які підтверджують ефективність запропонованого методу. Проведений аналіз показує, що якість моніторингу залежить від частоти збору даних, рівня шуму, топології мережі та обчислювальних можливостей вузлів. Встановлено, що використання адаптивних моделей машинного навчання дозволяє підвищити точність виявлення аномалій та зменшити кількість помилкових спрацьовувань у порівнянні з традиційними методами. Крім того, показано, що застосування розподілених підходів до обробки даних сприяє зниженню затримок і підвищенню масштабованості системи. Отримані результати можуть бути використані при розробці інтелектуальних систем моніторингу сенсорних мереж, орієнтованих на роботу в умовах невизначеності та обмежених ресурсів.

Список літератури

1. Dalal B., Kukarni S. Wireless Sensor Networks: Applications. Wireless Sensor Networks: Design, Deployment and Applications. IntechOpen, 2021. P. 1–23. http://dx.doi.org/10.5772/intechopen.97079.

2. Ramesh S., Rajalakshmi R., Dwivedi J. N., Selvakanmani S., Pant B., Bharath Kumar N., Fissiha Demssie Z. Optimization of Leach Protocol in Wireless Sensor Network Using Machine Learning. Comput Intell Neurosci, 2022. P.1–8. https://doi.org/10.1155/2022/5393251.

3. Saad H.M., Shdefat A., Nawaz A., El-Sherbeeny A.M., El-Meligy M.A., Rana M.R.R. Enhancing energy balance in wireless sensor networks through optimized minimum spanning tree. PeerJ Computer Science, 2024. doi: 10.7717/peerj-cs.2269

МЕТОД ОБРОБКИ ДАНИХ З ВИКОРИСТАННЯМ ІНСТРУМЕНТІВ МАШИННОГО НАВЧАННЯ

Міхаль О.П., Журнєв Д.Д.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням обсягів даних, що генеруються різноманітними інформаційними системами, сенсорними пристроями та цифровими сервісами, що зумовлює необхідність розробки ефективних методів їх обробки та аналізу [1]. Традиційні підходи до обробки даних, засновані на детермінованих алгоритмах і статистичних моделях, часто виявляються недостатньо ефективними при роботі з великими, великорозмірними та слабо структурованими наборами даних. Особливої складності набуває задача виявлення прихованих закономірностей, прогнозування та класифікації в умовах невизначеності, шумів і пропусків у даних. У зв'язку з цим актуальною є проблема розробки методів обробки даних із використанням інструментів машинного навчання, які здатні автоматично адаптуватися до властивостей даних і забезпечувати високу точність аналізу [2, 3]. Сучасні інструменти машинного навчання охоплюють широкий спектр методів, включаючи алгоритми класифікації, регресії, кластеризації та зниження розмірності, що дозволяє ефективно вирішувати різноманітні задачі обробки даних. Зокрема, застосування ансамблевих методів і глибоких нейронних мереж забезпечує можливість моделювання складних нелінійних залежностей між ознаками та підвищення здатності моделей стосовно узагальнення. Водночас важливим аспектом є попередня обробка даних, яка включає очищення, нормалізацію, відбір ознак та усунення надлишковості, що суттєво впливає на якість подальшого аналізу. Інтеграція таких процедур із сучасними бібліотеками та програмними платформами машинного навчання дозволяє створювати гнучкі та масштабовані системи обробки даних [4].

Метою доповіді є розробка методу обробки даних із використанням інструментів машинного навчання, який забезпечує підвищення точності аналізу та ефективності обробки за рахунок комплексного використання сучасних алгоритмів і процедур підготовки даних. Запропонований метод передбачає побудову багатоступеневої схеми обробки, що включає етапи попереднього очищення даних, трансформації ознак, навчання моделей і оцінку їх якості. Особливу увагу приділено автоматизації вибору моделей і налаштування їх параметрів із використанням методів оптимізації, що дозволяє зменшити вплив суб'єктивних факторів на результати аналізу.

У доповіді наведено результати експериментальних досліджень, виконаних на різних наборах даних [5, 6], які демонструють ефективність запропонованого методу у задачах класифікації та прогнозування. Проведений аналіз показує, що якість обробки даних значною мірою залежить від вибору інструментів машинного навчання, структури даних, а також від способів їх попередньої підготовки. Встановлено, що використання комплексних

підходів, які поєднують декілька алгоритмів і процедур обробки, дозволяє підвищити точність і стійкість результатів. Крім того, показано, що автоматизація процесів обробки даних сприяє підвищенню продуктивності систем і зменшенню витрат часу на їх розробку та налаштування. Отримані результати можуть бути використані при створенні інтелектуальних систем аналізу даних, орієнтованих на роботу з великими обсягами інформації в умовах невизначеності та змінного середовища.

Список літератури

1. Feng M., Deng L.-J., Chen F. Signal and Information Processing in Networks. Entropy, 2023. Vol. 25(12):1643. P. 1–5. https://doi.org/10.3390/e25121643.

2. Mao R., Zhang M., Wang Y., Li H., Xu J., Dong X., Zhang Y., Chen Z.X. An integrated framework for accelerating reactive flow simulation using GPU and machine learning models. Proceedings of the Combustion Institute, 2024. Vol. 40. https://doi.org/10.1016/j.proci.2024.105512.

3. Jawahar S., Kukunuri G.P., Devaraju S., Anandaram H., Gokuldev S., Jayaprakash S., Thenmozhi M. An Exploration of Python Libraries in Machine Learning Models for Data Science. Advanced Interdisciplinary Applications of Machine Learning Python Libraries for Data Science, 2023. P. 1–31. DOI: 10.4018/978-1-6684-8696-2.ch001.

4. Li X., Wu W., Guo H., Wu Y., Li S., Wang W., Lu Y. Smart Grain Storage Solution: Integrated Deep Learning Framework for Grain Storage Monitoring and Risk Alert. Foods, 2025; Vol. 14(6):1024. P. 1–24. https://doi.org/10.3390/foods14061024.

5. Kaggle. Intel Berkeley Research Lab Sensor Data. Data Collected from 54 sensors installed in the lab. URL: https://www.kaggle.com/datasets/divyansh22/intel-berkeley-research-lab-sensor-data.

6. Kaggle. Wireless Sensor Network Dataset. Optimized sensor node data for energy-efficient and adaptive signal detection. URL: https://www.kaggle.com/datasets/ziya07/wireless-sensor-network-dataset?resource=download.

МЕТОДИ ІНТЕЛЕКТУАЛЬНОЇ ОБРОБКИ ДАНИХ З ВИКОРИСТАННЯМ САМООРГАНІЗОВАНИХ КАРТ

Мальнєв Д.М., Сорокін А.Р.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні інформаційні системи характеризуються стрімким зростанням обсягів даних, що мають складну структуру, високу розмірність і неоднорідність, що ускладнює їх ефективний аналіз і виявлення прихованих закономірностей. Традиційні методи обробки даних часто не забезпечують необхідної якості результатів при роботі з такими даними, особливо в умовах відсутності попередньої розмітки та наявності шумів. У зв’язку з цим актуальною є задача розробки методів інтелектуальної обробки даних, які базуються на використанні нейронних мереж і здатні виконувати самонавчання без учителя. Одним із перспективних підходів у цьому напрямі є використання самоорганізованих карт, які дозволяють здійснювати проєкцію багатовимірних даних у простір меншої розмірності зі збереженням

топологічних властивостей [1, 2]. Самоорганізовані карти є ефективним інструментом для задач кластеризації, візуалізації та аналізу структури даних, оскільки дозволяють виявляти приховані групи та закономірності без необхідності попереднього визначення кількості кластерів. Вони базуються на принципі конкурентного навчання, у процесі якого нейрони мережі адаптують свої вагові коефіцієнти відповідно до вхідних даних, формуючи топологію впорядкованого представлення простору ознак. Сучасні дослідження демонструють ефективність поєднання самоорганізованих карт із іншими методами машинного навчання, зокрема алгоритмами кластеризації та зниження розмірності, що дозволяє підвищити точність аналізу та покращити візуальне представлення результатів [3].

Метою доповіді є аналіз існуючих та розробка методу інтелектуальної обробки даних із використанням самоорганізованих карт, які забезпечують ефективне виявлення структури даних і підвищення якості кластеризації в умовах високої розмірності та наявності шумів. Запропонований підхід передбачає використання самоорганізованих карт для попередньої обробки та візуалізації даних із подальшим застосуванням методів кластеризації для уточнення структури отриманих груп. Особлива увага приділяється адаптації параметрів навчання мережі, зокрема радіуса сусідства та швидкості навчання, що дозволяє підвищити стабільність і точність результатів.

У доповіді наведено результати експериментальних досліджень, виконаних на тестових наборах даних, які демонструють ефективність запропонованих методів у задачах кластеризації та візуалізації. Проведений аналіз показує, що використання самоорганізованих карт дозволяє суттєво покращити якість групування даних і зменшити вплив шумів та аномалій. Встановлено, що результати обробки значною мірою залежать від вибору параметрів мережі, структури вхідних даних і способу їх попередньої нормалізації. Крім того, показано, що інтеграція самоорганізованих карт із іншими методами машинного навчання дозволяє підвищити точність і стійкість результатів, а також забезпечити більш глибоке розуміння структури даних. Отримані результати можуть бути використані при створенні інтелектуальних систем аналізу даних, орієнтованих на роботу з великими та складними наборами інформації.

Список літератури

1. Alkawaz A.N., Kanesan J., Badruddin I.A., Kamangar S., Hussien M., Ali Baig M.A., Ahammad N.A. Adaptive Self-Organizing Map Using Optimal Control. Mathematics, 2023. Vol. 11(9):1995. P. 1–20. https://doi.org/10.3390/math11091995.

2. Fan X., Zhang S., Xue X., Jiang R., Fan S., Kou H. An Improved Self-Organizing Map (SOM) Based on Virtual Winning Neurons. Symmetry. 2025. Vol. 17(3):449. P. 1–22. https://doi.org/10.3390/sym17030449.

3. Nayak P., Trivedi V., Gupta S., Booba P.B., Soloveva O.V, Rozhdestvenskiy O.V., Joshi A. Artificial neural network-based clustering in Wireless sensor Networks to balance energy consumption. Cogent Engineering, 2024. P. 1–12. https://doi.org/10.1080/23311916.2024.2384652.

МЕТОД ОБРОБКИ ДАНИХ ДЛЯ ПІДВИЩЕННЯ ЕНЕРГОЗБЕРЕЖЕННЯ БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖ

Дяченко Д.О., Хомутов Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток безпровідних сенсорних мереж зумовлює широке їх застосування у задачах екологічного моніторингу, розумних міст, промислової автоматизації та системах контролю стану довкілля, що супроводжується необхідністю ефективного використання енергетичних ресурсів вузлів мережі [1]. Оскільки сенсорні вузли зазвичай мають обмежені джерела живлення та працюють у автономному режимі протягом тривалого часу, проблема енергозбереження стає ключовим фактором забезпечення надійності та довговічності функціонування таких систем. Значна частина енергії витрачається на передачу та обробку даних, що актуалізує необхідність розробки методів оптимізації обробки інформації безпосередньо в мережі. У зв'язку з цим особливої уваги набувають підходи, спрямовані на зменшення обсягів передаваних даних, оптимізацію протоколів маршрутизації та використання інтелектуальних алгоритмів агрегації інформації [2]. Сучасні дослідження [3, 4] показують, що ефективність енергоспоживання безпровідних сенсорних мереж значною мірою залежить від організації процесів збору, обробки та передачі даних. Використання методів локальної обробки, агрегації та стиснення даних дозволяє суттєво зменшити навантаження на канал зв'язку, що є найбільш енерговитратною операцією. Крім того, застосування адаптивних алгоритмів, які враховують зміну умов функціонування мережі, таких як щільність вузлів, рівень заряду батарей та інтенсивність трафіка, дозволяє підвищити ефективність використання ресурсів. У цьому контексті перспективним є поєднання класичних методів обробки сигналів із підходами машинного навчання, що дає змогу динамічно оптимізувати параметри функціонування мережі та зменшувати надлишковість переданих даних [5].

Метою доповіді є розробка методу обробки даних для підвищення енергозбереження безпровідних сенсорних мереж, який базується на використанні адаптивної агрегації даних та інтелектуального відбору інформації для передачі. Запропонований метод передбачає виконання попередньої обробки даних на рівні сенсорних вузлів із використанням алгоритмів фільтрації та виявлення значущих змін у параметрах, які спостерігаються. Передача даних здійснюється лише у випадку виявлення суттєвих відхилень або за умов перевищення заданих порогових значень, що дозволяє зменшити кількість повідомлень, що передаються, і, відповідно, знизити енергоспоживання. Додатково у методі враховується можливість кластеризації вузлів мережі з метою організації ефективної маршрутизації та зменшення дублювання інформації.

У доповіді наведено результати моделювання та експериментальних досліджень, які демонструють ефективність запропонованого підходу у порівнянні з традиційними методами передачі даних. Отримані результати

свідчать, що застосування адаптивної обробки та агрегації даних дозволяє суттєво зменшити обсяг трафіка в мережі та продовжити час автономної роботи сенсорних вузлів. Встановлено, що на ефективність методу впливають такі фактори як топологія мережі, частота збору даних, рівень шуму у вимірюваннях та стратегія вибору вузлів-агрегаторів. Крім того, показано, що використання інтелектуальних алгоритмів прийняття рішень дозволяє досягти компромісу між точністю відтворення даних і рівнем енергоспоживання, що є критично важливим для практичного застосування безпровідних сенсорних мереж. Запропонований метод може бути використаний при розробці енергоефективних систем моніторингу та управління, орієнтованих на тривалу автономну роботу в умовах обмежених ресурсів.

Список літератури

1. Harmash V., Diachenko V., Mikhal O., Znaidiuk V. Energy-Saving Method In Wireless Sensor Networks. Control, Navigation and Communication Systems. Vol. 2 (80), 2025. P. 54–58. DOI:10.26906/SUNZ.2025.2.054.
2. Shwetha G.R., Dr. Murthy S.V.N. Wireless Sensor Networks: A Critical Review of the State of the Art Solutions for Localization, Aggregation, Routing and Attacks. Neuroquantology, 2022. Vol. 20. P. 513 -5157. DOI: 10.14704/NQ.2022.20.15.NQ88517.
3. Дяченко В.О., Міхаль О.П. Перспективність застосування вдосконаленого класичного алгоритму карт Кохонена у розподілених енергокритичних сенсорних мережах. Системи управління, навігації та зв'язку. Збірник наукових праць. Т. 4 (74), 2023. С. 75–79. https://doi.org/10.26906/SUNZ.2023.4.075.
4. Zakizadeh M., Zand M., Goundar S. Energy Efficiency and Power Management in Wireless Sensor Networks: A Comprehensive Analysis, 2025. P. 1–45. DOI:10.13140/RG.2.2.29891.31526.
5. Jeong J.-H., Jo H., Zhou Q., Nishat T.A.H., Wu L. Active management of battery degradation in wireless sensor network using deep reinforcement learning for group battery replacement. Computer Science. Machine Learning, 2025. P. 1–13. https://doi.org/10.48550/arXiv.2503.15865.

МЕТОД КЛАСТЕРИЗАЦІЇ ДАНИХ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

Дяченко Д.О., Олефіренко Я.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Зростання обсягів даних у сучасних інформаційних системах зумовлює необхідність розробки ефективних методів їх аналізу та структурування, серед яких особливе місце займають методи кластеризації [1]. Кластеризація дозволяє виявляти приховані закономірності у даних без попередньо заданих міток класів, що робить її важливим інструментом у задачах аналізу великих даних, обробки сигналів, маркетингових досліджень та систем підтримки прийняття рішень. Водночас складність і різноманіття сучасних наборів даних, а також наявність шумів і аномалій суттєво обмежують ефективність класичних алгоритмів кластеризації, таких як k-середніх або ієрархічні

методи. У зв'язку з цим актуальною є проблема розробки нових підходів до кластеризації, що базуються на використанні методів машинного навчання [2] та здатні адаптуватися до складної структури даних [3].

Особливістю сучасних підходів до кластеризації є використання моделей, які здатні враховувати нелінійні залежності між ознаками та працювати з просторами великої розмірності. Зокрема, застосування методів глибокого навчання, таких як автоенкодери, дозволяє здійснювати ефективне зниження розмірності даних із збереженням їх суттєвих характеристик, що покращує якість подальшої кластеризації. Крім того, значного поширення набули щільнісні методи, зокрема DBSCAN, які дозволяють виявляти кластери довільної форми та автоматично ідентифікувати шуми. Інтеграція таких підходів із алгоритмами оптимізації та адаптивного налаштування параметрів відкриває нові можливості для підвищення точності кластеризації.

Метою доповіді є розробка методу кластеризації даних із використанням машинного навчання, який забезпечує підвищення точності групування об'єктів у складних багатовимірних просторах за рахунок поєднання процедур зниження розмірності та адаптивної кластеризації. Запропонований метод передбачає попередню обробку даних із використанням нейронних мереж для виділення інформативних ознак, після чого виконується кластеризація у зменшеному просторі ознак із застосуванням алгоритмів, стійких до шумів. Особлива увага приділяється автоматичному визначенню кількості кластерів і налаштуванню параметрів алгоритму, що дозволяє зменшити залежність результатів від початкових умов. У доповіді наведено результати експериментальних досліджень, виконаних на стандартних тестових наборах даних, які демонструють переваги запропонованого методу порівняно з класичними підходами. Проведений аналіз показує, що якість кластеризації суттєво залежить від вибору метрики відстані, способу нормалізації даних, а також від наявності шумів і аномальних значень. Встановлено, що використання комбінованих підходів, які поєднують методи машинного навчання та класичні алгоритми кластеризації, дозволяє досягти більш високої точності та стабільності результатів. Отримані результати можуть бути використані при розробці інтелектуальних систем аналізу даних, орієнтованих на роботу з великими та складними наборами інформації.

Список літератури

1. V. Diachenko, O. Mikhal. Perspectives of application of the advanced classical algorithm of Kohonen maps in distributed energy-critical sensor networks. Control, Navigation and Communication Systems, vol. 4, 2023. P.75-79. https://doi.org/10.26906/SUNZ.2023.4.075.

2. 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/CBO9780511973000.

3. I. Surenther, K.P. Sridhar, Michaelraj Kingston Roberts. Maximizing energy efficiency in wireless sensor networks for data transmission: A Deep Learning-Based Grouping Model approach, 2023. P. 53-65. https://doi.org/10.1016/j.aej.2023.10.016.

МЕТОДИ РЕАЛІЗАЦІЇ ВІРТУАЛІЗОВАНИХ РОЗПОДІЛЕНИХ ОБЧИСЛЮВАЛЬНИХ СЕРЕДОВИЩ

Дяченко В.О., Чижов О.Б.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток сучасних інформаційних технологій, зокрема хмарних обчислень, великих даних та сервіс-орієнтованих архітектур, зумовлює необхідність створення ефективних віртуалізованих розподілених обчислювальних середовищ (ВРОС), здатних забезпечити гнучке використання обчислювальних ресурсів і масштабованість сервісів.

Традиційні підходи до організації обчислювальної інфраструктури, що базуються на використанні фізичних серверів із фіксованими характеристиками, не дозволяють ефективно реагувати на зміну навантаження та потреб користувачів.

У зв'язку з цим віртуалізація ресурсів, яка передбачає абстрагування фізичної інфраструктури та створення віртуальних машин і контейнерів, стає ключовим інструментом побудови сучасних розподілених систем. Це дозволяє підвищити ефективність використання апаратних ресурсів, знизити витрати на обслуговування інфраструктури та забезпечити гнучкість управління обчислювальними процесами [1, 2].

Віртуалізовані розподілені обчислювальні середовищ характеризуються складною багаторівневою архітектурою, яка включає рівні фізичної інфраструктури, віртуалізації, управління ресурсами та прикладних сервісів.

Однією з ключових задач є ефективне розподілення обчислювальних ресурсів між користувачами та сервісами з урахуванням їх вимог до продуктивності, затримок і надійності. У цьому контексті широко застосовуються методи планування задач, балансування навантаження та динамічного масштабування ресурсів.

Особливу роль відіграють технології контейнеризації та оркестрації, які забезпечують швидке розгортання та управління додатками у розподіленому середовищі.

Використання таких підходів дозволяє підвищити ефективність використання ресурсів і забезпечити високу доступність сервісів [3, 4].

Важливим аспектом функціонування ВРОС є забезпечення їх надійності та стійкості до відмов.

У розподілених системах відмови окремих вузлів є неминучими, тому необхідно використовувати механізми реплікації даних, резервування ресурсів і автоматичного відновлення сервісів.

Крім того, значну увагу приділяють питанням безпеки, зокрема ізоляції віртуальних середовищ, контролю доступу та захисту даних під час передачі та зберігання.

У цьому контексті застосовуються сучасні підходи до забезпечення безпеки хмарних середовищ і платформ з контейнеризацією, а також методи виявлення аномалій у розподілених системах [5, 6].

Метою доповіді є дослідження та розробка методів реалізації ВРОС, які забезпечують ефективне використання ресурсів, масштабованість і надійність функціонування систем. Запропонований підхід базується на використанні комбінованих механізмів віртуалізації, що поєднують можливості віртуальних машин і контейнерів, а також адаптивних алгоритмів управління ресурсами. У межах методу передбачено використання систем моніторингу стану інфраструктури та прогнозування навантаження, що дозволяє динамічно змінювати конфігурацію середовища відповідно до поточних умов функціонування.

У доповіді наведено результати експериментальних досліджень, спрямованих на оцінку ефективності запропонованих методів у різних сценаріях навантаження. Отримані результати свідчать, що застосування віртуалізації у поєднанні з адаптивними методами управління ресурсами дозволяє суттєво підвищити продуктивність систем, зменшити час відгуку сервісів і забезпечити більш рівномірне використання обчислювальних ресурсів. Встановлено, що ефективність функціонування середовища залежить від характеристик робочих навантажень, топології мережі та обраних стратегій розподілу ресурсів. Крім того, показано, що використання механізмів автоматичного масштабування та балансування навантаження дозволяє забезпечити стабільну роботу системи навіть у умовах значних коливань інтенсивності запитів. Запропоновані методи можуть бути використані при побудові сучасних хмарних платформ і корпоративних розподілених систем, орієнтованих на обробку великих обсягів даних і забезпечення високої доступності сервісів.

Список літератури

1. Qi Zhang, Lu Cheng, Raouf Boutaba.Cloud computing: state-of-the-art and research challenges. J Internet Serv Appl, 2010. P. 7–18. DOI 10.1007/s13174-010-0007-6.

2. B. Varghese, R. Buyya. Next generation cloud computing: New trends and research directions. Future.Generation Computing Systems, 79(3), 2017. P. 849-861. https://doi.org/10.1016/j.future.2017.09.020.

3. C. Pahl, A. Brogi, J. Soldani and P. Jamshidi, "Cloud Container Technologies: A State-of-the-Art Review," in *IEEE Transactions on Cloud Computing*, vol. 7, no. 3, pp. 677-692, 1 July-Sept. 2019, doi: 10.1109/TCC.2017.2702586.

4. Brendan Burns, Joe Beda, Kelsey Hightower. Kubernetes: Up and Running. Dive into the Future of Infrastructure. O'Reilly Media, 2019. 257 p. https://eddiejackson.net/azure/Kubernetes_book.pdf .

5. Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo and J. Zhang, "Edge Intelligence: Paving the Last Mile of Artificial Intelligence With Edge Computing," in *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1738-1762, Aug. 2019, doi: 10.1109/JPROC.2019.2918951.

6. Shankarwar, M.U., Pawar, A.V. (2015). Security and Privacy in Cloud Computing: A Survey. In: Satapathy, S., Biswal, B., Udgata, S., Mandal, J. (eds) Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014. Advances in Intelligent Systems and Computing, vol 328. Springer, Cham. https://doi.org/10.1007/978-3-319-12012-6_1.

МЕТОД ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ГОРИЗОНТАЛЬНОГО МАСШТАБУВАННЯ В СИСТЕМІ ОРКЕСТРАЦІЇ

Дяченко В.О., Кондрацький Г.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Зростання навантаження на сучасні інформаційні системи, зокрема вебсервіси та мікросервісні архітектури, зумовлює необхідність забезпечення ефективного масштабування обчислювальних ресурсів [1]. Горизонтальне масштабування, яке передбачає збільшення кількості екземплярів сервісів, є одним із ключових механізмів забезпечення продуктивності та стійкості до відмов розподілених систем [2]. У середовищах контейнерної оркестрації, таких як Kubernetes [3], цей процес автоматизується за допомогою спеціалізованих механізмів керування ресурсами. Проте існуючі підходи до горизонтального масштабування часто базуються на обмеженій кількості метрик, що може призводити до неефективного використання ресурсів і затримок у реакції на зміну навантаження. У зв'язку з цим актуальною є задача розробки методів підвищення ефективності горизонтального масштабування в системах оркестрації.

Сучасні підходи до масштабування передбачають використання автоматичних механізмів, таких як механізм HPA [4], які здійснюють зміну кількості екземплярів сервісів на основі показників завантаження процесора або пам'яті. Водночас такі метрики не завжди адекватно відображають реальний стан системи, особливо в умовах нерівномірного навантаження або складної взаємодії між мікросервісами. У цьому контексті перспективним є використання додаткових показників, зокрема затримок обробки запитів, кількості активних сесій та характеристик мережевого трафіка. Крім того, застосування методів машинного навчання дозволяє прогнозувати зміну навантаження та здійснювати проактивне масштабування, що підвищує ефективність використання ресурсів і зменшує час відгуку системи [5].

Метою доповіді є розробка методу підвищення ефективності горизонтального масштабування в системі оркестрації, який забезпечує адаптивне управління ресурсами на основі комплексного аналізу стану системи. Запропонований метод передбачає інтеграцію декількох джерел метрик, включаючи системні, мережеві та прикладні показники, а також використання алгоритмів прогнозування для оцінювання майбутнього навантаження. У межах методу реалізується механізм прийняття рішень щодо масштабування, який враховує як поточний стан системи, так і очікувані зміни, що дозволяє уникнути як надлишкового, так і недостатнього виділення ресурсів.

У доповіді наведено результати досліджень, проведених у середовищі контейнерної оркестрації з використанням тестових навантажень, які імітують роботу реальних інформаційних систем. Отримані результати свідчать, що застосування запропонованого методу дозволяє зменшити час реакції системи

на зміну навантаження, підвищити стабільність її роботи та оптимізувати використання обчислювальних ресурсів. Встановлено, що ефективність масштабування залежить від точності прогнозування, вибору метрик і параметрів алгоритму управління. Крім того, показано, що використання комбінованих підходів, які поєднують реактивні та проактивні механізми масштабування, забезпечує найкращі результати у динамічних середовищах. Запропонований метод може бути використаний при розробці систем з високим навантаженням, орієнтованих на забезпечення якості обслуговування та ефективного використання ресурсів.

Список літератури

1. Jawaddi SNA, Johari MH, Ismail A. A review of microservices autoscaling with formal verification perspective. Softw Pract Exper. Vol. 52, is.11, 2022. P. 2476–2495. https://doi.org/10.1002/spe.3135.

2. Pintye, I., Kovács, J. & Lovas, R. Enhancing Machine Learning-Based Autoscaling for Cloud Resource Orchestration. J Grid Computing 22, 68 (2024). https://doi.org/10.1007/s10723-024-09783-1.

3. S.N. Agos Jawaddi, A. Ismail, M.S. Sulaiman et al. Analyzing Energy-Efficient and Kubernetes-Based Autoscaling of Microservices Using Probabilistic Model Checking. J Grid Computing 23, 3, 2025. https://doi.org/10.1007/s10723-024-09789-9.

4. Dang-Quang N-M, Yoo M. Deep Learning-Based Autoscaling Using Bidirectional Long Short-Term Memory for Kubernetes. *Applied Sciences*. 2021; 11(9):3835. https://doi.org/10.3390/app11093835.

5. Javid Taheri, Arvid Gördén, and Auday Al-Dulaimy. Using Machine Learning to Predict the Exact Resource Usage of Microservice Chains. In Proceedings of the 16th IEEE/ACM International Conference on Utility and Cloud Computing (UCC '23). New York, USA, Article 25, 2024. P. 1–9. https://doi.org/10.1145/3603166.3632166.

МЕТОД МОНІТОРИНГУ ДАНИХ У КОРПОРАТИВНІЙ КОМП'ЮТЕРНІЙ МЕРЕЖІ

Дяченко В.О., Коломійченко О.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні корпоративні комп’ютерні мережі характеризуються високою складністю, розподіленою обробкою даних та інтенсивним обміном даними між великою кількістю користувачів і сервісів, що зумовлює необхідність ефективного моніторингу їх стану та функціонування. Зростання обсягів мережевого трафіка, використання хмарних сервісів і впровадження віртуалізованих ресурсів обчислювальної техніки ускладнюють процеси контролю та аналізу мережевих подій. Традиційні методи моніторингу, що базуються на статичних правилах і порогових значеннях, часто не забезпечують достатнього рівня адаптивності та не дозволяють своєчасно виявляти складні аномалії та загрози безпеці [1, 2]. У зв’язку з цим актуальною є проблема розробки методів моніторингу даних у корпоративних мережах, які забезпечують високу точність аналізу та оперативність реагування на зміни стану мережі.

Особливістю сучасних корпоративних мереж є наявність великої кількості різнорідних джерел даних, включаючи журнали подій, мережеві пакети, показники продуктивності серверів і мережевого обладнання. Ефективний моніторинг таких систем потребує інтеграції даних із різних джерел та їх комплексного аналізу. У цьому контексті перспективним є використання методів машинного навчання [3], які дозволяють автоматично виявляти аномальні шаблони поведінки та прогнозувати можливі відмови або перевантаження мережі. Застосування алгоритмів аналізу часових рядів, кластеризації та класифікації дозволяє підвищити точність виявлення відхилень та зменшити кількість хибних спрацьовувань.

Метою доповіді є розробка методу моніторингу даних у корпоративній комп'ютерній мережі, який забезпечує підвищення ефективності виявлення аномалій та оцінювання стану мережі за рахунок використання адаптивних моделей аналізу даних. Запропонований метод передбачає збір і попередню обробку даних із різних джерел, їх нормалізацію та агрегування, після чого здійснюється аналіз із використанням моделей машинного навчання. Особливу увагу приділено виявленню аномальних подій у мережевому трафіку, які можуть свідчити про збої, перевантаження або кіберзагрози. Метод також передбачає використання механізмів самоадаптації, що дозволяють враховувати зміну умов функціонування мережі та підвищувати точність аналізу з часом.

У доповіді наведено результати експериментальних досліджень, виконаних на основі даних корпоративних мереж, які демонструють ефективність запропонованого підходу. Проведений аналіз показує, що якість моніторингу суттєво залежить від повноти та достовірності вхідних даних, а також від вибору моделей аналізу. Встановлено, що використання комбінованих підходів, які поєднують статистичні методи та алгоритми машинного навчання, дозволяє підвищити точність виявлення аномалій і зменшити час реагування на інциденти. Крім того, показано, що застосування автоматизованих систем моніторингу сприяє підвищенню надійності та безпеки корпоративних мереж, а також оптимізації використання їх ресурсів. Отримані результати можуть бути використані при розробці систем управління та захисту корпоративних інформаційних ресурсів обчислювальної техніки.

Список літератури

1. Blazquez-Gartfa, A., Conde A., Mori U., Lozano J. A review on outlier/anomaly detection in time series data, ACM Comput. Surv. Vol. 54. No. 3. 2021. DOI: http://dx.doi.org/10.1145/3444690.

2. Vaishali Bhatia; Shabnam Choudhary; K.R Ramkumar. A Comparative Study on Various Intrusion Detection Techniques Using Machine Learning and Neural Network. 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2020. https://doi.org/10.1109/ICRITO48877.2020.9198008.

3. 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/CBO9780511973000.

ACCELERATING COLOR CONVERSION METHODS IN THE CONTEXT OF INCLUSIVE GRAPHICAL USER INTERFACES

Shcholkin M., Barkovska O.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

Today, color vision deficiency (CVD) is not an isolated problem but a global challenge [1]. Approximately 8% of men and 0.4% of women suffer from various forms of color blindness, which amounts to over 300 million people worldwide. Despite technological advancements, most modern image correction software solutions rely on CPU-based computations. This has become a “bottleneck” because traditional sequential algorithms cannot keep up with processing high-definition video or live streams in real time, which significantly limits users [2].

The goal of this work is to accelerate the color conversion process for the subsequent implementation of improved methods in inclusive graphical user interfaces while preserving the clarity of interface details by adapting contrast for three forms of color blindness – protanopia, deuteranopia, and tritanopia–which is particularly critical when working with high resolutions ranging from HD to 4K.

The goal was achieved by leveraging the computational capabilities of massively parallel GPU architecture through a comparative analysis of three color conversion methods – per-pixel, matrix, and hybrid (the Machado transformation adapts the color gamut, while the CLAHE algorithm evens out the image histogram so that the image does not lose contrast or fine details after color adjustment), using the CuPy library and CUDA architecture [3]. This allowed data to be cached directly in video memory. It was shown that using CUDA reduces the processing time for a single 4K frame from over 80 seconds (when using a “pixel-by-pixel” algorithm on the CPU) to 0.23 seconds, while a hybrid approach on the GPU reduces this time even further–to 0.13 seconds. It was found that for the 4K format, the acceleration is approximately 12 times faster than the traditional matrix method on the CPU. The proposed hybrid approach is promising for inclusive systems, as it combines high performance with enhanced image information. Further avenues for developing this topic include researching the capabilities of neural networks to create personalized correction profiles for each specific user.

References

1. Alnasser S. et al. A Global Perspective of Color Vision Deficiency: Awareness, Diagnosis, and Lived Experiences. Healthcare. 2025. Vol. 13, No. 16. P. 2031. DOI: https://doi.org/10.3390/healthcare13162031.

2. Jamil, A., & Denes, G. (2024). Investigating Color-Blind User-Interface Accessibility via Simulated Interfaces. Computers, 13(2), 53. https://doi.org/10.3390/computers13020053

3. Zhou, H., Huang, W., Zhu, Z. et al. Fast image recoloring for red–green anomalous trichromacy with contrast enhancement and naturalness preservation. Vis Comput 40, 4647–4660 (2024). https://doi.org/10.1007/s00371-024-03454-8

РОЗПОДІЛЕНА БІОАКУСТИЧНА СИСТЕМА МОНІТОРИНГУ ЛІСОВИХ МАСИВІВ НА ОСНОВІ MESH-МЕРЕЖІ СЕНСОРНИХ ВУЗЛІВ

Барковська О.Ю., Соколов Я.Б.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток штучного інтелекту та технологій вбудованих обчислень відкриває нові перспективи для Інтернету речей, що дозволяє впроваджувати автономні розподілені системи у сфери управління та захисту природних об'єктів, які традиційно потребували значних людських і технологічних ресурсів [1]. Одним із таких об'єктів є лісові масиви – екосистеми, що мають для більшості країн не лише економічну, але й культурно-соціальну цінність. Охорона лісів завжди була пов'язана з необхідністю залучення великої кількості ресурсів через масштаб задачі та складність середовища. При цьому актуальність даної проблеми лише зростає на тлі погіршення екологічних умов та збільшення антропогенного тиску на природні екосистеми.

Метою доповіді є розробка архітектури та принципів побудови розподіленої біоакустичної mesh-мережі для автономного моніторингу лісових масивів з метою раннього виявлення несанкціонованого антропогенного впливу – незаконних вирубок, браконьєрства та пожеж, а також для автоматизованого екологічного спостереження в лісових масивах і на природоохоронних територіях.

Наукова значущість полягає в інтеграції методів мультимодального біоакустичного аналізу, мультисенсорного злиття даних, просторової локалізації джерел звуку та агентної взаємодії вузлів. Запропонований підхід розширює можливості автоматизованого виявлення загроз і моніторингу біорізноманіття в природних екосистемах.

У доповіді розглядаються результати біоакустичного аналізу середовища окремими вузлами mesh-мережі. Наведені дані свідчать про те, що на якість акустичного аналізу впливають фоновий шум середовища, погодні умови, характеристики апаратної частини окремих вузлів, а також внутрішні апаратні перешкоди [2]. Використання розподіленої мережі передбачає врахування цих факторів через колективний аналіз даних з множини вузлів, що дозволяє знизити вплив локальних похибок та забезпечити динамічне налаштування порогів чутливості відповідно до змінних зовнішніх умов.

Список літератури

1. Mporas I. et al. Illegal Logging Detection Based on Acoustic Surveillance of Forest // Applied Sciences. – 2020. – Vol. 10, № 20. – P. 7379. DOI: 10.3390/app10207379

2. Andreadis A., Giambene G., Zambon R. Monitoring Illegal Tree Cutting through Ultra-Low-Power Smart IoT Devices // Sensors. – 2021. – Vol. 21, № 22. – P. 7593. DOI: 10.3390/s21227593 .

РЕАЛІЗАЦІЯ ГІБРИДНОЇ СИСТЕМИ ВІЗУАЛІЗАЦІЇ З ВИКОРИСТАННЯМ АПАРАТНОГО ТРАСУВАННЯ ПРОМЕНІВ У VULKAN

Скороход М.М., Барковська О.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні системи комп'ютерної графіки дедалі частіше потребують поєднання високої швидкодії з підвищенням фізичної реалістичності зображення. Традиційні растрові методи забезпечують достатню продуктивність для інтерактивних застосувань, проте мають суттєві обмеження під час формування коректних тіней, відбиттів та інших ефектів, пов'язаних із поширенням світла. У зв'язку з цим актуальною задачею є побудова гібридної системи візуалізації, у якій переваги растеризації та апаратного трасування променів поєднуються в межах єдиного рішення на основі API Vulkan [1]. Такий підхід дозволяє використовувати стабільність растрового конвеєра для відображення основної геометрії, одночасно залучаючи потужність сучасних графічних процесорів для обчислення складних оптичних явищ.

Метою роботи є розробка та дослідження гібридної системи візуалізації, що базується на інтеграції Vulkan Ray Tracing у загальну структуру графічного рендерера. Запропонований шлях розв'язання ґрунтується на побудові дворівневої ієрархії структур прискорення: Bottom-Level Acceleration Structures (BLAS), що містять вершини та індекси геометрії об'єктів, та Top-Level Acceleration Structures (TLAS), які керують екземплярами об'єктів та їх трансформаціями у світовому просторі. Це дозволило оптимізувати процес перетину променів із геометрією та зосередити основну увагу на логіці взаємодії між растровим G-буфером та трасованими ефектами. Важливим технічним етапом стала організація Shader Binding Table (SBT), яка забезпечує коректну диспетчеризацію різних типів шейдерів: Ray Generation для генерації первинних або вторинних променів, Closest Hit для обчислення освітлення в точці зіткнення та Miss шейдерів для опрацювання променів, що не перетнули жодного об'єкта [2]. Такий підхід продемонстрував значні переваги апаратного прискорення під час обробки складної геометрії, дозволяючи динамічно керувати глибиною рекурсії променів залежно від типу матеріалу

На поточному етапі реалізовано базовий рендеринг тривимірних об'єктів, що підтверджується отриманими результатами візуалізації. Зокрема, на наведеному рисунку 1 зображено рендер класичної 3D-моделі чайника, виконаний із застосуванням апаратного трасування променів. На зображенні чітко помітна висока якість відтворення поверхонь, що досягається завдяки фізично коректному розрахунку напрямків променів, що було б значно складніше реалізувати виключно растровими методами. Отримані дані свідчать, що використання готової архітектурної основи суттєво зменшує складність впровадження Vulkan Ray Tracing та створює надійний фундамент для подальшого розширення системи.

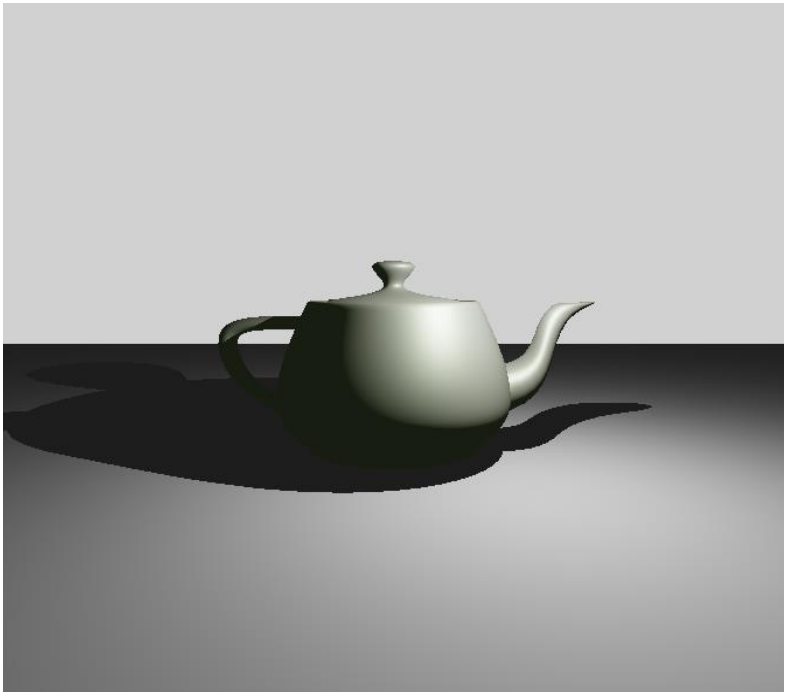


Рисунок 1 – Рендер 3д-моделі чайника
з використанням апаратного трасування променів

У результаті виконаної роботи обґрунтовано доцільність побудови гібридних систем, які дозволяють досягти компромісу між швидкістю оновлення кадрів та візуальною достовірністю. Подальші дослідження будуть спрямовані на реалізацію складніших моделей глобального освітлення та проведення порівняльного аналізу трасованих ефектів із класичними підходами, такими як Shadow Maps, за показниками обчислювальної складності. Практичне значення результатів полягає у можливості їх застосування при створенні сучасних графічних рушіїв, інженерних симуляторів та інших систем візуалізації реального часу, де критично важливим є поєднання продуктивності та високої якості графіки.

Список літератури

1. YU, Geng, et al. A survey of real-time rendering on Web3D application. *Virtual Reality & Intelligent Hardware*, 2023, 5.5: 379-394. https://doi.org/10.1016/j.vrih.2022.04.002

2. Ray Tracing Gems II: Next Generation Real-Time Rendering with DXR, Vulkan, and OptiX / ed. by Adam Marrs, Peter Shirley, and Colin Barré-Brisebois. Apress, 2021. 819 p. doi: 10.1007/978-1-4842-7185-8.

ВІРТУАЛІЗАЦІЯ GPU ДЛЯ РЕАЛІЗАЦІЇ PC-AS-A-SERVICE. ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

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

Концепція PC-as-a-Service передбачає перенесення обчислювальних ресурсів персонального комп'ютера до центру обробки даних із наданням користувачеві доступу до персоналізованого робочого середовища через тонкий клієнт, планшет або смартфон. Поширення такої моделі пов'язане зі зростанням попиту на мобільний доступ до застосунків, переходом від володіння обладнанням до підпискових сервісів, а також із розвитком хмарної інфраструктури та сервісів віддалених робочих столів. Для масового впровадження PC-as-a-Service критично важливо забезпечити не лише доступність ресурсів, а й стабільний користувацький досвід, близький до локального ПК [1].

Ключовим технічним бар'єром у цій моделі залишається віртуалізація GPU. На відміну від CPU та оперативної пам'яті, ресурси графічного процесора складніше ділити між кількома користувачами через пропрієтарні драйверні стеки, складний внутрішній стан пристрою, високу вартість перемикання контексту та наявність спільних вузьких місць, зокрема пам'яті, кешів, міжз'єднання PCIe та мультимедійних модулів [2]. Для інтерактивних сценаріїв критичними стають не лише середні показники продуктивності, а й хвости затримки, стабільність часу формування кадру, якість кодування відеопотоку та передбачуваність реакції системи на дії користувача.

Сучасні платформи реалізують кілька базових підходів до поділу GPU-ресурсів. Direct pass-through забезпечує майже нативну продуктивність, але не дозволяє ефективно обслуговувати кількох користувачів одним пристроєм.

Mediated pass-through та SR-IOV дають змогу представляти один фізичний адаптер у вигляді набору віртуальних функцій або віртуальних GPU, однак якість сервісу в такому разі залежить від політики планування й ступеня апаратної ізоляції.

У промислових рішеннях NVIDIA vGPU широко застосовується часовий поділ, що підвищує утилізацію обладнання, але може породжувати джитер і міжорендний вплив.

Просторове розбиття, зокрема NVIDIA MIG, забезпечує кращу ізоляцію обчислювальних і пам'яттєвих ресурсів, проте супроводжується жорсткою профілізацією, фрагментацією та складністю динамічного перепризначення ресурсів.

Аналогічний напрям апаратної віртуалізації підтримується AMD MxGPU на базі SR-IOV [2-4].

Отже, для систем PC-as-a-Service GPU-ресурс доцільно розглядати не як одне скалярне значення, а як сукупність взаємопов'язаних характеристик:

– обчислювальної потужності,

– обсягу та пропускної здатності пам’яті,

– доступу до PCIe,

– графічних, відеокодерних і відеодекодерних модулів.

Існуючі дослідження демонструють, що навіть за наявності часткової апаратної ізоляції проблема справедливого розподілу, гарантованого QoS та зменшення tail latency залишається відкритою [2].

Тому подальший розвиток PC-as-a-Service потребує нових механізмів керування GPU, орієнтованих не лише на максимізацію завантаження пристрою, а й на забезпечення передбачуваної якості сервісу для інтерактивних навантажень.

Метою подальшого дослідження є розробка та експериментальна перевірка підходу до розподілу ресурсів GPU у системах PC-as-a-Service, який забезпечуватиме високу сумісність із реальними програмними середовищами та мінімізуватиме погіршення якості для кінцевого користувача.

Для досягнення цієї мети доцільно:

– проаналізувати існуючі механізми віртуалізації GPU;

– визначити набір метрик якості сервісу для віддаленого персонального комп’ютера;

– дослідити вплив різних способів поділу GPU на затримки, стабільність кадру та взаємний вплив користувачів;

– запропонувати концепцію механізму планування або QoS-контракту, який враховуватиме обчислювальні, пам’яттєві та комунікаційні ресурси графічного процесора.

Практичне значення роботи полягає у створенні підґрунтя для побудови платформ віддалених робочих столів і хмарних персональних комп’ютерів із вищою щільністю розміщення користувачів без суттєвого погіршення користувацького досвіду.

Список літератури

1. R. Shea, J. Liu, E. C. . -H. Ngai and Y. Cui, "Cloud gaming: architecture and performance," in *IEEE Network*, vol. 27, no. 4, pp. 16-21, July-August 2013, doi: 10.1109/MNET.2013.6574660

2. Cheol-Ho Hong, Ivor Spence, and Dimitrios S. Nikolopoulos. 2017. GPU Virtualization and Scheduling Methods: A Comprehensive Survey. ACM Comput. Surv. 50, 3, Article 35 (May 2018), 37 pages. https://doi.org/10.1145/3068281

3. NVIDIA Virtual GPU Software User Guide. NVIDIA Documentation. URL: https://docs.nvidia.com/vgpu/latest/grid-vgpu-user-guide/ (дата звернення: 07.04.2026).

4. NVIDIA Multi-Instance GPU User Guide. NVIDIA Documentation. URL: https://docs.nvidia.com/datacenter/tesla/mig-user-guide/ (дата звернення: 07.04.2026).

ВИКОРИСТАННЯ МОДЕЛЕЙ ШІ ДЛЯ АНАЛІЗУ ЛОГУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ

Омельницький А. А., Барковська О.Ю.
Національний університет «Київський авіаційний інститут», Київ, Україна

Аналіз логування інформаційних систем є важливою складовою розробки IT-рішень, яке дозволяє віднайти несправності програмного продукту на ранніх етапах та скоротити час, витрачений на тестування представленого рішення. Актуальність роботи полягає у використанні моделей ШІ для читання журналів із записом подій та станів системи із ціллю пришвидшення обробки великих об'ємів даних та пошуку місць вразливості програмного забезпечення до атак та кіберзагроз.

Метою доповіді є дослідження ефективності використання штучного інтелекту для аналізу логування інформаційних та комп'ютерних систем. Для виконання роботи визначено показники ефективності, проведено емпіричні дослідження, зібрано та проаналізовано отримані результати.

Для рішення задачі було представлено декілька метрик ефективності аналізу логування, до яких увійшли: кількість пропущених повідомлень в журналі, витрачений об'єм часу для аналізу та кількісний показник створених багів.

Для вирішення даної проблеми було обрано Claude Sonnet 4.6, як основну модель ШІ. Числові показники ефективності аналізу логів збирались ручним шляхом, а також за допомоги залучення штучного інтелекту.

Результат дослідження показав, що за останні три оновлення системи відсоткове співвідношення кількості пропущених записів у журналі між аналізом ШІ та людиною зменшився на 73.8%, витраченого часу стало менше на 83.7%, а кількість детектованих багів після аналізу була збільшена на 104%. Отже, дослідження показало, що залучення моделей ШІ для читання та обробки повідомлень в журналі підвищує ефективність роботи, зменшує вплив людського фактору та зменшує залучений час для вирішення поставлених проблем. Наступними кроками дослідження стануть аналіз додавання гібридного формату, розширення вибірки вхідних даних для аналізу та впровадження нових метрик ефективності для валідації роботи штучного інтелекту.

Список літератури

1. Du M., Li F., Zheng G., Srikumar V. DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017. С. 1285–1298. DOI: https://doi.org/10.1145/3133956.3134015.

2. He S., Zhu J., He P., Lyu M. R. LogHub: A Large Collection of System Log Datasets for AI-driven Log Analytics. 2018 IEEE 27th International Symposium on Software Reliability Engineering (ISSRE). 2018. С. 1–5. DOI: https://doi.org/10.1109/ISSRE.2018.00010.

МЕТОД ДИНАМІЧНОЇ ПЕРЕБУДОВИ МАРШРУТУ В СИСТЕМІ АСИСТИВНОЇ ВНУТРІШНЬОЇ НАВІГАЦІЇ

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

Однією з актуальних задач при створенні інклюзивного середовища в громадських місцях є забезпечення навігації в супермаркетах для людей з порушенням зору [1]. Традиційні підходи побудови маршрутів не враховують динамічні зміни середовища, такі як наявність людей, перешкод та зміну конфігурації проходів, що знижує ефективність пересування користувачів.

Метою роботи є розробка інтелектуальної системи навігації на основі зваженого графа, яка забезпечує побудову оптимального маршруту в реальному часі з урахуванням динамічних факторів середовища.

Розглянута система складається з центрального модуля аналізу, мережі камер у магазині, та інтелектуального візка користувача, оснащеного датчиками відстані та камерами, які здійснюють збір даних про навколишнє середовище. Центральний модуль формує зважений граф простору магазину на основі отриманої інформації [2].

У даному графі вершини відповідають ключовим точкам (перехрестям), а ребра - можливим шляхам пересування. Кожному ребру призначається вага, що визначається як сума базової довжини та штрафних коефіцієнтів, які враховують додаткові фактори: щільність людей, наявність перешкод, кількість поворотів, часові умови та ширину проходів. Ваги ребер динамічно змінюються на основі даних, отриманих з камер. Для одного пункту призначення маршрут будується за алгоритмом A* з динамічною перебудовою при зміні умов середовища.

Для кількох пунктів призначення застосовується гібридний підхід, у якому визначається оптимальна послідовність відвідування точок, а маршрути між ними формуються за допомогою A* з урахуванням поточних змін. Таким чином, у роботі описано метод адаптивної маршрутизації в супермаркеті, який передбачає динамічну зміну ваг ребер графа залежно від поточних перешкод і умов пересування та автоматичну перебудову маршруту для користувача з порушенням зору у залежності від кількості пунктів призначення.

Список літератури

1. Barkovska, O., Holovchenko, O., Storchai, D., Kostin, A., & Lehezin, N. (2025). Investigation of computer vision techniques for indoor navigation systems. Innovative technologies and scientific solutions for industries, (2(32), 5–15. https://doi.org/10.30837/2522-9818.2025.2.005.

2. Wang, Z., & Fan, X. (2024, April). A systematic review and analysis of A-star pathfinding algorithms and its variations. In Fourth International Conference on Signal Processing and Machine Learning (CONF-SPML 2024) (Vol. 13077, pp. 157-182). https://doi.org/10.1117/12.3027132.

A STUDY OF THE RESOURCE EFFICIENCY OF VOICE COMMAND RECOGNITION METHODS IN PORTABLE COMPUTING SYSTEMS

Barkovska O., Romanenkov Yu., Trunov V.
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

The relevance of research on the development of inclusive voice-controlled systems for people with visual impairments, elderly users, and individuals with temporary or permanent mobility limitations is beyond doubt today [1, 2]. This research topic takes on particular importance in the context of implementing solutions on portable computing devices capable of operating in real time without relying on a powerful server infrastructure.

A practical application of the aforementioned systems could be guiding people through hospitals, shopping malls, government offices, universities, and other large facilities where speech signals are distorted by background noise, reverberation, and overlapping voices.

This leads to a decrease in the accuracy of voice command recognition related to finding a destination or clarifying a route.

Thus, there is a need to develop robust algorithms for processing and recognizing voice commands that ensure resource efficiency for implementation in modern assistive navigation systems.

The aim of this study is a comparative analysis of the resource efficiency of two proposed voice signal processing pipelines under acoustic noise conditions. The conditions of the study are as follows: a single computing device, identical conditions, and a duration of three minutes, with metrics recorded every second.

The algorithm of the first pipeline under study is shown in Fig. 1.

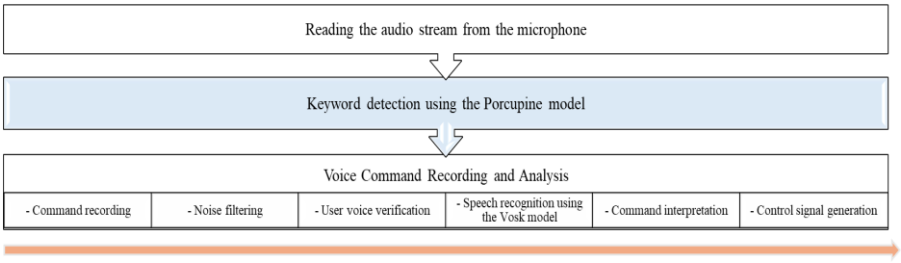


Figure 1 – Pipeline for the detection, processing, and analysis of voice commands

The combination of the Porcupine and Vosk neural network models—where a separate wakeword module continuously monitors the channel and only transfers control to the main command processing loop upon detection of a wakeword—allows the main STT model to remain in standby mode, thereby ensuring greater resource efficiency.

The second approach under investigation relies solely on the Vosk speech recognition model, which is constantly involved in both keyword detection attempts

and subsequent processing. This increases the duration and intensity of the computational load.

For the Porcupine-based approach, typical CPU utilization after the initial phase is around 10% and increases primarily only during keyword triggering and the transition to command analysis.

For the Vosk-only approach, the load is more often in the 30–50% range and periodically reaches values close to 100% (Fig. 2).

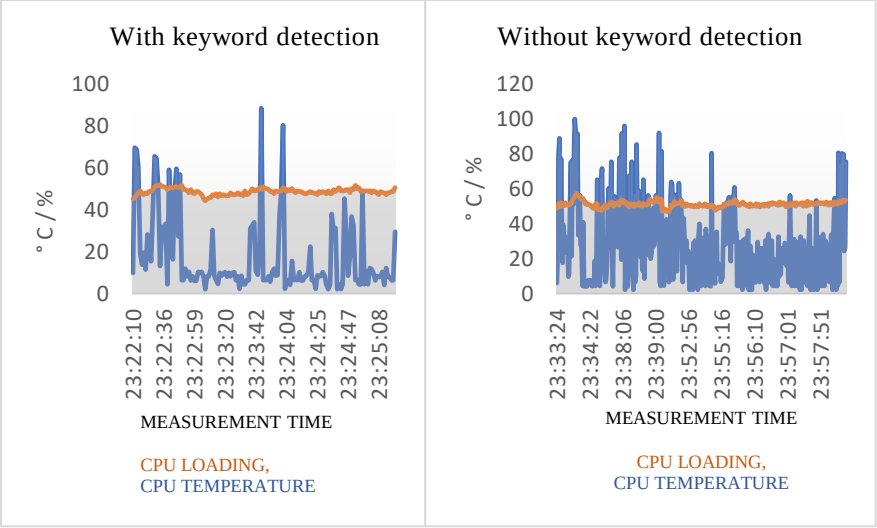


Figure 2 – Graph showing CPU temperature and load
with and without a dedicated wakeword processing module

Analysis of the results shows that extending the standard voice command processing pipeline with a separate keyword detection module based on the Porcupine model results in lower CPU load and fewer peak loads, demonstrating the higher resource efficiency of the proposed approach.

References

1. Hariharan, S., Abinaya, A., Anjuga, V., & Bhuvaneshwari, V. (2025). Voice Controlled Wheelchair for Physically Disabled People and Blind People. *Asian Journal of Applied Science and Technology (AJAST)*, *9*(1), 21-28. : https://doi.org/10.38177/ajast.2025.9103

2. Barkovska, O. and Serdechnyi, V. (2024) “Intelligent assistance system for people with visual impairments”, *INNOVATIVE TECHNOLOGIES AND SCIENTIFIC SOLUTIONS FOR INDUSTRIES*, (2(28), pp. 6–16. https://doi.org/10.30837/2522-9818.2024.28.006 .

АВТОМАТИЗОВАНЕ ВИЯВЛЕННЯ ПОШКОДЖЕНЬ СІЛЬСЬКОГОСПОДАРСЬКИХ ЗЕМЕЛЬ НА ОСНОВІ ДАНИХ SENTINEL-1 ТА АНСАМБЛЕВИХ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Світенко Г.М., Романенков Ю.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Повномасштабне вторгнення спричинило масштабні пошкодження сільськогосподарських угідь через артилерійські обстріли, рух важкої техніки та облаштування фортифікаційних споруд. Традиційні підходи до моніторингу за допомогою оптичних знімків суттєво обмежені погодними умовами, оскільки середня кількість хмарних днів в Україні становить 130-150 на рік, що знижує частку придатних для аналізу оптичних знімків на 30-40 %. Альтернативою є радарні дані місії Sentinel-1 у С-діапазоні, які забезпечують всепогодне спостереження та є високочутливими до фізичної структури поверхні (шорсткості) та структури рослинного покриву. Окрім цього більшість існуючих методів детекції змін базуються на використанні тривалих (двотижневих або місячних) часових композитів, що призводить до згладжування і втрати короткочасних сигналів локальних пошкоджень [1].

Метою доповіді є обговорення результатів отриманих в ході розробки моделі автоматизованого виявлення пошкоджень сільськогосподарських земель за допомогою радарних даних Sentinel-1 та ансамблевих методів машинного навчання, а також аналіз впливу просторової автокореляції та обсягу навчальної вибірки на точність класифікації.

У дослідженні прийнято рішення відмовитись від тривалих композитів на користь аналізу «моментальних» зрізів – порівняння вузьких 7-денних часових вікон (25-31 серпня) 2021 та 2022 років. Такий підхід забезпечив чітке розділення станів «до» та «після» та мінімізував фенологічний шум, оскільки поля порівнювалися в ідентичній фазі зрілої вегетації [2]. Для ідентифікації зон вогневого впливу використовувалась база даних конфліктних подій ACLED (категорії «Explosions/Remote violence» та «Battles»).

Функціональна модель обробки даних була реалізована в середовищі Google Earth Engine і включала три етапи: просторово-часову нормалізацію, попіксельну детекцію аномалій та генерацію табличних ознак. На відміну від традиційного усереднення сигналу по всьому полю [3], яке «розмиває» локальні пошкодження, що займають лише 2-10 % площі, використано метрику кількості аномальних пікселів, де зміна сигналу перевищувала оптимізований поріг у 4,5 дБ.

Первинні експерименти з випадковим розбиттям даних показали F1-score на рівні 87,3 %, проте виявили оптимістичне завищення через просторову автокореляцію, коли моделі машинного навчання «запам’ятовували» регіональні особливості. Для об'єктивної оцінки впроваджено стратегію просторової крос-валідації Leave-One-Region-Out (LORO) на даних з 5 областей України (925 полів).

Отримані результати підтвердили перевагу ансамблевих методів машинного навчання: Stacking досяг F1-score 0,7769, а Voting – 0,7756.

Серед одиночних класифікаторів кращими стали Random Forest (0,7667) та XGBoost (0,7626). Тест Фрідмана ($p = 0,7$) засвідчив відсутність статистично значущої різниці між топ-моделями, що доводить першочергову важливість якісної інженерії ознак порівняно з вибором архітектури.

Аналіз важливості ознак показав, що найсильнішим предиктором є «VH_anomaly_count» (кількість аномальних пікселів у перехресній поляризації, яка найбільш чутлива до руйнування об'ємної структури рослинності).

Окремо досліджено вплив обсягу вибірки.

Розширення датасету з 4 до 5 регіонів покращило середній F1-score на 0,03-0,1 для всіх моделей.

Найбільш показовим став випадок Луганської області – збільшення навчальної вибірки з 37 до 81 поля підняло F1-score з 0,47-0,55 (рівень випадкового вгадування) до 0,69-0,77. Це дозволило встановити емпіричний поріг (мінімум 40 полів на регіон) для забезпечення адекватного узагальнення моделі при застосуванні LORO.

Таким чином, запропонований підхід продемонстрував стабільність, просторову переносимість на нові території без додаткового калібрування та значний практичний потенціал для швидкої автоматизованої оцінки збитків в аграрному секторі.

Список літератури

1. Svitenko H., Romanenkov Yu. Analysis of changes in selected characteristics of SAR data depending on damage to agricultural land. Information systems and innovative technologies in project and program management, 2025. С. 254-256.

2. Veloso A., Mermoz S., Bouvet A., Le Toan T., Planells M., Dejoux J.-F., Ceschia E. Understanding the temporal behavior of crops using Sentinel-1 and Sentinel-2-like data for agricultural applications. Remote Sensing of Environment. 2017. Т. 199. С. 415-426. DOI: https://doi.org/10.1016/j.rse.2017.07.015.

3. Hussain M., Chen D., Cheng A., Wei H., Stanley D. Change detection from remotely sensed images: From pixel-based to object-based approaches. ISPRS Journal of Photogrammetry and Remote Sensing, 2013. Т. 80. С. 91-106. DOI: https://doi.org/10.1016/j.isprsjprs.2013.03.006.

МЕТОДИ ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ КОНТЕЙНЕРИЗОВАНИХ ЗАСТОСУНКІВ У ХМАРНОМУ СЕРЕДОВИЩІ

Дадикін В.О., Чепурна І.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Останнє десятиліття спостерігається стійка тенденція до впровадження хмарних застосунків для забезпечення сучасних бізнес-процесів. Розробка програмних продуктів з мікросервісною архітектурою базується на технологіях контейнеризації, що дозволяє розгортати окремі компоненти в ізольованих середовищах [1]. Підтримка контейнеризації багатьма хмарними вендорами забезпечує широкий спектр доступних та різноманітних сервісів в межах моделей надання послуг та стимулює зростання кількості хмарних застосунків. Водночас їх експлуатація актуалізує потребу методологічного забезпечення їх стабільного та безперервного функціонування в умовах зростаючої кількості користувачів та динамічно змінного навантаження [2].

Метою доповіді є огляд та систематичний аналіз існуючих методів підвищення продуктивності контейнеризованих застосунків з мікросервісною архітектурою, що розгорнуті в середовищах провідних хмарних вендорів.

В доповіді наводяться результати аналізу останніх публікацій та досліджень методів підвищення продуктивності хмарних програмних застосунків, що функціонують в умовах динамічно змінного навантаження. Наведені дані показують, що такі методи базуються на застосуванні механізмів масштабування, балансування навантаження або їх комбінації. Зокрема застосування хмарних балансувальників, таких як Azure Load Balancer та Google Cloud Load Balancer, забезпечує динамічний розподіл трафіку з регламентованим доступом до компонентів інфраструктури застосунку, ізолюючи їх від прямого зовнішнього потоку користувацьких запитів. Такий підхід забезпечує високу доступність сервісів, мінімізацію затримок при обробці запитів та стабільне функціонування хмарних застосунків в умовах динамічно змінного навантаження [3]. Перспективи подальших досліджень спрямовані на розробку методу підвищення продуктивності ASP.NET-застосунку, розгорнутого в середовищі Google Cloud, в умовах динамічно змінного навантаження.

Список літератури

1. Khunjush F., Namvar R., Dogani J. Auto-scaling techniques in container-based cloud and edge/fog computing: Taxonomy and survey. *Computer Communications*. 2023. Vol. 209. P. 120–150. DOI: https://doi.org/10.1016/j.comcom.2023.06.010

2. Rabiu S., Huah Yong C., Mashita Syed Mohamad S. A Cloud-Based Container Microservices: A Review on Load-Balancing and Auto-Scaling Issues. *Int. Journal on Data Science*. 2022. Vol. 3, № 2. P. 80–92. DOI: https://doi.org/10.18517/ijods.3.2.80-92.2022

3. Beshley H., Bodnar S., Seliuchenko M., Beshley M., Klimash M. Development of a platform for researching automatic container scaling and load balancing in distributed systems. *Вісник НУ «ЛП»*. 2024. С. 1–9. DOI: https://doi.org/10.23939/ictee2024.02.038

УПРАВЛІННЯ МЕРЕЖНИМИ РЕСУРСАМИ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Ярошевич Р. О., Коваленко А. А.,
Порошенко А.І., Філіппов В.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Ускладнення структури трафіку та зростання його обсягів є характерними ознаками еволюції комп'ютерних мереж. Якщо раніше основну частину інтернет-трафіку генерували персональні комп'ютери, то зараз провідну роль відіграють мобільні пристрої, вбудовані обчислювальні системи та сервіси передавання мультимедійних потоків в реальному часі. Поширення хмарних обчислень додатково підвищує вимоги до пропускної здатності, затримки, надійності та адаптивності мережної інфраструктури.

Метою доповіді є узагальнення сучасних підходів до інтелектуального управління мережними ресурсами на основі методів штучного інтелекту (ШІ) та визначення перспектив їх застосування в комп'ютерних мережах.

Методи ШІ забезпечують перехід до проактивного керування мережею на основі аналізу телеметрії, історичних даних і прогнозованого стану мережі [1]. Для задач прогнозування навантаження особливий інтерес становлять моделі глибокого навчання RNN, LSTM і GRU, що дають змогу ефективно прогнозувати трафік у коротко- та середньостроковій перспективі.

Перспективною платформою для реалізації інтелектуального керування є програмно-конфігуровані мережі (SDN), що відокремлюють логіку управління від безпосереднього пересилання пакетів [2]. Централізований SDN-контролер надає ШІ-агентам повний огляд стану мережі, що дозволяє застосування методів навчання з підкріпленням (Reinforcement Learning), зокрема алгоритмів DQN та A3C – для динамічного розподілу ресурсів без явного програмування правил.

Разом із тим існуючі підходи мають суттєві обмеження: потреба у великих обсягах розмічених даних, низька інтерпретованість рішень ШІ-агента, а також деградація моделі за умов зміни топології чи появи нових класів трафіку.

Подолання цих обмежень є актуальним напрямом досліджень у галузі інтелектуального керування комп'ютерними мережами.

Список літератури

1. Ospina Cifuentes B. J. et al. Analysis of the Use of Artificial Intelligence in Software-Defined Intelligent Networks: A Survey. Technologies. 2024. Vol. 12, No. 7. Art. 99.

2. Ярошевич Р.О., Аналіз технологій підвищення ефективності тактильного інтернету у комп'ютерних мережах / Ярошевич Р.О., Коваленко А.А., // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2022. – Т. 1 (67). – С. 106-110. – https://doi.org/10.26906/SUNZ.2022.1.106.

ЕФЕКТИВНІСТЬ МЕТОДІВ АВТОМАТИЧНОГО МАСШТАБУВАННЯ В ОРКЕСТРАТОРІ КОНТЕЙНЕРІВ KUBERNETES

Кондрацький Г.О., Ярошевич Р.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні інформаційні системи функціонують в умовах постійно зростаючих вимог до продуктивності та доступності, що зумовлено переходом до мікросервісних архітектур.

Платформа Kubernetes [1] стала стандартом оркестрації контейнерів, проте більшість організацій стикаються з труднощами налаштування автомасштабування: неправильний вибір стратегії призводить до надмірного споживання ресурсів або порушення SLA при пікових навантаженнях. Існуючі методи HPA, VPA та KEDA мають принципові архітектурні відмінності, однак систематичний порівняльний аналіз із кількісними критеріями вибору відсутній [2].

Метою доповіді є порівняльний аналіз ефективності методів автомасштабування в Kubernetes на основі комплексного навантажувального тестування у відтворюваному середовищі..

HPA регулює кількість реплік за співвідношенням поточної та цільової метрики з часом реакції 30-120 секунд без перезапуску робочих одиниць, проте не підтримує зменшення реплік до нуля, а його ефективність критично залежить від коректності запитів на ресурси.

VPA оптимізує ресурсні запити на основі реального споживання, але вимагає перезапуску при оновленні та несумісний з HPA при масштабуванні за однаковими метриками.

KEDA забезпечує масштабування на основі зовнішніх подій із понад 50 джерел і підтримує зменшення реплік до нуля (до 42 % економії ресурсів), проте затримка відновлення з нуля становить 40-90 с.

Порівняльний аналіз показує, що HPA є оптимальним для мікросервісів без збереження стану, KEDA – для подієво-орієнтованих архітектур, а VPA – для початкової калібрації ресурсних запитів.

Для гібридних сценаріїв запропоновано алгоритм HAM, що поєднує HPA та KEDA з адаптивним контролером стабілізації і скорочує вікно очікування на 15-35 %, а також метрику QRCA для оцінювання точності подієво-орієнтованого масштабування.

Список літератури

1. Kubernetes Documentation. Horizontal Pod Autoscaling. 2026. URL: https://kubernetes.io/docs/tasks/run-application/horizontal-pod-autoscale/

2. Hightower K., Burns B., Beda J., Evenson L. Kubernetes: Up and Running: Dive into the Future of Infrastructure. 3rd ed. Sebastopol: O'Reilly Media, 2022. 328 p. ISBN 9781098110208.

ПРОБЛЕМА МЕРЕЖЕВОЇ СИНХРОНІЗАЦІЇ БАГАТОКОРИСТУВАЦЬКИХ СИСТЕМ ТА ЇЇ ВИРІШЕННЯ ЗА ДОМОГОЮ ДЕТЕРМІНОВАНОЇ АРХІТЕКТУРИ

Різник О.В., Холєв В.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У створенні додатків розрахованих на багато користувачів у реальному часі існує критична проблема синхронізації великої кількості незалежних об'єктів. Традиційна клієнт-серверна архітектура, де центральний сервер постійно розраховує фізику та передає координати та стан кожного об'єкта всім клієнтам, потребує великої пропускної спроможності мережі. Якщо на мапі одночасно взаємодіють тисячі активних об’єктів, це призводить до миттєвого навантаження каналу та затримок, що робить обчислення на стороні сервера неефективними або неможливими в умовах низького трафіку [1].

Ефективним вирішенням цієї проблеми є перехід до однорангової мережі (Peer-to-Peer) з використанням архітектури Deterministic Lockstep [2]. Суть підходу полягає в тому, що мережею передаються не стани об'єктів, а виключно команди користувачів. Кожен комп'ютер-клієнт має абсолютно ідентичний математичний рушій і локально симулює весь процес на основі отриманих команд кадр у кадр [3].

Еталонним та найбільш відомим прикладом впровадження цієї технології стала гра StarCraft (1998). Розробники відмовилися від використання серверів для розрахунку матчів, сервер виконував лише роль «лобі» для з’єднання гравців. Це рішення дозволило обробляти дії сотень об’єктів без затримок незважаючи на дуже повільне з’єднання, оскільки пакети даних важили лічені байти. Модель Deterministic Lockstep довела свою високу інженерну ефективність як спосіб радикального зниження мережного трафіку. Натомість ця архітектура має свої недоліки високий ризик розсинхронізації при втраті пакетів і вразливість до зовнішніх втручань, через що більшість сучасних рішень працюють через виділені сервери. Натомість для систем з масовою симуляцією незалежних об’єктів, наприклад жанру класичних RTS (Real Time Strategy), такими як наприклад Supreme Commander, підхід безперервного локального обчислення на основі P2P залишається безальтернативним і найоптимальнішим архітектурним рішенням. Таким чином, незважаючи на зазначені вразливості, використання архітектури Deterministic Lockstep у поєднанні з одноранговою мережею (Peer-to-Peer) залишається найоптимальнішим та функціонально безальтернативним рішенням для систем із масовою симуляцією незалежних об'єктів (зокрема класичних RTS) [4]. Цей підхід високоефективно розв'язує проблему пропускної здатності каналу, переносячи навантаження з мережі на локальні обчислювальні потужності клієнтів.

Список літератури

1. Fiedler, G. (2004). What Every Programmer Needs To Know About Game Networking. Gaffer On Games. (Базова література з мережевої синхронізації).

2. Terrano, M., & Bettner, P. (2001). 1500 Archers on a 28.8: Network Programming in the Age of Empires and Beyond. GDC Proceedings. (Класична стаття про реалізацію Lockstep в RTS).
3. Kirmse, A. (2004). Game Programming Gems 4 (Section 5: Network and Multiplayer). Charles River Media.
4. Shiratori, T., & Hodgins, J. K. (2008). Synchronization of multiplayer physical simulations. ACM Transactions on Graphics.

VECTOR-LOGIC MODELS OF DIGITAL CIRCUITS FOR SIMULATION

Хаханова А.В., Різник М.А.
Харківський національний університет радіоелектроніки, Харків, Україна

It is proposed to create vector-logical in-memory computing for a cost-effective, low-budget solution to modeling and simulation problems by using read-write transactions without processor instructions [1]. A mechanism for modeling a fault simulation matrix as the addresses of the deductive vector bits for each test set element has been developed [2]. The results of the good-value and fault-as-address simulations are rendered and synchronized in the good-value simulation, fault-as-address simulation [3], and fault simulation matrices on the input set and along the lines of the logical circuit displayed on the monitor.

The aim of the study is to develop a vector-logical in-memory computer [4] as a cost-effective solution for modeling and simulation problems using read-write transactions without processor instructions. Research objectives include: 1) Creating a vector-logical model of a digital circuit for efficient simulation of input test sets, represented as addresses of logical vector elements. 2) Building deductive vectors within a vector-logical model of a logical circuit for fault simulation based on address inputs [5]. 3) Designing fault simulation matrices as bit addresses within the deductive vector of each element of the test set. Scientific innovations include: 1) Vector-logical models of circuit elements that enable good-value simulation of input test sets and fault simulation via bits of logical and deductive vectors based on read-write transactions. 2) Good-value simulation mechanisms that operate without processor participation. 3) Fault simulation as an address-based mechanism functioning independently of a processor [6]. A mechanism for constructing a deductive vector on the input set using explicit addresses in the truth table is considered. This mechanism is easily scalable to any truth table from n variables. The mechanism can also be used to identify faults in test sets of any function or structure. Initial data (Fig. 1): logical vector Y of functionality, test input set T.

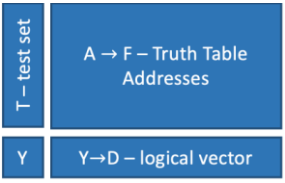


Figure 1 – Data structures for modeling deductive vector

Algorithm of modeling deductive vector for the test set 011 for the logic vectors 01111110, 11100111 (Fig. 6): 1) The output function good-value state is calculated as the address of the truth table Y_T=f(F). 2) Vector xor operations L=TY⊕AY create an active unordered truth table on the test set. 3) Ordering the resulting truth table according to the HDL address following standard A creates a deductive vector D_A=L in three operations.

Vector-logical modeling of a digital circuit. The goal is to significantly reduce the time and energy costs of simulation modeling by using read-write in-memory computing transactions on vector-logical models of digital circuit elements. Vector Logic Modeling Metric (fig. 2) [6]:

L-matrix								H-matrix								D-matrix								C-matrix or testing map							
0	1	0	0	0	0	1	0									000	001	010	011	100	101	110	111	000	001	010	011	100	101	110	111
0		1					1	0	1	2	3	4	5	6	7	000		1				1		000		..1				11.	
1	1		1	1	1	1		1	1	0	3	2	5	4	7	6	001		1	1	1	1	1	001		..0	.1.	.10	1..	1.0	11.	
0		1					1	2	3	0	1	6	7	4	5	010				1	1			010				.01	1..			
0		1					1	3	2	1	0	7	6	5	4	011			1			1		011			.0.			1.0		
0		1					1	4	5	6	7	0	1	2	3	100			1			1		100			.1.			0.1		
0		1					1	5	4	7	6	1	0	3	2	101				1	1			101				.10	0..			
1	1		1	1	1	1		1	6	7	4	5	2	3	0	1	110		1	1	1	1	1	1	110		..1	.0.	.01	0..	0.1	00.	
0		1					1	7	6	5	4	3	2	1	0	111		1					1	111		..0					00.	

Figure 2 – Matrix vector-logical modeling of the testing map

1) A logical vector (01000010) is all that is needed to describe any functionality or structure.

2) A read-write transaction based on an explicit binary address of a logical vector bit is all that is needed to compute the state of any logical element.

3) Any two-seat operation is specified by a logical vector of 4 bits in length.

4) A two-place operation on a logical vector also generates a logical vector or matrix of length 2^{2n}.

5) An Xor operation on a logical vector generates a disordered L-matrix of activity or a complete set of unordered deductive vectors and derivatives.

6) Ordering the activity matrix according to the HDL standard (H-matrix) by following the addresses of logical variables generates a deductive D-matrix D =L_H. It contains the complete set of deductive vectors in rows and the complete set of derivatives in the columns of the matrix.

7) A deductive vector is a logical vector that determines the conditions for activating (changing) the output of an element by input logical faults on a given input set. 7) The Boolean derivative is a logical vector that determines the conditions for activating the output when a given number of input variables change on an exhaustive test.

8) C-matrix or testing map is a matrix of relationships between an exhaustive test and the complete set of all combinations of input variable faults. The coordinates of the matrix are determined by the F-vectors of the faults to be detected in alphabetical order (01), where the "dot" denotes a non-fault detected on the corresponding input variable. Each significant (0,1) coordinate of the F-vector is

defined at the locations with 1-value of the address bits at the top of the C-matrix, which are further determined by the inverse value of the corresponding bits of the input test set on the left side of the matrix.

Vector-logical in-memory computing is proposed as a cost-effective, low-budget solution for modeling and simulation problems that uses read-write transactions rather than processor instructions. A vector-logical model of a digital circuit for efficient simulation of input test sets, using logical vector bit addresses, has been implemented. A mechanism for generating deductive vectors based on a vector-logical model of a digital circuit is proposed for fault-as-address simulation of input test sets. A mechanism for modeling a fault simulation matrix as the addresses of the deductive vector bits of each element on the test set has been created. The results of the good-value and fault-as-address simulations were rendered and synchronized in the tables for good-value simulation, fault-as-address simulation, fault-modeling matrices on the input set, and the lines of the logical scheme displayed on the monitor screen. The processing time of logic circuits and mechanisms for fault modeling and good-value simulation is presented.

The scientific novelty of the study lies in vector-logical models of digital circuit elements, high-value simulation of the test set, address- and fault-as-address simulation of the digital circuit, and fault-as-address simulation of the input set, all using a quadratic simulation matrix. Implemented mechanisms for ergonomic rendering and synchronization of modeling results in four scalable windows displayed on the monitor screen. All of these innovative solutions are unparalleled worldwide and create a cost-effective future of mass computing. Cloud services [6] can be useful to students and engineers engaged in verifying digital projects based on vector logic elements.

References

1. N. R. Shanbhag and S. K. Roy, "Benchmarking In-Memory Computing Architectures," in IEEE Open Journal of the Solid-State Circuits Society, vol. 2, pp. 288-300, 2022, doi: 10.1109/OJSSCS.2022.3210152.

2. V. Hahanov, S. Chumachenko, E. Litvinova, I. Hahanov, Z. Davitadze, and D. Devadze, "Vector Logic of Computing," 2025 IEEE 13th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Gliwice, Poland, pp. 1-5, 2025, doi: 10.1109/IDAACS68557.2025.11322309.

3. V. Hahanov, W. Gharibi, S. Chumachenko, E. Litvinova, “Vector Synthesis of Fault Testing Map For Logic,” in IAES International Journal of Robotics and Automation (IJRA), vol. 13, no. 3, pp. 293-306, 2024, doi:10.11591/ijra.v13i3.pp293-306.

4. T. Sharma, I. Chakraborty, M. Ali, and K. Roy, "Evaluating Compute in Memory Architectures for Matrix Multiplication: A Dataflow-Centric Perspective," 2025 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS), Ghent, Belgium, pp. 1-3, 2025, doi: 10.1109/ISPASS64960.2025.00056.

5. H. Guo, J. Chen and H. Jiao, "A 15T SRAM Cell-Based Fully Digital Computing-in-Memory Macro Supporting High Parallelism and Fine-Grained Simultaneous Read + Write + MAC Operations," in IEEE Solid-State Circuits Letters, vol. 8, pp. 153-156, 2025, doi: 10.1109/LSSC.2025.3567840.

6. https://vector-simulation-model.vercel.app/. Accessed 09.02.2026.

ОПТИМІЗАЦІЯ С-КОДУ В СЕРЕДОВИЩІ ВИСОКОРІВНЕВОГО СИНТЕЗУ

Шкіль О.С., Карманський Б.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних вбудованих системах на основі технології «система на кристалі» (SoC) оптимізація алгоритмів, реалізованих мовами високого рівня, є критично важливою для ефективного використання обмежених апаратних ресурсів. Швидкий розвиток систем реального часу вимагає високої продуктивності при мінімальному енергоспоживанні, що робить використання засобів високорівневого синтезу (HLS) стандартом індустрії. Особливу увагу привертають обчислювально-навантажені алгоритми цифрової обробки сигналів, такі як множення матриць, швидке перетворення Фур'є (FFT) та вейвлет-перетворення, які складають математичне ядро більшості сучасних систем інтелектуального аналізу даних та телекомунікацій. Проблема полягає у тому, що пряма трансляція С-коду в апаратні описи (HDL) часто призводить до надлишкових витрат логічних елементів, тому застосування специфічних стратегій оптимізації на етапі розробки є необхідною умовою створення конкурентоспроможних систем.

Метою доповіді є порівняльний аналіз впливу способів оптимізації С-коду на ефективність реалізації алгоритмів множення матриць, швидкого перетворення Фур'є та вейвлет-перетворення для платформ SoC, ПК та одноплатних комп'ютерів [1].

Дослідження показало, що на ПК з ARM M1 оптимізація скорочує час виконання всіх алгоритмів на 30–70%. Для вбудованих ARM-платформ (Raspberry Pi, Zynq PS) найбільший ефект досягнуто для FFT (до 90%) та множення матриць (30%), тоді як вейвлет-перетворення майже не прискорюється. Використання арифметики з фіксованою крапкою є найбільш ефективним: для FFT воно дає прискорення до 90% на процесорній частині (PS), а для програмованої логіки (PL) – скорочення апаратних витрат до 80% для матриць та до 40% для FFT. Розгортання циклів із типом float не дає суттєвого ефекту для вбудованих систем та не впливає на ресурси PL.

Висновки. стратегія оптимізації повинна обиратися відповідно до архітектури SoC. Для процесорних систем пріоритетною є оптимізація циклів, тоді як для апаратної реалізації на базі SoC ключовим є перетворення типів даних та паралелізм операцій, що мінімізує апаратні витрати при високій швидкодії.

Список літератури

1. Шкіль О.С. Оптимізація програмного коду для високорівневого синтезу при апаратній реалізації обчислювально-навантажених алгоритмів / О.С. Шкіль, О.І. Філіпенко, Д.Ю. Рахліс, І.В. Філіпенко, В.Р. Корнієнко // Сучасний стан наукових досліджень та технологій в промисловості. – 2025. – No 3 (33). – С. 189-202. DOI: https://doi.org/10.30837/2522-9818.2025.3.189

АПАРАТНО-ОРІЄНТОВАНА МОДЕЛЬ АДАПТИВНОГО КОДУВАННЯ ДЛЯ ЕНЕРГОЕФЕКТИВНИХ СЕНСОРНИХ МЕРЕЖ

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

Нестабільність електромагнітного фону та постійні динамічні зміни в каналах зв'язку автономних вузлів IoT мають значний вплив на енергоспоживання та загальну надійність передачі даних. Це робить традиційні статичні методи завадостійкого кодування (FEC), які зазвичай розраховані на найгірші сценарії перешкод, вкрай неефективними [1, 2]. Використання таких жорстких статичних підходів за сприятливих умов радіоканалу створює непотрібну обчислювальну надлишковість, що неминуче призводить до нераціонального споживання обмеженого заряду батареї та помітного зниження корисної пропускної здатності.

Метою доповіді є розробка апаратно-орієнтованої моделі адаптивної системи корекції помилок, яка б динамічно підлаштовувала параметри кодування під безперервно змінюваний стан середовища та залишковий внутрішній ресурс пристрою. Це досягається шляхом інтеграції оцінки якості каналу, поточного рівня заряду батареї та вимог до затримок у єдиний контур управління.

В доповіді детально розглядаються результати розробки архітектури системи на базі скінченного керуючого автомата (FSM). Використання гістерезису при визначенні порогових значень є критично важливим для уникнення ефекту «ping-pong» – частих та енергозатратних перемикань алгоритмів при незначних коливаннях якості сигналу. Така архітектура забезпечує безперебійне та обґрунтоване перемикання між трьома основними стратегіями: енергозберігаючим режимом (прості коди Геммінга при високому SNR), захищеним (потужні LDPC-коди при погіршенні каналу для уникнення масових запитів на повторну передачу) та критичним режимами (пріоритет на виживання вузла при критичному розряді батареї). Крім того, висвітлюються особливості апаратної реалізації на базі ПЛІС (FPGA) [3]. Гібридний підхід з локальним моніторингом безпосередньо на стороні передавача мінімізує затримки зворотного зв'язку, а застосування низькорівневої техніки Clock Gating дозволяє апаратно «заморожувати» неактивні обчислювальні блоки (наприклад, складний кодер та декодер у сприятливих умовах).

Аналітичні дані показують, що запропонована комплексна модель дозволяє досягти оптимального балансу між необхідною надійністю, швидкістю передачі та загальною енергоефективністю в умовах мінливого середовища. Завдяки динамічному регулюванню надмірності кодування, система уникає перевантаження каналу. Її застосування не лише радикально знижує динамічне енергоспоживання цифрового ядра в енергозберігаючому режимі, але й ефективно запобігає значним втратам енергії через неефективний радіообмін – зокрема, мінімізує енергозатратні цикли повторних передач пошкоджених пакетів (ARQ) при раптовому погіршенні

сигналу. У підсумку це дозволяє в рази подовжити час автономної роботи важкодоступних сенсорних вузлів, наприклад, у промисловому IoT або системах "розумного міста", де заміна елементів живлення є фізично складною або економічно недоцільною. Такий комплексний підхід є фундаментальною стратегією для розгортання стійких, масштабованих та повністю самоорганізованих інтелектуальних мереж майбутнього.

Список літератури

1. Alhmiedat T. An Adaptive Energy-Efficient Data Collection System for ZigBee Wireless Sensor Networks. *International Journal of Distributed Sensor Networks.* 2015. Vol. 11, no. 12.

2. Migabo E., Djouani K., Kurien A. An Energy-Efficient and Adaptive Channel Coding Approach for Narrowband Internet of Things (NB-IoT) Systems. *Sensors*. 2020. Vol. 20, no. 12.

3. Філіппенко І. В., Кулак Е. М., Сергієнко В. І. Система завадостійкого кодування даних на пліс. *Радіоелектроніка та інформатика*. 2019. № 4. С. 38–45.

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ ДЛЯ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ

Рябінін Д.В, Філіппенко І.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Стрімке розширення телекомунікаційних систем призводить до значного ускладнення процесів обміну даними [1].

Класичні підходи до управління маршрутизацією та моніторингу стану вузлів поступово втрачають свою ефективність через величезні обсяги інформації.

Динамічні зміни в мультисервісних мережах створюють локальні перевантаження та флуктуації, які вкрай важко передбачити за допомогою стандартних математичних моделей. Через це виникає практична необхідність переходу до адаптивних систем управління, що базуються на технологіях штучного інтелекту.

Традиційні алгоритми виявлення аномалій або балансування навантаження зазвичай спираються на жорсткі набори правил. Коли мережева топологія розширюється або з'являються нові вимогливі типи інформаційних додатків, такі статичні обмеження починають давати збої.

Адміністраторам доводиться вручну переналаштовувати обладнання, що займає час і призводить до зниження загальної пропускної здатності віртуальних з'єднань.

Використання машинного навчання дозволяє автоматизувати цей процес, оскільки система здатна самостійно знаходити приховані закономірності у нелінійній поведінці трафіку [2].

Метою доповіді є аналіз перспектив впровадження технологій штучного інтелекту, зокрема штучних нейронних мереж, у системи управління сучасними

телекомунікаційними мережами для підвищення їх адаптивності, ефективності маршрутизації, виявлення аномалій та загальної відмовостійкості в умовах швидкого зростання обсягів трафіку та динамічних змін топології.

Найбільш перспективним напрямком є впровадження штучних нейронних мереж безпосередньо в інфраструктуру програмно-конфігурованих мереж. Нейромережа аналізує великі масиви історичних даних про проходження пакетів і формує базову еталонну модель нормального стану системи [3].

Алгоритм постійно враховує такі динамічні параметри як затримки передачі, обсяг заповнення буферів проміжних маршрутизаторів та кількість активних сесій користувачів. Якщо в сегменті мережі виникає нестандартна активність, алгоритм одразу фіксує відхилення від норми без потреби у попередньо написаних скриптах.

Важливою перевагою такого підходу є здатність моделей до постійного донавчання в процесі експлуатації мережі.

На відміну від сигнатурних методів аналізу, які здатні розпізнавати лише вже відомі патерни перевантажень чи загроз, предиктивні моделі можуть виявляти абсолютно нові типи мережевих аномалій або апаратних збоїв ще до того, як вони спричинять відмову цілого вузла. Це суттєво підвищує загальну відмовостійкість інфраструктури та зменшує кількість втрачених пакетів даних.

Інтеграція методів штучного інтелекту в процеси міжмережевої взаємодії частково вирішує проблему масштабованості сучасних комп'ютерних мереж.

Розробка нових оптимізованих систем управління на базі нейромереж дозволяє не тільки пришвидшити обробку інформації, але й мінімізувати вплив людського фактору на стабільність роботи мережевого обладнання.

Подальші дослідження у цій сфері мають бути зосереджені на пошуку балансу між точністю роботи алгоритмів машинного навчання та обчислювальним навантаженням, яке вони самі створюють на комутатори.

Список літератури

1. Єршова О. Л., Бажан Л. І. Штучний інтелект – технологічна основа цифрової трансформації економіки. Статистика України. 2021. № 3. С. 47–55. DOI: https://doi.org/10.31767/su.3(94)2021.03.06. ORCID: https://orcid.org/0000-0002-6211-202X

2. Савицька Л. А., Коробейнікова Т. І., Волос О. П., Тарновський М. Г. Метод та засіб моніторингу безпеки в комп'ютерній мережі засобами SIEM. Інформаційні технології та комп'ютерна інженерія. 2023. № 3(58). С. 22–32. DOI: https://doi.org/10.31649/1999-9941-2023-58-3-22-32.

3. Базилевич В., Мальцева М. Побудова захищеної системи розумного дому з використанням IoT. Технічні науки та технології. 2020. № 2(20). С. 218–228. DOI: https://doi.org/10.25140/2411-5363-2020-2(20)-218-228.

ОПТИМІЗАЦІЯ ОБЧИСЛЮВАЛЬНИХ ПРОЦЕСІВ У СИСТЕМАХ УЛЬТРАЗВУКОВОГО СКАНУВАННЯ В РЕАЛЬНОМУ ЧАСІ НА БАЗІ SOC ZYNQ-7000

Рахліс Д.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток автономної робототехніки потребує малогабаритних систем сканування з мінімальною затримкою обробки даних. Традиційні мікроконтролери не забезпечують детермінованості процесів при паралельному позиціюванні сенсора та аналізі вимірювань, що призводить до критичних часових затримок. Гетерогенні системи на кристалі (SoC) вирішують цю проблему шляхом апаратного прискорення критичних операцій у програмованій логіці (PL) та перенесення аналітики на процесорну систему (PS). Взаємодія через інтерфейси AXI забезпечує паралельність обчислень, недосяжну для класичних архітектур, що є критичним для стабільності систем реального часу.

Метою роботи є підвищення точності та швидкодії ультразвукового сканування шляхом впровадження методів паралельної обробки даних у архітектурі SoC Zynq-7000 [1]. Для досягнення поставленої мети необхідно вирішити такі завдання:

– розробити апаратні модулі на PL частині SoC для точного вимірювання дистанції до перешкоди, керування приводом, підготовки даних та UART передавач;

– спроєктувати топологію з’єднань у середовищі IP Integrator для забезпечення швидкісного обміну даними між PL та PS через шину AXI;

– реалізувати алгоритми статистичного аналізу в PS для оперативної оцінки параметрів сканування та формування діагностичних звітів;

– розробити програмний інтерфейс для динамічної візуалізації результатів сканування та побудови карти навколишнього простору в реальному часі.

Оптимізація обчислювальних процесів досягалася завдяки розподілу функцій між апаратною (PL) та програмною (PS) частинами SoC. Як доведено в [3], такий розподіл у SoC Zynq-7000 мінімізує затримки та гарантує детерміновану швидкість обробки незалежно від складності алгоритмів.

Апаратна частина реалізована в середовищі AMD Vivado [2] як структурна VHDL-модель (рис. 1), що складається з наступних модулів:

1) HCSR04_sensor здійснює керування ультразвуковим сенсором та апаратну верифікацію сигналу Echo з багатоступеневою синхронізацією для усунення метастабільності та хибних спрацювань;

2) Motor_SG90 – інтелектуальний драйвер сервоприводу з апаратною широтно-імпульсною модуляцією, що реалізує алгоритм крокового сканування, синхронізований із роботою сенсора для виключення похибки вимірювання під час руху;

3) Data_Formatter включає в себе модуль ASCII-конвертації двійкових значень та формування готового текстового повідомлення у форматі *“Angle: XXX°, Distance: XXX.XX cm”;*

4) UART_Sender координує роботу черги повідомлень (uart_fifo) та передавача (uart_tx), забезпечуючи стабільну передачу даних.

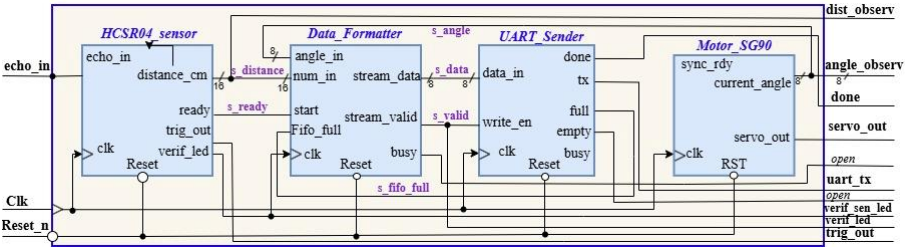


Рисунок 1 – Структурна VHDL-модель керування системою ультразвукового сканування

На рівні системної інтеграції обмін даними між PL та PS реалізовано через шину AXI та комутатор AXI Peripheral Interconnect. Це забезпечує процесору прямий доступ до результатів вимірювань через контролер AXI GPIO, що відображає стан регістрів відстані та кута в єдиному адресному просторі (рис. 2).

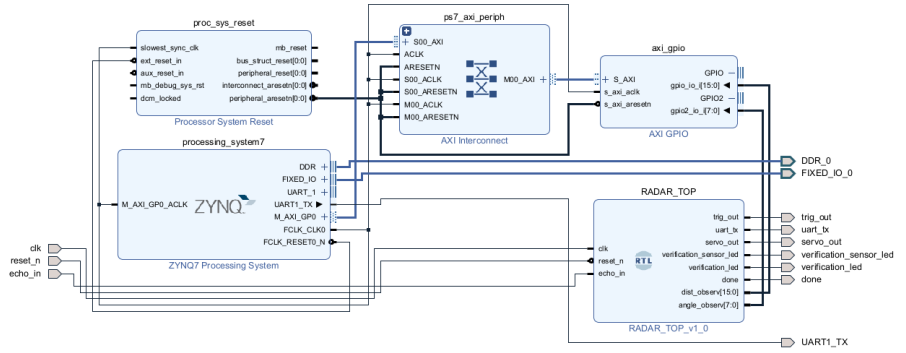
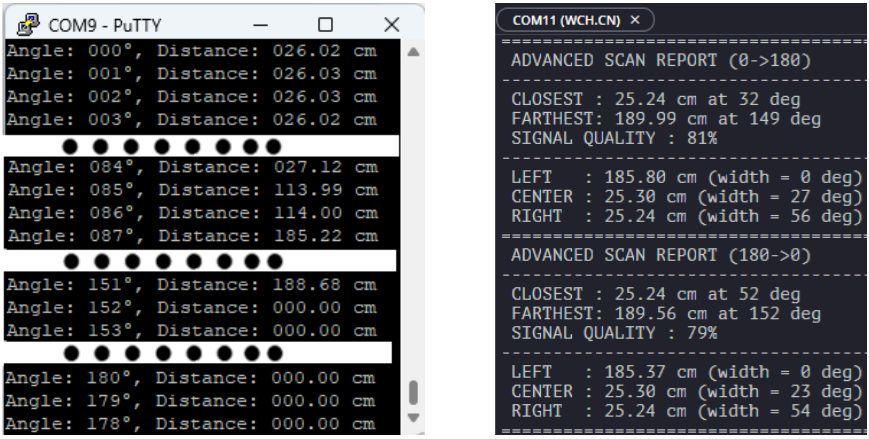


Рисунок 2 – Блочна модель системи керування ультразвуковим скануванням

Програмний рівень реалізовано мовою C у середовищі AMD Vitis. Алгоритм керування забезпечує ініціалізацію апаратних ресурсів та зчитування даних із адресного простору PL за допомогою системних бібліотек Xilinx.

Для реалізації системи використано гетерогенну платформу на базі SoC Zynq-7000, до якої інтегровано ультразвуковий сенсор HC-SR04 та сервопривід SG90. Зв'язок із зовнішнім терміналом забезпечено через інтерфейс UART-USB (CP2104). При експериментальній апробації макета об’єктами сканування виступали: картонна перешкода з похилими площинами (відстань 25-26 см), стіна (186 см) та м’які меблі (>140 см). Аналіз даних монітора порта (рис. 3, а) засвідчив стабільну реєстрацію об’єктів у ближній та дальній зонах. Поява нульових значень на граничних кутах (152°-180°) зумовлена фізичними ефектами дзеркального відбиття від похилих площин або поглинанням ультразвуку оббивкою меблів під гострим кутом. Отримані результати підтвердили коректну роботу апаратного UART, блока форматування Data_Formatter та високу точність ШІМ-контролера (крок 1°).

Ефективна фільтрація недостовірних сигналів на рівні PL гарантувала передачу в PS виключно верифікованої інформації, на базі якої після кожного циклу сканування алгоритм генерував аналітичні звіти, а саме відстань до об’єктів (min/max), їхню кутову ширину в різних секторах (Left, Center, Right) та рівень достовірності сигналу (signal quality).



а б

Рисунок 3 – Моніторинг даних від PL (а) та PS (б) частин

Для візуалізації даних у середовищі VS Code розроблено Python-застосунок. Радіус побудови мап обмежено 200 см для підвищення деталізації об’єктів у ближній зоні (рис. 4).

Лівий графік («Ультразвуковий сканер») відображає дані в полярних координатах. Кольоровий градієнт (від червоного до блакитного) та динамічний шлейф дозволяють миттєво оцінити дистанцію до перешкод і напрямок руху сенсора. Правий графік («Мапа статичних перешкод») формує хмару точок із ефектом накопичення. Це дозволяє диференціювати нерухомі

об'єкти, що стають яскравішими при повторному скануванні, від динамічних завад, які залишають лише слабкий слід. Таблиця замірів у центрі інтерфейсу підтверджує стабільність системи та відсутність аномальних «стрибків» значень.

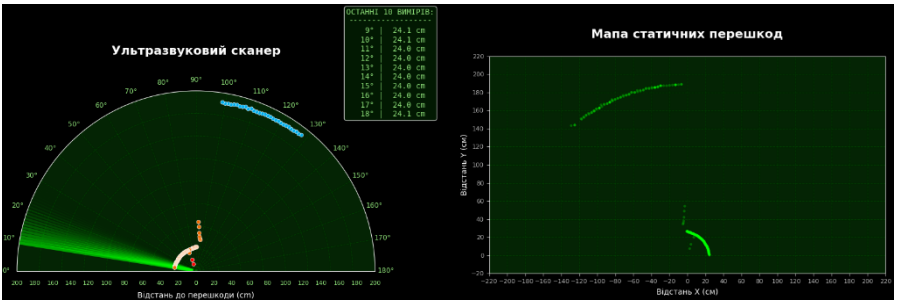


Рисунок 4 – Візуалізація роботи ультразвукового сканера

Висновки. У роботі оптимізовано обчислювальні процеси в системах реального часу шляхом детермінованого розподілу функцій між PL та PS гетерогенної SoC. Експериментальна апробація макета на базі Zynq-7000 підтвердила працездатність обраної архітектури. Тестування показало високу повторюваність вимірювань та стабільність апаратної фільтрації у PL. Детерміноване керування в "залізі" усунуло накопичувальну похибку кута, забезпечивши точну реконструкцію мапи статичних перешкод у реальному часі без перевантаження процесора. **Наукова новизна** полягає у розробці архітектури системи сканування простору на базі SoC Zynq-7000, що поєднує: апаратну верифікацію та фільтрацію сигналів у PL для повного усунення програмного джиттера; апаратну ASCII-конвертацію даних, що мінімізує навантаження на процесор; та паралельну ієрархію обробки, де статистичний аналіз у PS виконується незалежно від низькорівневого керування периферією в PL. **Практична цінність** полягає у створенні готового модуля для робототехніки, який завдяки апаратній обробці сигналів забезпечує миттєву реакцію на перешкоди та легко інтегрується в системи автономного керування.

Список літератури

1. Vivado design suite user guide: design flows overview. 2022. 96 p. URL: https://docs.amd.com/r/en-US/ug904-vivado-implementation (дата звернення: 15.03.2026).

2. Crockett L. H., Elliot R. A., Enderwitz M. A., Stewart R. W. The Zynq Book: Embedded Processing with the ARM® Cortex®-A9 on the Xilinx® Zynq®-7000 All Programmable SoC. URL: http://www.zynqbook.com (дата звернення: 15.03.2026).

3. Shkil O., Filippenko O., Rakhlis D., Filippenko I., Kornienko V. Analysis of the implementation efficiency of digital signal processing systems on the technological platform SoC Zynq 7000. *Radioelectronic and Computer Systems*. 2024. No. 4(112). P. 168-177. DOI: https://doi.org/10.32620/reks.2024.4.14.

МАТЕМАТИЧНА ТА АВТОМАТНА МОДЕЛІ ФУНКЦІОНАЛЬНОГО ПОТОКОВОГО ONLINE-ОБЧИСЛЮВАЧА

Ларченко Л.В., Павлюк С.Я.
Харківський національний університет радіоелектроніки, Харків, Україна

В розподілених системах управління реального часу отримала розвиток концепція присенсорних обчислень, що передбачає переміщення обробки даних ближче до сенсорних компонентів [1]. Для обробки частотних на широтномодульованих сигналів сенсорів знаходять використання потокові обчислювачі, що виконують перетворення сигналів в реальному часі за певною функцією і мають спрощені архітектурні рішення за рахунок представлення даних бітовими (імпульсними) потоками [2].

Метою дослідження є розробка математичної моделі біт-потокового дробово-раціонального обчислювача з мінімізацією абсолютної похібки відтворення функції та автоматної моделі пристрою на основі кінцевого автомата.

В роботі розроблено удосконалену математичну модель обчислювача, що являє собою систему різницевих нерівностей і реалізує алгоритм безперервного паралельного обчислення значень двох раціональних функцій.

Практичне значення результатів полягає в розробці автоматної моделі пристрою, що сформована на основі кінцевого автомата моделі Мура. Графові моделі включають ГСА, створений на основі конвеєрної архітектури обчислювача, та граф переходів, що забезпечує чіткий порядок виконання алгоритму обчислень.

На основі графових моделей створено HDL-модель пристрою в якості шаблону для реалізації алгоритмів дробово-раціональних функцій засобами САПР. Проведено експериментальне дослідження моделей, верифікацію та імплементацію пристрою в FPGA**.**

Розроблені моделі забезпечують абсолютну точність відтворення функцій на рівні 0,5 одиниці молодшого біту аргументу, розширення функціональних можливостей та значно скорочують час процесу проєктування, що підвищує його ефективність.

Список літератури

1. Vasyliev O., Larchenko L., Parkhomenko A., Larchenko B. et al. Research and Development of Design Models of Bit-Stream Fractional-Rational Real-Time Computer, *13th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Sep. 2025, Gliwice, Poland, Vol.1, pp. 1-6. DOI: 10.1109/IDAACS68557.2025.11322041

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.

МЕТОДИ ВИЯВЛЕННЯ АНОМАЛІЙ ДЛЯ ВИЯВЛЕННЯ КІБЕРАТАК В ПРОМИСЛОВИХ СИСТЕМАХ УПРАВЛІННЯ

Зінченко Д.Р. Гудзинський І.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Динамічні процеси в промислових системах управління (ICS/SCADA) мають суттєвий вплив на надійність, безпеку та безперервність функціонування критичної інфраструктури. Зростання рівня цифровізації виробництва, інтеграція з корпоративними мережами та використання IoT-технологій призводять до підвищення вразливості таких систем до кіберзагроз. Особливу небезпеку становлять цілеспрямовані атаки, які можуть порушувати технологічні процеси, спричиняти аварії та економічні збитки. У зв'язку з цим актуальною є задача розробки ефективних методів виявлення аномалій для своєчасного виявлення кібер атак у промислових системах управління [1].

Із завданнями підвищення рівня кібербезпеки ICS пов'язана необхідність аналізу великого обсягу телеметричних даних, що генеруються сенсорами, контролерами та мережевими пристроями. Такі дані характеризуються високою регулярністю, але водночас можуть містити приховані аномальні відхилення, пов'язані з атаками або відмовами обладнання. Традиційні сигнатурні методи виявлення вторгнень є недостатньо ефективними для виявлення нових або модифікованих атак, що обумовлює доцільність використання методів аномального аналізу на основі машинного навчання [2].

Метою доповіді є дослідження та розробка методів виявлення аномалій для ідентифікації кібер атак у промислових системах управління. Запропонований підхід базується на поєднанні статистичного аналізу часових рядів технологічних параметрів і алгоритмів машинного навчання, зокрема автоенкодерів та методів кластеризації. Це дозволяє формувати модель нормального функціонування системи та виявляти відхилення, що можуть свідчити про наявність атаки.

У доповіді наведено результати аналізу даних, отриманих із реальних і тестових середовищ ICS. Встановлено, що нормальна робота систем характеризується високим рівнем повторюваності та кореляції між параметрами технологічного процесу.

У той же час кібер атаки, такі як підміна даних, атаки типу replay або несанкціоноване втручання в керування, призводять до порушення цих залежностей та появи аномальних патернів [3].

Запропоновані методи дозволяють виявляти як відомі, так і раніше невідомі типи атак за рахунок аналізу відхилень від нормальної поведінки системи. Проведений експериментальний аналіз показує, що використання моделей глибинного навчання забезпечує підвищення точності виявлення аномалій та зменшення кількості хибних спрацьовувань у порівнянні з класичними підходами.

Таким чином, застосування методів виявлення аномалій є ефективним інструментом підвищення кібербезпеки промислових систем управління та

може бути використане для побудови інтелектуальних систем моніторингу критичної інфраструктури в реальному часі.

Список літератури

1. Goh, Jonathan, et al. "Anomaly detection in cyber physical systems using recurrent neural networks." 2017 IEEE 18th international symposium on high assurance systems engineering (HASE). IEEE, 2017. DOI: https://doi.org/10.1109/HASE.2017.36
2. Moshe Kravchik and Asaf Shabtai. 2018. Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC '18). Association for Computing Machinery, New York, NY, USA, 72–83. https://doi.org/10.1145/3264888.3264896
3. МАРТОВИЦЬКИЙ, ВО, et al. "Дослідження методів виявлення аномалій у api журналах для забезпечення безпеки та надійності програмних систем." Вісник Херсонського національного технічного університету 2.1 (92) (2025): 142-148. DOI: https://doi.org/10.35546/kntu2078-4481.2025.1.2.19

МЕТОД ЦИФРОВОГО ВОДЯНОГО МАРКУВАННЯ ЗОБРАЖЕНЬ НА ОСНОВІ ПРОМІЖНИХ ЗНАЧУЩИХ БІТІВ ІЗ ПІДВИЩЕНОЮ СТІЙКІСТЮ ДО АТАК

Шевченко С.Р., Бологова Н.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Динамічні процеси обробки та передачі цифрових зображень у сучасних інформаційних системах супроводжуються зростанням ризиків несанкціонованого доступу, копіювання та модифікації мультимедійного контенту. У зв’язку з цим важливого значення набувають методи захисту авторських прав і забезпечення цілісності даних, зокрема технології цифрового водяного маркування (Digital Watermarking). Особливо актуальним є підвищення стійкості водяних знаків до атак, таких як стиснення, фільтрація, шумові впливи та геометричні перетворення [1].

Існуючі методи водяного маркування можна умовно поділити на просторові та частотні. Просторові методи (наприклад, LSB) відзначаються низькою обчислювальною складністю, проте мають недостатню стійкість до атак. Частотні методи (на основі DCT, DWT, SVD) забезпечують вищу стійкість, однак потребують значних обчислювальних ресурсів. У зв’язку з цим перспективним напрямком є використання проміжних значущих бітів, що дозволяє досягти компромісу між непомітністю та стійкістю водяного знака [2, 3]. Метою доповіді є розробка методу цифрового водяного маркування зображень на основі проміжних значущих бітів із підвищеною стійкістю до атак. Запропонований метод передбачає адаптивний вибір бітових площин залежно від локальних характеристик зображення, таких як контраст, текстурна насиченість та рівень шуму. Це дозволяє підвищити прихованість водяного знака та зменшити ймовірність його спотворення при обробці

зображення. У доповіді наведено результати експериментальних досліджень, які демонструють, що запропонований підхід забезпечує кращу стійкість до JPEG-стиснення, адитивного шуму та фільтрації у порівнянні з класичними LSB-методами. Аналіз показує, що використання проміжних бітів дозволяє зменшити втрати інформації про водяний знак при збереженні високої якості зображення (PSNR > 35 дБ).

Особливістю запропонованого методу є можливість його адаптації до різних типів зображень та умов передачі даних. Використання гібридного підходу, що поєднує просторові та статистичні характеристики, дозволяє підвищити ефективність вбудовування та витягування водяного знака навіть у складних умовах обробки. Таким чином, розроблений метод цифрового водяного маркування забезпечує підвищену стійкість до атак при збереженні високої якості зображення та може бути використаний у системах захисту мультимедійної інформації.

Список літератури

1. Wahyudi, M. Iman, Izza Fauzi, and Dwi Atmojo. "Robust image watermarking based on hybrid IWT-DCT-SVD." IJACI: International Journal of Advanced Computing and Informatics 1.2 (2025): 89-98.

2. Naem, Saif Aldeen S., and Sarab M. Hameed. "Digital watermarking techniques, challenges, and applications: A review." Mesopotamian Journal of CyberSecurity 5.2 (2025): 453-476.

3. Martovytskyi, Vitalii, et al. "Development of methods for generation of digital watermarks resistant to distortion." Eastern-European Journal of Enterprise Technologies 6.2 (2021): 114.

МЕТОД ІНТЕЛЕКТУАЛЬНОЇ ОБРОБКИ ДАНИХ В ІОТ

Дяченко Д.О., Шраменко К.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Інтенсивний розвиток концепції Інтернету речей (IoT) [1] супроводжується стрімким зростанням кількості підключених пристроїв, що генерують великі обсяги різнорідних даних у режимі реального часу, що, у свою чергу, зумовлює необхідність створення ефективних методів їх інтелектуальної обробки. Потоки даних IoT характеризуються високою варіативністю, наявністю шумів, пропусків та нерегулярністю надходження, що суттєво ускладнює застосування традиційних підходів до аналізу інформації. Крім того, обмежені обчислювальні ресурси периферійних пристроїв, затримки передачі даних і вимоги до енергоефективності створюють додаткові обмеження для побудови аналітичних систем. У зв’язку з цим виникає актуальна проблема розробки нових методів інтелектуальної обробки даних, які поєднують алгоритми машинного навчання [2], методи попередньої обробки сигналів і розподілені обчислювальні підходи, зокрема Edge та Fog обчислення, що дозволяють частково переносити обробку даних ближче до джерел їх генерації.

Особливістю сучасних IoT-систем є тісний зв'язок між просторовими та часовими характеристиками даних, що вимагає використання моделей, здатних враховувати такі залежності. Застосування глибоких нейронних мереж, зокрема рекурентних та згорткових архітектур, дозволяє ефективно виявляти приховані закономірності у складних потоках даних, однак потребує значних обчислювальних ресурсів і оптимізації для використання у вбудованих середовищах. Водночас сучасні дослідження демонструють ефективність комбінування методів глибокого навчання з алгоритмами фільтрації, агрегації та редукції розмірності, що дозволяє підвищити якість аналізу та знизити обчислювальне навантаження. Таким чином, розробка гібридних підходів до інтелектуальної обробки даних є перспективним напрямом досліджень у галузі IoT.

Метою доповіді є розробка методу інтелектуальної обробки даних в IoT, який забезпечує підвищення точності виявлення закономірностей та аномалій у потоках даних за рахунок інтеграції адаптивних моделей машинного навчання з процедурами попередньої обробки. Запропонований метод базується на використанні багаторівневої архітектури обробки даних, у якій первинна фільтрація та нормалізація здійснюється на рівні периферійних вузлів, тоді як більш складний аналіз виконується у хмарному середовищі. Такий підхід дозволяє зменшити обсяг даних, що передаються, і знизити затримки, що є критично важливим для систем реального часу. Крім того, у методі враховано адаптацію до зміни статистичних характеристик даних, що дозволяє підвищити стійкість моделей.

У доповіді наведено результати експериментальних досліджень, виконаних із використанням відкритих наборів даних IoT та змодельованих потоків інформації, які імітують роботу реальних сенсорних мереж. Проведений аналіз показує, що на якість інтелектуальної обробки даних суттєво впливають такі фактори, як частота збору даних, пропускна здатність мережі, топологія з'єднань, а також типи сенсорів, які використовуються, і характер прикладних задач. Встановлено, що застосування адаптивних алгоритмів дозволяє ефективно компенсувати вплив шумів і пропусків у даних, а також забезпечує підвищення точності прогнозування та виявлення аномалій у порівнянні з класичними статистичними. Отримані результати підтверджують доцільність використання інтегрованих підходів до обробки даних у середовищі IoT та можуть бути використані при побудові інтелектуальних систем моніторингу, управління та підтримки прийняття рішень.

Список літератури

1. J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. Vol.29, iss.7, Elsevier, 2013. P. 1645-1660. https://doi.org/10.1016/j.future.2013.01.010.

2. M. Alsheikh; S. Lin; D. Niyato; H. Tan. Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications. IEEE Communications Surveys & Tutorials, Vol. 16, 2014. P. 1996 – 2018. https://doi.org/10.1109/COMST.2014.2320099.

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

RESEARCH OF THE BANDWIDTH HIDDEN NETWORK COMMUNICATION CHANNELS

Tahirova K.M.
National Defense University; Baku, Azerbaijan

Attention to covert channels has largely increased due to the documents published by E.Snowden, which described the software and hardware embedding that implement undeclared features covert information transfer in the Huawei and Juniper network equipment, Apple mobile phones and computers with the Windows XP operating system [1]. A covert channel can be built using any information technology, but often attackers build covert channels in IP networks, since they are widespread, have a high information transfer rate, and ubiquitous information security measures, such as traffic encryption, do not affect the possibility of covert transmission of information via some types of such channels. The limitation of their bandwidth is a promising direction for countering information leakage via network covert channels [2, 3]. This study considers network timing covert channels, provides a method for assessing their capacity, proposes and investigates a way to counter information leakage via such covert channels by introducing noise having added delays before sending packets [3, 4]. A covert channel is a communication channel not intended for the transmission of information [1, 5]. In 2008, a covert channel was defined as a communication channel that can be used to violate information security policies. The problem of information leakage via network covert channels is widespread due to the widespread use of the IP protocol and its many features that allow it to be used for covert information transmission [6].

Covert channels are typically divided into two groups based on transmission techniques: memory-based and time-based covert channels. Modifying network packet lengths is used to transmit information via memory-based covert channels in IP networks [1, 2, 4, 7]. Modifying packet header fields can serve as another example of memory-based network covert channels. To construct time-based covert channels in IP networks, packet reordering [4, 7-9] and modification of interpacket interval lengths and packet transmission rates are used. Methods for countering information leakage through covert network channels typically include detection, mitigation, and bandwidth limitation. The first method-detection-allows for efficient use of the communication channel's bandwidth. However, it has been proven that an attacker with knowledge of the security system's parameters can create a covert

communication channel undetectable to the controlling entity. For this study, we selected two network covert channels based on time: one based on changing packet transmission rates (on/off covert channel) and the length of inter packet intervals. We further assume that the "0" and "1" bits transmitted over the covert channel are transmitted with different probabilities [1, 5]:

$$P_{\text{in.}}(0) = q, \quad p_{\text{in.}}(1) = 1 - q. \tag{1}$$

To verify the obtained formulas used in calculating the throughput of covert communication channels, the authors studied a local network with a single router; the ping utility was used to obtain the transit time of more than 10 thousand IP packets. The throughput of a covert channel with errors can be estimated using the following formula [1]:

$$C_{\max}(\mu) = \max_{X} \frac{I(X,Y)}{T + \mu} \quad , \tag{2}$$

where I - is the mutual information of random variables X, Y, describing the input and output characteristics of the covert communication channel; T –average packet transmission time; $\mu -$ the average time required for a packet to move through the data transmission channel.

References

1.Ibrahimov, B. G. (2021).Telecommunication systems and technologies. Textbook for technical higher schools. AzTU, Baku. 354 P.

1. İbrahimov B.G. Research and analysis of fiber-optic communication lines based on wave multiplexing technology. *In* Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. 2023, Том 2. p.4-5

2.Yusifbayli, N., Guliyev, H. Intellectual voltage management in electrical networks. Isgt Innovative smart grid technologies europa 2011, IEEE, PES, Manchester UK, 05-07 December 2011.pp.235-246.

3.Ibrahimov B.G. et al. Research throughput multiservice telecommunication networks. *In* Сучасні напрями розвитку ІКТ та засобів управління. 2020. Том 1. с.30

4.Sheloukhin O. I., Sakalema D. Zh., Filinova A. S. Detection of intrusions into computer networks (network anomalies). Textbook for universities. / Edited by Professor O. I. Sheloukhin - M .: Hotline – Telecom, 2016.220 p.

5.Ibrahimov, B. G. (2025, November). Research Quality of Communication in Multiservice Telecommunication Networks. In *2025 Intelligent Technologies and Electronic Devices in Vehicle and Road Transport Complex (TIRVED)* (pp. 1-5). IEEE.

6.Ibrahimov, B., & Varlamov, O. (2024). Efficiency analysis of switching converter-modulator. *Synchroinfo Journal*, *10*(2), 12-20.

7. Hashimov E.G. (2026). Research of the efficiency multiservice networks using MIMO technology. *Advanced Information Systems*, *10*(1), 66–71. https://doi.org/10.20998/2522-9052.2026.1.08

8. Ibrahimov B.G. et al. Research and analysis of efficiency indicators of critical infrastructures in the communication system //Advanced Information Systems. – 2024. – Т. 8. – №. 2. – С. 58-64.

9. Ibrahimov B. G., & Hashimov E. G. (2025). Special purpose machine learning and data mining methods. *In* Current directions of development of information and communication technologies and control tools. 2025. Volume 2: sections 2. -p.90.

FEATURES OF APPLYING AN ARTIFICIAL INTELLIGENCE-BASED OPTIMAL MODEL TO ENSURE CYBERSECURITY IN THE CASPIAN SEA AREA

Suleymanov I.I.[1], Kishiev H.T.[1], Huseynov A.G.[1,2], Abdullayeva.A.J.[1]
[1]National Defense University, Baku, Azerbaijan
[2]Baku Engineering University. Baku, Azerbaijan

In the second decade of the 21st century, the rapid digitalization of maritime transportation, along with the intensive integration of port and ship systems with information and communication technologies, has created new opportunities while simultaneously expanding the attack surface for cyber threats. This issue is of particular strategic importance for the Caspian Sea region, as its ports, energy infrastructure, maritime transportation networks, and regional trade routes can become potential targets for various cybercriminal activities. In such a complex and critical infrastructure environment, the application of **artificial intelligence (AI)** has become a crucial component for establishing effective cybersecurity defense mechanisms.

The primary advantage of AI in the maritime domain lies in its capabilities for anomaly detection, real-time threat monitoring, and risk assessment. While traditional security systems operate based on predefined rules, AI-based models analyze large volumes of heterogeneous data to learn global network behavior and accurately identify deviations from normal patterns [1]. Anomaly detection within the system can be performed using both **Automatic Identification System (AIS)** data and other inter-ship traffic analyses, which is essential for the early detection of potential cyberattacks [1].

AI-based models also play a crucial role in the protection of navigation and communication systems. Threats such as GPS signal spoofing, manipulation of AIS data, and cyberattacks on **SCADA (Supervisory Control and Data Acquisition)** systems pose significant risks to real-world maritime operations. AI models can perform contextual analysis of sensor data and automatically detect unusual behavioral patterns, providing timely alerts to defense systems and thereby minimizing the real impact of cyberattacks [1].

An **optimal model** is a mathematical or computer-based model designed to deliver the best possible outcome for a given system or process. Such a model is structured around an objective function, constraints, and a set of variables to minimize existing cyber threats, utilize resources efficiently, and maximize defense capabilities [1, 2]. The implementation of an optimal model is of particular strategic importance for the Caspian Sea region, as this area exhibits high-risk and high-target potential due to its port infrastructure, energy transportation networks, shipping routes, and regional trade connections. Any cybercriminal interference in maritime operations here can have not only economic but also geopolitical and security consequences.

The AI-based optimal model, tailored to the specific conditions of the Caspian Sea region, analyzes large volumes of heterogeneous data in real time. For instance, **AIS data**, ship management systems, SCADA networks, and regional maritime traffic information are monitored and analyzed simultaneously. This approach enables early detection of network anomalies, prediction of potential future attacks, and dynamic optimization of security protocols. Consequently, human intervention is minimized, the real impact of cyberattacks is reduced, and operational continuity in the Caspian Sea region is ensured [1].

The optimal model also ensures the **efficient management of resources**. For example, defense measures for port equipment, server infrastructure, surveillance cameras, and communication systems are automatically prioritized, thereby maximizing protection in high-risk areas while minimizing additional resource allocation in lower-risk zones [2]. Additionally, the model takes regional variations into account: differences in technological levels among ports, the diversity of energy and information infrastructures, and the potential attack risks along regional trade routes are all incorporated into the model's objective function.

The implementation of an optimal model in the Caspian Sea region also lays the groundwork for **future development and adaptation**. AI algorithms continuously learn over time, update their understanding of new attack scenarios, and adapt security measures accordingly. This not only strengthens defenses against cyberattacks but also contributes to the establishment of a sustainable, agile, and reliable maritime cybersecurity environment in the region [1, 3].

Another key approach in AI implementation is the **Zero Trust security model**. In this model, no user or device is considered inherently trustworthy; contextual authentication is required for every request and access, which enhances the security of AI-based systems in accordance with the Zero Trust principle [2].

The application of AI becomes even more powerful when integrated with **digital twin technology**. A digital twin is a virtual replica of real port and ship systems that can simulate all behaviors and states in parallel with the real system. When combined with embedded AI algorithms, digital twins provide a secure environment for simulating attack scenarios, testing vulnerabilities, and detecting performance anomalies and potential threats in advance [3].

Nevertheless, the implementation of AI-based models faces a number of challenges and limitations. The most significant of these is the lack of high-quality, extensive, and specialized datasets. In the Caspian Sea region, the limited availability of data related to maritime operations, port infrastructure, shipping routes, and energy transportation can significantly restrict the learning and adaptation capabilities of AI models. This limitation may adversely affect the system's performance in real-world conditions and delay the timely detection of potential anomalies and cyberattacks [4].

Furthermore, the "black-box" nature of deep learning models makes it difficult to explain their decision-making processes. This characteristic can create **transparency and trust issues** in ensuring the security of critical infrastructure, particularly in ports and ship management systems. For instance, when security

managers and regional regulatory authorities cannot understand why an AI model has identified a particular risk or anomaly, optimizing decision-making and response measures becomes challenging [1].

At the same time, these challenges are further complicated by regional characteristics. Ports in the Caspian Sea exhibit varying technological levels; some rely on older technologies, while others are equipped with modern sensors and communication systems. This heterogeneity makes it difficult for AI models to analyze data harmoniously, thereby necessitating additional adaptation and optimization for the universal and sustainable deployment of the model across the region.

Experts recommend the use of **Explainable AI (XAI)** approaches, **federated learning** technologies, and model interpretation techniques to address these challenges. These approaches not only provide transparency in AI decision-making but also enable the development of security strategies tailored to various ports and ship systems across the region. As a result, the effectiveness and reliability of AI-based optimal models implemented in the Caspian Sea region are enhanced, and the regional cybersecurity level is continuously improved [4, 1].

Another critical factor for the application of AI is the presence of a **regulatory and legal framework** and its alignment with international standards. The adaptation of these frameworks is required for the effective implementation of maritime cybersecurity strategies in the region [5].

In conclusion, the deployment of AI-based optimal models in the Caspian Sea region is of significant importance not only from a technological perspective but also from strategic and operational viewpoints. Such a model can perform real-time threat analysis, anomaly detection, and risk assessment, enabling the early identification of potential cyberattacks in regional port infrastructure, shipping routes, energy transportation, and communication systems.

When the optimal model is combined with a **Zero Trust security framework**, all devices, users, and network connections within a port are individually verified, and contextual authentication is enforced for each access request. This approach ensures operational continuity in Caspian Sea ports and maritime infrastructure, limits the spread of potential attacks, and effectively reduces in-system risks.

Furthermore, the integration of **digital twin technology** provides broader and more adaptive cybersecurity capabilities in the region. Acting as a virtual replica of real port and ship systems, a digital twin simulates all behaviors and states of the system in parallel with the real environment. When combined with AI algorithms, various attack scenarios are analyzed, vulnerabilities are tested, and potential risks are identified in advance. This enables not only reactive defense but also the implementation of **proactive and adaptive security strategies.**

Thus, in the Caspian Sea region, an AI-based optimal model—integrating **real-time threat analysis, anomaly detection, risk assessment, Zero Trust principles, and digital twin technology**—contributes to the creation of a **sustainable, agile, and resilient maritime cybersecurity environment.** This approach ensures the continuity of economic activities, provides strategic advantages for the protection of

energy and transportation infrastructure, and lays the foundation for the development of a long-term, sustainable security policy.

References

1. Miller, T., et al. (2025). Artificial intelligence in maritime cybersecurity: A systematic review of AI-driven threat detection and risk mitigation strategies. Electronics, 14(9), 1844.

2. Nkoro, E.C. et al. (2024). Zero-Trust marine cyberdefense for IoT-based communications: An explainable approach. Electronics, 13(2), 276.

3. Madusanka, N.S. et al. (2023). Digital twin in the maritime domain: A review and emerging trends. Marine Science and Engineering, 11(5), 1021.

4. Prakoso, L. Y., et al. (2025). Artificial intelligence for maritime security resilience. Interdisciplinary Research in Science and Technology.

5. Romanini, D., et al. (2025). From the Baltic to the Mediterranean: A comparative review of cloud-based maritime cybersecurity strategies.

6.Ibrahimov B. et al. Research and analysis of efficiency indicators of critical infrastructures in the communication system //Advanced Information Systems. – 2024. – Т. 8. – №. 2. – С. 58-64.

7. Ibrahimov, B.G., et al. Research throughput multiservice telecommunication networks. *In* Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. 2020. Том1. с.30

8. Гасанов А.Р., Гусейнов А. Г. К использованию особенностей фотоупругого эффекта для решения некоторых радиотехнических задач //Труды международной научной конференции «Актуальные вопросы прикладной физики и энергетики. – 2018. – С. 9-11.

9.Гасанов АР Г. Р. А., Гусейнов А. Г. К использованию особенностей фотоупругого эффекта для решения некоторых радиотехнических задач //Труды международной научной конференции «Актуальные вопросы прикладной физики и энергетики. – 2018. – С. 9-11.

10. Гусейнов А. Г., Сулейманов И. И. Некоторые способы определения общей и принимаемой мощности оптического излучения //Перспективные технологии в средствах передачи информации-ПТСПИ-2019. – 2019. – С. 209-213.

11. Abdullaeva A. J. et al. Analysis of the functioning of an atmospheric acousto-optical locator with an electronic scanner. – 2025.

12. Hashimov E. G. About one method of navigation task solution //АНМС after H. Aliyev. Scientific Review. – 2013. – Т. 1. – №. 20. – С. 45-49.

13. Гашимов Э. Г., Байрамов А. А. Пьезоэлектрических композиты для разработки на их основе приемно-передающих акустических антенн //Евразийский Союз Ученых. – 2015. – №. 5-3 (14). – С. 38-40.

14. Zulfugarov B., et al. Comparative analysis of the efficiency of various energy storages //Modeling, Control and Information Technologies: Proceedings of International scientific and practical conference. – 2023. – №. 6. – С. 42-45.

15. Hashimov E.G. Detection unobserved moving armored vehicles by seismic method //National Security and Military Sciences. – 2015. – Т. 1. – №. 1. – С. 128-132.

16. İbrahimov, B.G. Research and analysis of fiber-optic communication lines based on wave multiplexing technology // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. 2023, Том 2: - pp.4-5.

ISSUES OF ARTIFICIAL INTELLIGENCE IN ENSURING THE CYBERSECURITY OF PORT INFRASTRUCTURE AND SHIP CONTROL SYSTEMS IN MARITIME BASINS

Quliev R.S.[1], Mirzazade N.B.[2], Kishiev H.T.[1], Huseynov A.G.[12],
[1]National Defense University, Baku, Azerbaijan
[2]Baku Engineering University. Baku, Azerbaijan

Modern maritime transport is increasingly based on digital systems. Ports, ships, cargo operations, navigation, communication, and control systems are now interconnected. This accelerates operations and facilitates management. However, it also increases cyber threats. As digitalization in the maritime sector grows, the attack surface expands, and cybersecurity becomes not only a technical issue but also an operational and safety concern [1].

Port infrastructure consists of several key systems. These include terminal management, cargo movement, logistics, surveillance, energy supply, and information exchange. These systems operate as an integrated network. Therefore, a cyber issue in one component can affect other parts as well. Such attacks may disrupt port operations, cause data loss, and even create physical safety risks. Studies indicate that maritime and port infrastructure, as critical infrastructure, is particularly vulnerable [1].

The risk is even more serious in ship control systems, as it is not limited to data alone. Navigation, direction, speed, sensor data, and communication are all linked to these systems. As automation in modern ships increases, the likelihood of cyber interference also rises. Threats such as spoofed signals, unauthorized network access, data manipulation, and interference with control systems are now considered real risks [3].

Such intrusions can be carried out particularly through GPS signal spoofing and the interception of communication channels, which may lead to a vessel being misdirected.

Under such conditions, artificial intelligence plays a crucial role. Traditional security systems often rely on predefined rules. They are more effective at detecting known attacks, but they are not always sufficient against new and evolving threats. Artificial intelligence, however, analyzes large volumes of data, learns normal behavior patterns, and can more quickly detect deviations from them. This capability is particularly important for the maritime sector. Recent studies show that artificial intelligence is effective in anomaly detection and risk assessment [2].

One of the most useful aspects of artificial intelligence is anomaly detection. This means that behaviors deviating from the system's normal operation are automatically identified. For example, unexpected traffic spikes in a port network or unusual activity in a ship's system can be detected at an early stage. This helps prevent attacks in a timely manner [3]. In addition, AI-based systems can integrate data from multiple sources, enabling more comprehensive analysis and the identification of correlated threats.

In ports, artificial intelligence is used not only to detect attacks but also to assess the overall risk landscape. It helps identify which systems are more vulnerable and from which points an attack may originate. This enables decision-makers to make more informed decisions [2]. At the same time, it allows for risk prioritization and more efficient allocation of resources.

In ship control systems, this issue becomes even more critical. If an attack alters navigation or sensor data, it directly turns into a safety problem. Especially in automated systems, cybersecurity and operational safety are closely interconnected [3]. For this reason, improving the cybersecurity awareness and knowledge of crew members and technical personnel is of particular importance.

Another advantage of artificial intelligence is its ability to operate in real time. This allows threats to be detected at an early stage. Deep learning models can detect intrusions in maritime radar networks with high accuracy [4]. In addition, automated response systems can immediately react when a threat is detected, preventing its spread.

However, there are also some challenges. For artificial intelligence systems to function effectively, large volumes of high-quality data are required.

However, in the maritime sector, such datasets are still limited and often do not fully reflect real attack scenarios. This restricts the learning capability of models and may lead to poor performance in practical applications. On the other hand, some artificial intelligence models, especially those based on deep learning, operate as "black boxes." That is, they make decisions, but it is difficult to explain how those decisions are formed. This creates issues of trust and transparency in critical infrastructure sectors.

Moreover, artificial intelligence systems themselves are also vulnerable to cyber threats. For example, training a model with incorrect or intentionally manipulated data (data poisoning) can alter its behavior and weaken security mechanisms. At the same time, adversarial attacks may cause the system to make incorrect decisions, which can lead to serious risks in real-world environments [2].

The human factor is also of particular importance in this context. Operators and engineers must possess not only technical knowledge but also practical cybersecurity skills. Correctly interpreting system alerts and responding in a timely manner plays a decisive role in preventing attacks. If personnel fail to properly understand or act upon these signals, even the most advanced technologies may lose their effectiveness. Therefore, the organization of continuous training programs is essential. In particular, simulation-based training allows the replication of real attack scenarios and enhances personnel's operational decision-making capabilities. In addition, the development and regular updating of standard operating procedures are important to minimize human errors.

In conclusion, technology and the human factor must complement each other; only in this case can an effective and resilient cybersecurity environment be established [1].

Furthermore, international cooperation also plays a significant role. Since maritime transport is inherently global, the exchange of information between

countries and the implementation of common security standards are essential. Standardized approaches can create a more unified and effective defense system for both ports and ships.

In this field, the regulatory and legal framework is also evolving. International organizations are developing cybersecurity recommendations and standards. These standards help port operators and ship owners manage risks in a more systematic manner. At the same time, audits and compliance checks ensure the continuous assessment of security levels [5].

The "Zero Trust" approach is widely applied in modern systems. In this model, no user is considered trustworthy by default. No device is assumed to be secure in advance. Every access request is individually verified, and every action must be explicitly authenticated. The system validates the user's identity, assesses the device's status, considers the origin of the access request, and analyzes other contextual data. This approach differs from traditional models because even the internal network is treated as potentially risky. This is particularly important in complex environments such as ports, where many users operate simultaneously and various systems are interconnected. The model enforces strict access controls, granting only the permissions that are necessary. This principle is known as "least privilege." Such an approach reduces the spread of attacks and limits risks within the system.

Digital twin technology is also important. This technology creates a virtual model of a real system, which replicates its behavior. System performance and behavior can be monitored within this environment, and various scenarios can be tested. Cyberattacks can be simulated in a safe environment without causing damage to the real system. This is a significant advantage. Vulnerabilities can be identified in advance, and risks can be detected earlier. System performance can also be monitored, and anomalies can be observed at early stages. This technology supports decision-making and is particularly useful in complex systems.

Cloud technologies can be widely used in port and ship systems. This approach enhances security [6,7]. Data is stored on remote servers, which provides flexibility and convenience. However, it also introduces new risks, as data becomes dependent on third parties and requires additional protection. Encryption is the primary method used to ensure security. Data is protected both during transmission and while at rest. Multi-factor authentication is also applied, increasing access security. A single password is not sufficient; additional verification is required.

Access control is equally important, with users granted limited permissions. Not everyone can access all resources, as role-based systems are implemented. Continuous monitoring is also carried out, ensuring that the system is constantly observed. Regular audits are conducted, and security policies are updated. All these measures work together to reduce risks and improve overall system reliability.

In the future, the development of quantum computing technologies may also impact cybersecurity. The potential weakening of existing encryption methods will necessitate the development of new security approaches. This may lead to technological transformations in the maritime sector as well. At the same time, more

advanced forms of artificial intelligence are being developed. Explainable AI models will make it possible to better understand the reasoning behind decisions.

This will increase human trust, especially in critical decision-making processes.

Thus, cybersecurity of port infrastructure and ship control systems is one of the key issues in modern maritime transport. Artificial intelligence provides powerful capabilities in this field. It helps in the early detection of attacks and accurate risk assessment. However, its effective use requires both advanced technology and well-trained personnel.

This approach contributes to safer, more resilient, and more reliable maritime systems and will play a fundamental role in shaping the future digital maritime ecosystem [2].

References

1. Alcaide, J. I., & Garcia Llave, R. (2020). Critical infrastructures cybersecurity and the maritime sector. https://doi.org/10.1016/j.trpro.2020.03.058

2. Martínez, F., et al. (2024). Maritime cybersecurity: protecting digital seas. https://doi.org/10.1007/s10207-023-00800-0

3. Lan, D., et al. (2024). Application of Artificial Intelligence Technology in Vulnerability Analysis of Intelligent Ship Network. https://doi.org/10.1007/s44196-024-00539-z

4. Shakil, M. M. N., et al. (2025). A novel deep learning approach for intrusion detection in maritime radar networks. https://doi.org/10.1038/s41598-025-34353-0

5. Kavallieratos, G., et al. (2020). Cybersecurity in Maritime Industry: A systematic survey of modern threats and countermeasures. Marine Science and Engineering, 8(6), 415.

6.Ibrahimov B. et al. Research and analysis of efficiency indicators of critical infrastructures in the communication system //Advanced Information Systems. – 2024. – Т. 8. – №. 2. – С. 58-64.

7. Ibrahimov, B.G., et al. Research throughput multiservice telecommunication networks. *In* Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. 2020. Том1. с.30

8. Гасанов А.Р., Гусейнов А. Г. К использованию особенностей фотоупругого эффекта для решения некоторых радиотехнических задач // Актуальные вопросы прикладной физики и энергетики. – 2018. – С. 9-11.

9.Гасанов АР Г. Р. А., Гусейнов А. Г. К использованию особенностей фотоупругого эффекта для решения некоторых радиотехнических задач //Труды международной научной конференции «Актуальные вопросы прикладной физики и энергетики. – 2018. – С. 9-11.

10. Гусейнов А. Г., Сулейманов И. И. Некоторые способы определения общей и принимаемой мощности оптического излучения //Перспективные технологии в средствах передачи информации-ПТСПИ-2019. – 2019. – С. 209-213.

11. Abdullaeva A. J. et al. Analysis of the functioning of an atmospheric acousto-optical locator with an electronic scanner. – 2025.

12. İbrahimov, B.G. Research and analysis of fiber-optic communication lines based on wave multiplexing technology // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. 2023, Том 2: - pp.4-5.

CYBER RESILIENCE OF MILITARY COMMUNICATION AND COMMAND SYSTEMS UNDER HYBRID ATTACKS

Hasanov A.H.[1], Hashimov E.G.[12], Akhundov R.G.[1]
[1]National Defense University, Baku, Azerbaijan
[2]Azerbaijan Technical University, Baku, Azerbaijan

Introduction

Military communication and command systems are increasingly exposed to hybrid attacks that combine cyber intrusion, electronic interference, disinformation, supply-chain compromise, and attempts to disrupt operational continuity. NATO states that cyber threats to the Alliance are complex, destructive, coercive, and increasingly frequent, while hybrid threats deliberately combine military and non-military methods in order to destabilize and undermine targeted systems and societies. In such conditions, the protection of communication and command networks cannot be reduced to perimeter defense alone. The objective of this study is to determine the principles by which cyber resilience of military communication and command systems can be strengthened under hybrid attack conditions while preserving mission continuity, secure data exchange, and command effectiveness.

Methodology

The research is based on a systems approach, structural-functional analysis, and scenario-based modeling. Military communications and command infrastructures are examined as interconnected operational systems that include users, devices, applications, data flows, network segments, cloud and edge components, and command interfaces. The analytical framework evaluates resilience across five functions: prevention, detection, containment, continuity, and recovery. The study compares traditional perimeter-oriented security with data-centric and zero-trust-oriented models. The working hypothesis states that cyber resilience under hybrid attacks increases when communications, access control, threat correlation, incident response, and operational recovery are integrated into a unified security architecture rather than treated as separate technical tasks. This logic is consistent with current U.S. defense and NSA guidance, which emphasizes that perimeter defenses alone are insufficient and that zero trust requires continuous authentication, authorization, and risk-based security decisions.

The first argument of the study is that the main vulnerability of military communication and command systems lies in their operational interdependence. Modern command effectiveness depends on continuous exchange of trusted data between headquarters, mobile users, sensors, platforms, and supporting digital services. Official DoD guidance emphasizes the need for a seamlessly integrated digital ecosystem in which the right users access the right data at the right time, while protecting confidentiality, integrity, and availability across diverse communication platforms. This means that cyber resilience must be understood not simply as technical hardening of networks, but as preservation of command functionality under attack. If authentication, routing, mission applications, or data integrity fail,

command effectiveness degrades even when parts of the infrastructure remain technically available.

The second argument is that hybrid threats target both the cyber layer and the operational logic of command systems. NATO notes that hybrid attacks combine cyber activities with broader coercive methods designed to blur the line between war and peace and to create uncertainty in the target's perception and response. For military communications, this means that resilience must address not only malware, exploitation, or credential compromise, but also overload, deception, information manipulation, and disruptions that are synchronized with wider operational pressure. As a result, secure communication cannot be treated as an isolated IT task. It must be linked to situational awareness, command discipline, protected fallback procedures, and coordination between military and civil stakeholders. NATO's recent resilience work also stresses consequence management and joint planning between civil and military actors as necessary elements of resilience.

The third argument is that zero trust provides a more appropriate security model for military command systems operating across dispersed and contested environments. The DoD Zero Trust Strategy states that defending networks with increasingly powerful perimeter defenses is no longer sufficient for achieving cyber resiliency, especially where users, systems, and mission partners operate beyond traditional boundaries. Current guidance further identifies reduced attack surface, effective damage containment, rapid recovery, and resilient information enterprise operation as direct benefits of zero trust implementation. In operational terms, this means continuous verification of users and devices, conditional access to mission data, microsegmentation, and prevention of lateral movement after compromise. Such an approach is particularly relevant for command and communication systems because compromise of one enclave, credential set, or application must not be allowed to cascade into theater-wide disruption.

The fourth argument is that resilience depends on detection and correlation quality, not merely on preventive controls. NSA guidance highlights the need to integrate validated threat intelligence, develop correlation rules, use enriched log data and entity behavior, and tune alert logic so that security systems support timely and data-driven decisions. This is especially important for military command networks, where hybrid attacks may unfold gradually through reconnaissance, privilege escalation, anomalous access, and disruption of communications at decisive moments. Therefore, resilience requires a detection layer capable of correlating technical anomalies with operational context. A surge in failed authentications, abnormal data access, routing irregularities, or device behavior may have greater significance in wartime or crisis conditions than in peacetime enterprise settings.

The fifth argument concerns continuity and recovery. DoD budget documents describing Cyber Security Service Provider functions repeatedly stress 24/7 network defense, vulnerability assessment, incident response, situational awareness, and support to network command and control, secure communications, and assured data integrity.

This demonstrates that resilience in practice is maintained by continuous defensive operations rather than by static compliance alone. Under hybrid attack conditions, communication systems must therefore include incident playbooks, segmented fallback modes, restoration priorities for mission-essential services, and predefined procedures for degraded operations.

A resilient military command system is not one that never suffers intrusion, but one that continues to function, contains damage, restores trusted communications quickly, and prevents local compromise from becoming operational paralysis.

Results and Conclusions

The study supports the hypothesis that cyber resilience of military communication and command systems under hybrid attacks increases when security is organized as a unified operational architecture combining zero trust, continuous monitoring, threat correlation, segmented access, incident response, and recovery planning. The analysis shows that perimeter-oriented models are insufficient for modern command environments characterized by distributed users, contested communications, and combined cyber and non-cyber pressure.

The main conclusion is that military cyber resilience should be defined as the capacity of command and communication systems to preserve trusted operation, contain compromise, and restore mission-critical functionality under sustained hybrid attack. The practical significance of the study lies in its applicability to the modernization of military C2 infrastructures, secure communication architectures, doctrinal planning for degraded operations, and the development of technical requirements for next-generation defense information systems.

References

1. Gasimov V. et al. Evaluation of alternative solutions for the effective structure of the cyber security system in critical information infrastructures by the hierarchical analysis method. Advanced Information Systems. 2026, Vol.10, No.2. p.87-99. https://doi.org/10.20998/2522-9052.2026.2.10

2. Akhundov, R. et al. (2026). Conceptual models of multi-level physical protection systems for special-purpose and critical infrastructure facilities. Grail of Science, (61), 591–608. https://doi.org/10.36074/grail-of-science.23.01.2026.066

3. Radovanovic M. et al. Unleashing autonomous forces: Integrating AI-driven drones in modern military strategy //Системи управління, навігації та зв'язку. Збірник наукових праць. – 2024. – Т. 3. – №. 77. – С. 55-69.

4. Rustamov, A. et al. (2025). Application of artificial intelligence in the command and control system of naval forces. Collection of scientific papers «SCIENTIA», (November 7, 2025; Strasbourg, France), 103-111.

5. Valehov, S. A. et al. AI-based efficiency model in university governance. *In* Problems of informatization. 2025. Vol. 1., section 1,2. p.26-28.

6. Dergachov, K. et al. AI based physical and cyber defense for energy grids and transportation systems. *In* Problems of informatization. 2025. Vol. 1., section 1,2. p. 75-78

7. Balayev F.R, et al. Methodology and applications of Aİ enabled image recognition in UAVs *In* Problems of informatization. 2025. Vol. 1., section 1,2. p.102-103

8. Hashimov, E. et al. Research of the efficiency multiservice networks using MIMO technology. *Advanced Information Systems.* 2026. 10(1), 66-71.

9. Kovalev V.A, et al. AI assisted control model for strike UAV swarms *In* Problems of informatization. 2025. Vol. 1., section 1,2. p.108-109

10. Piriyev, H. et al. Optimizing intelligence, surveillance, and assessment in urban environments. Матеріали конференцій МЦНД, (07.11. 2025; Дніпро, Україна), 246-256.

11. Huseynov, M. et al. Integrated application of remote sensing in defense and environmental oversight. In Problems of Informatization. 2025. Vol. 2, p. 114-115.

12. Barbashin, V. K. et al. Enhancement of operational readiness via predictive maintenance and network optimization. *In* Problems of informatization. 2025. Vol. 1., section 1,2. p. 72-74

13. Krikun, V. L. et al. Accelerating decision making and operational efficiency through C4ISR architecture. *In* Problems of informatization. 2025. Vol. 2., section 3,7..p.120-121

14. Maharramov, R. R. et al. Impact of high-frequency electromagnetic fields on UAV swarms and countermeasures. *In* Problems of informatization. 2025. Vol. 2., section 3,7..p.122-123

15. Kartashov, O. S. et al. (2025). Hybrid acoustic seismic approach for the identification of moving targets. *In* Problems of informatization. 2025. Vol. 2., section 3,7..p.118-119

16. Muradov, S. A. et al. (2025). System-level methods for enhancing UAV flight safety and resource efficiency. *In* Problems of informatization. 2025. Vol. 2., section 3,7..p.124-126

17. Javadov, J. M. et al. (2025). Integrating UAV imagery with GIS-based spatial analytics to forecast border risks. *In* Problems of informatization. 2025. Vol. 2., section 3,7..p.116-117

18. Sadiqli, A. B. et al. GIS-based evaluation of road traffic emissions and substantiation of control measures. *In* Problems of Informatization. 2025. (Vol. 4, pp. 101-104).

19. Mashaev E.T. et al. System of systems at war: UAV enabled sensing and strike integration. *In* Problems of informatization. 2025. Vol. 2., section 3,7. p.112-113

20. Petrovski, A. A. et al. A multi criteria AHP framework for hybrid renewable supply in suburban contexts. In Problems of Informatization: Proceedings of the 13th International Scientific and Technical Conference. 2025. (Vol. 4, pp. 97-100).

21. Rustamov, A. R. et al. A systems approach to urban operations for the protection of critical infrastructure and the management of civilian risks. In *Problems of Informatization*. 2025. Vol. 4, pp. 80-82.

22. Sakov, A. A. et al. Policy-oriented technology selection for environmental security assurance. In *Problems of Informatization.* 2025. Vol. 4, pp. 52-54.

23. Muradova E.E., et al. Analytical evaluation of UAV-based logistical operations in contemporary military systems // Актуальні питання розвитку галузей науки: збірник науковихпраць з матеріаламиVIМіжнародної наукової конференції. 2025. p.351-360

24. Elshan, H. et al. (2026). Constrained optimization of an integral security indicator for adaptive management of hazardous facilities. Grail of Science, (62), 1003–1014. https://doi.org/10.36074/grail-of-science.20.02.2026.109

25. Akhundov, R. et al. (2026). Methodological limitations of normative design of physical protection systems for critical and military facilities in a dynamic threat environment // International scientific journal «Grail of Science». 2026. № 62. С. 873–889.

РОЗРОБКА НАВЧАЛЬНОЇ СИСТЕМИ ШИФРУВАННЯ ЗА ДОПОМОГОЮ ШИФРУ «КАЛИНА»

Губка О. С., Губка С. О.
Національний аерокосмічний університет
"Харківський авіаційний інститут", Харків, Україна

У сучасних умовах кібербезпеки вивчення національних стандартів криптографічного захисту є пріоритетним завданням для майбутніх фахівців. Шифр «Калина», що прийшов на зміну застарілому ГОСТ 28147-89 (ДСТУ 28147:2009), є складним для розуміння через свою блочну структуру та специфічні операції.

Створення навчальної системи дозволяє візуалізувати складні математичні процеси та сприяє глибшому засвоєнню матеріалу.

Метою доповіді є розробка програмного забезпечення, яке демонструє роботу алгоритму «Калина» в «покроковому» режимі для освітніх цілей.

Розроблена навчальна система складається з трьох основних модулів:

1. **Теоретичний модуль:** Короткий довідник з математичних основ (поля Галуа, XOR-операції).
2. **Демонстраційний модуль:** Візуалізація стану (State) після кожного перетворення: *AddRoundKey* (додавання раундового ключа); *SubBytes* (таблична заміна); *ShiftRows* (циклічний зсув рядків); *MixColumns* (перемішування стовпців).
3. **Лабораторний модуль:** Можливість самостійного введення ключа та повідомлення з перевіркою проміжних результатів.

Для розробки обрано мову Python завдяки її високій читабельності коду та наявності бібліотек для роботи з двійковими даними. Графічний інтерфейс реалізовано на базі PyQt для забезпечення кросплатформенності.

Розроблена система дозволяє візуалізувати для здобувача процес вивчення алгоритму шифрування. Вона допомагає здобувачам не просто отримати зашифрований результат, а зрозуміти логіку трансформації інформації на кожному етапі, що є критично важливим для аналізу стійкості шифрів.

Система може бути впроваджена в навчальний процес закладів вищої освіти при вивченні дисциплін «Криптографія», «Захист інформації» та аналогічних.

Список літератури

1. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення : **ДСТУ 7624:2014**. — [Чинний від 2015-07-01]. — Київ : Мінекономрозвитку України, 2015. — 105 с. — (Національний стандарт України).

2. Горбенко І. Д. Прикладна криптологія : підручник / І. Д. Горбенко, Ю. І. Горбенко. — 2-ге вид., переробл. та доповн. — Харків : Форт, 2012. — 878 с.

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ЯК ІНСТРУМЕНТУ АУДИТУ ISMS

Нехороших Д.М.
Харківський національний університет радіоелектроніки, Харків, Україна

На сьогоднішній день автоматизація аудиту системи управління інформаційною безпекою (ISMS) – один із найважливіших напрямів розвитку штучного інтелекту (ШІ, AI) в галузі кіберзахисту [1-3]. Раніше ШІ переважно використовувався як допоміжний інструмент для використання окремих завдань. Водночас автоматизація аудиту ISMS тривалий час залишалася складною та фактично неможливою задачею. Однак вектор почав змінюватися із появою великих мовних моделей (LLM) та моделей AI Scient.

Розвиток технологій штучного інтелекту у сфері інформаційної безпеки підтримується міжнародними ініціативами, такими як ISO 42001 AI Management framework, NIST AI Risk Management Framework (2023) та ISO/IEC 38507:2022, які регламентують етичні, правові та управлінські аспекти використання AI. На цьому тлі актуальним є створення AI-аудитора ISMS, який може забезпечити постійний аудит без необхідності людського втручання у рутинні процеси, що особливо важливо для підприємств із обмеженими ресурсами. Одночасно з цим сучасний ландшафт кіберзагроз дедалі більше формується під впливом технологій штучного інтелекту. Як захисники, так і зловмисники використовують AI-технології для автоматизації аналізу, пошуку вразливостей, проведення атак і реагування на інциденти. У цих умовах особливого значення набуває проблема побудови нового інструменту внутрішнього аудиту, здатного забезпечити безперервний моніторинг, динамічну оцінку ризиків, перевірку відповідності стандартам та підтримку прийняття управлінських рішень. На відміну від існуючих рішень, цей інструмент має поєднувати операційний рівень кібербезпеки з процесами управління ризиками та вдосконаленням ISMS у межах циклу PDCA.

Метою доповіді є дослідження підходу AI як інструменту повної автоматизації постійного контролю, оцінки ризиків та аудиту системи управління інформаційною безпекою.

Одним із найважливіших завдань у сфері загального штучного інтелекту є розробка агентів, здатних проводити збір та оцінювати кореляції подій безпеки, виконувати виявлення та реагування на загрози, оцінювати ризики та управління ними, готувати звітність та документування. Хоча наукова спільнота з кіберзахисту досягла значного прогресу в автоматизації окремих компонентів аудиту, система, яка б самостійно керувала всім циклом аудиту системи управління інформаційною безпекою– від створення, впровадження до постійного контролю стану захисту – досі залишається недосяжною [1].

Для вирішення цієї проблеми було представлено в перше модель AI-Аудитора ISMS. Архітектура AI-Аудитора ISMS складається з восьми взаємопов’язаних модулів:

- модуль загального аналізу;
- модуль аналізу контексту;
- модуль інвентаризації активів;
- модуль управління ризиками;
- модуль SOC-моніторингу;
- модуль управління відповідністю;
- модуль зворотного зв'язку (Feedback Loop);
- агенти аудиту.

Кожен із модулів виконує окремі функції і вони інтегровані в процес безперервного внутрішнього аудиту.

З огляду на сучасні тенденції розвитку кіберзагроз і зростання складності інформаційних систем, забезпечення ефективного функціонування систем управління інформаційною безпекою стає дедалі складнішим завданням. Традиційні підходи до внутрішнього аудиту ISMS, що базуються на періодичних перевірках і ручному аналізі, не завжди дозволяють оперативно реагувати на зміни в середовищі загроз. Виклики сучасності, з повязані з використанням AI, вимагають підвищення вимог до постійного внутрішнього аудита, яки має бути динамічним, постійно діючим, що постійно вдосканалює систему, постійно орієнтований на завнішній та внутрішній контекст.

Сучасна проблематика безпеки AI полягає в створені підконтрольної моделі, яка має відповідати не тільки технічним вимогам. Це виклики, пов'язані з стратегічними основами системи управління інформаційною безпекою AI: зрілістю системи управління; прозорістю рішень, організаційною культурою, усвідомленням лідерства. Це відкрита тема, що до якої тільки формуються думки експертів.

Перспективи подальших досліджень пов'язані з практичною реалізацією агентних моделей аудиту, розвитком методів автоматизованого аналізу політик безпеки та використанням компактних AI-моделей, здатних працювати у захищених внутрішніх середовищах організацій. Такі підходи можуть стати основою для створення нових поколінь систем управління інформаційною та кібербезпекою, у яких ШІ виступатиме інтелектуальним інструментом підтримки рішень для фахівців з інформаційної безпеки.

Список літератури

1. Integrating Artificial Intelligence in Audit Workflow: Opportunities, Architecture, and Challenges: A Systematic Review. https://www.preprints.org/manuscript/202601.2060/v1/download?utm_source=chatgpt.com
2. Microsoft Security, "Microsoft raises the bar: a smarter way to measure AI for cybersecurity (ExCyTIn-Bench)," Microsoft Security Blog, 2025.
3. Building Trustworthy AI with ISO/IEC 42001 and the NIST AI Framework https://pecb.com/en/past-webinars/building-trustworthy-ai-with-iso-iec-42001-and-the-nist-ai-framework

ОПТИМІЗАЦІЯ КВАНТОВИХ ЛОГІЧНИХ СХЕМ ДЛЯ ПРИХОВУВАННЯ ІНФОРМАЦІЇ У КВАНТОВИХ ЗОБРАЖЕННЯХ

Головко Є.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Квантові обчислення відкривають нові підходи до захисту інформації, серед яких особливу увагу привертає квантова стеганографія. Вона дозволяє приховувати повідомлення у квантових інформаційних структурах, використовуючи властивості суперпозиції та квантового паралелізму, що робить передачу даних більш прихованою та стійкою до виявлення. Квантові підходи забезпечують значно ширші можливості для обробки великих обсягів інформації одночасно, однак їх практична реалізація безпосередньо залежить від ефективності використання квантових ресурсів. Обмежена кількість кубітів у сучасних квантових системах, а також високий рівень шуму вимагають перегляду принципів побудови квантових алгоритмів і логічних схем, що застосовуються для вбудовування прихованих повідомлень у квантові зображення.

Метою доповіді є дослідження підходів до оптимізації квантових логічних схем, що використовуються у процесах приховування інформації у квантових зображеннях, а також визначення шляхів зменшення обчислювальної складності таких схем шляхом скорочення кількості квантових вентилів, мінімізації CNOT-операцій та зниження глибини квантових кіл. У квантовій стеганографії логічна схема виконує функцію середовища, у якому здійснюється кодування зображення, формування прихованого повідомлення та його інтеграція у контейнерне зображення. Будь-який етап обробки супроводжується використанням квантових вентилів, що змінюють стани кубітів відповідно до заданої логіки алгоритму. Серед усіх операцій особливу роль відіграють двокубітні контрольовані вентилі, зокрема вентиль CNOT Controlled NOT gate, який є базовим елементом реалізації залежних логічних перетворень між кубітами. Практика використання квантових схем показує, що саме CNOT-операції суттєво впливають на складність квантового кола [1]. Це пояснюється тим, що двокубітні операції потребують більшої тривалості виконання та характеризуються вищою ймовірністю виникнення помилок порівняно з однокубітними перетвореннями. В умовах сучасних квантових платформ навіть незначне збільшення кількості таких операцій може призводити до накопичення шуму та зниження точності результатів. Тому оптимізація алгоритмів приховування інформації спрямована на скорочення числа контрольованих логічних переходів. Ефективність квантової стеганографії значною мірою визначається моделлю квантового представлення зображення. У моделі FRQI квантове зображення формується шляхом амплітудного кодування, за якого значення інтенсивності пікселів включаються у параметри квантового стану. Такий підхід забезпечує компактність представлення, однак потребує великої кількості керованих квантових поворотів, що ускладнює побудову логічної схеми. Натомість модель NEQR передбачає безпосереднє двійкове кодування значень

інтенсивності, коли кожен біт представлено окремим кубітом. Саме така структура є більш придатною для реалізації операцій приховування інформації, оскільки дозволяє використовувати стандартні квантові логічні елементи без складної багаторівневої підготовки стану [2]. Під час побудови квантових схем важливим напрямом оптимізації є виявлення надлишкових операцій. У багатьох випадках послідовність квантових вентилів містить операції, що взаємно компенсують одна одну або можуть бути об'єднані без зміни кінцевого результату. Усунення таких елементів дозволяє скоротити довжину квантового кола та зменшити загальне навантаження на систему. Особливо ефективним це є у схемах, де однакові логічні дії виконуються над кількома ділянками зображення. З практичної точки зору доцільно застосовувати блокову організацію квантового зображення, за якої кілька суміжних пікселів розглядаються як єдина логічна структура. У такому випадку одна й та сама контрольована операція може використовуватися для групи елементів, що дозволяє зменшити кількість необхідних квантових переходів. Це не лише скорочує використання кубітів, а й позитивно впливає на загальну швидкодію алгоритму. Окремо слід зазначити значення глибини квантової схеми. Глибина визначає кількість послідовних логічних рівнів, які проходить квантова інформація до завершення обчислення. Чим меншою є глибина, тим вища ймовірність збереження когерентності квантового стану [3].Саме тому сучасні підходи до оптимізації орієнтуються на паралельне виконання незалежних операцій, коли декілька частин квантового зображення обробляються одночасно. Важливо враховувати також архітектурні особливості сучасних квантових платформ, зокрема IBM, де фізична топологія процесора визначає допустимі зв'язки між кубітами. Якщо логічно пов'язані кубіти фізично розташовані на значній відстані, виникає необхідність у додаткових перестановках, що ускладнює схему. Тому оптимізація логічного розміщення кубітів є не менш важливою, ніж оптимізація самих логічних операцій. Таким чином, результати проведеного аналізу підтверджують, що оптимізація квантових логічних схем є необхідною умовою підвищення ефективності квантових стеганографічних систем. Зменшення кількості квантових вентилів, скорочення числа CNOT-операцій та зниження глибини квантових кіл забезпечують підвищення стійкості алгоритмів до шуму, покращують використання обмежених квантових ресурсів і розширюють можливості практичної реалізації алгоритмів приховування інформації.

Список літератури

1. Методи захисту інформації на основі квантової стеганографії зображень / О. Федюшин, Є. Головко, А. Смірнов, В. Сухотеплий, О. Чечуй // Радіотехніка. – 2024. – Вип. 218. – С. 44–55. – DOI: https://doi.org/10.30837/rt.2024.3.218.03

2. Головко Є. В. Методи квантової стеганографії зображень та їх застосування в системах захисту // Проблеми інформатизації: тези доп. тринадцятої міжнар. наук.-техн. конф., 27-28 листопада 2025 р., м. Баку, м. Харків, м. Бельсько-Бяла : [у 4 т.]. Т. 2: секції 3, 7. – Харків: НТУ "ХПІ", 2025. – С. 65-66.

3. Preskill, J. Quantum Computing in the NISQ era and beyond. *arXiv* 2019, arXiv:1801.00862v3.

АНАЛІЗ МЕХАНІЗМІВ БЕЗПЕКИ ZIGBEE В СИСТЕМАХ РОЗУМНОГО БУДИНКУ

Касьяненко С.Ф., Сидоренко З.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Система «розумного будинку» базується на мережі взаємопов'язаних пристроїв, які обмінюються даними для забезпечення автоматизованого та безперебійного керування. У даних IoT системах широко застосовується протокол ZigBee - бездротовий протокол зв'язку, розроблений для мереж з низьким енергоспоживанням і невеликою швидкістю передачі даних.

Попри наявність механізмів захисту, ZigBee має низку слабких місць:

- перехоплення ключа мережі (особливо під час приєднання пристрою);
- Replay-атаки при неправильній реалізації лічильників;
- атаки типу "Man-in-the-Middle";
- використання стандартних (default) ключів;
- фізичний доступ до пристроїв (витяг ключів із пам'яті).

Однією з ключових загроз у таких системах є атака типу «людина посередині» (Man-in-the-Middle), під час якої зловмисник може перехоплювати передані дані, отримувати несанкціонований доступ до пристроїв або навіть встановлювати контроль над центральним вузлом керування. Для ефективного захисту від подібних атак необхідно впроваджувати комплексні заходи безпеки, що включають надійний контроль доступу, використання криптографічного шифрування даних та механізми перевірки їх цілісності. Такі підходи дозволяють мінімізувати ризики несанкціонованого втручання та забезпечити безпечне функціонування системи [1].

Метою доповіді є аналіз механізмів захисту від MitM-атак у системах «розумного будинку» на прикладі технології ZigBee.

Технологія ZigBee забезпечує надійну передачу даних у мережі завдяки механізмам маршрутизації. Якщо пряме з'єднання з пристроєм відсутнє, дані передаються альтернативними шляхами через інші вузли мережі, доки не досягнуть кінцевого отримувача. Це підвищує стійкість системи до збоїв і забезпечує безперервність обміну інформацією. Архітектура ZigBee має багаторівневу будову і включає чотири основні рівні прикладний, мережевий, рівень керування доступом до середовища MAC та фізичний рівень. Кожен із цих рівнів виконує окремі функції, що забезпечують організацію передавання даних, керування мережею та фізичну взаємодію пристроїв. Такий підхід дозволяє досягти ефективної роботи мережі, її гнучкості та надійності [2].

Основними рівнями, на яких реалізуються механізми безпеки в ZigBee, є рівень керування доступом до середовища (MAC) та мережевий рівень. У межах цієї технології передбачено три базові механізми захисту контроль доступу, який здійснюється через авторизацію пристроїв, шифрування даних, що забезпечує їх доступність лише для уповноважених користувачів, а також

контроль цілісності, який реалізується за допомогою використання мережевого ключа.

Водночас технологія має певні обмеження [4]. Зокрема, призначений мережевий ключ не підлягає зміні, що може створювати потенційні ризики для безпеки системи. ZigBee є вразливим до MitM-атак через: бездротову природу передачі даних; обмежені ресурси пристроїв (спрощені механізми безпеки); складність централізованого управління в mesh-мережах.

Механізми захисту ZigBee забезпечують базовий рівень протидії Man-in-the-Middle attack, однак їх ефективність значною мірою залежить від правильної реалізації та конфігурації засобів захисту. Найбільш критичним аспектом є безпечне управління ключами та процес приєднання пристроїв до мережі.

У зв'язку з цим використання ZigBee у системах «розумного будинку» потребує додаткового посилення захисту. Доцільним є впровадження механізмів регулярної ротації ключів, використання багатофакторної автентифікації та застосування захищених протоколів передавання даних, що дозволяє підвищити загальний рівень безпеки мережі.

Отже, системи «розумного будинку» є вразливими до атак типу «людина посередині», що може призвести до перехоплення даних і несанкціонованого контролю над пристроями.

Використання технології ZigBee забезпечує надійну передачу інформації та базові механізми захисту, зокрема контроль доступу, шифрування та перевірку цілісності даних [5].

Водночас наявні обмеження, такі як неможливість зміни мережевого ключа, знижують загальний рівень безпеки. Тому для ефективного захисту системи необхідне впровадження додаткових заходів, зокрема ротації ключів, багатофакторної автентифікації та використання захищених протоколів обміну даними. Це дозволяє підвищити стійкість мережі до атак і забезпечити її надійне та безпечне функціонування.

Список літератури

1. Бабич, М.Г., Городецький, С.Л. (2025). Архітектура системи розумного будинку для людей з інвалідністю // Збірник наукових праць за матеріалами XI Всеукраїнської наук.-практ. конф. «Електронні та мехатронні системи: теорія, інновації, практика», 18 грудня, 2025 р. / Національний університет «Полтавська політехніка імені Юрія Кондратюка». – Полтава, 10.

2. Zillner, T., & Strobl, S. (2015). ZigBee exploited: The good, the bad and the ugly. Black Hat–2015. Available online: https://www. blackhat. com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly. pdf (accessed on 21 March 2018).

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

4. Zohourian, A., Dadkhah, S., Neto, E. C. P., Mahdikhani, H., Danso, P. K., Molyneaux, H., & Ghorbani, A. A. (2023). IoT Zigbee device security: A comprehensive review. Internet of Things, 22, 100791.

АНАЛІЗ ВРАЗЛИВОСТЕЙ КОМПОНЕНТА WEBVIEW У МОБІЛЬНИХ ДОДАТКАХ ANDROID ТА МЕТОДИ ЇХ УСУНЕННЯ

Іванов Є.В., Сидоренко З.М.
Харківський національний університет радіоелектроніки, Харків, Україна

WebView – це масштабний програмний компонент, що дозволяє використовувати веб-контент у додатках [1]. У сучасній розробці на платформі Android компонент WebView набув надзвичайної популярності завдяки своїй здатності значно оптимізувати процес створення програмного забезпечення. Саме тому у деяких випадках уся функціональність додатка реалізована через веб-браузер.

Однак, оскільки WebView функціонує як своєрідний міст між зовнішнім веб-середовищем та внутрішніми нативними API операційної системи, він суттєво розширює поверхню атаки та стає привабливим для зловмисників. Аналіз вразливостей WebView та своєчасне застосування методів їх усунення здатні суттєво зменшити такі ризики, як: несанкціонований доступ до локальних файлів, витік сесійних даних через XSS, обхід механізмів пісочниці, а також віддалене виконання коду шляхом експлуатації небезпечних JavaScript-інтерфейсів [2].

Метою доповіді є дослідження вразливостей, що виникають при використанні компонента WebView в додатках на платформі Android, аналіз векторів атак на них та надання рекомендацій щодо їх усунення для підвищення загального рівня безпеки мобільного програмного забезпечення.

Головна причина виникнення вразливостей полягає у некоректній конфігурації класу WebSettings, який за замовчуванням може надавати надмірні привілеї в залежності від рівня API.

Найбільш критичним вектором атаки є зловживання мостом між JavaScript та нативним кодом Android. Використання методу addJavascriptInterface() дозволяє веб-сторінці викликати Java методи додатку. Якщо у конфігурації WebView дозволено виконання JavaScript коду завдяки методу setJavaScriptEnabled(enabled), то зловмисник може посилити вразливість від XSS до RCE.

Іншим поширеним вектором є експлуатація доступу до локальної файлової системи.

Якщо розробник залишає увімкненими параметри доступу до файлів через схему file://, або до контент провайдерів через схему content://, зловмисник може використати Universal XSS або символічні посилання для читання конфіденційних файлів додатку, до яких належать бази даних SQLite, файли SharedPreferences або токени сесій, що зберігаються в ізольованому середовищі.

Для підвищення стійкості мобільних додатків та усунення вразливостей компонента WebView необхідно імплементувати наступні елементи захисту на рівні конфігурації [3, 4].

1. Необхідно заборонити несанкціонований доступу до WebView з боку інших додатків на пристрої. Якщо Activity, що містить WebView, не передбачає виклику ззовні, її необхідно жорстко ізолювати, встановивши атрибут android:exported="false" у файлі маніфесту.

2. Вимкнути доступ до контент провайдерів, викликавши WebSettings.setGeolocationEnabled(false).

3. Вимкнути доступ до файлів, викликавши WebSettings.setAllowFileAccess(false), якщо minSdkVersion дорівнює 29 або менше.

4. Вимкнути доступ до файлів за URL-адресами, викликавши WebSettings.setAllowFileAccessFromFileURLs(false), якщо minSdkVersion дорівнює 15 або менше.

5. Заборонити універсальний доступ до файлів за URL-адресами, викликавши WebSettings.setAllowUniversalAccessFromFileURLs(false), якщо minSdkVersion дорівнює 15 або менше.

6. Якщо у WebView завантажуються зовнішні посилання, необхідно обов'язково перевірити, чи правильно завантажено джерело, – перевіривши як схему, так і ім'я хоста.

7. В усіх випадках, коли JavaScript викликається з даними, отриманими ззовні, необхідно переконатися, що вони пройшли санитизацію.

На основі цих принципів розробники можуть побудувати безпечне середовище для відображення веб-контенту, що дозволить мінімізувати поверхню атаки та захистити конфіденційні дані користувачів.

На основі цих досліджень можна стверджувати, що суворе дотримання принципу найменших привілеїв при конфігурації WebSettings та надійна ізоляція компонента від зовнішніх IPC-викликів (Intent) суттєво підвищують стійкість мобільних додатків на платформі Android.

У сукупності з ретельною валідацією вхідних даних це значно ускладнює експлуатацію вразливостей навіть для кваліфікованих зловмисників, що знижує ризик витоку конфіденційної інформації та компрометації сесій користувачів.

Список літератури

1. Contributors to Wikimedia projects. WebView - wikipedia. *Wikipedia, the free encyclopedia.* URL: https://en.wikipedia.org/wiki/WebView (дата звернення: 01.04.2026)/

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

3. Android security checklist: WebView. *News, Techniques & Guides.* URL: https://blog.oversecured.com/Android-security-checklist-webview#recommendations (дата звернення: 02.04.2026).

4. Mobile application security weakness enumeration (MASWE) - OWASP mobile application security. *OWASP Mobile Application Security - OWASP Mobile Application Security.* URL: https://mas.owasp.org/MASWE/ (дата звернення: 01.04.2026).

ВПЛИВ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ НА ЕФЕКТИВНІСТЬ МОДЕЛЕЙ РОЗПІЗНАВАННЯ ФІШИНГОВИХ ЛИСТІВ

Леонова А.О., Сидоренко З.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні фішингові атаки значно змінилися через появу генеративного штучного інтелекту (Gen-AI). Завдяки Gen-AI зловмисники можуть автоматично створювати велику кількість різних повідомлень, які виглядають природно, написані без помилок і добре підлаштовані під конкретну ситуацію. Через це такі повідомлення стають більш переконливими й їх складніше розпізнати як шахрайські. Раніше фішингові листи часто можна було впізнати за помилками або дивною мовою. Тепер же, завдяки великим мовним моделям (LLM), такі повідомлення виглядають майже так само, як звичайне офіційне листування, і їх набагато складніше відрізнити від справжніх. Через це виникло своєрідне технологічне протистояння, у якому ті самі інструменти використовуються і для захисту, і для здійснення атак. У результаті традиційні методи виявлення фішингу стають менш ефективними, що потребує їх переоцінки та вдосконалення [1]. Попри це, фішинг залишається однією з найпоширеніших кіберзагроз, що підтверджує необхідність подальших досліджень у цій сфері [2].

Метою доповіді є аналіз впливу генеративного штучного інтелекту на ефективність сучасних моделей виявлення фішингових повідомлень, а також визначення перспективних методик підвищення їх стійкості з огляду на нові типи атак.

Традиційно фішингові листи виявляють за допомогою методів машинного та глибокого навчання. Сучасні моделі на основі трансформерів, такі як BERT і RoBERTa, показують дуже високу точність, приблизно 98,9–99,1% на стандартних наборах даних [3]. Це пов’язано з тим, що вони добре розуміють контекст тексту і можуть знаходити складні смислові зв’язки, наприклад ознаки терміновості, маніпуляції або спроби видати себе за надійне джерело.

Аналіз досліджень показує, що моделі глибокого навчання значно ефективніші за класичні алгоритми, оскільки вони самі визначають важливі ознаки та здатні працювати з неструктурованими даними [2]. Отже, на сьогодні саме моделі глибокого навчання є більш результативним підходом для виявлення фішингових листів.

Водночас поява Gen-AI значно ускладнила виявлення фішингових повідомлень. Дослідження показують, що навіть невелике перефразування таких повідомлень за допомогою LLM може помітно знизити точність традиційних методів їх виявлення [1]. Це пояснюється тим, що генеративні моделі прибирають типові ознаки фішингу, наприклад, граматичні помилки чи неприродні мовні конструкції, на яких раніше часто базувалося навчання моделей. У результаті системи, які показували дуже високі результати на класичних наборах даних, працюють значно гірше в реальних умовах. Це

призводить до так званої «ілюзії безпеки», коли модель здається точною, але насправді не враховує сучасні загрози, створені за допомогою штучного інтелекту [2]. Класичні моделі машинного та глибокого навчання залишаються швидкими та стабільними, проте вони обмежені у здатності розпізнавати складні контекстуальні маніпуляції та визначати справжній намір повідомлення.

Сучасні великі мовні моделі, особливо квантовані середньорозмірні, краще справляються з аналізом змісту тексту та можуть виявляти приховані стратегії соціальної інженерії [1]. Однією з їхніх важливих переваг є здатність пояснювати, чому було прийнято те чи інше рішення, що підвищує довіру до систем виявлення та робить їх більш корисними на практиці. Разом із тим, їхня точність поки що трохи нижча, ніж у спеціалізованих моделей глибокого навчання, тому для ефективного застосування потрібна додаткова інтеграція з іншими методами.

Одним із перспективних напрямів є застосування квантованих великих мовних моделей (LLM), які забезпечують оптимальний баланс між продуктивністю та обчислювальними витратами [1]. Такі моделі краще адаптуються до нових видів атак і можуть проводити більш глибокий аналіз контексту повідомлень. Також великі можливості дають гібридні підходи, що поєднують високу точність моделей глибокого навчання з пояснювальними властивостями LLM. Не менш важливим є оновлення навчальних наборів даних із додаванням прикладів, згенерованих штучним інтелектом, що дозволяє робити оцінку моделей більш реалістичною та підвищує їх стійкість до сучасних загроз [2, 3].

Генеративний штучний інтелект змінює сам підхід до виявлення фішингу. Якщо раніше це була відносно проста задача визначити, чи є повідомлення шкідливим чи ні, то тепер усе складніше. Сучасні системи повинні не просто класифікувати повідомлення, а аналізувати його зміст, розуміти контекст і намагатися визначити справжній намір. Тобто йдеться вже не тільки про перевірку ознак, а про глибше розуміння сенсу повідомлення. Незважаючи на високі показники сучасних моделей глибокого навчання, їх ефективність знижується у разі використання LLM для генерації атак. Це свідчить про необхідність розробки адаптивних, комбінованих і пояснюваних систем, здатних враховувати контекст, протистояти перефразуванню та працювати з актуальними даними.

Список літератури

1. Thakur K., Ali M. L., Obaidat M. A., Kamruzzaman A. A Systematic Review on Deep-Learning-Based Phishing Email Detection. Electronics. 2023. Vol. 12, No. 21. Art. No. 4545. DOI: https://doi.org/10.3390/electronics12214545.

2. Thapa J., Chahal G., Gabreanu Ș. V., Otoum Y. Phishing Detection in the Gen-AI Era: Quantized LLMs vs Classical Models. arXiv preprint. 2025. arXiv:2507.07406v1. URL: https://arxiv.org/abs/2507.07406v1.

3. Alhuzali A., Alloqmani A., Aljabri M., Alharbi F. In-Depth Analysis of Phishing Email Detection: Evaluating the Performance of Machine Learning and Deep Learning Models Across Multiple Datasets. Applied Sciences. 2025. Vol. 15, No. 6. Art. No. 3396. DOI: https://doi.org/10.3390/app15063396.

ПРОБЛЕМИ ТА РИЗИКИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ

Бабич М.Г.
Харківський радіотехнічний фаховий коледж, Харків, Україна
Городецький С.Л.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному цифровому середовищі кібербезпека є ключовою умовою функціонування держави, бізнесу та суспільства. Зростання кількості кіберзагроз сприяло впровадженню в цю сферу штучного інтелекту (ШІ), який дозволяє автоматизувати виявлення атак, аналізувати великі обсяги даних і ефективно ідентифікувати потенційні ризики. Водночас використання ШІ супроводжується появою нових проблем, його вразливістю, можливістю зловживання та моральними викликами, що зумовлює необхідність наукового аналізу цих аспектів.

Метою доповіді є аналіз основних проблем і ризиків, пов'язаних із використанням ШІ у сфері кібербезпеки, а також обґрунтування доцільності його застосування з урахуванням сучасних викликів і загроз цифрового середовища. Однією з головних проблем систем ШІ є те, що вони можуть помилятися. Якщо в них потрапляють неправильні або неповні дані, вони можуть зробити хибний висновок і не помітити загрозу або, навпаки, помилково вважати безпечні дії небезпечними. Ще одна важлива проблема полягає в тому, що багато систем ШІ працюють як «чорна скринька», це означає, що навіть фахівці не завжди можуть пояснити, чому система прийняла те чи інше рішення. У кібербезпеці це дуже важливо, адже потрібно розуміти, як саме було виявлено загрозу. Серйозним ризиком є те, що штучний інтелект можуть використовувати не лише для захисту, а й для атак. Хакери можуть застосовувати ШІ для створення складних вірусів, автоматичних атак або обману користувачів. Це робить кіберзагрози більш небезпечними і масштабними. Традиційні методи захисту, зокрема сигнатурний аналіз, вже не завжди є ефективними через можливість модифікації шкідливого коду, тому використання ШІ стає необхідним для більш гнучкого та інтелектуального виявлення загроз [1]. Важливим викликом у використанні ШІ в кібербезпеці є проблема надмірної довіри до автоматизованих рішень. У разі, коли фахівці повністю покладаються на результати роботи ШІ, існує ризик втрати контролю над ситуацією, оскільки помилки алгоритмів можуть призводити до серйозних наслідків для інформаційної безпеки. Особливо це проявляється в умовах, коли система генерує велику кількість автоматичних сповіщень, що здатне перевантажувати спеціалістів із кібербезпеки та ускладнювати своєчасне реагування на реальні загрози [2]. Додатковою проблемою є те, що системи штучного інтелекту працюють із великими обсягами інформації, серед якої можуть міститися конфіденційні дані. Це створює ризик їх витоку та зумовлює необхідність забезпечення належного захисту інформаційних ресурсів на всіх етапах функціонування таких систем.

Суттєві складнощі завдає також потреба у великих обсягах якісних даних для навчання моделей, значні фінансові витрати на впровадження, підтримку

та постійне оновлення інтелектуальних систем, а також складність інтерпретації результатів, отриманих за допомогою алгоритмів ШІ.

Окрему загрозу становить можливість обходу систем захисту шляхом обфускації даних, коли зловмисники змінюють структуру інформації таким чином, щоб приховати шкідливу активність від алгоритмів аналізу [3]. У зв'язку з цим доцільним є комбіноване використання різних технологій захисту, що дозволяє підвищити стійкість систем до складних і нетипових кіберзагроз. Сучасні моделі ШІ, такі як ChatGPT та GitHub Copilot, здатні автоматично генерувати значну частину програмного коду. Це підвищує продуктивність розробників, але ускладнює визначення, чи створений код людиною чи ШІ. Код, згенерований ШІ, відзначається структурною одноманітністю, типовими назвами змінних і передбачуваною синтаксичною структурою, тоді як людський код має індивідуальний стиль та непослідовні відступи. Відмінності поступово зникають із розвитком технологій, що ускладнює контроль і потребує впровадження цифрових підписів або водяних знаків для підтвердження людського авторства [3]. Попри всі ризики, використання штучного інтелекту в кібербезпеці є необхідним. Сучасні загрози настільки складні та швидкі, що без автоматизації їх важко виявити. ШІ допомагає економити час, підвищує ефективність захисту та дозволяє працювати з великими обсягами інформації. ШІ значно прискорює процес виявлення шкідливої активності порівняно з традиційними підходами та підвищує ефективність аналізу великої кількості подій інформаційної безпеки. Однак найкращий результат досягається тоді, коли ШІ використовується разом із людським контролем, а не замість нього, бо навіть найсучасніші системи штучного інтелекту не можуть повністю замінити фахівців з кібербезпеки, оскільки потребують налаштування, контролю та адаптації до конкретних умов.

Отже, штучний інтелект у кібербезпеці має як переваги, так і значні ризики. Основні проблеми пов'язані з помилками в даних, складністю роботи алгоритмів, можливістю зловживання та залежністю від автоматизації. Для зменшення ризиків важливо контролювати якість даних, перевіряти роботу систем і не відмовлятися від участі людини в процесах безпеки. У майбутньому роль штучного інтелекту буде лише зростати, тому важливо навчитися використовувати його відповідально та безпечно.

Список літератури

1. Постіл, С. Д., Любушкін, Д. (2025). Впровадження штучного інтелекту у кібербезпеці. Збірка праць XIX Міжнародної наукової конференції «Наука та освіта», 15–22 січня 2025 р., м. Хайдусобосло, Угорщина. – Хмельницький: ХНУ. С. 14-18.

2. Оніщенко Є., Мальцев В. Застосування штучного інтелекту в кібербезпеці // Theoretical and Applied Cybersecurity: Матеріали III Всеукраїнської наук.-практ. конф. (TACS-2025), [Київ], 29 травня 2025 р. - Київ, 2025. - С. 313-314.

3. Бабич М. Г. Цемма Д.О. Розпізнавання програмного коду, створеного штучним інтелектом // Проблеми інформатизації: тези доп. тринадцятої міжнар. наук.-техн. конф., 27-28 листопада 2025 р., м. Баку, м. Харків, м. Бельсько-Бяла : [у 4 т.]. Т. 3: секції 4. – Харків : НТУ "ХПІ", 2025. – С. 46.

МЕТОДИ ПОШУКУ ВРАЗЛИВОСТЕЙ WEB-РЕСУРСІВ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Цемма Д.О., Городецький С.Л.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні WEB-ресурси є невід'ємною складовою цифрової інфраструктури та часто стають об'єктами кібератак. Зростання складності веб-додатків, використання API та мікросервісної архітектури підвищує ризик виникнення вразливостей. У зв'язку з цим актуальним є застосування методів штучного інтелекту (ШІ) та машинного навчання для автоматизації процесів виявлення загроз [1, 2]. **Метою доповіді** є аналіз методів пошуку вразливостей WEB-ресурсів із використанням ШІ та оцінка ефективності їх застосування у сучасних системах кібербезпеки. Основними типами вразливостей веб-додатків залишаються SQL-ін'єкції, XSS, CSRF та інші атаки, що пов'язані з некоректною обробкою даних. В умовах постійного ускладнення атак традиційні методи, засновані на сигнатурному аналізі, стають менш ефективними. Методи машинного навчання дозволяють виявляти аномалії та нові типи атак за рахунок аналізу поведінкових характеристик систем. У сучасних дослідженнях розглядається застосування ШІ для автоматизації тестування на проникнення, що дозволяє значно зменшити участь людини у процесі пошуку вразливостей. Зокрема, використання алгоритмів класифікації та нейронних мереж дозволяє ефективно аналізувати мережевий трафік та поведінку веб-додатків. Крім того, перспективним напрямком є використання інтелектуальних систем для генерації тестових сценаріїв та fuzzing-тестування. Такі системи здатні адаптуватися до структури додатка та знаходити складні логічні помилки, які важко виявити традиційними методами [3].

Дослідження також показують ефективність гібридних підходів, які поєднують класичні методи кібербезпеки з алгоритмами машинного навчання. Це дозволяє підвищити точність виявлення атак, зокрема у випадках zero-day вразливостей та складних багатокрокових атак [3]. Водночас використання ШІ має певні обмеження, зокрема залежність від якості навчальних даних, складність інтерпретації результатів та можливість помилкових спрацювань.

Таким чином, використання методів штучного інтелекту є перспективним напрямком розвитку систем кібербезпеки WEB-ресурсів, що дозволяє автоматизувати процес пошуку вразливостей та підвищити ефективність захисту інформаційних систем.

Список літератури

1. Іваніченко Є., Сабліна М., Кравчук К. Використання машинного навчання в кібербезпеці. Кібербезпека: освіта, наука, техніка. 2021. DOI: https://doi.org/10.28925/2663-4023.2021.12.132142
2. Кавецький, М. С., Сєвєрінов, О. В., Гвоздьов, Р. Ю., Смірнов, А. О. (2024). Використання машинного навчання для класифікації атак типу DOS/DDOS.
3. Савчук К. Гібридні стратегії кібербезпеки для веб-додатків з використанням штучного інтелекту. Кібербезпека: освіта, наука, техніка. 2025. DOI: https://doi.org/10.28925/2663-4023.2025.31.969

ПОРІВНЯЛЬНИЙ АНАЛІЗ КОМУТАТИВНИХ І НЕКОМУТАТИВНИХ КРИПТОГРАФІЧНИХ МОДЕЛЕЙ

Фроленко В.О.
Харківський національний університет радіоелектроніки, Харків, Україна
Сухотеплий В.М.
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна

Безпека цифрових даних та транзакцій є ключовою умовою розвитку сучасних інформаційних технологій. Традиційні криптографічні методи засновані на комутативних групах і довели свою ефективність, проте розвиток квантових обчислень ставить під сумнів їхню довгострокову стійкість. За таких умов зростає значення некомутативних криптографічних моделей, які пропонують нові можливості для анонімності та постквантової безпеки.

Метою доповіді є порівняльний аналіз комутативних і некомутативних криптографічних моделей та оцінка їх доцільності для сучасних і постквантових цифрових систем.

Комутативні криптографічні моделі ґрунтуються на структурах, де порядок виконання операцій не впливає на результат. Вони включають модульну арифметику, що використовується у RSA та ElGamal, і еліптичні криві, застосовані в ECDSA та EdDSA. Основною перевагою таких моделей є швидкодія, відносно невеликий розмір ключів і простота реалізації алгоритмів перевірки. Ці характеристики роблять комутативні моделі оптимальними для масового використання у сучасних системах. Водночас розвиток квантових алгоритмів, таких як алгоритм Шора, ставить під загрозу їхню стійкість, оскільки ці алгоритми здатні ефективно розв’язувати задачі дискретного логарифма та факторизації великих чисел, на яких базується безпека комутативних схем [1, 2]. Таким чином, хоча комутативні моделі залишаються швидкими та практичними, їхня криптографічна надійність у перспективі може знижуватися.

Некомутаційні моделі базуються на структурах, де порядок виконання операцій критично важливий, що створює додатковий рівень обчислювальної складності [3, 4]. До таких структур належать групи кіс, матричні групи над некомутативними кільцями та групи перетворень із некомутативними операціями. Складність вирішення пов’язаних задач, таких як задача спряження або декомпозиції, забезпечує високий рівень стійкості до атак, включаючи потенційні квантові. Некомутативні моделі дозволяють реалізовувати анонімні цифрові підписи, що важливо для захисту приватності користувачів у блокчейн-мережах та системах електронного голосування.

Перевага некомутативних моделей полягає не лише у стійкості до квантових атак, але й у здатності забезпечити анонімність підписантів у схемах кільцевих або групових підписів. Така анонімність стає критичною у фінансових системах і децентралізованих платформах, де конфіденційність користувачів є ключовою вимогою. Водночас недоліком таких моделей є

більша обчислювальна складність, що може обмежувати швидкодію та збільшувати витрати на формування і перевірку підписів. Для практичного застосування важливо оптимізувати алгоритми обчислення групових операцій і зменшити обсяг даних, що передаються, без втрати криптографічної стійкості.

Порівняння показує, що комутативні моделі залишаються ефективними для задач, де пріоритетом є швидкодія та простота реалізації, тоді як некомутативні моделі забезпечують вищий рівень безпеки та анонімності. У сучасних блокчейн-системах доцільно застосовувати некомутативні підходи, особливо у тих випадках, коли важлива захищеність даних від майбутніх квантових обчислень та конфіденційність користувачів.

Подальший розвиток полягає у пошуку ефективних представлень груп і оптимізації обчислювальних алгоритмів, що дозволить інтегрувати некомутативні моделі у великі децентралізовані мережі без значних втрат у продуктивності [5].

Порівняльний аналіз комутативних і некомутативних криптографічних моделей показує, що обидва підходи мають свої переваги та обмеження. Комутативні моделі залишаються швидкими та простими у реалізації, але їхня довгострокова безпека під питанням через розвиток квантових обчислень. Некомутативні моделі забезпечують підвищену стійкість і анонімність, що робить їх перспективними для постквантових систем і блокчейн-платформ. Оптимізація алгоритмів і гібридні підходи дозволять поєднувати ефективність та безпеку, формуючи основу для нового покоління криптографічних механізмів у цифрових інфраструктурах.

Список літератури

1. Khalimov, G., Sievierinov, O., Khalimova, S., Kotukh, Y., Chang, S. Y., & Balytskyi, Y. (2021, October). Encryption Based on the Group of the Hermitian Function Field and Homomorphic Encryption. In 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T) (pp. 465-469). IEEE.

2. Kotukh, E. V., Severinov, O. V., Vlasov, A. V., Kozina, L. S., Tenytska, A. O., & Zarudna, E. O. (2021). Методи побудови та властивості логарифмічних підписів. Radiotekhnika, (205), 94-99.

3. Поддубний В. О. Методи електронного підпису на основі некомутативних груп / В. О. Поддубний, Р. Ю. Гвоздьов, О. В. Сєвєрінов // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : матеріали дванадцятої міжнар. НПК, 27-28 квітня 2022 р. – Баку – Харків – Жиліна, 2022. – С. 149.

4. Гвоздьов, Р.Ю., Сєвєрінов, О.В. (2022). Метод шифрування на основі багатопараметричних груп // Проблеми інформатизації: десята міжнародна науково-технічна конференція, 24 – 25 листопада 2022 року, Том 1. - Черкаси – Баку – Бельсько-Бяла – Харків – 2022.

5. Фроленко В.О. Кільцеві підписи у блокчейн системах на основі некомутативних груп / В. О. Фроленко // Проблеми інформатизації: тези доп. тринадцятої міжнар. наук.-техн. конф., 27-28 листопада 2025 р., м. Баку, м. Харків, м. Бельсько-Бяла: [у 4 т.]. Т. 2 : секції 3, 7 – Харків : НТУ "ХПІ", 2025. – С. 54-55.

ОПТИМІЗАЦІЯ ПАКЕТНИХ ГОМОМОРФНИХ СХЕМ ДЛЯ ОБРОБКИ ВЕЛИКИХ МАСИВІВ ДАНИХ

Гущин Б.-Д.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні системи працюють з великими обсягами конфіденційних даних, і традиційне шифрування вимагає розшифрування перед обчисленнями, що підвищує ризик компрометації інформації. Повністю гомоморфне шифрування дозволяє виконувати обчислення над зашифрованими даними, зберігаючи їх конфіденційність. Попри це, практичне застосування таких схем обмежене високою обчислювальною складністю та великим розміром шифротекстів. Використання пакетних схем, де один шифротекст містить кілька повідомлень і операції виконуються одночасно, дозволяє значно підвищити ефективність гомоморфних обчислень.

Метою доповіді є дослідження способів оптимізації пакетних гомоморфних схем для роботи з великими масивами даних, зменшення обчислювальних витрат та підвищення ефективності криптографічних операцій.

Пакетні гомоморфні схеми забезпечують одночасну обробку декількох повідомлень у межах одного шифротексту. Кожен шифротекст представляється у вигляді матриці, елементами якої є поліноми над кільцем. Таке подання дозволяє виконувати арифметичні та логічні операції одночасно над усіма елементами матриці, значно зменшуючи кількість обчислень і витрати обчислювальних ресурсів.

Важливою особливістю є можливість перестановки слотів у матриці без розшифрування, що надає гнучкість у побудові складних обчислювальних алгоритмів та дозволяє ефективно реалізовувати паралельні операції.

Матричні поліноми також дозволяють більш рівномірно розподіляти шум, який накопичується під час послідовних гомоморфних операцій, що підвищує допустиму глибину обчислень без необхідності частого виконання bootstrap-перетворень [1]. Завдяки оптимальному розміщенню повідомлень у слотах матриці, можна забезпечити баланс між швидкістю обчислень та криптографічною стійкістю, що особливо важливо при роботі з великими масивами даних.

Сучасні дослідження показують, що вибір структурованих матричних поліномів і спеціальних алгоритмів кодування може ще більше підвищити ефективність пакетних схем. Оптимізація включає не тільки розмір пакетів, а й підбір параметрів кілець, поліноміальних базисів та стратегій розподілу повідомлень у слотах, що зменшує рівень шуму та дозволяє зберігати точність обчислень навіть при великій кількості операцій [2]. Важливим аспектом є вибір ступеня полінома та модуля, які безпосередньо впливають на рівень шуму і глибину допустимих обчислень.

Оптимізація пакетних гомоморфних схем включає вибір розміру пакетів, структури матриць і параметрів поліноміальних кілець. Великий розмір

пакетів дозволяє одночасно обробляти більше даних, проте підвищує рівень шуму, що потребує коректної балансування параметрів.

Застосування SIMD-підходу дає змогу ефективно використовувати сучасні багатоядерні процесори для паралельного виконання обчислень, що істотно прискорює обробку даних у реальному часі.

Варто також зазначити, що інтеграція адаптивного вибору параметрів матричних поліномів та автоматичне регулювання структури пакетів у реальному часі дозволяє динамічно балансувати між швидкістю обчислень і криптографічною стійкістю, підвищуючи загальну ефективність системи. [2-3].

Практична реалізація оптимізованих пакетних схем ефективна у хмарних обчисленнях та захищених базах даних, де необхідна обробка великих масивів конфіденційної інформації без розкриття даних. Прикладом може бути обчислення сум, середніх величин або простих статистичних характеристик на зашифрованих даних. Використання матричних поліномів дозволяє зменшити кількість шифротекстів та прискорити обчислення, що забезпечує ефективність і масштабованість криптографічних сервісів.

Проведений аналіз підтверджує, що оптимізація пакетних гомоморфних схем за допомогою матричних поліномів підвищує ефективність обробки великих обсягів даних.

Матричні структури дозволяють одночасно кодувати декілька повідомлень, рівномірно розподіляти шум та збільшувати глибину обчислень без частого bootstrap-перетворення [3, 4].

Оптимізація параметрів пакетів і структури матриць забезпечує баланс між продуктивністю та криптографічною стійкістю, що робить такі схеми перспективними для хмарних обчислень, захищених баз даних та систем делегованих обчислень.

Отримані результати підтверджують доцільність подальших досліджень щодо адаптивного вибору параметрів матричних поліномів і практичної реалізації пакетних схем у сучасних бібліотеках гомоморфного шифрування.

Список літератури

1. Гущин Б.-Д. І. Аналіз ефективності повністю гомоморфного шифрування шляхом використання матричних поліномів // Проблеми інформатизації: тези доп. тринадцятої міжнар. наук.-техн. конф., 27-28 листопада 2025 р., м. Баку, м. Харків, м. Бельсько-Бяла : [у 4 т.]. Т. 2 : секції 3, 7. – Харків : НТУ "ХПІ", 2025. – С. 86-87.

2. Chen, Y., Huang, R., & Yang, B. (2022). Efficient batch fully homomorphic encryption with a shorter key from ring-lwe. *Applied Sciences*, *12*(17), 8420.

3. Hushchyn Bohdan-Danylo Analysis of Homomorphic Encryption Algorithms / Hushchyn Bohdan-Danylo // Computer and information systems and technologies : Seventh International Scientific and Techn. Confe., september 2024. – Kharkiv : NURE, 2024. – P. 56.

4. Белей, О. І. (2018) «Гомоморфне шифрування даних у хмарних сховищах методом матричних поліномів», Сучасний стан наукових досліджень та технологій в промисловості, (4 (6), с. 5–14. doi: 10.30837/2522-9818.2018.6.005.

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ КРИПТОСИСТЕМ NTRU В IOT-СИСТЕМАХ

Товма О.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток технологій Інтернету речей (IoT) супроводжується збільшенням кількості пристроїв, що автоматично обмінюються даними в мережі. Оскільки більшість таких пристроїв має обмежені ресурси пам'яті, енергоспоживання та обчислювальної потужності, використання традиційних криптографічних алгоритмів є ускладненим. Одночасно зростає потреба в надійному захисті даних через підвищену вразливість IoT-систем до кіберзагроз. Розвиток квантових обчислень додатково посилює цю проблему, оскільки традиційні алгоритми, зокрема RSA, можуть втратити стійкість. У зв'язку з цим NTRU розглядається як перспективне постквантове рішення для IoT завдяки високій швидкодії та придатності до роботи на обмежених пристроях

Метою доповіді є визначення особливостей використання криптосистем NTRU в IoT-середовищі, аналіз їхньої ефективності при роботі на ресурсно обмежених пристроях, а також оцінювання практичної доцільності впровадження в сучасних мережевих архітектурах. Криптосистема NTRU базується на операціях у поліноміальному кільці, де шифрування і дешифрування виконуються через відносно прості арифметичні перетворення [1].Саме ця математична конструкція забезпечує нижчі обчислювальні витрати порівняно з багатьма іншими постквантовими алгоритмами. Для IoT-пристроїв така особливість є принципово важливою, оскільки навіть незначне збільшення криптографічного навантаження може впливати на час автономної роботи, стабільність передачі даних і швидкість реакції системи. Практичні дослідження показують, що NTRU демонструє високу швидкість генерації ключів та виконання операцій дешифрування навіть на мікроконтролерах із невеликою частотою процесора. У порівнянні з класичними алгоритмами відкритого ключа час виконання криптографічних процедур скорочується, що дозволяє використовувати захищений обмін ключами без суттєвого впливу на продуктивність сенсорних вузлів. Додатковою перевагою є можливість інтеграції NTRU у гібридні криптографічні схеми, де постквантовий алгоритм використовується паралельно з класичними механізмами захисту. Такий підхід дозволяє забезпечити сумісність із чинними протоколами безпеки та поступово адаптувати IoT-інфраструктуру до нових криптографічних стандартів. [1, 2]. Окремою перевагою NTRU є передбачуваність обчислювальних витрат. У багатьох IoT-сценаріях система повинна гарантувати стабільний час відповіді незалежно від навантаження. Решіткові алгоритми добре адаптуються до таких вимог, оскільки більшість операцій виконуються в межах фіксованої арифметичної структури. Це спрощує планування навантаження в реальному часі та підвищує стабільність роботи критичних пристроїв. Важливим фактором є також криптографічна стійкість NTRU у довгостроковій перспективі. Безпека алгоритму базується на

складності задач пошуку коротких векторів у структурованих решітках, для яких сьогодні не існує ефективного квантового алгоритму поліноміального часу. На відміну від традиційних схем, де квантові методи можуть суттєво скоротити складність зламу, у випадку NTRU навіть часткове квантове прискорення не призводить до практичного компрометування правильно вибраних параметрів [3].

Для IoT це означає можливість побудови захищених систем із тривалим життєвим циклом, де пристрої можуть працювати багато років без повної заміни криптографічної архітектури. Такий аспект особливо важливий для промислових сенсорних мереж, інфраструктурних контролерів та медичних пристроїв, де оновлення програмного забезпечення часто є складним або дорогим. Разом із перевагами існують і практичні обмеження. Одним із них є відносно більший розмір відкритих ключів порівняно з окремими класичними схемами.

Для мереж із дуже низькою пропускною здатністю це може створювати додаткове навантаження на канали передачі. Проте для більшості сучасних IoT-сценаріїв цей недолік компенсується швидкістю обробки та зниженням обчислювального навантаження на вузол, що особливо важливо в системах реального часу [2, 3].

Сучасні тенденції розвитку постквантової криптографії показують, що NTRU розглядається як перспективний компонент гібридних схем захисту, де традиційні алгоритми тимчасово поєднуються з постквантовими механізмами. Такий підхід дозволяє поступово адаптувати IoT-інфраструктуру до нових стандартів без радикальної перебудови всієї системи безпеки. У практичному сенсі впровадження NTRU в IoT-середовищі є доцільним насамперед там, де потрібне поєднання швидкодії, енергетичної ефективності та довгострокового криптографічного захисту. Саме ці властивості роблять алгоритм особливо перспективним для мереж розумних сенсорів, систем автоматизації та захищених комунікацій між вбудованими пристроями. Отже, криптосистеми на основі NTRU демонструють високий рівень придатності до використання в IoT-системах завдяки здатності забезпечувати постквантову стійкість без суттєвого перевантаження обмежених апаратних ресурсів. Їхнє практичне значення визначається поєднанням математичної надійності та технічної ефективності, що дозволяє розглядати NTRU як один із реальних інструментів формування безпечної інфраструктури майбутніх мережевих технологій.

Список літератури

1. Семеренська, В. (2025). Квантово-стійкі криптографічні алгоритми для критичних інфраструктур. Вісник ХНТУ, 2(1 (92)), 204-209.

2. Kotukh, Y., Severinov, E., Vlasov, O., Tenytska, A., & Zarudna, E. (2021). Some results of development of cryptographic transformations schemes using non-abelian groups. Radiotekhnika, 1(204), 66-72..

3. Petrenko O., Petrenko O., Sievierinov O., Fiediushyn O., Zubrych A., & Shcherbina, D. (2021). Analysis of ways to increase stability of cryptographic algorithms on algebraic lattices against time attacks. *Radiotekhnika*, *4*(207), 59–65.

ІНТЕГРАЦІЯ SOC ТА ISMS ЧЕРЕЗ AI

Іванський І.О., Нехороших Д.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Управління інформаційною безпекою щороку стає складнішим зі зростанням вимог стандартів, зокрема ISO/IEC 27001. Традиційні підходи із базою ручного зіставлення контролів та перевірці підтверджуючих документів, вже не відповідають сучасним потребам. Такі процеси є повільними, вони створюють значне навантаження для всіх учасників та є недостатньо впорядкованими.

Традиційні методи управління інцидентами часто передбачають використання ручних процесів та обмежену автоматизацію, і саме через це вони не здатні впоратися зі складністю сучасних кібератак.

Зростаюча складність загроз у сфері кібербезпеки зумовила нагальну необхідність застосування більш інтелектуальних і динамічних механізмів захисту [1, 2].

Впровадження модулів на базі штучного інтелекту (ШІ) розглядається не лише як спосіб підвищення ефективності, а також як інструмент оптимізації витрат.

У довгостроковій перспективі дане рішення може сприяти здешевленню впровадження та підтримки рішень інформаційної безпеки, роблячи їх більш доступними для організацій з обмеженими ресурсами.

Метою доповіді є дослідження можливостей інтеграції операційних систем кібербезпеки (SOC) та систем управління інформаційною безпекою (ISMS) із використанням технологій штучного інтелекту, а також обґрунтування доцільності застосування ШІ-модулів для автоматизації процесів аудиту, управління ризиками та контролю відповідності стандартам з метою підвищення ефективності та зниження витрат на забезпечення інформаційної безпеки.

SOC AI – це система, розроблена для вдосконалення реагування на інциденти за допомогою автоматизації та передових технологій штучного інтелекту [1].

AI SOC описується як центр операцій з безпеки, в якому штучний інтелект виконує роботи з розслідування, сортування та кореляції, які в іншому випадку виконували б аналітики 1-го та 2-го рівнів. Подібна модель описується так, де ШІ допомагає визначати пріоритетність сповіщень, розслідувати інциденти, запускати сценарії реагування та генерувати докази, готові до аудиту.

Обидва описи вказують на одну й ту саму основну зміну: ШІ більше не використовується лише всередині окремих інструментів, а як рівень міркування, що працює у всьому середовищі [3].

ISO заявляє, що ISO 27001 є найвідомішим стандартом для систем управління інформаційною безпекою. ШІ може створювати нові моделі ризиків, але це не робить класифікацію даних, контроль доступу, управління

постачальниками, реагування на інциденти або управління активами менш важливими. Це робить їх ще важливішими [3].

Оптимізований процес, впроваджений в компанії Oplium, має на меті представити нову процедуру SOC, яка дозволяє ефективно реагувати на інциденти та підвищити продуктивність команди з безпеки при роботі зі складними загрозами.

З метою інтеграції SOC AI з провідними інструментами, що забезпечують комплексне виявлення загроз, такими як Rapid7 InsightIDR, та надійне управління квитками, такими як Jira, Oplium розробила добре інтегровану процедуру для автоматизації та підвищення якості на кількох етапах управління інцидентами.

Цей процес працює на віртуальній машині, розміщеній на Oracle Cloud Infrastructure.

Налаштування віртуальної машини використовує всі 24 ГБ оперативної пам'яті, доступні в безкоштовному тарифі, і тому ідеально підходить для роботи SOC [1].

Контейнеризація робить систему масштабованою, модульною та простішою в управлінні.

Ця віртуальна машина працює за дуже суворими правилами безпеки, які дозволяють отримати доступ до інфраструктури SOC лише користувачам, підключеним через VPN.

Така конфігурація гарантує, що лише авторизовані користувачі, які безпечно підключені, можуть взаємодіяти з проектом, тим самим підвищуючи безпеку середовища, конфіденційних даних SOC та запущених процесів [1].

Процес роботи центру реагування на інциденти (SOC) компанії Oplium складається з п’яти основних етапів:

1) виявлення інциденту та створення запиту;

2) класифікація та розслідування інциденту;

3) аналіз інциденту та реагування;

4) закриття інциденту;

5) аналіз після інциденту та постійне вдосконалення.

Впровадження SOC AI демонструє, що використання штучного інтелекту дозволяє автоматизувати та інтегрувати процеси реагування на інциденти, підвищуючи ефективність SOC, зменшуючи навантаження на аналітиків і забезпечуючи більш швидке та якісне управління кіберзагрозами.

З огляду на те, що такі стандарти, як ISO/IEC 27001 та SOC 2, встановлюють дедалі вищі вимоги, ручне зіставлення контрольних заходів та перевірка доказів просто не встигають за ними: ці процеси повільні та хаотичні.

Водночас управління системою управління інформаційною безпекою (ISMS) – супроводжується значними обсягами документації, збором доказів, зіставленням політик із усіма цілями контролю [4].

Дослідження пропонують аналізатор відповідності та доказів на базі модуля ШІ. Він використовує штучний інтелект, обробку природної мови

(NLP) та машинне навчання (ML) для автоматичного виконання перевірок відповідності та підготовки до аудиту. Система спирається на семантичні вбудовування, технологію RAG на базі LangChain та векторний пошук FAISS, щоб пов’язати політику компанії та докази з відповідними заходами контролю СУІБ.

Тепер штучний інтелект може фактично читати політики, досліджувати конфігурації системи, переглядати докази та автоматично пов'язувати все з відповідними елементами контролю ISMS [4].

Даний підхід формує передумови для переходу від періодичного до безперервного аудиту, в межах якого перевірка відповідності виконується постійно на основі актуальних даних із SOC. Таке рішення дозволяє своєчасно виявити відхилення, зменшити ризики невідповідності та підвищити ефективність функціонування ISMS.

Система, що розробляється – «AI-Driven Control Mapping and Evidence Analyzer», значно спрощує перевірку відповідності вимогам СУІБ. Вона використовує штучний інтелект та обробку природної мови для виконання трьох основних завдань:

зіставлення політик із заходами контролю;

аналіз доказів;

формування звітів про відповідність вимогам.

Цей підхід поєднує машинне навчання, векторний пошук за схожістю та міркування штучного інтелекту, тому результати не тільки точні, але й масштабовані, і можливо реально зрозуміти, як вони були отримані. Коли завантажується файл політики або доказів, двигун штучного інтелекту створює вбудовування для вхідного даних, а потім шукає в індексі FAISS найближчі заходи контролю ISMS [4].

Найбільш надійна архітектура зазвичай починається з систем управління і закінчується доказами під час виконання. В основі лежить ISO 27001, оскільки без функціонуючої ISMS решта, як правило, стає фрагментованою та залежить від особистості.

З операційної сторони лежить AI SOC або еквівалентна функція, оскільки середовище контролю не має великого значення, якщо ніхто не може розслідувати, що насправді відбувається [3].

Ефективне управління штучним інтелектом вимагає, щоб безпека не була лише додатковим елементом, а стала фундаментальною складовою, інтегрованою на кожному етапі життєвого циклу систем. Підхід «безпека за замовчуванням» є необхідним для проактивного управління ризиками, забезпечення стійкості та створення надійного штучного інтелекту [5].

Впровадження ШІ-рішень потребує забезпечення прозорості та пояснюваності рішень, оскільки існують ризики помилкових висновків, а також актуальним залишається питання довіри до автоматизованих систем. З цієї причини ключовим принципом залишається підхід, за якого остаточні рішення приймаються фахівцями з інформаційної безпеки. Керівник служби інформаційної безпеки (CISO) забезпечує інформаційну безпеку організації,

включаючи всі інформаційні системи, і в контексті штучного інтелекту (ШІ) його роль стає ще більш важливою.

CISO повинен впроваджувати заходи безпеки, забезпечуючи захист моделей від зловмисних атак, витоку інформації або маніпуляцій під час навчання. Він також бере активну участь в оцінці ризиків, пов'язаних із використанням ШІ, розробляючи превентивні заходи та плани реагування на інциденти [5].

Таким чином, штучний інтелект виступає не окремим інструментом, а інтегруючим аналітичним шаром, що поєднує операційний рівень кібербезпеки з процесами управління ISMS, формуючи єдине інформаційне середовище для прийняття рішень.

Отже, традиційні ручні підходи до управління інформаційною безпекою та реагування на інциденти є занадто повільними для сучасних кіберзагроз і вимог стандартів, таких як ISO/IEC 27001.

Впровадження модуля ШІ вирішує цю проблему, перетворюючись на інтегруючий аналітичний блок, що поєднує стратегічне управління з операційним рівнем кібербезпеки.

З одного боку, моделі AI SOC оптимізують витрати та беруть на себе базові завдання аналітиків з розслідування та кореляції інцидентів. З іншого боку, технології обробки природної мови та машинного навчання дозволяють перейти до безперервного аудиту, автоматично зіставляючи докази та політики з вимогами ISMS.

Таким чином формується комплексна архітектура, де ISMS забезпечує впорядковане середовище управління, а AI SOC – можливість швидкого розслідування та реагування.

Проте, оскільки сам ШІ піддається специфічним ризикам, зокрема маніпуляціям під час навчання, тому критичною залишається роль CISO у захисті цих моделей за принципом «безпека за замовчуванням», де остаточні рішення все одно мають прийматися фахівцями для збереження довіри та прозорості.

Список літератури

1. Licitra S. Leveraging AI Techniques for Automated Security Incident Response: Master Degree Thesis. Politecnico di Torino, 2024. URL: https://webthesis.biblio.polito.it/33833/1/tesi.pdf

2. Sievierinov, O., Ovcharenko, M., & Vlasov, A. (2021). Enterprise Security Operations Center. 2021: Fifth International Scientific and Technical Conference "*Computer and information systems and technologies*".

3. AI SOC, ISO 27001, SOC 2, and the Security Stack Real AI Teams Need in 2026 / Penligent. 2026. URL: https://www.penligent.ai/hackinglabs/ai-soc-iso-27001-soc-2-and-the-security-stack-real-ai-teams-need-in-2026/

4. AI-Driven Control Mapping and Evidence Analyzer / Y. S. Zope, V. N. Sukale, Y. S. Kakade et al. // International Journal of Innovative Research in Technology (IJIRT). 2025. Vol. 12, Iss. 6. URL: https://ijirt.org/publishedpaper/IJIRT186166_PAPER.pdf

5. Study on AI Governance / ISMS Forum. 2025. URL: https://www.ismsforum.es/ficheros/descargas/en---gobierno-de-la-ia1765878738.pdf

ІНТЕГРАЦІЯ SIEM В СТРУКТУРІ ISMS ІЗ ЗАСТОСУВАННЯМ AI

Іванський І.О., Нехороших Д.М.
Харківський національний університет радіоелектроніки, Харків, Україна

В сучасних умовах зростання кількості кіберзагроз, ефективне управління інформаційною безпекою стає критично важливим для організацій. Системи SIEM відіграють ключову роль у структурі ISMS, забезпечуючи централізований збір і аналіз подій безпеки. Однак традиційні SIEM-рішення мають обмеження у виявленні складних та невідомих атак. Інтеграція технологій штучного інтелекту дозволяє підвищити ефективність SIEM за рахунок автоматизації аналізу даних, виявлення аномалій та швидшого реагування на інциденти. Водночас така інтеграція потребує врахування низки технічних і організаційних викликів.

Метою доповіді є дослідження особливостей інтеграції SIEM у структуру ISMS із використанням технологій штучного інтелекту, зокрема аналіз їх впливу на ефективність виявлення загроз, автоматизацію процесів моніторингу та реагування, а також визначення основних переваг та ризиків, пов'язаних із застосуванням AI у кібербезпеці.

SIEM – це настроювана система обліку подій безпеки, яка збирає та аналізує дані про події безпеки з локальних і хмарних середовищ. SIEM допомагає вживати заходів реагування для усунення проблем, що завдають шкоди організації, а також забезпечує дотримання вимог щодо відповідності та звітності [1]. SIEM виконує роль центрального аналітичного та оперативного компонента в рамках Системи управління інформаційною безпекою (ISMS), забезпечуючи підтримку таких ключових процесів, як оцінка ризиків, виявлення інцидентів, реагування на інциденти та моніторинг дотримання вимог. Система інтегрується з іншими елементами ISMS, зокрема з політиками безпеки, системами контролю доступу та інструментами управління вразливостями, утворюючи єдину екосистему безпеки.

Постійний моніторинг інформаційної безпеки (ISCM) визначається як постійне відстеження стану інформаційної безпеки, вразливостей та загроз з метою забезпечення прийняття обґрунтованих рішень щодо управління ризиками в організації. Програма допомагає забезпечити, щоб впроваджені засоби контролю безпеки залишалися ефективними, а операції не виходили за межі встановлених організаційних рівнів прийнятного ризику з огляду на неминучі зміни, що відбуваються з часом. ISCM, як важливий етап у системі управління ризиками (RMF) організації, надає посадовим особам організації доступ до інформації, пов'язаної з безпекою, на запит, що дозволяє своєчасно приймати рішення з управління ризиками, включаючи рішення щодо авторизації [2]. Забезпечити ефективний моніторинг у масштабах всієї організації неможливо лише за допомогою ручних або лише за допомогою автоматизованих процесів. У випадках, коли застосовуються ручні процеси, вони мають бути повторюваними та піддаватися перевірці, щоб забезпечити послідовність їхнього виконання. Автоматизовані процеси, зокрема

використання автоматизованих допоміжних інструментів, наприклад, інструментів сканування вразливостей, пристроїв для сканування мережі, можуть зробити процес безперервного моніторингу більш економічно вигідним, послідовним та ефективним [2]. Типова архітектура SIEM з використанням штучного інтелекту включає джерела даних, зокрема кінцеві точки, мережеві пристрої, хмарні сервіси, рівні збору та нормалізації даних, системи зберігання даних, такі як «озера даних» (data lakes), аналітичні механізми на базі моделей штучного інтелекту та машинного навчання, а також компоненти для координації реагування, наприклад, SOAR. Така багаторівнева архітектура забезпечує масштабованість та гнучкість операцій з безпеки. Традиційні системи управління інформацією та подіями безпеки (SIEM) мають обмеження в обробці великих обсягів даних та виявленні складних загроз. Щоб подолати ці обмеження, інтеграція платформ SIEM з озерами даних та штучним інтелектом є перспективним напрямком розвитку. [3] Алгоритми штучного інтелекту та машинного навчання здатні виявляти складні схеми атак і нові загрози, які можуть залишитися непоміченими традиційними системами SIEM [2].

Ці технології постійно навчаються на основі даних, покращуючи свою здатність виявляти нові та невідомі загрози (атаки «нульового дня») шляхом розпізнавання ледь помітних закономірностей або аномалій у поведінці, які можуть свідчити про зловмисну діяльність. Системи на основі штучного інтелекту та машинного навчання можуть інтелектуально аналізувати дані, щоб зменшити кількість помилкових спрацьовувань, розрізняючи звичайну активність і реальні загрози [2].

Інтеграція штучного інтелекту та машинного навчання в існуючі системи SIEM може бути складним і ресурсомістким процесом. Однією з проблем, пов'язаних із застосуванням штучного інтелекту та машинного навчання в системах SIEM, є брак прозорості, який часто називають проблемою «чорного ящика» [2]. Отруєння даних: ця загроза пов'язана з введенням помилкових, сфальсифікованих або неправильних даних у навчальний або валідаційний набір шляхом отримання законного або незаконного доступу через зловживання недосконалими механізмами аутентифікації та авторизації. Бекдори в моделях: отримані моделі можуть бути схильні до загроз у вигляді бакдорів, які розкривають їх внутрішню роботу (порушення конфіденційності), впливають на їх функціонування (порушення цілісності) або погіршують/скасовують їх продуктивність (вплив на доступність) [4].

Впровадження технологій генеративного штучного інтелекту в операції з кібербезпеки відкриває як безпрецедентні можливості, так і значні ризики для організацій у всьому світі [5]. Наприклад, недостатня надійність та вразливість моделей і алгоритмів ШІ, як-от, суперечливе виведення та маніпулювання моделями, атаки на кіберфізичні системи на базі ШІ, маніпулювання даними, що використовуються в системах ШІ [4]. Сьогодні організації стикаються зі змінами в ландшафті загроз, де фішингові кампанії, створені за допомогою ШІ, досягають безпрецедентного рівня складності, атаки на основі супротивного

машинного навчання націлені на системи виявлення, а автоматизовані зловмисники діють у масштабах, які раніше були неможливими. Організації впроваджують гібридні системи прийняття рішень, процеси аналізу з використанням штучного інтелекту та моделі співпраці на основі ескалації, які зберігають людський контроль, водночас використовуючи штучний інтелект для масштабування та прискорення процесів [5].

Перехід від статичного виявлення загроз на основі сигнатур до динамічних моделей з інтегрованим штучним інтелектом є найфундаментальнішою адаптацією архітектури, що спостерігається в різних організаційних контекстах.

Замість повної заміни існуючих систем організації демонструють моделі еволюційної адаптації, які ґрунтуються на вже сформованих основах, водночас враховуючи специфічні особливості та можливості штучного інтелекту [5].

Отже, інтеграція систем управління інформацією та подіями безпеки (SIEM) у структуру системи управління інформаційною безпекою (ISMS) із використанням технологій штучного інтелекту є важливим етапом розвитку сучасних підходів до кіберзахисту. Використання AI та машинного навчання дозволяє значно підвищити ефективність виявлення загроз, зокрема складних та невідомих атак, а також автоматизувати процеси моніторингу та реагування на інциденти.

Застосування інтелектуальних алгоритмів сприяє зменшенню кількості помилкових спрацьовувань, підвищує швидкість аналізу великих обсягів даних та забезпечує більш адаптивний підхід до управління безпекою.

Разом із тим інтеграція AI у SIEM супроводжується рядом викликів, серед яких складність впровадження, недостатня прозорість моделей, ризики отруєння даних та наявність потенційних вразливостей у самих алгоритмах.

Список літератури

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

2. National Institute of Standards and Technology. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (NIST SP 800-137. URL: https://csrc.nist.gov/pubs/sp/800/137/final

4. Integrating Security Information and Event Management (SIEM) with Data Lakes and AI: Enhancing Threat Detection and Response URL: https://www.researchgate.net/publication/384905295_Integrating_Security_Information_and_Event_Management_SIEM_with_Data_Lakes_and_AI_Enhancing_Threat_Detection_and_Response

5. European Union Agency for Cybersecurity. Artificial Intelligence Cybersecurity Challenges URL: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

6. Advances in AI-driven Cybersecurity Systems URL: https://arxiv.org/abs/2506.12060

ЦИФРОВЕ ВОДЯНЕ МАРКУВАННЯ ЯК ЕФЕКТИВНИЙ МЕТОД ЗАХИСТУ ВІДЕОКОНТЕНТУ ВІД НЕСАНКЦІОНОВАНОГО КОПІЮВАННЯ

Кібірєв Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Поширення стрімінгових сервісів, соціальних мереж і онлайн-платформ призвело до стрімкого зростання обсягів відеоконтенту. Водночас актуальною проблемою залишається його несанкціоноване копіювання та розповсюдження. Навіть за наявності шифрування або обмеження доступу, після перегляду відео користувач може легко його записати або зберегти.

Тому зростає потреба у таких методах захисту, які дають змогу не лише контролювати доступ, а й встановлювати походження відео після його копіювання. Одним із найбільш ефективних підходів у цьому напрямі є цифрове водяне маркування, що широко використовується для захисту авторських прав [1]. Окрім захисту авторських прав, водяне маркування відіграє важливу роль у задачах автентифікації цифрового контенту та забезпечення довіри до мультимедійних даних [2].

Метою доповіді є дослідження принципів цифрового водяного маркування та аналіз його можливостей як ефективного засобу захисту відеоконтенту від несанкціонованого копіювання з урахуванням сучасних умов обробки мультимедійних даних.

Цифрове водяне маркування ґрунтується на ідеї вбудовування додаткової інформації безпосередньо у відеоконтент. Ця інформація не сприймається користувачем під час перегляду, але може бути виявлена за допомогою спеціальних алгоритмів. Фактично відео отримує прихований «ідентифікатор», який пов'язує його з власником або джерелом розповсюдження. Такий підхід дозволяє також виявляти несанкціоновані зміни контенту та використовувати його у цифровій експертизі [1].

Особливість такого підходу полягає в тому, що водяний знак не є окремим файлом або метаданими, які легко видалити, а інтегрується у саму структуру відео. Для цього змінюються окремі характеристики зображення, наприклад значення пікселів або коефіцієнти після математичних перетворень. Завдяки цьому навіть після стиснення, зміни якості чи інших типових операцій обробки відео водяний знак може зберігатися.

Методи цифрового водяного маркування можуть відрізнятися за різними ознаками, що дозволяє класифікувати їх залежно від поставлених завдань. Зокрема, за способом сприйняття розрізняють видимі та невидимі водяні знаки: перші безпосередньо відображаються у відео у вигляді логотипів або написів, тоді як другі залишаються непомітними для користувача. За рівнем стійкості водяні знаки можуть бути робастними або крихкими. Крім того, важливою є класифікація за способом вбудовування. Виділяють три основні групи методів: традиційні, гібридні та методи на основі глибокого навчання, що відрізняються рівнем стійкості, складністю реалізації та адаптивністю.

Методи на основі глибокого навчання демонструють здатність автоматично підлаштовуватися під характеристики сигналу та підвищувати якість вбудовування [1]. У відеоконтенті водяний знак може розподілятися як у межах окремих кадрів, так і по всій часовій послідовності. Такий підхід підвищує стійкість до різних втручань. Сучасні методи водяного маркування часто використовують перетворення сигналів, зокрема косинусне або вейвлет-перетворення. Це дозволяє досягти балансу між непомітністю та стійкістю водяного знаку. Гібридні підходи, що поєднують кілька перетворень (наприклад, DWT, DCT, SVD), забезпечують ще вищу надійність і стійкість до атак [2]. Такі методи дозволяють ефективно протидіяти як простим, так і комбінованим атакам на відеодані.

Окремим напрямом розвитку є персоналізоване або форензічне водяне маркування. Підходи включають використання нейронних мереж, які дозволяють автоматично адаптувати процес вбудовування та забезпечують стійкість до складних атак, включаючи геометричні спотворення.

Разом із тим цифрове водяне маркування має певні обмеження, воно не запобігає самому факту копіювання, а лише дозволяє виявити порушення після його здійснення. Існують виклики що пов’язані з високими обчислювальними витратами сучасних методів, відсутністю стандартизації та необхідністю протидії новим типам атак, зокрема deepfake та AI-обробці контенту [2]. Попри ці обмеження, водяне маркування є важливою складовою сучасних систем захисту. Воно добре поєднується з іншими підходами. Зокрема, перспективним є поєднання з криптографією та блокчейн-технологіями для забезпечення надійної ідентифікації та відстеження цифрового контенту .

Цифрове водяне маркування є ефективним і практичним методом захисту відеоконтенту. Його ефективність визначається здатністю забезпечувати баланс між прозорістю, стійкістю до атак та обчислювальною ефективністю . Найбільш ефективними є методи, які використовують перетворення сигналів і враховують часову структуру відео. Ключовим критерієм якості є мінімальний вплив на візуальне сприйняття при максимальній збереженості водяного знака.

Подальший розвиток цього напряму пов’язаний із підвищенням стійкості водяних знаків до складних атак та адаптацією методів до обробки великих потоків відеоданих у реальному часі. Особливу увагу приділяють розробці масштабованих, адаптивних та інтелектуальних систем водяного маркування, здатних працювати в умовах цифрової трансформації та зростаючих вимог до безпеки. Перспективним є також використання штучного інтелекту для автоматизації процесів вбудовування та детектування водяних знаків.

Список літератури

1. Кібірєв, Д.О., Федорченко В.М. Аналіз методів захисту відеоконтенту від несанкціонованого копіювання. ХНУРЕ, 2023

2. Ланських Є., Наумов О. (2025). Сучасні методи цифрового водяного маркування зображень: класифікація, аналіз і тенденції розвитку. *Інформаційні технології та суспільство*, (2 (17)), 89-95.

ДОСЛІДЖЕННЯ МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ У API ЖУРНАЛАХ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА НАДІЙНОСТІ ПРОГРАМНИХ СИСТЕМ

Свиридов А.С., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

На сьогоднішній день захист програмних інтерфейсів (API) застосунків є серйозною задачею. Більшість сучасних компаній надають доступ до своїх послуг через вебзастосунки, де клієнти регулярно обмінюються конфіденційною інформацією між клієнтською і серверною частиною. Це вимагає забезпечення високого рівня захисту таких API-інтерфейсів [1]. Кібернетичний вплив на такі системи може призвести до значних фінансових та технічних збитків.

Традиційний ручний аналіз log-файлів є дуже трудомістким та ресурсозатратним процесом. Автоматизувати процес аналізу великих обсягів даних дозволяють методи штучного інтелекту, зокрема неконтрольованого машинного навчання, оскільки вони здатні виявляти шаблони аномальної активності без попередньої розмітки даних [2].

Окрім цього, для специфічних галузей (наприклад, FinTech) активно досліджуються й інші комбіновані підходи на базі генетичних алгоритмів [3].

Метою доповіді є розробка та оцінка ефективності методів виявлення аномалій у API журналах з метою підвищення безпеки та надійності програмних систем.

Дослідження процесу виявлення аномалій включає в себе чотири основні етапи: підготовка даних, безпосереднє виявлення аномалій, отримання та оцінка результатів.

Підготовча фаза включає збір журналів, вилучення ознак та їхню нормалізацію, що була виконана в цій роботі для підвищення точності передбачення.

Для процесу неконтрольованого виявлення аномалій було обрано чотири моделі: алгоритми кластеризації K-means та GMM, ансамблеву модель пошуку викидів Isolation Forest, а також метод OCSVM (One-Class SVM).

Для зменшення часу обчислень моделі OCSVM через високу розмірність набору даних було використано метод аналізу головних компонентів (PCA).

Експерименти проводилися на наборі даних HTTP Dataset CSIC [4], що містить 61 000 автоматично згенерованих вебзапитів (36 000 нормальних та 25 000 аномальних), включаючи SQL-ін’єкції та XSS.

Аналіз результатів показав, що модель GMM досягла найбільш збалансованого результату з показником F1-міри 0.65 та площею під кривою AUC на рівні 0.78 при швидкому часі навчання.

Модель Isolation Forest продемонструвала найвищу точність (Precision = 0.78) та високу швидкість обробки даних (0.18 с), проте через низьку повноту (Recall = 0.27) вона пропускає значну кількість реальних аномалій.

Модель K-means показала слабку роздільну здатність, оскільки її показник AUC (0.56) наближений до випадкового вгадування.

Алгоритм OCSVM забезпечив прийнятний баланс точності (0.55) та повноти (0.66), проте вимагає значно більших обчислювальних ресурсів та часу на навчання.

Окрім класичних методів, вагомого значення набуває моніторинг динамічних середовищ, де використовується метод виявлення аномалій у Kubernetes-кластерах з використанням LSTM Autoencoder [5].

Завдяки архіте-ктурі рекурентних мереж, цей підхід дозволяє ефективно аналізувати часові послідовності журналів та ідентифікувати приховані залежності через оцінку помилки реконструкції даних. Інтеграція таких нейромережевих моделей із методами неконтрольованого навчання забезпечує масштабовану систему захисту як на рівні окремих API-запитів, так і на рівні всієї хмарної інфраструктури. Крім того, використання механізмів автоматичного навчання дозволяє системі динамічно адаптуватися до змін у структурі трафіку без необхідності ручного перенавчання моделей при кожному оновленні мікросервісів.

В роботі досліджено методи виявлення аномалій у API журналах. Встановлено, що використання методів неконтрольованого навчання є ефективним інструментом для підвищення надійності та безпеки програмних систем.

Зокрема, доведено, що для захисту сучасних хмарних сервісів критично важливим є поєднання базових алгоритмів аналізу з нейромережевими підходами на основі LSTM-автоенкодерів для моніторингу Kubernetes-кластерів.

Подальші дослідження будуть спрямовані на оптимізацію алгоритмів для роботи в реальному часі та інтеграцію з іншими системами кібербезпеки.

Список літератури

1. OWASP, OWASP API Security Project. URL: https://owasp.org/www-project-api-security/ (дата звернення: 25.02.2026).

2. Catherine A. et al. Enhancing API Security in FinTech with Genetic Algorithm-Based Machine Learning Models. 2025.

3. Aharon U., Dubin R., Dvir A., Hajaj C. A classification-by-retrieval framework for few-shot anomaly detection to detect API injection. Computers & Security. 2025. Vol. 150. 104249. DOI: https://doi.org/10.1016/j.cose.2024.104249

4. Sánchez-Zas C. et al. Design and Evaluation of Unsupervised Machine Learning Models for Anomaly Detection in Streaming Cybersecurity Logs. Mathematics. 2022. Vol. 10, No. 21. P. 4043. DOI: https://doi.org/10.3390/math10214043

5. Свиридов, А., Сєвєрінов, О. (2026). Метод виявлення аномалій у kubernetes-кластерах з використанням LSTM Autoencoder. Herald of Khmelnytskyi National University. Technical Sciences, 361(1), 501-509. https://doi.org/10.31891/2307-5732-2026-361-70

ПРОБЛЕМИ ЗАСТОСУВАННЯ ВОДЯНИХ ЗНАКІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Іщук О.Р., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Цифровий водяний знак (ЦВЗ) – це інформація пов'язана з певним цифровим об'єктом. Застосування ЦВЗ є одним із методів захисту інформації від різного роду протиправних дій проти контенту. Досить простий метод і досі має шляхи розвитку в наш час, адже знаходяться нові способи його застосування з різними видами даних [1, 2].

Метою доповіді є висвітлення сучасного стану розвитку та застосування ЦВЗ, які є одним з інструментів захисту інформації, аналіз проблем їх застосування в інформаційно-комунікаційних системах.

Цифровий водяний знак вже застосовуються у таких напрямках, а саме нижчеперерахованих:

1. Захист авторських прав. Нанесений знак на різних типах контенту частково або взагалі унеможливлює копіювання інформації. Це є особливо актуальним для зображень, відео та цифрових документів, які легко поширюються мережею.

2. Захист автентичності даних. Водяний знак допомагає перевіряти цілісність даних. Якщо змінити інформацію, то водяний знак буде пошкоджено, що і є сигналом про втручання в структуру даних.

3. Відстеження витоків. Існують методи завдяки яким можна відстежувати джерело інформації шляхом вбудовування унікальних ідентифікаторів для кожного користувача.

4. Автентифікація. Є підходи до застосування певних видів ЦВЗ при автентифікації в системах, наприклад для підтвердження справжності цифрових документів або мультимедійного контенту.

Хоча ЦВЗ вже широко застосовуються у різних напрямках людської діяльності, вони мають ряд недоліків [3]:

– пошкодження візуального контенту. Якщо кажемо про зображення, то нанесенням водяного знаку ми псуємо певну область зображення, а іноді й значну його частину.

– можливість вирізати знак. Розвиток нейронних мереж дозволив створити сервіси по видаленню водяних знаків.

Незважаючи на значний потенціал, впровадження цифрових водяних знаків в ІКС супроводжується низкою проблем.

1. Обмежена стійкість до атак. У реальних умовах функціонування ІКС водяні знаки можуть піддаватися різним впливам: стисненню, фільтрації, масштабуванню або навмисному видаленню. Це знижує їх ефективність як механізму захисту.

2. Компроміс між непомітністю та надійністю. Чим менш помітний водяний знак, тим складніше забезпечити його стійкість до атак, і навпаки.

3. Обчислювальні витрати. Вбудовування та перевірка ЦВЗ потребують додаткових обчислювальних ресурсів, що є критичним для систем реального часу та ресурсно-обмежених пристроїв.

4. Проблеми масштабованості. У великих ІКС (наприклад, хмарних або IoT-системах) ускладнюється управління великою кількістю унікальних водяних знаків.

5. Вразливість до атак із використанням штучного інтелекту. Сучасні методи, зокрема нейронні мережі, дозволяють ефективно видаляти або модифікувати водяні знаки без суттєвої втрати якості контенту.

6. Відсутність уніфікованих стандартів. Наразі не існує єдиного підходу до реалізації ЦВЗ, що ускладнює їх інтеграцію в різні системи.

Паралельно розвитку водяних знаків йде розробка алгоритмів так званих нульових водяних знаків, які усувають недоліки звичайних ЦВЗ. Їх головна відмінність це відсутні візуальної складової в контенті, тобто у випадку застосування нульового водяного знаку в зображенні, ми абсолютно ніяк не змінюємо саме зображення [4]. Такий підхід надає можливість уникати недоліків звичайного нульового знаку, а саме проблем з погіршенням, спотворенням зображень і подібного контенту.

В основі створення нульового водяного знаку лежить підхід по виділенню певних ознак, наприклад коефіцієнтів перетворення (DWT, DCT), ключових точок або інших характеристик. На основі цих даних можна створити унікальний «відбиток», який при поєднанні з інформацією поміщається на зберігання як еталонна модель. При необхідності перевірки цілісності чи інших ознак, ми витягуємо ті самі ознаки із наданого контенту і порівнюємо з еталонним. Якщо ознаки збігаються – можна підтвердити цілісність даних.

Таким чином, цифрові водяні знаки залишаються ефективним інструментом захисту інформації, однак їх використання в ІКС пов’язане з низкою технічних і організаційних викликів. Подальший розвиток, зокрема у напрямі нульових водяних знаків, дозволяє підвищити надійність захисту без впливу на якість контенту.

Список літератури

1. Зубко І.С., Мартовицький В.О. Огляд методів нанесення цифрових водяних знаків для захисту зображень. Системи управління, навігації та звязку. 2024. №3, С. 121-125. DOI: https://doi.org/10.26906/SUNZ.2024.3.121

2. Gvozdov, R., Poddubnyi, V., Sieverinov, O., Buhantsov, A., Vlasov, A., & Sukhoteplyi, V. (2021, October). Method of Biometric Authentication with Digital Watermarks. In 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T) (pp. 569-571). IEEE.

3. Martovytskyi, V., Ruban, I., Bolohova, N., Sievierinov, O., Zhurylo, O., Permiakov, O., ... & Krylenko, I. (2021). Development of methods for generation of digital watermarks resistant to distortion. Eastern-European Journal of Enterprise Technologies, 6(2), 114.

4. Поддубний В.О. Методи та огляд багатофакторної автентифікації в інформаційно-комунікаційних системах на основі нульових водяних знаків. 2025. URL: https://nure.ua/poddubniy-vadym-oleksandrovich.

ОЦІНКА СТІЙКОСТІ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ЗІ СКОРОЧЕНИМИ КОДАМИ ГОППИ

Сидоренко З.М., Сєвєрінов О.В.
Харківський національний університет радіоелектроніки, Харків, Україна

В даний час забезпечення цілісності даних у системах IIoT є критичним аспектом інформаційної безпеки, оскільки у промисловому середовищі порушення цілісності може призвести до неправильного функціонування обладнання, аварій та втрати довіри до системи [1].

Перспективним рішенням для забезпечення цілісності даних у системах IIoT є поєднання криптографії та завадостійкого кодування. Запропоновано для забезпечення цілісності даних використовувати завадостійкі коди Гоппи, що дозволить вирішувати такі завдання, як забезпечення цілісності та інформаційної скритності каналів передачі даних у системах IIoT [1, 2].

Для забезпечення функціонування даної системи забезпечення цілісності з скороченими кодами Гоппи необхідно провести оцінку її стійкості.

Метою доповіді є оцінка стійкості системи забезпечення цілісності зі скороченими кодами Гоппи у системах промислового Інтернету речей.

Основним методом перевірки стійкості будь-якої криптосистеми є експертний криптоаналіз в умовах, сприятливих для криптоаналітика [3]. Стійкість більшості систем цілісності спирається не на теоретичну неможливість їхнього розкриття, а на практичну складність такого розкриття, що звичайно виражається в необхідних для цієї мети часових працевтратах (безпечному часі Tsec). При обчисленні нижньої границі цього часу виникає складна задача: знайти найкращий спосіб розкриття системи захисту інформації, тому що завжди існує можливість, що криптоаналітик знайде новий метод аналізу, що вимагає значно менших часових працевтрат.

Стійкість схем, побудованих на кодах Гоппи заснована на складності рішення відомої в теорії завадостійкого кодування важко вирішуваної задачі декодування випадкового коду. Дана задача є NP-важкою, що означає відсутність відомих ефективних (поліноміальних) алгоритмів її точного розв'язання для довільних кодів. Аналогічна обчислювальна складність лежить в основі побудови кодових криптосистем, таких як система Мак-Еліса.

В роботі була проведена оцінка стійкості кодових конструкцій скорочених кодів Гоппи при повному переборі всіх можливих ключів, а також оцінка, заснована на визначенні даних кодів в часовій та частотній області.

При аналізі можливих шляхів розкриття ключових даних системи забезпечення цілісності виходили з того, що задачею криптоаналітика є одержання насамперед закону формування кодових послідовностей.

Одним зі шляхів розкриття будь-якої системи захисту є повний перебір усіх можливих ключів. Однак даний метод не завжди є самим коротким. Тому що для кодів Гоппи вся безліч кодових слів задається за допомогою одного багаточлена G(x), то зловмисник може спробувати розкрити ключові дані,

ґрунтуючись на визначенні даного коду. У цьому випадку розкриття ключового багаточлена еквівалентно рішенню деякої математичної задачі.

Так як тільки один багаточлен Гоппи фіксованого ступеня визначає відповідну безліч кодових слів скороченого коду заданої довжини. Час криптоаналізу Tstar у випадку повного перебору всіх можливих ключів буде визначатися виразом

$$T_{star} = P_д \, I/V = 2^i \, C^i_n \, N_q(t) \, n\log^2 n \, Pд/V,$$

де I – обчислювальна складність криптоаналізу;

V – максимальна продуктивність ЕОМ зловмисника;

n – довжина коду Гоппи;

$N_q(t)$ – кількість багаточленів Гоппи, що неприводяться;

I – кількість символів скорочення коду;

Рд - припустима імовірність успішного криптоаналізу.

Проведена оцінка стійкості системи забезпечення цілісності, заснована на визначенні даних кодів в часовій області. У цьому випадку безпечний час T_{math} буде дорівнювати:

$$T_{math} = I/V = 5 \cdot 2^i C^i_n \, w^2 n\log^2 n \, / \, V,$$

де w – вага кодового слова скороченого коду Гоппи.

В роботі проведена оцінка стійкості системи забезпечення цілісності, заснована на визначенні даних кодів в частотній області. Безпечний час T_{math} у цьому випадку буде дорівнювати:

$$T_{math} = I/V = 3 \cdot 2^i C^i_n \cdot (n\text{-}z) z^2 n\log n \, / \, V,$$

де z – кількість нульових символів у кодовому слові скороченого коду Гоппи.

Порівнюючи вирази оцінки стійкості можна помітити, що при рівному числі символів скорочення, найменшу обчислювальну складність дає криптоаналіз в часовій області. що приблизно в n/3logn раз менше обчислювальних операцій, чим у частотній області. Тому при виборі кодів Гоппи, що задовольняють заданим вимогам до цілісності інформації і стійкості ключа доцільно використовувати вираз, заснований на визначенні даних кодів в часовій області. За результатами криптоаналізу в часовій області були отримані характеристики, що дозволяють визначити необхідні умови реалізації заданої стійкості ключа.

Список літератури

1. Yevheniev, A. M., Sydorenko, Z. M., & Sievierinov, O. V. (2025). Забезпечення цілісності даних у системах промислового інтернету речей на основі використання завадостійких кодів. Radiotekhnika, (221), 46-50.

2. Євгеньєв, А. М., Сидоренко, З. М., & Сєвєрінов, О. В. (2025). *Метод забезпечення цілісності даних у системах промислового інтернету речей*. Тези доповідей п'ятнадцятої міжнародної науково-технічної конференції, 24–25 квітня 2025 року, Том 3: секції 3, 4. - Баку – Харків – Жиліна – 2025.

3. Горбенко, Ю. І., & Ганзя, Р. С. (2014). Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем. *Восточно-Европейский журнал передовых технологий*, *1*(9 (67)), 8-16.

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ OPENGFW ЩОДО ВИЯВЛЕННЯ СУЧАСНИХ ПРОТОКОЛІВ ОБФУСКАЦІЇ МЕРЕЖЕВОГО ТРАФІКУ

Пліщенко В.С., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасний розвиток технічних засобів мережевої цензури та систем глибокого аналізу пакетів зумовлює постійне удосконалення протоколів обфускації мережевого трафіку. Протоколи обфускації нового покоління, такі як Hysteria V2 та стек протоколів Xray/V2Ray, розроблені для максимальної імітації легітимного вебтрафіку, що суттєво ускладнює їх виявлення [1]. У зв'язку з цим традиційні системи виявлення мережевих вторгнень (NIDS) та стандартні мережеві фільтри на основі сигнатурного аналізу стають практично неефективними, що створює нові виклики для моніторингу мережевої безпеки [2-4]. **Метою доповіді** є експериментальна перевірка здатності імітаційної моделі цензора OpenGFW виявляти обфускований мережевий трафік, згенерований протоколами VLESS з розширенням XTLS-Reality та Hysteria V2, а також пошук комплексних методів їх детектування.

В ході практичних експериментів базова архітектура OpenGFW не продемонструвала достатньої ефективності у класифікації обфускованого трафіку як аномального, оскільки зазначені протоколи успішно обходять сигнатурний аналіз та імітують легітимні з'єднання. Отримані результати свідчать, що для виявлення подібних обфускованих VPN-тунелів є необхідною інтеграція більш просунутих рішень, зокрема платформ розширеного виявлення і реагування (XDR/EDR). Окрім цього, критично важливим є впровадження методів активного зондування (active probing), індивідуально змодельованих для кожного протоколу обфускації.

Для підвищення ймовірності виявлення обфускованого трафіку варто поєднувати застосування методів активного втручання разом з одночасною інтеграцією пасивних методів аналізу трафіку, наприклад, виявлення специфічних характеристик мережевого з'єднання, таких як використання самопідписаних сертифікатів тощо.

Список літератури

1. L. Al-Bakhat and S. Almuhammadi. «Intrusion Detection on QUIC Traffic: A Machine Learning Approach». 7th International Conference on Data Science and Machine Learning Applications (CDMA). pp. 194-199. 2022. DOI: 10.1109/CDMA54072.2022.00037.

2. Sina Ahmadi. «Network Intrusion Detection in Cloud Environments: A Comparative Analysis of Approaches». International journal of advanced computer science and applications. 2024. 15 (3). DOI: 10.14569/IJACSA.2024.0150301.

3. Wails, Ryan, et al. «Censorship evasion with unidentified protocol generation». 34th USENIX Security Symposium (USENIX Security 25). pp. 763-782. 2025.

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

ВИЯВЛЕННЯ ОБФУСКОВАНОГО МЕРЕЖЕВОГО ТРАФІКУ В NEXT-GEN SIEM-СИСТЕМАХ

Пліщенко В.С., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Стрімкий розвиток інформаційно-комунікаційних систем, мережевих технологій та глобальна цифровізація призвели до використання зловмисниками складних векторів атак, що включають використання обфускованих каналів передачі інформації для приховування командно-контрольної інфраструктури (C2) та ексфільтрації даних [1]. Традиційні системи глибокої інспекції пакетів (DPI) та сигнатурного аналізу втрачають ефективність проти сучасних протоколів обфускації, що здатні імітувати легітимний мережевий трафік та підміняти TLS-сертифікати популярних сервісів [2, 3].

Метою дослідження є експериментальна перевірка ефективності систем Next-Gen SIEM на базі Wazuh та Suricata NIDS щодо виявлення обфускованих каналів комунікації, які використовують імітацію легітимних протоколів і підміну TLS-сертифікатів.

У ході практичного експерименту в хмарному середовищі за допомогою стеку Xray було розгорнуто обфускований VPN-тунель із використанням протоколу VLESS та розширення XTLS-Reality. Після цього було налаштовано дзеркалювання трафіку для його подальшого аналізу. Тунель було сконфігуровано з параметрами uTLS: chrome і цільовим доменом google.com для маскування з'єднання. Аналіз метаданих потоку та відбитка TLS-рукостискання системою моніторингу дозволив зафіксувати аномалію: було згенеровано сповіщення «CRITICAL: Xray Reality Anomaly (Malformed TLS Record to google.com)», що відповідає техніці Protocol or Service Impersonation з бази знань MITRE ATT&CK (T1001.003). Це дало змогу виявити підроблений самопідписний TLS-сертифікат, який був згенерований і використаний під час підключення до віддаленого сервера Xray.

Таким чином, проведений експеримент показав, що використання глибокого аналізу метаданих у поєднанні з правилами кореляції Next-Gen SIEM-систем дає змогу частково ідентифікувати сучасні методи обфускації.

Список літератури

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

2. M. Fuentes-García, J. Camacho and G. Maciá-Fernández, «Present and Future of Network Security Monitoring». IEEE Access, vol. 9. pp. 112744-112760. 2021. DOI: 10.1109/ACCESS.2021.3067106.

3. Sina Ahmadi. «Network Intrusion Detection in Cloud Environments: A Comparative Analysis of Approaches». International journal of advanced computer science and applications (IJACSA), 15 (3). 2024. DOI: 10.14569/IJACSA.2024.0150301.

МЕТОДИ ВИЯВЛЕННЯ ФІШИНГОВИХ ВЕБ-РЕСУРСІВ

Бочарова М.І., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком цифрових технологій та активним використанням веб-сервісів у повсякденному житті проблема фішингових атак набуває дедалі більшої актуальності [1, 2]. Фішинг є одним із найпоширеніших видів атак соціальної інженерії, метою яких є введення користувача в оману для отримання його конфіденційних даних [3]. Зловмисники часто використовують підроблені електронні листи, повідомлення в месенджерах або SMS-повідомлення, що містять посилання на фальшиві веб-сайти, зовні схожі на офіційні ресурси банків, онлайн-сервісів або державних установ. Унаслідок цього користувач може помилково ввести логін, пароль, реквізити банківської картки або іншу конфіденційну інформацію [4].

Метою роботи є дослідження актуальних методів виявлення фішингових веб-ресурсів та визначення ознак, які можуть бути використані для їх автоматичної класифікації.

У результаті проведеного дослідження визначено найбільш поширені ознаки фішингових веб-ресурсів, зокрема використання доменних імен, подібних до назв відомих сервісів, нетипову структуру URL-адрес, наявність форм введення конфіденційних даних, а також елементи, що імітують інтерфейс легітимних веб-ресурсів.

На основі виявлених ознак визначено основні методи виявлення фішингових веб-ресурсів, а саме: методи аналізу URL-адреси, методи аналізу домену та інфраструктури ресурсу, методи аналізу HTML/DOM-структури веб-сторінки, а також методи виявлення візуальної подібності до легітимних сервісів.

Отримані результати можуть бути використані як основа для формування набору ознак та подальшої побудови моделей машинного навчання в системах автоматичного виявлення фішингових веб-ресурсів.

Список літератури

1. Moruf Akin Adebowale, Khin T. Lwin, Mohammad Alamgir Hossain. Intelligent phishing detection scheme using deep https://doi.org/10.1108/jeim-01-2020-0036
2. Д'якова, Н. Є., Сєвєрінов, О. В. (2022). Тестування вразливостей сучасних веб-ресурсів / Проблеми інформатизації: десята міжнародна науково-технічна конференція, 24–25 листопада 2022 року, Том 1. - Черкаси – Баку – Бельсько-Бяла – Харків.
3. Shivam Lohani. Social Engineering: Hacking into Humans. International Journal of Advanced Studies of Scientific Research, Vol. 4, No. 1, 5 лютого 2019, URL: https://ssrn.com/abstract=3329391
4. Голубничий, Д.Ю., Сєвєрінов, О.В., Коломійцев, О.В., Місюра, О.М., Третяк, В.Ф., Власов, А.В., Крук, Б.М. (2021). Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації.
5. Що таке фішинг і фішингова атака. HostIQ. URL: https://hostiq.ua/blog/ukr/internet-phishing/

ЗАХИСТ ВЕБ-СЕРВІСУ ОБМІНУ ПОВІДОМЛЕННЯМИ ВІД СПАМУ ТА BRUTE-FORCE АТАК

Кот А.В., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Веб-сервіси обміну повідомленнями широко використовуються для організації комунікації в режимі реального часу, однак вони є вразливими до кіберзагроз, зокрема спам-активності та атак типу brute-force. Недостатній рівень захисту може призводити до перевантаження системи, зниження продуктивності та несанкціонованого доступу до облікових записів.

Відповідно до міжнародних стандартів інформаційної безпеки, захист веб-сервісів повинен включати механізми автентифікації, контролю доступу і моніторингу подій [1]. Особливу роль відіграє обмеження кількості спроб входу, що дозволяє зменшити ефективність brute-force атак [2].

Метою роботи є розробка системи захисту веб-сервісу обміну повідомленнями від спам-активності та brute-force атак. У роботі реалізовано веб-сервіс обміну повідомленнями з механізмами захисту, зокрема:

- обмеження частоти запитів (rate limiting);
- виявлення повторюваних повідомлень;
- обмеження кількості невдалих спроб автентифікації;
- журналювання подій безпеки;
- інформування адміністратора про інциденти.

Механізм обмеження частоти запитів базується на аналізі активності користувача у визначеному часовому інтервалі, що дозволяє запобігти надмірному навантаженню системи. Виявлення підозрілої активності здійснюється шляхом аналізу поведінки користувачів. Використання журналювання подій відповідає рекомендаціям щодо моніторингу безпеки веб-додатків і дозволяє своєчасно виявляти інциденти [3, 4]. Запропонований підхід забезпечує підвищення рівня захисту веб-сервісу та зменшує ризик реалізації атак.

Список літератури

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. 3rd ed. [Чинний від 2022-10]. Вид. офіц. Geneva: ISO/IEC, 2022. 19 с.

2. NIST SP 800-63B-4. Digital Identity Guidelines: Authentication and Authenticator Management/ D. Temoshok, J. L. Fenton, Y. Y. Choong, N. Lefkovitz, A. Regenscheid, R. Galluzzo, J. P. Richer. [Чинний від 2025-07]. Вид. офіц. Gaithersburg, MD: NIST, 2025. 118 с.

3. OWASP Top 10:2025. URL: https://owasp.org/Top10/2025/ (дата звернення: 01.04.2026).

4. Дорофєєва, К., Сєвєрінов, О., Сидоренко, З., & Сухотеплий, В. (2025). Застосування інструмента аналізу безпеки для виявлення критичних вразливостей у веб-додатках. *Вісник Херсонського національного технічного університету*, *3*(4 (95)), 62-68.

МЕТОДИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ У ЛАНЦЮГУ ПОСТАЧАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Сухарєв І.С., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Забезпечення безпеки ланцюга постачання програмного забезпечення (ПЗ) та контроль використання сторонніх бібліотек наразі є важливою складовою сучасного процесу розробки ПЗ. Значна частина сучасних програмних продуктів створюється з активним використанням готових бібліотек і пакетів відкритого коду [1], що дає змогу скоротити час і вартість розробки. Водночас використання зовнішніх залежностей створює додаткові ризики, пов'язані з можливими вразливостями, компрометацією пакетів або використанням застарілих компонентів. Ускладнення структури залежностей, зокрема транзитивних, ускладнює своєчасне виявлення таких загроз [2].

Метою доповіді є дослідження методів автоматизованого виявлення вразливостей у зовнішніх залежностях програмних проєктів із використанням спеціалізованих баз даних і сервісів безпеки, а також розробка алгоритму формування рекомендацій щодо оновлення, заміни або вилучення потенційно небезпечних компонентів.

У доповіді наводяться результати розробки програмного засобу мовою Python, який реалізує функції побудови повного дерева залежностей проєкту, автоматичного зіставлення версій бібліотек із записами в базах CVE та OSV [3], оцінювання критичності виявлених вразливостей за метрикою CVSS [4], а також формування звітів з рекомендаціями щодо зниження ризиків шляхом оновлення компонентів, їх заміни або пошуку безпечніших альтернатив.

Наведені результати свідчать, що впровадження подібних інструментів у CI/CD-процеси дозволяє значно зменшити ймовірність успішних атак на ланцюжок постачання та забезпечує безперервний моніторинг безпеки програмного продукту без суттєвого ускладнення процесу розробки. Отримані результати підтверджують необхідність комплексного підходу до аудиту стороннього коду як важливої складової методології DevSecOps.

Список літератури

1. OWASP Top 10 Software Supply Chain Security. OWASP Foundation. 2023. URL: https://owasp.org/www-project-top-10-software-supply-chain-security-risks/.

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. Vulnerability Analysis in Open Source Dependencies. GitHub Security Advisory Database. URL: https://github.com/advisories .

4. CVSS v3.1 Specification Document. FIRST.org. URL: https://www.first.org/cvss/v3.1/specification-document .

АЛГЕБРАЇЧНІ ВЛАСТИВОСТІ АЛГОРИТМУ ASCON У КОНТЕКСТІ КУБІЧНИХ АТАК

Руженцев В.І., Куценко Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток сучасних стандартів легковагової криптографії обумовлює необхідність поглибленого аналізу їхньої стійкості до алгебраїчних атак, які базуються на поданні криптографічних перетворень у вигляді систем булевих рівнянь над полем GF(2). Такий підхід дозволяє досліджувати криптографічні алгоритми з позицій їхньої внутрішньої алгебраїчної структури та виявляти потенційні вразливості, що не завжди очевидні при класичному аналізі. Особливу увагу в цьому контексті привертає алгоритм Ascon, який у 2023 році був стандартизований Національним інститутом стандартів і технологій США як базовий алгоритм легковагової криптографії

Алгоритм Ascon побудований на губчастій конструкції та використовує внутрішній стан фіксованого розміру, до якого послідовно застосовуються раундові перетворення. Кожен раунд включає додавання константи, нелінійне перетворення у вигляді 5-бітного S-блоку та лінійний дифузійний шар [1].

Нелінійний шар реалізується у bit-sliced формі, що забезпечує ефективність реалізації, але водночас обмежує початкову алгебраїчну складність функції. Лінійний шар, заснований на операціях XOR і циклічних зсувах, забезпечує швидке розповсюдження впливу окремих бітів по всьому стану. Така архітектура дозволяє досягти високої продуктивності, однак з точки зору алгебраїчного криптоаналізу вона створює передумови для побудови компактних поліноміальних моделей.

Алгебраїчне представлення алгоритму здійснюється через запис кожного вихідного біта як булевої функції від вхідних змінних у вигляді алгебраїчної нормальної форми. У цьому випадку функція описується поліномом над GF(2), а її складність визначається алгебраїчним ступенем, тобто максимальним ступенем мономів у цьому поліномі. Алгебраїчний ступінь є одним із ключових параметрів, що визначають стійкість до алгебраїчних атак. Для алгоритму Ascon характерно, що S-блоки мають обмежений розмір входу, що призводить до відносно низького початкового ступеня. У результаті після одного або декількох раундів ступінь функції зростає поступово, а не досягає максимального значення миттєво. Це явище є критично важливим, оскільки повільний ріст алгебраїчного ступеня створює передумови для застосування спеціалізованих методів криптоаналізу, зокрема кубічної атаки.

Кубічна атака (cube attack) належить до класу алгебраїчних атак і базується на аналізі багатовимірних булевих функцій шляхом варіювання підмножини їхніх змінних. Нехай криптографічний алгоритм задає функцію f (k,v), де k — секретний ключ, а v — набір відкритих або керованих змінних. Обирається підмножина змінних C={v1,v2,…,vt}, яка називається кубом, після чого виконується повний перебір усіх можливих значень цих змінних. Для кожної комбінації обчислюється значення функції, і результати підсумовуються за модулем два. У результаті отримується нова функція від ключа p(k)), яка називається суперполіномом.

Ключова властивість cube attack полягає в тому, що при певному виборі куба всі члени полінома, які містять хоча б одну змінну з куба у степені менше за максимальний, занулюються при підсумовуванні. У результаті залишається лише частина функції, яка залежить від змінних поза кубом, зокрема від бітів ключа. Якщо алгебраїчний ступінь функції обмежений, то існує можливість підібрати такий куб, для якого суперполіном буде або лінійною функцією від ключа, або функцією низького ступеня. Це дозволяє відновлювати ключ або його частини шляхом розв'язання значно спрощеної системи рівнянь [2].

Ефективність cube attack визначається кількома факторами. По-перше, це алгебраїчний ступінь функції: чим він нижчий, тим більша ймовірність існування корисних кубів. По-друге, важливу роль відіграє структура залежностей між змінними, яка визначає, які мономи залишаються після підсумовування. По-третє, критичним є вибір самого куба, оскільки від цього залежить форма суперполінома. У загальному випадку задача вибору куба є складною комбінаторною проблемою, що має експоненційну складність, однак на практиці можуть застосовуватися евристичні підходи, які дозволяють знаходити ефективні куби. Особливий інтерес становлять так звані high-dimensional cube атаки, в яких розмір куба є великим. Зі збільшенням розмірності куба зростає ймовірність того, що всі небажані мономи будуть занульовані, однак різко зростає обчислювальна складність атаки. Теоретично складність такої атаки становить 2t, де t - розмір куба. Проте важливо відзначити, що навіть при великих значеннях ttt можливе використання статистичних методів, які дозволяють оцінювати властивості суперполінома без повного перебору, що відкриває нові можливості для практичної реалізації атак. У контексті алгоритму Ascon cube attack є особливо релевантною через його алгебраїчну структуру. Обмежений алгебраїчний ступінь S-блоків та поступове зростання складності функції по раундах створюють умови, за яких для скорочених версій алгоритму можуть існувати куби, що призводять до інформативних суперполіномів. Це означає, що для певної кількості раундів можливе відновлення залежностей від ключа з меншою складністю, ніж це передбачено теоретичними оцінками.

Важливим аспектом є також те, що сучасні оцінки криптостійкості часто базуються на припущенні про повне насичення алгебраїчного ступеня після достатньої кількості раундів. Проте відсутність точних аналітичних результатів щодо швидкості цього насичення залишає відкритим питання про реальний запас стійкості алгоритму. У цьому контексті існує обґрунтоване припущення, що оцінки стійкості можуть бути завищеними, особливо для сценаріїв, де використовуються скорочені версії алгоритму або специфічні режими роботи. У рамках даного дослідження пропонується підхід до аналізу стійкості алгоритму Ascon, що базується на побудові його алгебраїчної моделі, дослідженні властивостей S-блоків та аналізі динаміки зростання алгебраїчного ступеня. Особлива увага приділяється дослідженню cube attack, включаючи аналіз умов її ефективності, та оцінки властивостей суперполіномів. Передбачається проведення експериментального аналізу для скорочених версій алгоритму з метою перевірки теоретичних висновків та оцінки практичної складності атаки [3].

У контексті cube-атак оцінка криптостійкості алгоритмів, зокрема Ascon, суттєво залежить від набору параметрів, які в класичних підходах часто інтерпретуються неточно або надто оптимістично. Cube attack ґрунтується на алгебраїчному представленні криптографічної функції у вигляді булевого полінома та використанні властивостей алгебраїчної нормальної форми (ANF), зокрема ефекту елімінування мономів при сумуванні по підмножинах змінних. У цьому контексті ключовими стають такі характеристики, як алгебраїчний степінь функції, розмір і структура cube, а також поведінка суперполіномів, які утворюються після сумування.

Одним із найбільш неточних показників у контексті cube attack є алгебраїчний ступінь функції як “гарантія стійкості”. У класичній інтерпретації вважається, що високий ступінь булевої функції автоматично ускладнює алгебраїчні атаки. Проте для cube attack цей показник є лише верхньою межею складності, оскільки атака експлуатує не загальний ступінь функції, а ступінь суперполінома, який може бути значно нижчим за глобальний алгебраїчний ступінь алгоритму. Таким чином, навіть функції з високим ступенем після достатньої кількості раундів можуть залишати локальні структури низького ступеня, що робить можливим побудову ефективних cube-атак, особливо для скорочених версій алгоритму.

У класичних моделях вважається, що після достатньої кількості ітерацій ступінь функції досягає максимального значення і подальші алгебраїчні атаки стають неефективними. Проте для cube attack критичною є не лише глобальна поведінка ступеня, а й локальні алгебраїчні структури, які можуть зберігатися навіть після досягнення високого ступеня. Це означає, що навіть “насичені” перетворення можуть залишати підструктури, придатні для побудови ефективних кубічних атак. Отримані результати свідчать про те, що алгебраїчні властивості алгоритму Ascon, зокрема обмежений ступінь нелінійних перетворень та його поступове зростання, можуть створювати передумови для застосування cube attack. Це підкреслює необхідність більш детального аналізу криптостійкості легковагових алгоритмів з урахуванням їхньої алгебраїчної структури та потенційних векторів атак.

Список літератури

1. Lightweight cryptography project of the American National Institute of Standards and Technology, 2015. Електронний ресурс. Режим доступу: https://csrc.nist.gov/projects/lightweight-cryptography

2. Lars R. Knudsen. Truncated and higher order differentials. In Bart Preneel, editor, Fast Software Encryption, pp. 196–211, Berlin, 1995. Springer Berlin Heidelberg. Електронний ресурс. Режим доступу: https://doi.org/10.1007/3-540-60590-8_16

3. Jules Baudrin, Anne Canteaut, and Léo Perrin. Practical cube attack against nonce misused Ascon. IACR Transactions on Symmetric Cryptology, 2022(4): pp. 120–144, Dec. 2022. Електронний ресурс. Режим доступу: https://doi.org/10.46586/tosc.v2022.i4.120-144

4. Cihangir Tezcan. Truncated, impossible, and improbable differential analysis of ascon. Cryptology ePrint Archive, Paper 2016/490, 2016. Електронний ресурс. Режим доступу: https://eprint.iacr.org/2016/490

МЕТОД РАННЬОГО ВИЯВЛЕННЯ МІЖЛАНЦЮГОВИХ SANDWICH-АТАК У МОСТОВИХ ПРОТОКОЛАХ ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМ

Антіпін В.С., Олійников Р.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток міжланцюгових протоколів у децентралізованих системах ускладнив структуру MEV-загроз. Якщо в межах одного блокчейна перевага нападника зазвичай формується через спостереження за публічним мемпулом і зміну порядку включення транзакцій, то в міжланцюговому середовищі вона може виникати ще на етапі появи події у вихідному ланцюгу, коли операція в цільовій мережі ще не стала локально видимою [2, 3, 5]. Саме тому міжланцюговий MEV сьогодні розглядається як окремий напрям, для якого визначальними є затримки між доменами, різна фіналізація та прозорість міжланцюгових повідомлень.

Одним із найнебезпечніших проявів цього механізму є міжланцюгові sandwich-атаки в мостових протоколах на основі пулів ліквідності [5]. Їхня особливість полягає в тому, що подія у вихідному ланцюгу може розкривати параметри майбутнього обміну раніше, ніж відповідна операція стане видимою в мережі призначення. Унаслідок цього нападник отримує структурну інформаційну перевагу й може підготувати front-run-транзакцію ще до появи транзакції жертви в локальному середовищі. Дослідження на даних протоколу Symbiosis за період з 10 серпня до 10 жовтня 2025 року показало, що сукупний прибуток таких атак перевищив 5,27 млн дол. США, або 1,28 % загального обсягу міжланцюгових переказів у вибірці [5].

Звичайні засоби виявлення MEV, орієнтовані на локальний мемпул, перестановку транзакцій у блоці або аномальну поведінку окремого пулу ліквідності, у такому випадку виявляються недостатніми. Ключова ознака атаки виникає не в одному блокчейні, а в причинному зв'язку між подією у вихідному ланцюгу та виконанням у цільовому. Це підтверджують і дослідження міжланцюгового арбітражу, які показують, що вирішальну роль у таких сценаріях відіграють саме часові затримки та інфраструктурні переваги [1].

Запропонований підхід спирається не на аналіз окремої транзакції, а на виявлення причинно пов'язаного міжланцюгового ланцюжка подій. На відміну від підходів, що фіксують лише локальні ознаки front-running у межах одного блокчейна, така схема враховує зв'язок між подією ініціації, мостовим повідомленням і виконанням у цільовому ланцюгу. Основою виявлення виступають не ізольовані транзакції, а цілісний шаблон поведінки, для якого обчислюється показник ранньої поінформованості Δ_{info} та інтегральна оцінка підозрілості. Саме ця зв'язка – міжланцюговий причинно-часовий ланцюжок, показник ранньої поінформованості та комбінований вектор ознак – і становить головну відмінність запропонованого методу від локальних детекторів, що бачать тільки цільовий ланцюг.

Міжланцюгову sandwich-атаку зручно подавати у вигляді ланцюжка

$$\mathrm{p} = \langle e_s,\ \mathrm{m_r},\ \mathrm{t_f},\ \mathrm{t_v},\ \mathrm{t_b} \rangle,$$

де e_s – подія ініціації міжланцюгового обміну у вихідному ланцюгу;

m_r – повідомлення мосту або релеєра;

t_f – front-run-транзакція нападника в цільовому ланцюгу;

t_v – транзакція користувача;

t_b – завершальна транзакція нападника (*back-run*), що фіксує результат після зміни ціни.

Атака має місце тоді, коли послідовність $t_f \to t_v \to t_b$ у цільовому ланцюгу з'являється не лише як реакція на локальний мемпул, а як наслідок події e_s у вихідному ланцюгу.

Інакше кажучи, нападник використовує міждоменний інформаційний витік для отримання переваги ще до того, як жертва стає помітною у звичайному локальному середовищі. Така постановка відповідає механіці, описаній у свіжому дослідженні саме цього класу атак.

Економічний зміст атаки можна подати через функцію

$$\Pi(p) = \Delta V - C_{gas} - C_{bridge} - C_{time} - R_{fail},$$

де ΔV – вартість, отримана внаслідок зміни ціни в пулі ліквідності;

C_{gas} – витрати на транзакції нападника;

C_{bridge} – супутні витрати міжланцюгової інфраструктури;

C_{time} – втрати, пов'язані із затримками між доменами;

R_{fail} – ризик неповного або повного зриву сценарію.

Для одно-ланцюгової sandwich-атаки головним є місце у блоці та ціна газу, тоді як у міжланцюговому сценарії критичною стає також затримка між появою події у вихідному ланцюгу й фактичним виконанням у цільовому. Саме часовий розрив між цими фазами створює простір для випереджального впливу на ціну в пулі ліквідності.

Для виявлення таких шаблонів використовується вектор ознак

$$x(p) = \langle \Delta_{sm}, \Delta_{mv}, \Delta_{fv}, \Delta_{vb}, \delta_{price}, \sigma_{slip}, \rho_{pool}, \kappa_{addr}, \eta_{route} \rangle,$$

де Δ_{sm} – проміжок між подією ініціації та появою мостового повідомлення;

Δ_{mv} – інтервал між мостовим повідомленням і входом операції користувача до вікна виконання в цільовому ланцюгу;

Δ_{fv} – випередження front-run-транзакції нападника відносно транзакції користувача;

Δ_{vb} – інтервал між операцією користувача та завершальною транзакцією нападника;

δ_{price} – відхилення ціни після front-run;

σ_{slip} – фактичне прослизання користувача;

ρ_{pool} – частка ліквідності пулу, на яку вплинув шаблон атаки;

κ_{addr} – повторюваність тих самих адрес або кластерів адрес у суміжних випадках;

η_{route} – стабільність одного й того самого міжланцюгового маршруту в серії підозрілих епізодів.

Такий набір поєднує часові, економічні, маршрутні й поведінкові сигнали, що особливо важливо для міжланцюгового середовища, де жодна окрема ознака сама по собі не є достатньою.

Метод виявлення будується як трирівневий позаланцюговий конвеєр і може застосовуватися в системах спостереження за мостовими маршрутами в режимі, наближеному до реального часу.

На першому етапі формується журнал подій, у який потрапляють події ініціації міжланцюгового обміну, повідомлення мостів і релеєрів, а також події обміну в пулах ліквідності цільового ланцюга.

На другому етапі у ковзному часовому вікні для заздалегідь визначених маршрутів і пар активів будуються кандидатні причинно пов'язані ланцюжки між двома мережами. Це зменшує обчислювальну складність, оскільки аналіз виконується не по всіх можливих подіях глобально, а в межах конкретних маршрутів, активів і часових інтервалів.

На третьому етапі для кожного ланцюжка обчислюється інтегральна оцінка підозрілості

$$S(p) = \sum w_i z_i(x_i),$$

де z_i – нормалізовані значення ознак;

w_i – ваги цих ознак.

Якщо $S(p) \geq \theta$ – ланцюжок позначається як потенційна міжланцюгова sandwich-атака.

Ваги w_i пропонується задавати комбіновано: експертно – на основі механіки атаки та емпірично – за історичними інцидентами і фоновою легітимною активністю. Це зменшує залежність від ручного налаштування та не потребує великої розміченої вибірки.

Показник ранньої поінформованості пропонується подавати у вигляді

$$\Delta_{info} = t(t_f) - t(e_s),$$

де $t(t_f)$ – час появи front-run-транзакції нападника;

$t(e_s)$ – час події ініціації у вихідному ланцюгу.

Якщо це значення систематично менше за типовий час реакції локального ринку, можна припустити, що нападник використовує не лише локальний мемпул, а й інформацію з іншого домену. Це дозволяє відокремити міжланцюгову sandwich-атаку від звичайної конкуренції торгових ботів у межах одного блокчейна. Метод є найбільш придатним для маршрутів, у яких мостові події або повідомлення дозволяють відновити параметри майбутнього обміну до етапу виконання.

Порогове значення для інтегральної оцінки підозрілості не слід вважати фіксованим. Його варто калібрувати на валідаційній вибірці з урахуванням хибнопозитивних і хибнонегативних спрацювань. Тому поріг має залежати від профілю ризику конкретного маршруту, активу або пулу ліквідності.

З метою оцінювання ефективності, для порівняння потрібен базовий детектор, який аналізує лише локальні події цільового ланцюга без урахування подій ініціації у вихідному. Такий підхід фіксує локальні шаблони front-running і цінового впливу, але не виявляє міждоменний інформаційний витік. Порівняння з ним дозволяє перевірити, чи справді врахування причинно-часового зв'язку між двома ланцюгами зменшує кількість пропущених атак. Ефективність методу можна оцінювати за метриками precision, recall, F1-score, а також за середнім часом випереджального виявлення, часткою випадків із підтвердженим прибутком нападника та повторюваністю маршрутів і адресних шаблонів.

Регулярна поява ланцюжків $e_s \to t_f \to t_v \to t_b$, мала варіативність інтервалу Δ_{fv}, повторюваність адресних кластерів і суттєве прослизання в користувачів вказують на те, що міст або маршрут розкриває надмірний обсяг інформації до етапу виконання. Це дозволяє використовувати метод не лише для виявлення атак, а і для оцінювання інформаційної вразливості конкретних мостових протоколів.

Обмеженням підходу є залежність від повноти журналу подій, точності часової синхронізації між мережами та доступності даних про маршрути виконання. У сценаріях із непрозорими каналами передавання або багатокроковими маршрутами побудова причинно пов'язаного ланцюжка ускладнюється, що підвищує вимоги до калібрування порогового значення та збільшує ризик хибнопозитивних спрацювань.

Протидія таким атакам має бути спрямована насамперед на зменшення інформативності подій у вихідному ланцюгу. Для цього можуть застосовуватися відкладене розкриття параметрів обміну, схеми commit–reveal, приватні канали передавання повідомлень або зміна структури мостових подій так, щоб із них неможливо було завчасно відновити намір користувача. Отже, міжланцюгові sandwich-атаки доцільно виявляти не за ізольованими локальними подіями, а за причинно пов'язаними ланцюжками між двома мережами. Такий підхід дає змогу фіксувати сценарії, які залишаються непомітними для локальних детекторів, і краще відповідає природі міжланцюгового MEV.

Список літератури

1. Cross-Chain arbitrage: the next frontier of MEV in decentralized finance / B. Öz et al. URL: https://arxiv.org/abs/2501.17335.
2. Flash boys 2.0: frontrunning, transaction reordering, and consensus instability in decentralized exchanges / P. Daian et al. URL: https://arxiv.org/abs/1904.05234.
3. Mancino D., Sevim H. O. SoK: the evolution of maximal extractable value, from miners to cross-chain. URL: https://arxiv.org/abs/2603.07716.
4. Qin K., Zhou L., Gervais A. Quantifying blockchain extractable value: how dark is the forest?. URL: https://arxiv.org/abs/2101.05511.
5. The walls have ears: unveiling cross-chain sandwich attacks in defi / C. Li et al. URL: https://arxiv.org/abs/2511.15245.

ПОВЕДІНКОВІ ІНДИКАТОРИ КОМПРОМЕНТАЦІЇ ТА МЕТОДИ ДЕТЕКЦІЇ ФІШИНГОВОЇ АТАКИ BRATA В СЕРЕДОВИЩІ ANDROID

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

Операційна система Android є однією з найпоширеніших платформ для мобільних пристроїв у світі. Її популярність обумовлена відкритістю, гнучкістю та широкими можливостями кастомізації, що сприяє активному використанню як у споживчому секторі, так і в корпоративному середовищі.

Але зростання популярності Android безпосередньо впливає на їх безпеку.

Найбільш поширеними загрозами є malware (трояни, spyware), фішингові атаки, перехоплення даних, несанкціонований доступ до пристрою, вразливості в застосунках [1, 2].

Фішингові атаки на мобільні пристрої використовують підроблені інтерфейси або повідомлення для отримання конфіденційних даних; близько 30–40% мобільних інцидентів пов'язані із соціальною інженерією. Зростання таких загроз зумовлене активним використанням смартфонів у фінансових операціях, а кількість атак щорічно зростає на 15-25% [3].

Особливу небезпеку становить шкідливе ПЗ класу Remote Access Trojan, зокрема BRATA, що поєднує фішинг і віддалене керування пристроєм та маскується під легітимні застосунки для прихованого перехоплення даних [4].

Метою дослідження є визначення поведінкових індикаторів компрометації BRATA та аналіз методів її виявлення на основі статичного, динамічного й мережевого аналізу.

Визначення поведінкових характеристик BRATA здійснювалося шляхом поєднання статичного, динамічного та мережевого аналізу відповідно до сучасних підходів, описаних у звітах ENISA та рекомендаціях OWASP Foundation.

Статичний аналіз дозволив дослідити структуру застосунку, перелік дозволів, виклики API та використання служб доступності. Динамічний аналіз у контрольованому середовищі забезпечив спостереження за реальною поведінкою програми під час виконання, включаючи взаємодію з інтерфейсом користувача та ініціювання мережевих з'єднань. Мережевий аналіз доповнив дослідження шляхом виявлення шаблонів взаємодії з командними серверами та інтенсивності передачі даних, що узгоджується з результатами досліджень ThreatFabric і Cleafy. Такий підхід допомагає сформувати повний профіль поведінки шкідливого застосунку.

Аналіз функціонування BRATA показує, що програма використовує приховування структури коду, динамічне завантаження компонентів і служби доступності Android для отримання контролю над інтерфейсом пристрою [5]. У шкідливих застосунках такі механізми застосовуються у 70-90% випадків, тоді як у легітимних - лише у 5-10%. Крім того, BRATA взаємодіє з командними серверами (C2) та передає зібрані дані.

Індикаторами компрометації є надмірна кількість дозволів (20-30 проти 8-15), використання служб доступності без необхідності, інтенсивна мережева активність (до 30-40 запитів за хвилину), приховування іконки та підвищена фонова активність.

Для оцінки ефективності виявлення зазначених ознак проведено порівняльний аналіз методів детекції (таблиця 1).

Таблиця 1 - Порівняльний аналіз методів детекції

Метод аналізу	Предмет аналізу	Виявлення ознак BRATA	Виявлення інших атак
Статичний	Код, структура APK, дозволи, API	Надмірна кількість дозволів, використання служб доступності, підозрілі компоненти	Банківські трояни, шпигунське ПЗ, рекламне ПЗ
Динамічний	Поведінка під час виконання	Фонова активність, взаємодія з UI, C2	RAT, шпигунське ПЗ, кейлогери
Мережевий	Трафік, домени, частота запитів	Інтенсивні запити, C2-з'єднання	Ботнети, шкідливе ПЗ для викрадення даних

Аналіз показав, що статичний метод є швидким і малоресурсним, але обмеженим через механізми приховування, динамічний - більш точним, проте ресурсоємним, тоді як мережевий дозволяє виявляти приховану активність, але ускладнюється при шифруванні трафіку.

У сукупності їх застосування забезпечує ефективну та універсальну основу для подальшого розвитку систем виявлення мобільних кіберзагроз.

Список літератури

1. Сєвєрінов, О. В., Федорченко, В. М., Перепадя, В. І., Северинов, А. В., Федорченко, В. Н., & Перепадя, В. И. (2016). Аналіз загроз персональним даним в мобільному пристрої під час використання різноманітних додатків.

2. Сєвєрінов, О. В., Федоров, І. А., & Власов, А. В. Аналіз методів детектування шкідливого програмного забезпечення // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Тези доповідей чотирнадцятої міжн. наук.-техн. конф., 25 – 26 квітня 2024 року. - Баку – Харків – Жиліна – 2024

3. ENISA. Threat Landscape Report 2023. - 2023. - URL: https://www.enisa.europa.eu/

4. ThreatFabric. Brata: a tale of three families. - 2022. - URL: https://www.threatfabric.com/blogs/brata-a-tale-of-three-families

5. Cleafy. BRATA is evolving into an Advanced Persistent Threat. - 2021. - URL: https://www.cleafy.com/cleafy-labs/brata-is-evolving-into-an-advanced-persistent-threat

БАГАТОРІВНЕВА СИСТЕМА МОНІТОРИНГУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ ІБ НА БАЗІ КОНВЕРГЕНЦІЇ SIEM, SOAR ТА XDR

Доленко О.Д., В'юхін Д.О., Городецький С.Л.
Харківський національний університет радіоелектроніки, Харків, Україна

Зростання інтенсивності цілеспрямованих атак та дефіцит аналітиків безпеки обумовлюють необхідність переходу від розрізнених інструментів захисту до конвергентних платформ. Основним завданням сучасного SOC (Security Operations Center) є мінімізація часових показників виявлення та нейтралізації загроз [1]. Сучасна стратегія побудови SOC базується на синергії трьох ключових компонентів. Системи класу SIEM (Security Information and Event Management) забезпечують збір, збагачення контекстом, кореляцію великих обсягів логів із різноманітних джерел IT-інфраструктури. XDR (Extended Detection and Response) збирає телеметрію з кінцевих точок, мережевих вузлів та електронної пошти, дозволяючи ідентифікувати складні багатоетапні атаки шляхом побудови єдиного контекстуального ланцюга подій [2]. Платформи SOAR (Security Orchestration, Automation and Response) функціонують як центральний вузол для керування засобами захисту, впроваджуючи автоматизовані сценарії, що дозволяють виконувати процедури стримування та усунення наслідків без втручання людини [3].

Метою доповіді є огляд конвергентного способу взаємодії систем збору, глибокого аналізу та автоматизації у боротьбі з кібератаками для забезпечення якомога нижчих метрик реагування на інциденти.

Розглянутий підхід полягає в об'єднаному використанні цих систем, і в такий спосіб відбувається трансформування класичної реактивної моделі безпеки у проактивну. Конвергентне використання технологій об'єднує глибокий аналіз кінцевих точок і ланцюгів процесів через XDR з кореляційною потужністю SIEM, а SOAR виступає як центральна консоль, що надає автоматизовані сценарії реагування. Аналітики мають можливість виявити загрози ще до їх безпосереднього впливу завдяки здатності системи ідентифікувати складні вектори атак, які виглядають як окремі законні дії в різних частинах мережі, але в поєднанні складають ланцюг підготовки до експлуатації. Одним з головних недоліків традиційного багатоконсольного підходу до моніторингу є розрізненість систем, через що аналітики витрачають додатковий час на перемикання між різними консолями під час обробки сповіщень; також існує проблема «втоми від сповіщень», через що аналітик може загубити реальну загрозу серед десятків хибних або не шкідливих спрацювань [2]. Об'єднана система дозволяє оптимізувати ключові метрики ефективності: показник MTTD (Mean Time to Detect/час виявлення) мінімізується за рахунок предиктивного аналізу аномалій та інтеграції з XDR, а MTTR (Mean Time to Respond/час реагування) скорочується завдяки виключенню людського фактору на етапі первинного реагування.

Як приклад реальної системи розглянуто захист пристроїв IIoT (Industrial Internet of Things), що беруть учать у технологічних процесах виробництва.

Особливістю критичної інфраструктури є використання специфічних пристроїв (ПЛК, сенсорів) та промислових протоколів (MQTT, Modbus, OPC UA), які зазвичай не підтримуються стандартними IT-засобами моніторингу. Згідно з дослідженнями [4], ефективна інтеграція IIoT у систему SIEM базується на розгортанні спеціалізованих зондів та брокерів повідомлень. Це дозволяє трансформувати низькорівневі події промислової мережі у стандартизовані логи. Таким чином IIoT-сегмент стає частиною XDR, забезпечуючи моніторинг параметрів критичної інфраструктури, SIEM збирає та нормалізує дані, що дозволяє виявляти спроби зловмисного впливу на виробничі цикли на всіх етапах кібератак, а SOAR забезпечує автоматизоване реагування на інциденти.

Порівняльний аналіз операційних метрик (табл. 1) демонструє, що впровадження конвергентної платформи дозволяє скоротити MTTD на більш ніж 90%, а MTTR до лічених секунд [4].

Таблиця 1 – Порівняння метрик для класичних та об'єднаних систем

	Classic SOC	Unified SOC
MTTD	45 хв	2 хв
MTTR	30 хв – 5 год	<40 сек

Це досягається за рахунок усунення часових затримок на передачу даних між різними системами і узгоджень між відділами співробітників та автоматизації етапу прийняття рішень у типових сценаріях атак на інфраструктуру. Таким чином, впровадження об'єднаних платформ безпеки є доцільним і необхідним кроком для підвищення рівня захищеності сучасних інформаційно-комунікаційних систем, що підтверджується значним покращенням операційних показників та ефективності реагування на інциденти інформаційної безпеки.

Список літератури

1. Sievierinov, O., Ovcharenko, M., & Vlasov, A. (2021). Enterprise Security Operations Center. 2021: Fifth International Scientific and Technical Conference "Computer and information systems and technologies".

2. Pavan Paidy. Unified threat detection platform with AI, SIEM, and XDR. International journal of artificial intelligence, data science, and machine learning. 2025. Vol. 6, no. 1.

3. Мартиненко, Я., Сєвєрінов, О., Євгеньєв, А., & Скибенко, М. (2025). Дослідження SOAR-платформ та обґрунтування вибору SPLUNK PHANTOM. *Вісник Херсонського національного технічного університету*, *3*(4 (95)), 145-152.

4. Timi Heino. Real-Time Threat Detection using SIEM for Industrial IoT Protocols. Finland : University of Turku, 2025. 54 p.

5. Москвін, К., Сєвєрінов, О., Сидоренко, З., Балагура, Д., & Литвин, А. (2025). Дослідження впливу інтеграції засобів кіберзахисту на захищеність IT-інфраструктури організації. *Вісник ХНТУ*, *2*(2 (93)), 246-255.

АНАЛІЗ ПРИЧИН ЗРОСТАННЯ ЧАСУ ПЕРЕБУВАННЯ ЗЛОВМИСНИКА В МЕРЕЖІ

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

Протягом останнього десятиліття скорочення часу перебування зловмисника в мережі (Dwell Time) вважалося ключовим показником ефективності кіберзахисту. Однак сучасні кіберінциденти демонструють зміну цієї тенденції: за даними Mandiant, у 2024 році глобальний медіанний показник зріс з 10 до 11 днів – вперше з 2010 року [1]. Це свідчить про адаптацію зловмисників і їхню здатність довше залишатися непоміченими в інформаційних системах.

Метою дослідження є ідентифікація та аналіз основних чинників, які зумовили збільшення часу перебування зловмисника в корпоративних мережах, на основі даних провідних наукових звітів у сфері кібербезпеки.

Однією із ключових причин є ускладнення початкових векторів проникнення. За даними Mandiant, експлуатація вразливостей залишається провідним способом компрометації, становлячи 33% випадків [1]. Зокрема, експлуатація невиправлених вразливостей дозволяє обходити традиційні механізми захисту та залишатися непоміченими на початкових етапах атаки, що створює передумови для подальшого закріплення в мережі.

Значну роль відіграють атаки на периферійні мережеві пристрої. За даними Verizon DBIR 2025, використання вразливостей у VPN та інших периферійних пристроях зросло майже у вісім разів [2]. Такі пристрої часто не інтегровані в централізований моніторинг, що ускладнює своєчасне виявлення.

Крім того, патерн «System Intrusion», який включає переміщення та ескалацію привілеїв, фіксується у 53% витоків даних [2], що сприяє збільшенню часу перебування зловмисника в мережі.

Зміна мотивації атак також впливає на тривалість перебування зловмисника. За даними Mandiant, кількість інцидентів зі шпигунською метою зросла на 163%, що орієнтує атаки на тривале приховане перебування в системі [1]. Водночас у випадках ransomware середній час перебування становить близько 6 днів, що свідчить про швидке завершення фінальної стадії атаки [1]. У 57% випадків організації дізнаються про компрометацію із зовнішніх джерел, що підкреслює обмеженість внутрішнього моніторингу [1].

Важливим чинником є зростання ролі сторонніх організацій. За даними Verizon DBIR, частка інцидентів за їх участю зросла з 15% до 30% [2]. Використання довірених каналів дозволяє зловмисникам маскувати активність і ускладнює її виявлення, що подовжує час перебування в мережі.

Отримані результати свідчать про неефективність традиційних підходів до кіберзахисту, орієнтованих на периметр мережі. Зростання часу перебування зловмисника до 11 днів зумовлене експлуатацією вразливостей, компрометацією облікових даних та залежністю від сторонніх сервісів. Значна

частина інцидентів виявляється зовнішніми джерелами, що підтверджує обмеженість внутрішнього моніторингу.

Необхідно забезпечити своєчасне усунення вразливостей, зокрема у VPN та мережевих пристроях, що може зменшити ризик початкового проникнення на 30-40%. Доцільно впровадити апаратну автентифікацію (FIDO2) та принцип тимчасового доступу (just-in-time), що знижує ймовірність компрометації облікових даних до 50%. Важливо обмежити збереження паролів і розмежувати робочі та особисті облікові записи. Підвищення ефективності виявлення можливе через інтеграцію журналів подій у системи SIEM та UEBA, що дозволяє скоротити час виявлення інцидентів до 30% [3].

Доцільним є перехід до моделі Zero Trust, що знижує ризик несанкціонованого доступу до 40% [4]. Регулярне проведення Red Teaming дозволяє виявляти до 60% критичних вразливостей до їх експлуатації. У сфері освіти необхідно змістити акцент на практичний аналіз інцидентів. Важливо також запровадити обов'язкові вимоги кібербезпеки для сторонніх організацій, що дозволяє зменшити ризики ланцюгових атак до-30%.

Практичні дослідження [5] показують, що навіть базове налаштування міжмережевих екранів і HTTPS-шифрування не забезпечує виявлення складних атак, які використовують легітимні облікові дані або приховані канали. Це свідчить про обмеженість ізольованого застосування засобів захисту, таких як фаєрволи, VPN чи антивіруси. Ефективний захист можливий лише за умови їх інтеграції в єдину адаптивну систему з можливостями поведінкового аналізу та виявлення аномалій.

Отже, зростання часу перебування зловмисника в системі є результатом складної взаємодії технічних, організаційних і поведінкових чинників: ускладнення векторів атак (периферійні пристрої), збільшення ролі сторонніх постачальників, поширення компрометації через infostealer malware, а також недостатня інтеграція засобів моніторингу. Зниження цього показника можливо лише за умови переходу до динамічних моделей захисту, що передбачають безперервний моніторинг, адаптацію політик безпеки та контроль доступу в режимі реального часу.

Список літератури

1. Mandiant M-Trends 2025 Report. Google Cloud Security. 2025. 94 p.
2. 2025 Data Breach Investigations Report. Verizon Business. 2025. 116 p.
3. Москвін, К., Сєвєрінов, О., Сидоренко, З., Балагура, Д., & Литвин, А. (2025). Дослідження впливу інтеграції засобів кіберзахисту на захищеність ІТ-інфраструктури організації. Вісник ХНТУ, 2(2 (93)), 246-255.
4. Moskvin K., Sievierinov O. Zero Trust Architecture in Corporate Cybersecurity Systems // Computer and information systems and technologies : Seventh International Scientific and Technical Conference, 2024. – Kharkiv : NURE, 2024. – p. 54-55.
5. Євтушенко Д. С. Порівняльний аналіз методів захисту інформації у мережах: кваліфікаційна робота магістра: спец. 172 «Електронні комунікації та радіотехніка» / Д. С. Євтушенко; ХНУРЕ. Харків, 2025. 58 с.

МЕТОДИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ У СМАРТ-КОНТРАКТАХ

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

Смарт-контракти набули широкого застосування у DeFi (Decentralized Finance, децентралізовані фінанси), системах цифрових активів та управлінні ідентичністю. Публічність коду, незворотність транзакцій та неможливість змін після розгортання формують підвищені вимоги до безпеки [1]. Інцидент із The DAO (2016), де через вразливість reentrancy було виведено значний обсяг активів, унаочнює ці ризики.

Найпоширеніші вразливості смарт-контрактів - це reentrancy, integer overflow/underflow, порушення контролю доступу та front-running, що актуалізує потребу у комплексних підходах - статичному, динамічному та формальному аналізі [2].

Метою доповіді є комплексний аналіз методів виявлення вразливостей у смарт-контрактах та порівняльна оцінка інструментів їх реалізації за критеріями точності, повноти та практичної застосовності для підвищення рівня безпеки децентралізованих систем.

Статичний аналіз передбачає дослідження програмного коду без його виконання шляхом побудови абстрактних синтаксичних дерев, графів потоку керування та аналізу потоків даних. Такий підхід дозволяє ідентифікувати типові шаблони вразливостей ще на етапі розробки та легко інтегрується в CI/CD. До основних інструментів відносяться Slither (швидкий, точний аналіз для Solidity), Mythril (символьне виконання байт-коду EVM) та Oyente (перший публічний аналізатор EVM, орієнтований на виявлення front-running і reentrancy). Перевагою є швидкість та повнота охоплення коду, проте метод схильний до хибнопозитивних спрацювань [4].

Динамічний аналіз досліджує поведінку контракту під час виконання в тестовому середовищі та дозволяє виявляти логічні помилки, що проявляються лише за певних умов. Різновидом цього підходу є фаззінг - генерація псевдовипадкових вхідних даних з метою провокування некоректної поведінки; зокрема інструмент Echidna інтегрується з локальними тестовими мережами Ethereum для перевірки інваріантів контракту. Динамічний аналіз виявляє реально експлуатаційні вразливості, однак не гарантує повноти покриття [3].

Формальна верифікація передбачає математично доведену коректність коду відносно формальної специфікації за допомогою методів перевірки моделей та доведення теорем. Інструмент Certora Prover, що активно використовується у DeFi-протоколах (Aave, Compound), дозволяє отримати строгі гарантії коректності зміни стану контракту та відсутності несанкціонованого доступу. Незважаючи на найвищу надійність, метод є ресурсомістким і потребує спеціалізованих знань [4].

Порівняльна характеристика інструментів виявлення вразливостей представлена у таблиці 1.

Таблиця 1 - Характеристика інструментів виявлення вразливостей

Інстру-мент	**Метод**	**Виявлювані вразливості**	**Точність**	**Орієнтовна вартість**
Slither	Статичний	Reentrancy, access control, tx.origin, shadowing	~90%	Безкоштовно (open-source)
Mythril	Статичний / символьне виконання	Reentrancy, integer overflow, unsafe delegatecall	~75%	Безкоштовно (open-source)
Oyente	Статичний / символьне виконання	Reentrancy, front-running, TOD	~70%	Безкоштовно (open-source)
Echidna	Динамічний / фаззінг	Логічні помилки, порушення інваріантів	Висока	Безкоштовно; витрати на тестову мережу мінімальні
Certora Prover	Формальна верифікація	Некоректна зміна стану, несанкціонований доступ	Доведена	Від $0 до $5000+

Жоден із методів не є універсальним. Статичний аналіз швидкий, але дає хибнопозитивні результати. В свою чергу динамічний виявляє реальні вразливості без повного покриття. Формальна верифікація найнадійніша, але ресурсомістка.

Таким чином пропонується оптимальна стратегія - їх комбінування. Для більшості проектів найбільш практичним вибором є Slither: безкоштовний, ~90 % точності, легко інтегрується в CI/CD. Certora Prover при тарифі від $5 000 не виправдовує себе там, де безкоштовні інструменти закривають переважну більшість вразливостей.

Список літератури

1. Терещенко Г. Ю., Кириченко І. В. Аналіз і обґрунтування використання наявних блокчейн-рішень для захисту цифрових активів. ХНУРЕ, 2024.

2. Peschanenko V., Rud V. Overview of Vulnerabilities in Smart Contracts Written in Solidity. Journal of Information Technologies in Education (ITE), 2024.

3. Luu L., Chu D.-H., Olickel H., Saxena P., Hobor A. Making Smart Contracts Smarter. Proceedings ACM SIGSAC CCS, 2016.

4. Tsankov P., Dan A., Drachsler-Cohen D., Gervais A., Bünzli F., Vechev M. Securify: Practical Security Analysis of Smart Contracts. Proceedings ACM SIGSAC CCS, 2018.

ПОРІВНЯННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ ТА ПРИВАТНОСТІ В ІНТЕРНЕТІ

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

Стрімкий розвиток цифрових технологій призвів до суттєвого збільшення обсягів персональних даних, що передаються та обробляються в мережі Інтернет. Сучасні онлайн-сервіси активно використовують інформацію про користувачів для персоналізації, аналітики та таргетованої реклами. Разом із цим зростає і кількість ризиків, пов'язаних із витоком конфіденційної інформації, відстеженням активності та втручанням у приватність користувача [1, 2].

Очікується, що глобальний ринок VPN-сервісів досягне $151,92 млрд у 2030 році, що підтверджує зростання попиту на технології цифрової приватності. Подальший розвиток засобів захисту приватності вимагає як технічного удосконалення інструментів, так і підвищення цифрової грамотності користувачів.

Метою доповіді є аналіз ефективності сучасних інструментів забезпечення анонімності в Інтернеті шляхом порівняння режимів підключення (без захисту, VPN, Tor) та оцінки їх впливу на IP-ідентифікацію, геолокацію, швидкість доступу та унікальність браузерного відбитка.

Значна частина інтернет-користувачів не усвідомлює масштаби збору цифрових слідів — IP-адреси, файлів cookies, інформації про браузер, мовні налаштування, часовий пояс тощо. За даними дослідження AmIUnique, до 81% мобільних браузерних відбитків є унікальними, що робить можливим точне відстеження поведінки окремих користувачів [3].

Анонімність та приватність в Інтернеті є взаємопов'язаними, проте не тотожними поняттями. Анонімність передбачає неможливість однозначної ідентифікації користувача, тоді як приватність стосується контролю над тим, які дані збираються та передаються третім сторонам. Важливою складовою забезпечення приватності є анонімізація даних, що передбачає вилучення ідентифікуючих характеристик таким чином, щоб особу неможливо було встановити навіть шляхом кореляції наборів даних [4].

Незважаючи на наявність технологій захисту, сучасні інструменти трекінгу дозволяють визначати поведінку користувачів високою точністю. Основні загрози включають:

- трекинг активності для рекламних цілей;
- cookies, що дозволяють повторну ідентифікацію;
- IP-ідентифікацію, яка дає змогу оцінити геолокацію;
- browser fingerprinting, який формує унікальний «цифровий профіль» пристрою.

Для мінімізації ризиків застосовуються VPN, мережа Tor, проксі-сервери та захищені месенджери. За даними GlobalStats, понад 54% користувачів не

використовують VPN, що свідчить про низьку цифрову культуру захисту приватності [5].

Порівняння режимів підключення за параметрами анонімності представлено в таблиці 1.

Таблиця 1 – Порівняння режимів підключення за параметрами анонімності.

Режим	**Без захисту**	**VPN**	**Tor**
IP-адреса	188.163.51.123	190.2.147.62	107.189.30.86
Локація	Ukraine	Netherlands	Luxembourg
Провайдер	Kyivstar PJSC	WorldStream LATAM	Luxembourg
Fingerprint унікальність (%)	unique among 4267710	VPN не змінює відбиток	unique among the 4267664
Статус збору даних (що вдалося отримати, а що ні)	Отримано реальні дані пристрою та користувача	Отримано реальні дані пристрою (VPN їх не приховує)	Реальні дані приховано (отримано лише підмінені уніфіковані дані)

Можна побачити, що мережа Tor забезпечує більший рівень анонімності, оскільки одночасно змінює IP та низку технічних параметрів браузера, проте це супроводжується суттєвим зниженням швидкості з'єднання. Варто зазначити, що висока анонімність завжди знижує швидкість інтернету через багаторазове шифрування трафіку.

У майбутньому знадобляться VPN нового покоління, які не лише змінюють IP-адресу, а й повністю маскують відбиток браузера. Так у VPN можна вбудувати функцію антидетекту, яка автоматично підмінятиме дані про пристрій користувача за окрему плату або додаткову функцію.

Список літератури

1. Computer Emergency Response Team of Ukraine Щодо обстановки в сфері кібер на 23-24 лютого 2024 року https://cert.gov.ua/article/6277822 (дата звернення 04.09.2025)

2. Голубничий, Д. Ю., Сєвєрінов, О. В., Коломійцев, О. В., Місюра, О. М., Третяк, В. Ф., Власов, А. В., & Крук, Б. М. (2021). Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації.

3. P. Laperdrix, W. Rudametkin and B. Baudry, "Beauty and the Beast: Diverting Modern Web Browsers to Build Unique Browser Fingerprints," *2016 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, 2016, pp. 878-894, doi: 10.1109/SP.2016.57.

4. Трибух А. О. «Дослідження архітектурних підходів до забезпечення приватності конфіденційних даних у хмарному середовищі» — пояснювальна записка до магістерської роботи, ХНУРЕ, 2024.

5. NordVPN 2025 VPN Usage Statistics https://www.security.org/vpn/statistics/ (дата звернення 04.09.2025)

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В АУДІОСИГНАЛАХ

Ткаченко О.Р., Садовий М.С., В'юхін Д.О.
Харківський Національний університет радіоелектроніки, м. Харків, Україна

Зростання обсягів передавання мультимедійних даних та поширення мережевих сервісів створює нові виклики у сфері інформаційної безпеки. В умовах, коли традиційні криптографічні підходи можуть привертати увагу потенційного зловмисника, методи приховування інформації в аудіосигналах дозволяють забезпечити не лише захист змісту повідомлення, але й сам факт його існування.

Частотні алгоритми та адаптивні психоакустичні методи є сучасними підходами до приховування інформації в аудіосигналах. Порівняння цих алгоритмів дозволяє оцінити їхні переваги та обмеження для практичного застосування [1].

Мета роботи полягає у проведенні порівняльного аналізу частотних алгоритмів та адаптивних психоакустичних методів приховування інформації в аудіосигналах, а також у визначенні їх ефективності за ключовими критеріями - прихованістю, стійкістю до обробки, ємністю даних і складністю реалізації.

У межах роботи передбачається дослідити особливості функціонування FFT-алгоритму, адаптивних психоакустичних підходів і базових методів стеганографії, встановити їх переваги та обмеження, а також обґрунтувати доцільність використання кожного з них залежно від вимог конкретної інформаційної системи.

У сучасній стеганографії важливо оцінювати ефективність алгоритмів не лише за технічними характеристиками, а й за практичними критеріями, такими як прихованість, стійкість до обробки та ємність даних.

У випадку використання методу прихованих символів (LSB або подібних підходів) зміни відбуваються на рівні окремих бітів цифрового представлення сигналу. Такі модифікації є мінімальними та практично не впливають на загальну структуру аудіофайлу. Однак через відсутність урахування особливостей людського слуху ці зміни можуть бути виявлені при детальному аналізі або після обробки сигналу (наприклад, стиснення чи фільтрації).

При застосуванні FFT-алгоритму зміни відбуваються у частотній області сигналу. Модифікуються амплітуди або фази окремих спектральних компонентів, що дозволяє більш гнучко контролювати вплив на сигнал. У результаті аудіофайл зазнає структурних змін у спектрі, але при цьому зберігає прийнятну якість звучання. Такі зміни є менш помітними для користувача, однак можуть бути виявлені при спектральному аналізі.

Адаптивні психоакустичні алгоритми змінюють аудіосигнал з урахуванням моделей сприйняття звуку людиною. Інформація вбудовується у ті частини сигналу, які маскуються більш гучними або домінуючими компонентами. У цьому випадку зміни є найбільш складними за структурою,

оскільки вони динамічно залежать від характеристик сигналу. Це забезпечує високий рівень прихованості, а самі модифікації практично неможливо виявити без спеціалізованого аналізу [2].

Результати аналізу ефективності алгоритмів за технічними характеристиками та практичними критеріями представлені у таблиці 1.

Таблиця 1 – Ефективність алгоритмів за технічними характеристиками та практичними критеріями

Критерій	Метод прихованих символів	FFT-алгоритм	Адаптивний психоакустичний алгоритм
Прихованість	40%	60%	90%
Стійкість до обробки	20%	70%	95%
Ємність даних	30%	60%	40%
Складність реалізації	10%	50%	80%

З аналізу таблиці видно, що давні алгоритми, хоча й прості у реалізації, мають низьку прихованість і стійкість, а їхня ємність обмежена [3]. FFT-алгоритм забезпечує середній рівень прихованості та достатню стійкість до стандартної обробки, зберігаючи при цьому помірну ємність даних. Адаптивний психоакустичний метод демонструє максимальну прихованість та стійкість, проте має обмежену ємність і високу складність реалізації.

FFT-алгоритм підходить для задач із середньою прихованістю та стійкістю, де важлива простота реалізації.

Адаптивний психоакустичний метод ефективний для систем з підвищеними вимогами до прихованості та стійкості, хоча має нижчу ємність та вищу складність реалізації. Вибір алгоритму визначається пріоритетами конкретної системи.

Список літератури

1. Голубничий, Д.Ю., Сєвєрінов, О.В., Коломійцев, О.В., Місюра, О.М., Третяк, В.Ф., Власов, А.В., Крук, Б.М. (2021). Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації.

2. Zhang J., Li S. A Survey of Audio Steganography. Journal of Information Security. 2018. 327 p.

3. Картушин, О. А. Дослідження моделей приховування інформації в мультимедійних даних з використанням стеганографічних перетворень.

4. Bhat V., Kamath S. Audio Steganography Techniques: A Review. International Journal of Computer Applications. 2015. 289 p.

КОМБІНОВАНИЙ МЕТОД ЗАХИСТУ АУДІОДАНИХ НА ОСНОВІ RSA-ШИФРУВАННЯ ТА LSB-СТЕГАНОГРАФІЇ В ЗОБРАЖЕННЯХ

Федюшин О.І., Безсонов М.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Захист аудіоінформації є актуальною задачею в умовах стрімкого розвитку засобів цифрової комунікації. Голосові повідомлення, аудіозаписи та інші акустичні дані нерідко містять конфіденційну інформацію, що потребує надійного захисту від несанкціонованого доступу та перехоплення. Існуючі методи захисту — симетричне шифрування (AES, ГОСТ), асиметричні криптосистеми (RSA, ECC) та стеганографія — зазвичай застосовуються окремо, що суттєво знижує загальний рівень захисту. Комбінування криптографічних і стеганографічних підходів дозволяє досягти синергетичного ефекту: криптографія забезпечує конфіденційність даних, тоді як стеганографія приховує сам факт передачі захищеної інформації [1]. Водночас питання практичної реалізації таких комбінованих методів для аудіоданих із збереженням прийнятної обчислювальної складності залишається актуальним. RSA є однією з найбільш відомих та досліджених асиметричних криптосистем, заснованих на обчислювальній складності задачі факторизації великих чисел [2]. Класична схема RSA передбачає вибір двох великих простих чисел p і q, обчислення модуля $n = p \cdot q$ та функції Ейлера $\varphi(n) = (p-1)\cdot(q-1)$. Відкритий ключ e обирається як взаємно просте з $\varphi(n)$ число, а закритий ключ d обчислюється як мультиплікативний обернений елемент e за модулем $\varphi(n)$, тобто задовольняє умову $e \cdot d \equiv 1 \pmod{\varphi(n)}$. Для ефективного обчислення d застосовується розширений алгоритм Евкліда (Extended GCD), що дозволяє знайти обернений елемент за $O(\log n)$ кроків [3].

Метою доповіді є розробка та аналіз комбінованого методу захисту аудіоданих, що поєднує RSA-шифрування на основі кольорового RGB-представлення аудіобайтів з LSB-стеганографією в зображеннях-контейнерах, а також оцінка криптостійкості та обчислювальної ефективності запропонованого підходу. У роботі розроблено та реалізовано систему захисту аудіоданих, що складається з двох взаємодоповнювальних рівнів захисту: криптографічного та стеганографічного. Загальна схема роботи системи передбачає наступну послідовність операцій. Перший рівень — криптографічне перетворення аудіоданих. На вхід системи подається аудіофайл у форматі WAV. Після зчитування файлу отримується масив байтів, кожен з яких набуває значень від 0 до 255. Для підготовки до шифрування кожен байт перетворюється на рядковий запис у форматі шестизначного HEX-кольору виду #XXXXXX. При цьому до запису додається випадкове символьне «сіль» (salt) з множини {a, b, c, d, e}, що заповнює незадіяні позиції до шести символів. Позиція значущого числа в рядку (на початку або в кінці) також визначається випадково (гейт). Такий підхід обфусковує розподіл значень вихідних байтів та ускладнює статистичний аналіз.

Отримані рядки інтерпретуються як HTML-кольори, з яких витягуються компоненти Alpha (A), Red (R), Green (G) та Blue (B). Кожна компонента шифрується окремо за формулою RSA:

$$c = m^{\wedge}e \bmod n$$

де m — значення компоненти кольору (0–255), e — відкрита експонента, $n = p \cdot q$ — модуль RSA. Оскільки значення m обмежені діапазоном [0, 255], а n може бути відносно невеликим, результат шифрування c не завжди вкладається у байтовий діапазон [0, 255]. У разі переповнення ($c \geq 256$) оригінальне значення m записується без шифрування, а індекс цієї позиції фіксується в окремому списку «позицій винятків». Це забезпечує коректну зворотну операцію дешифрування без втрати даних.

Закритий ключ d обчислюється за розширеним алгоритмом Евкліда. На відміну від класичного перебору, що використовується в деяких навчальних реалізаціях RSA, застосування Extended GCD гарантує знаходження оберненого елементу за детермінований час. У разі, якщо $\text{GCD}(e, \varphi(n)) \neq 1$, алгоритм повертає -1, що сигналізує про неможливість обчислення оберненого елементу для обраної пари $(e, \varphi(n))$. Алгоритм генерації e перебирає прості числа від 10-значного генератора та перевіряє взаємну простоту з $\varphi(n)$, фіксуючи до 80 кандидатів та обираючи мінімальний, що підвищує безпеку та відтворюваність генерації ключів.

Сформований масив зашифрованих байтів містить: послідовно записані індекси позицій винятків (по 4 байти кожен), маркер-роздільник (байт 254), кількість позицій винятків, поточну довжину масиву даних, та безпосередньо зашифровані компоненти кольорів. Значення d передається або зберігається окремо як закритий ключ і не включається до контейнера в незахищеному вигляді. Для зворотного перетворення (дешифрування) кожна компонента обробляється за формулою:

$$m = c^{\wedge}d \bmod n$$

При цьому для індексів із списку винятків оригінальне значення відновлюється безпосередньо, оминаючи операцію піднесення до степеня.

Другий рівень - стеганографічне приховування. Зашифрований масив байтів вбудовується у зображення-контейнер (формат PNG) методом найменш значущого біта (LSB). Реалізований алгоритм вбудовування спочатку кодує у молодших бітах пікселів 4-байтне ціле число - довжину прихованого повідомлення, а потім послідовно вбудовує всі біти зашифрованого масиву. Кожен піксель контейнера модифікується лише в одному молодшому біті (RGB-компоненти), що забезпечує мінімальне візуальне спотворення. У разі, якщо розмір повідомлення перевищує ємність наявного зображення, контейнер автоматично масштабується з використанням інтерполяції HighQualityBicubic до мінімального необхідного розміру, після чого виконується повторна перевірка ємності.

Алгоритм декодування виконує зворотню процедуру: послідовно зчитуються молодші біти пікселів контейнера, з яких спочатку відновлюється довжина повідомлення, а потім — масив зашифрованих байтів. Після

витягування даних зі стеганоконтейнера виконується RSA-дешифрування та зворотне перетворення з кольорового представлення в аудіобайти.

Запропонований метод реалізовано у вигляді API-сервісу на платформі .NET із використанням бібліотеки NAudio для роботи з аудіофайлами та System.Drawing для обробки зображень. Контролер надає ендпоінти для шифрування (Encrypt) та дешифрування (Decrypt) аудіоданих. Вхідні дані передаються у вигляді бінарних потоків, а результати повертаються у вигляді оброблених байтових масивів разом з діагностичними метаданими (значення e, d, проміжні розміри буферів).

Аналіз безпеки запропонованого методу показує, що дворівневий захист суттєво ускладнює несанкціоноване відновлення вихідних аудіоданих. Зловмисник, який перехопив стеганоконтейнер, стикається з необхідністю спочатку виявити сам факт приховування інформації (що ускладнюється мінімальними змінами LSB-вбудовування), а потім вирішити задачу RSA-дешифрування без знання закритого ключа d та параметрів p, q [4, 5] Додаткове рандомізоване «засолення» вхідних байтів перед шифруванням ускладнює атаки на основі відомого відкритого тексту. Обчислювальна складність одного акту шифрування одного байту визначається складністю операції $m^e \bmod n$, яка при розумному виборі параметрів становить $O(\log e \cdot \log^2 n)$.

Серед обмежень слід зазначити, що застосування RSA до окремих байтів (8-бітових значень) є нетиповим підходом і ефективним лише за умови вибору n у межах, що допускають значення ciphertext ≥ 256 для деяких входів, що і відстежується механізмом індексів-винятків. Вибір великих p та q збільшує безпеку, але також збільшує частку позицій-винятків, для яких шифрування фактично не застосовується. Оптимальний вибір параметрів RSA для 8-бітового вхідного простору є відкритим питанням, що потребує подальшого дослідження. Таким чином, запропонований комбінований метод захисту аудіоданих забезпечує двохрівневу безпеку завдяки поєднанню асиметричного шифрування на основі кольорового представлення аудіобайтів та LSB-стеганографії в зображеннях. Практична реалізація у вигляді .NET-сервісу підтверджує працездатність підходу та його придатність для захисту конфіденційних аудіоповідомлень у цифрових системах.

Список літератури

1. Kodlubovskyi D. Data hiding in images using combined steganography and cryptography. URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/688.

2. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM. 1978. Vol. 21, No. 2. P. 120–126.

3. Knuth D. E. The Art of Computer Programming. Vol. 2: Seminumerical Algorithms. 3rd ed. Addison-Wesley, 1997. 764 p.

4. Mustafa Sabah. Combination of Steganography and Cryptography. URL: https://iopscience.iop.org/article/10.1088/1757-899X/518/5/052003/pdf.

5. Chan C.-K., Cheng L. M. Hiding data in images by simple LSB substitution. Pattern Recognition. 2004. Vol. 37, No. 3. P. 469–474. cryptography. URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/688.

ВИКОРИСТАННЯ АІ ТА МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖАХ ІЗ НУЛЬОВОЮ ДОВІРОЮ

Куля В. М.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасна парадигма забезпечення кібербезпеки зазнає фундаментальних трансформацій через неефективність традиційних моделей захисту периметра в умовах інтенсивного впровадження хмарних обчислень та віддаленого доступу. Архітектура нульової довіри (Zero Trust Architecture, ZTA), яка базується на повній відсутності апріорної довіри до будь-якого суб'єкта, потребує миттєвого аналізу величезних масивів даних. Статичні правила доступу не здатні адаптуватися до динамічних змін у ландшафті загроз, що зумовлює критичну необхідність інтеграції штучного інтелекту та машинного навчання для забезпечення безперервної інтелектуальної верифікації.

Метою доповіді є обґрунтування ролі та визначення ключових напрямів застосування методів машинного навчання для виявлення аномалій у мережевих структурах, побудованих на принципах нульової довіри, а також аналіз механізмів трансформації статичних моделей безпеки в адаптивні системи предиктивного захисту.

Реалізація інтелектуальних систем у межах архітектури нульової довіри (Zero Trust Architecture, ZTA) вимагає концептуального переходу від традиційних статичних правил контролю доступу до динамічного механізму безперервного оцінювання довіри (Trust Engine) [1, 2]. В основі цього процесу лежить глибока інтеграція інструментів аналізу поведінки користувачів та сутностей (User and Entity Behavior Analytics, UEBA), які акумулюють розширену мережеву телеметрію для формування багатовимірних профілів нормальної активності. Застосування алгоритмів глибокого навчання без учителя (Unsupervised Deep Learning), зокрема автоенкодерів (Autoencoders), забезпечує високоточну ідентифікацію латентних відхилень шляхом обчислення помилок реконструкції даних, що дозволяє виявляти атаки нульового дня та компрометацію облікових даних [3]. Для аналізу часових і послідовних залежностей, які є характерними для складних цілеспрямованих загроз (APT) та етапів горизонтального переміщення (Lateral Movement), архітектура ефективно доповнюється рекурентними моделями, такими як двонаправлені мережі довгої короткострокової пам'яті (Bi-LSTM) [1, 3]. Комплексний аналіз цих поведінкових патернів дає змогу ML-моделям автоматично обчислювати динамічний коефіцієнт ризику (Risk Scoring) у реальному часі [1]. Зпираючись на цей показник, точка прийняття рішень щодо політик (Policy Decision Point, PDP) генерує контекстно-залежні інструкції для точки застосування політик (Policy Enforcement Point, PEP) [1]. Залежно від виявленого рівня загрози, система здатна автономно ініціювати посилену багатофакторну автентифікацію (MFA), обмежити привілеї користувача або виконати превентивну мікросегментацію для повної ізоляції скомпрометованого вузла.

Разом із тим, імплементація методів штучного інтелекту в критичні інфраструктури неминуче стикається з проблемою вразливості самих ML-моделей до змагальних атак (Adversarial Attacks), зокрема цілеспрямованого «отруєння даних» (Data Poisoning) під час навчання та ухилення від виявлення. Для підвищення загальної кіберстійкості архітектури доцільним є впровадження байєсівських нейронних мереж, які запобігають прийняттю системою надмірно впевнених хибних рішень під час реєстрації рідкісних або неоднозначних подій. Окрім того, фундаментальною вимогою залишається подолання проблеми алгоритмічного «чорного ящика» за допомогою інтеграції методів пояснюваного штучного інтелекту (Explainable AI, XAI), зокрема алгоритмів SHAP або LIME [3]. Це перетворює приховані процеси прийняття рішень на зрозумілі візуальні моделі, забезпечуючи інтерпретованість результатів, підтримуючи концепцію управління за участю людини та гарантуючи довіру до автономних предиктивних дій системи. Синергія принципів архітектури нульової довіри (Zero Trust Architecture, ZTA) та передових технологій машинного навчання (ML) є фундаментальним фактором формування резильєнтного кіберпростору, що остаточно нівелює обмеження традиційних статичних периметрових моделей. Інтеграція інтелектуальних інструментів, зокрема аналізу поведінки користувачів та сутностей (UEBA) на базі глибокого навчання, перетворює систему захисту на проактивну «імунну систему» мережі, здатну здійснювати безперервну автентифікацію та динамічно обчислювати оцінку ризику (Risk Scoring) у режимі реального часу [1]. Цей підхід забезпечує автоматизоване застосування політик безпеки, що мінімізує вплив людського фактора, критично зменшує площу атаки та ефективно блокує горизонтальне переміщення (Lateral Movement) зловмисників у багатохмарних середовищах шляхом превентивної мікросегментації [4]. Водночас надійність таких адаптивних систем безпосередньо залежить від їхньої захищеності від змагальних атак та цілеспрямованого отруєння даних, що вимагає застосування стійких імовірнісних моделей, таких як байєсівські нейронні мережі (BNN), для врахування прогностичної невизначеності середовища.

Список літератури

1. Sivanageswara Rao Gandikota. Deep learning-enabled zero trust architecture for intelligent identity and access management in cloud ecosystems 2024 DOI: https://doi.org/10.30574/wjarr.2024.22.3.1842

2. Moskvin K., Sievierinov O. Zero Trust Architecture in Corporate Cybersecurity Systems // Computer and information systems and technologies : Seventh International Scientific and Technical Conference, 2024. – Kharkiv : NURE, 2024. – p. 54-55.

3. Maria Gabriela Camila. A Multi-Tenant Cloud Security Framework Using Zero-Trust Architecture and AI-Based Anomaly Detection 2024 DOI:10.63282/3117-5481/AIJCST-V6I4P101

4. Ravi Gupta and Guneet Bhatia. Zero-trust industrial network security using AI and explainable inference novelty. World Journal of Advanced Research and Reviews, 2025. DOI: https://doi.org/10.30574/wjarr.2025.28.2.3705

ПРОЗОРІСТЬ РІШЕНЬ ГРАФОВИХ НЕЙРОННИХ МЕРЕЖ У ЗАДАЧАХ ВИЯВЛЕННЯ ТРАНЗАКЦІЙНИХ ЗАГРОЗ У БЛОКЧЕЙН-СИСТЕМАХ

Просолов В.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні блокчейн-системи характеризуються високою інтенсивністю транзакцій, псевдоанонімністю учасників та складними механізмами обфускації фінансових потоків. Це створює сприятливе середовище для реалізації схем відмивання коштів, ransomware-активності, мікшування та інших транзакційних аномалій.

Класичні методи виявлення загроз, що базуються на статичних евристиках або табличних алгоритмах машинного навчання, не дозволяють повноцінно враховувати топологічний контекст блокчейн-мережі. У зв'язку з цим графові нейронні мережі, зокрема GATv2, є більш придатними для аналізу ончейн-даних, однак їх практичне застосування стримується проблемою «чорної скриньки». У сферах кібербезпеки, фінансового моніторингу та цифрової криміналістики недостатньо лише отримати ризик-скоринг — необхідно також пояснити, які саме ознаки та зв'язки в графі стали підставою для класифікації транзакції як підозрілої [1, 2].

Метою роботи є підвищення прозорості та доказовості рішень нейромережевих класифікаторів у задачах виявлення транзакційних загроз у блокчейн-системах шляхом синергетичного поєднання локальних адитивних пояснень SHAP із ваговими коефіцієнтами шарів графової уваги GATv2 для формування структурованого вектора доказів, придатного до використання в аудиті, AML/CFT-процедурах і цифрових форензик-розслідуваннях.

У роботі як математичну основу використано апарат теорії графів, методи глибинного навчання, графові нейронні мережі з механізмами динамічної уваги, алгоритми балансування даних у латентному просторі та інструменти пояснювального штучного інтелекту. Запропонований підхід ґрунтується на аналізі транзакційного графа Bitcoin, у якому вузли описуються розширеним простором ознак, що включає 94 локальні мікроознаки та 72 топологічні макроознаки [3]. Такий 166-вимірний простір дозволяє моделі враховувати як фінансові параметри транзакцій, так і їх структурне оточення.

Ключовим результатом є удосконалення механізму математичної інтерпретації рішень графового класифікатора. На відміну від традиційних XAI-підходів, де пояснення формуються переважно на рівні окремих ознак, у запропонованому методі пояснення будуються одночасно у двох площинах. Перша площина — атрибутивна, у якій SHAP визначає внесок кожної окремої ознаки у фінальне рішення моделі. Друга площина — топологічна, у якій коефіцієнти уваги GATv2 відображають вагомість конкретних сусідів і ребер у процесі агрегації інформації [4, 5]. Поєднання цих двох механізмів дозволяє трансформувати фінальний ризик-скоринг моделі у структурований evidence vector, де кожен елемент пояснення має як числову, так і структурну інтерпретацію.

Практичне значення такого підходу полягає в тому, що аналітик безпеки отримує не лише оцінку ризику, а й пояснення причин, чому певний вузол або підграф було віднесено до класу підозрілих. Це особливо важливо для цифрової криміналістики, де потрібно аргументовано показати, які саме фінансові атрибути, часові характеристики або топологічні зв'язки стали тригерами класифікації.

Наприклад, SHAP може виділити найбільш впливові ознаки транзакції, а ваги уваги — вказати на підозрілі fan-in, peel chains чи інші аномальні маршрути руху активів у графі.

Таким чином забезпечується підвищення довіри до системи, спрощується аудит рішень та зменшується бар'єр до впровадження графових нейромереж у реальні SOC- та AML/CFT-середовища.

Додатково у роботі показано, що пояснюваність не суперечить високій якості класифікації. Запропонований метод, реалізований у складі програмного комплексу «AI Crypto Scanner», демонструє F1-score 0.8948 та Recall 0.9105 на еталонному Elliptic Dataset, що перевищує результати базових моделей. Отже, інтеграція XAI у графову архітектуру не лише зберігає високу ефективність виявлення аномалій, а й підвищує практичну цінність моделі за рахунок доказовості її рішень.

Запропонований підхід дозволяє підвищити прозорість рішень графових нейронних мереж у задачах виявлення транзакційних загроз у блокчейн-системах.

Поєднання SHAP-пояснень із ваговими коефіцієнтами графової уваги забезпечує формування структурованого вектора доказів, придатного для аудиту, цифрової криміналістики та систем фінансового моніторингу. Це підвищує практичну цінність моделі та розширює можливості її застосування в реальних умовах.

Список літератури

1. Veličković P., Cucurull G., Casanova A., Romero A., Liò P., Bengio Y. Graph Attention Networks // *International Conference on Learning Representations (ICLR).* 2018.

2. Brody S., Alon U., Yahav E. How Attentive are Graph Attention Networks? // *International Conference on Learning Representations (ICLR).* 2022.

3. Kushnerov, O., Prosolov, V., Dudykevych, V., Yevseiev, S., Ivanchenko, Y., Gorbulyk, V., ... & Sukhoteplyi, V. (2026). DEVELOPMENT OF A METHOD FOR IMPROVING THE EFFICIENCY OF TRANSACTION CLASSIFICATION IN THE BITCOIN NETWORK USING AN ATTENTION MECHANISM IN GRAPH NEURAL NETWORKS. *Eastern-European Journal of Enterprise Technologies*, №9. – P. 6-19. DOI: 10.15587/1729-4061.2026.351685

4. Lundberg S. M., Lee S.-I. A Unified Approach to Interpreting Model Predictions // *Advances in Neural Information Processing Systems.* 2017. Vol. 30.

5. Zhao T., Zhang X., Wang S., et al. GraphSMOTE: Imbalanced Node Classification on Graphs with Graph Neural Networks // *Proceedings of the 14th ACM International Conference on Web Search and Data Mining.* 2021.

МЕТОДОЛОГІЯ ВИЯВЛЕННЯ AI-ЗГЕНЕРОВАНОГО ТЕКСТУ УКРАЇНСЬКОЮ МОВОЮ

Ємельяненко А., Просолов В.В.
Харківський національний університет радіоелектроніки, Харків, Україна

З стрімким розвитком генеративного штучного інтелекту дедалі складніше стає відрізнити текст, згенерований штучним інтелектом (AI-generated text), від тексту, написаного людиною. Це створює низку проблем у суспільстві та наукових дослідженнях, зокрема сприяє поширенню фейкових новин, академічного плагіату та дезінформації.

Актуальною є проблема виявлення AI-згенерованого тексту, оскільки сучасні моделі здатні створювати тексти, які практично не відрізняються від написаних людиною.

Особливо це актуально для української мови. У порівнянні з англійською вона має складнішу морфологію, іншу структуру речень і меншу представленість у тренувальних даних мовних моделей. Це означає, що універсальні підходи детекції працюють менш ефективно і потребують адаптації.

Метою доповіді є розробка підходу до виявлення AI-згенерованого тексту українською мовою з урахуванням її мовних особливостей.

Сучасна методологія аналізу ефективності детекторів AI-тексту базується на різноманітних підходах до виявлення характерних ознак машинного авторства. Однією з основних стратегій є використання нейронних класифікаторів, які навчаються на корпусах текстів, створених людиною та штучним інтелектом. Наприклад, моделі на основі RoBERTa, донавчені для розрізнення людських і AI-текстів, демонструють здатність виявляти тонкі відмінності у стилі та структурі [1]. Інший підхід полягає у використанні статистичних метрик, таких як ентропія або перплексія. Інструменти на кшталт DetectGPT аналізують розподіл ймовірностей слів у тексті, виявляючи підвищену передбачуваність, притаманну AI-генерації.

Далі виконується аналіз текстів за кількома групами ознак. До них належать особливості словникового складу, структура речень, частота використання певних слів, а також загальна зв’язність тексту. Окремо враховуються морфологічні та синтаксичні характеристики, які мають важливе значення саме для української мови.

Ключовою проблемою у створенні інструкційно-налаштованих моделей для української мови, оптимізованих для редагування тексту, є обмежена доступність відповідних датасетів. Для вирішення цієї проблеми адаптують наявні датасети з української та англійської мов, перетворюючи їх на датасети для виконання інструкцій. Це дозволяє будувати сучасні моделі редагування тексту для української мови, яка здатна виконувати складні завдання редагування: граматичну корекцію, спрощення тексту, забезпечення зв’язності та перефразування [1].

Керовані методи виявлення AI-згенерованого тексту базуються на використанні розмічених датасетів, де кожен текст має мітку, що вказує на його походження - людське чи машинне. Ці підходи розглядають задачу як бінарну класифікацію, навчаючи моделі розрізняти тексти за допомогою різноманітних ознак.

Дослідження у цій сфері демонструють, що керовані методи зазвичай забезпечують високу точність виявлення, особливо коли для навчання доступна велика кількість якісних даних.

Проте, ці методи мають суттєві обмеження: вони схильні до перенавчання, особливо у випадках, коли навчальні дані обмежені за обсягом або специфічні для певної доменної області. Це може призводити до зниження ефективності при застосуванні моделей до текстів, що відрізняються від тих, на яких вони були навчені [2].

Гібридні підходи поєднують традиційні ознаки тексту, такі як кількість слів, багатство словника, індекси читабельності, з машинним навчанням або нейронними моделями.

Такі методи дозволяють враховувати як поверхневі, так і глибші лінгвістичні характеристики тексту, що підвищує загальну точність виявлення.

Часто для цього використовують ансамблеві стратегії, які комбінують результати кількох моделей або різних типів ознак, що дозволяє зменшити ймовірність помилкової класифікації [2].

Однією з ключових проблем для подальшого розвитку методології виявлення AI-згенерованого тексту українською мовою є обмежена доступність якісних датасетів для навчання та тестування моделей, орієнтованих на завдання редагування та аналізу тексту.

У відповідь на цю проблему дослідники адаптують існуючі датасети з української та англійської мов, перетворюючи їх на інструкційно-орієнтовані набори даних, що дозволяє будувати сучасні моделі для редагування тексту українською.

Такі підходи відкривають нові можливості для створення моделей, здатних не лише генерувати, а й аналізувати та розпізнавати AI-згенерований текст, враховуючи специфіку української мови [3].

Список літератури

1. A. Saini, A. Chernodub, V. Raheja, and V. Kulkarni, "Spivavtor: An Instruction Tuned Ukrainian Text Editing Model," arXiv:2404.18880, 2024. URL: https://arxiv.org/abs/2404.18880

2. S. Agrahari and S. R. Singh, "Tracing Thought: Using Chain-of-Thought Reasoning to Identify the LLM Behind AI-Generated Text," arXiv:2504.16913, 2025. URL: https://arxiv.org/abs/2504.16913

3. I. David and A. Gervais, "AuthorMist: Evading AI Text Detectors with Reinforcement Learning," arXiv:2503.08716, 2025. URL: https://arxiv.org/abs/2503.08716

ПОРІВНЯЛЬНИЙ АНАЛІЗ ХЕШ-ОРІЄНТОВАНИХ СХЕМ ЦИФРОВОГО ПІДПИСУ XMSS ТА SPHINCS+

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

Розвиток квантових комп'ютерів робить необхідним перегляд підходів до забезпечення криптографічної стійкості цифрових підписів. Адже складність факторизації та дискретного логарифмування, на яких базується стійкість багатьох асиметричних алгоритмів, є вразливою до квантових обчислень. Через це сучасна постквантова криптографія звертається до цифрових підписів, безпека яких базується на інших математичних задачах, наприклад на властивостях криптографічних хеш-функцій [1, 2]. Особливе місце серед них посідають XMSS і SPHINCS+. Перший належить до схем зі станом (stateful), а другий не потребує зовнішнього керування станом (stateless) [3, 4].

Метою доповіді є порівняння хеш-орієнтованих схем цифрового підпису XMSS і SPHINCS+ з урахуванням їх криптографічних властивостей, зазначених в документах NIST (National Institute of Standards and Technology) та особливостей рекомендацій Федерального управління інформаційної безпеки Німеччини (BSI — Bundesamt für Sicherheit in der Informationstechnik) щодо їх застосування [1, 3, 4].

У рекомендаціях BSI зазначається, що для хеш-орієнтованих схем критичне значення має стійкість до знаходження їх прообразу, тоді як колізійна стійкість не виступає основною визначальною вимогою [1].

Ключова особливість XMSS полягає в тому, що алгоритм безпечний лише за умови ретельного керування станом, тобто для кожного нового підпису має використовуватися новий внутрішній елемент структури (дерева), а повторне використання вже задіяного стану може поставити безпеку під загрозу. Відтак XMSS не подається як універсальне рішення загального призначення, а рекомендується для тих систем, де можна гарантувати відповідальне використання особистого конфіденційного ключа та безпечне ведення стану. Додатково в документі зазначається, що генерація ключів і створення підписів мають виконуватися в апаратних криптомодулях. Тобто NIST пов'язує XMSS не лише з математичною задачею, а й із наявністю контрольованої апаратної інфраструктури [3].

У рекомендаціях BSI вказується, що однією з проблем є необхідність безпомилкового керування станом, зокрема монотонного збільшення лічильника при кожному новому підписі. Через це схеми зі станом рекомендуються для спеціальних сценаріїв, наприклад підписування програмного забезпечення та оновлень прошивки [1, 3].

SPHINCS+ у нормативному полі NIST представлений через стандарт FIPS 205, у якому стандартизовано алгоритм SLH-DSA [4]. У документі прямо зазначено, що SLH-DSA базується на SPHINCS+, тобто є його стандартизованою формою. Головною його відмінністю від XMSS є відсутність потреби у зовнішньому керуванні станом. Такий підхід значно

знижує організаційні ризики, пов'язані з неправильним веденням лічильника або повторним використанням стану, що робить цю схему більш придатною для широкого використання [1, 4].

BSI у своїх технічних документах зазначає, що для SLH-DSA рекомендується hedged-варіант. Це означає, що під час створення підпису використовується не лише сам конфіденційний особистий ключ і повідомлення, а й додатково рандомізація.

Також зазначається, що перевага надається Pure-version SLH-DSA, у якому схема підписує вихідне повідомлення без попереднього зовнішнього хешування цього повідомлення. Тоді як Pre-hash-version допускається лише для спеціальних випадків [1].

BSI чітко формулює свої вимоги до параметрів SLH-DSA. У документі зазначено, що рекомендуються усі набори параметрів, які відповідають NIST Security Strength Category 3 та NIST Security Strength Category 5, але саме в hedged-варіанті.

Таким чином, порівняння XMSS і SPHINCS+ виявляє насамперед різницю між різними схемами зі станом та без стану. XMSS розглядається як схема, придатна для контрольованих сценаріїв, де гарантується надійне ведення стану, апаратний захист ключового матеріалу та обмежена кількість підписів. SPHINCS+ позиціонується як цифровий підпис без стану, що є більш зручним для широкого використання, хоча BSI і додає окремі уточнення щодо параметрів.

У німецькому контексті це добре узгоджується з дослідженнями, які присвячені розвитку квантово-стійких криптографічних технологій Німеччини, де хеш-орієнтовані цифрові підписи розглядаються як довгостроковий захист [2].

У такому випадку XMSS і SPHINCS+ є двома різними підходами до реалізації хеш-орієнтованих цифрових підписів.

У результаті проведеного аналізу визначено, що XMSS і SPHINCS+ належать до одного класу хеш-орієнтованих схем цифрового підпису, але істотно відрізняються в технічній будові схем і моделі їх безпечного застосування.

Список літератури

1. Bundesamt für Sicherheit in der Informationstechnik. *Kryptographische Verfahren: Empfehlungen und Schlüssellängen*. BSI TR-02102-1. Bonn : BSI, 2025.

2. Мельникова О. А., Грасмік С. В. Становлення та розвиток квантово-стійких криптографічних технологій у Німеччині. *Вісник Херсонського національного технічного університету*. 2025. № 4 (95). Т. 2. С. 119–124. DOI: https://doi.org/10.35546/kntu2078-4481.2025.4.2.15

3. *Recommendation for Stateful Hash-Based Signature Schemes: NIST Special Publication 800-208* / National Institute of Standards and Technology. Gaithersburg, MD : NIST, 2020.

4. *Stateless Hash-Based Digital Signature Standard: FIPS PUB 205* / National Institute of Standards and Technology. Gaithersburg, MD : NIST, 2024.

АРХІТЕКТУРНА ОПТИМІЗАЦІЯ ЛОКАЛЬНИХ RAG-СИСТЕМ ДЛЯ АВТОМАТИЗАЦІЇ КОМПЛАЄНСУ NIST SP 800-53 НА БАЗІ APPLE SILICON

Надточий М. М., Балагура Д. С.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні процеси SecOps (Security Operations) вимагають швидкого доступу до нормативної документації, зокрема до стандарту NIST SP 800-53, що містить сотні контролів безпеки. Використання публічних великих мовних моделей (LLM), таких як ChatGPT, для аналізу внутрішньої інфраструктури на відповідність стандартам є неприпустимим через критичні ризики витоку чутливих даних. Ефективним рішенням є розгортання локальних AI-асистентів на базі Retrieval-Augmented Generation (RAG), проте спроби використання стандартних "коробкових" рішень часто призводять до галюцинацій або відмов моделі генерувати відповідь

Метою доповіді є визначення оптимальної архітектури локальної RAG-системи, здатної коректно інтерпретувати ієрархічні стандарти безпеки на обмежених обчислювальних ресурсах на базі Apple Silicon, та вирішення проблем стандартного парсингу документів.

Дослідження проводилося на апаратній платформі Apple MacBook Pro (процесор M1 Pro, Unified Memory), яка забезпечує високу пропускну здатність пам'яті для швидкого інференсу квантованих моделей. Програмний стек включав Ollama, LangChain та ChromaDB; тестувалися моделі Llama 3.1 (8B), Qwen 2.5 (7B) та Gemma 2 (9B). На першому етапі було реалізовано стандартний підхід "Naive RAG" (парсинг офіційного PDF-файлу з розбиттям на частини), який показав незадовільні результати. Було зафіксовано, що моделі невеликого розміру, зокрема Llama 3.2 3B, у 100% випадків відмовлялися давати відповідь ("I don't know") на специфічні запити щодо багаторівневих контролів, таких як SC-7 Boundary Protection.

Аналіз виявив проблему "Фрагментації контексту": механічний поділ тексту розриває семантичний зв'язок між ідентифікатором контролю безпеки та його описом. Крім того, було виявлено феномен "витіснення батьківського контексту" (Vector Dilution), коли векторна база повертала підконтролі, залишаючи загальний опис батьківського контролю нижче порогу відсікання Top-K.

Для розв'язання цих проблем було розроблено покращений конвеєр обробки даних (ETL Pipeline). По-перше, здійснено перехід від PDF до структурованих даних у форматі CSV із застосуванням методу "Context Injection", де кожен векторний документ примусово включав метадані у тілі тексту, що зробило фрагменти самодостатніми. По-друге, впроваджено алгоритм гібридного пошуку Hybrid Retrieval, який ефективно поєднує Regex-пошук ідентифікаторів, прямий запит у базу метаданих (Hard Filtering) та

традиційний семантичний векторний пошук. Таке дворівневе архітектурне рішення не лише повністю усунуло феномен "витіснення батьківського контексту", але й по-різному вплинуло на продуктивність інференсу квантованих моделей у форматі GGUF на базі Ollama.

Детальніший аналіз впровадженого конвеєра обробки даних ETL Pipeline та результатів тестування розкриває специфіку роботи алгоритму гібридного пошуку та реакцію різних архітектур мовних моделей на структурований контекст. Індустріальний стандарт Llama 3.1 (8B Instruct) продемонструвала "парадокс швидкості" зі зменшенням загального часу генерації на 16,4% та максимальною експертною оцінкою якості RAG у 5.0 балів, що пояснюється тим, що за наявності чіткого контексту модель припиняє генерувати надлишковий текст та галюцинації, видаючи точну й лаконічну відповідь. Для інших перевірених архітектур було зафіксовано так званий "Time Penalty" — затримку через обробку розширеного промпту. Для перспективної моделі Qwen 2.5 (7B Instruct) час генерації збільшився на 5,8%, хоча якість згенерованої відповіді також залишилася на еталонному рівні у 5.0 балів без жодних галюцинацій. Водночас модель Gemma 2 (9B) виявилася найменш оптимізованою для даного RAG-пайплайну: її час відповіді суттєво зріс на 30,7%, а експертна оцінка якості знизилася до 4.0 балів. Ці порівняльні метрики переконливо доводять, що саме моделі розміром 7-8 мільярдів параметрів є оптимальним вибором для локальних SecOps-завдань, оскільки вони забезпечують ідеальний баланс між швидкістю інференсу та абсолютною точністю цитування стандарту. Усі протестовані моделі класу 7B-9B стабільно працювали на 16GB Unified Memory, що підтверджує високу апаратну ефективність Apple Silicon для локальних задач SecOps.

Практична значущість отриманих результатів полягає у доведенні того факту, що побудова ефективного локального AI-асистента для завдань кібербезпеки неможлива шляхом простого поєднання неструктурованих документів ("PDF + LLM").

Критичним фактором успіху виступає саме якість підготовки даних (Data Engineering) та обов'язкове використання гібридного пошуку (Lexical/Metadata + Semantic).

Впровадження запропонованої архітектури локального RAG не лише гарантує приватність чутливих даних, але й оптимізує час отримання критично важливої інформації за рахунок генерації моделлю відповідей без надлишкового тексту.

Список літератури

1. Lewis, Patrick, et al. "Retrieval-augmented generation for knowledge-intensive nlp tasks." Advances in neural information processing systems 33 (2020): 9459-9474. DOI: https://doi.org/10.48550/arXiv.2005.11401

2. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53, Revision 5. National Institute of Standards and Technology. 2020. DOI: https://doi.org/10.6028/NIST.SP.800-53r5

МЕХАНІЗМИ ВИЯВЛЕННЯ ФІШИНГОВИХ РЕСУРСІВ У КОМП'ЮТЕРНИХ МЕРЕЖАХ НА ОСНОВІ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Рязанов Є.О., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Фішингові атаки залишаються однією з найбільш деструктивних загроз у кіберпросторі через постійну еволюцію методів обходу статичних фільтрів. Сучасні зловмисники дедалі частіше використовують короткоживучі домени, динамічну генерацію URL-адрес та обфускацію контенту, що робить використання традиційних «чорних списків» недостатнім для забезпечення прийнятного рівня безпеки. Крім того, значну проблему становить швидкість поширення нових фішингових кампаній, коли час між створенням шкідливого ресурсу та його виявленням може становити лише кілька годин. Це зумовлює необхідність впровадження інтелектуальних систем, здатних виявляти аномалії в структурі вебресурсів у реальному часі, незалежно від наявності ресурсу у базах відомих загроз [1]. У цьому контексті особливого значення набувають підходи, що базуються на аналізі ознак та поведінкових характеристик, а не лише на сигнатурному пошуку.

Метою доповіді є обґрунтування структури та розробка концепції та механізмів детекції фішингових посилань на основі вилучення лексичних ознак URL-адрес та їх подальшої класифікації за допомогою методів машинного навчання[2]. Зазначений підхід має збільшити ефективність захисту від фішингових атак.

В основу підходу, що пропонується, покладено багатофакторний аналіз характеристик підозрілих ресурсів. Процес виявлення загрози поділяється на кілька етапів. На першому етапі здійснюється лексичний аналіз URL-адреси, що включає перевірку певних ознак, як: загальна довжина посилання, кількість субдоменів, наявність символів «@» та дефісів, а також використання IP-адрес замість доменних імен [3]. Для протидії атакам типу тайпосквотинг передбачається використання метрики відстані Левенштейна відносно переліку довірених брендів, що дозволяє ідентифікувати візуально схожі, але шкідливі домени. Математичне ядро може бути реалізуване із застосуванням ансамблевих методів, зокрема алгоритму випадкового лісу (Random Forest), що дозволить забезпечити стійкість до перенавчання та високу точність класифікації на зашумлених мережевих даних. Перевагою такого підходу є також інтерпретованість результатів, зокрема можливість оцінки важливості окремих ознак, що може бути використано для подальшої оптимізації моделі. Крім того, ансамблеві методи добре масштабуються та можуть бути адаптовані до змін у характері загроз шляхом періодичного донавчання моделі на нових даних.

З точки зору реалізації, зазначений підхід може бути запропонований у вигляді браузерного розширення, що функціонує як проміжний вузол контролю. Архітектура рішення включає аналітичний сервер (на базі

Flask/FastAPI), який прийматиме сформований вектор ознак, опрацьовуватиме його та повертатиме ймовірність належності ресурсу до шкідливих. Для мінімізації затримок можливе використання кешування результатів перевірок та асинхронної обробки запитів. У разі перевищення встановленого порогу ризику, розширення буде блокувати доступ до сторінки та виводити попередження для користувача. Такий підхід дозволить реалізувати проактивний захист, по суті не даючи зловмисним механізмам бути запущеними у системі, що атакується. Разом з тим, використання аналітичного серверу дозволить централізувати базу знань, тобто отримувати нові дані для навчання та, одночасно, знизити навантаження на обчислювальні ресурси клієнтської системи.

Важливим етапом розробки системи є оцінювання ефективності її функціонування. Зважаючи на неможливість проводити тестування у реальних умовах, основними механізмами тестування будуть синтетичні тести з використанням відкритих наборів даних (UCI Machine Learning Repository та PhishTank), а також крос-валідація для оцінки узагальнюючої здатності моделі. Для більш повної оцінки якості класифікації доцільно використовувати такі метрики, як precision, recall, F1-score та ROC-AUC, що дозволяють врахувати баланс між виявленням загроз і рівнем хибних спрацювань. Очікується, що використання ансамблевих моделей машинного навчання дозволить досягти високих показників точності при мінімальному рівні помилкових спрацювань (False Positives), що є критично важливим для збереження зручності користування системою з точки зору доступності доменів, що не несуть загроз.

Подальші дослідження можуть бути спрямовані на інтеграцію аналізу контенту сторінок за допомогою методів обробки природної мови (NLP). Також перспективним напрямком є використання гібридних моделей, які поєднують лексичний аналіз URL з поведінковим аналізом вебсторінок та характеристиками мережевої взаємодії, що дозволить суттєво підвищити рівень виявлення складних багаторівневих атак [4].

Список літератури

1. Jain A. K., Gupta B. B. A novel approach to detect phishing websites using self-structuring neural network. *EURASIP Journal on Information Security*. 2020. Vol. 2020, No. 4. P. 1–11.

2. Проблема недостатньої адаптивності традиційних систем мережевої безпеки до сучасних кіберзагроз: аналіз та шляхи вирішення / М. Надточий, Д. Балагура, П. Шулік, В. Просолов // *«Вісник Хмельницького національного університету.»* Том 359 № 6.1/2025, с. 63-69. https://doi.org/10.31891/2307-5732-2025-359-7

3. Verma R., Das A. What's in a URL? Fast Feature Extraction and Malicious URL Detection. *Proceedings of the 3rd ACM on International Workshop on Security And Privacy Analytics (IWSPA '17)*. 2017. P. 55–63.

4. Дорофєєва, К., Сєвєрінов, О., Сидоренко, З., Сухотеплий, В. (2025). Застосування інструмента аналізу безпеки для виявлення критичних вразливостей у веб-додатках. Вісник Херсонського національного технічного університету, 3(4 (95)), 62-68.

ПОРІВНЯЛЬНИЙ АНАЛІЗ СУЧАСНИХ МЕНЕДЖЕРІВ ПАРОЛІВ

Ганзя Р.С., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному цифровому середовищі проблема безпечного зберігання облікових даних стає дедалі актуальнішою, адже кількість сервісів і акаунтів постійно зростає. Користувачі змушені взаємодіяти з великою кількістю інформаційних систем, що потребує створення та використання унікальних і складних паролів. Менеджер паролів – це окрема програма або частина більшого середовища (наприклад, браузера), що відповідає за керування важливими даними, як-от логіни та паролі облікових записів або PIN-коди. Використання такого інструменту значно спрощує взаємодію з інформаційними системами, оскільки позбавляє необхідності запам'ятовувати велику кількість облікових даних. Крім того, програми цього типу забезпечують зберігання інформації у зашифрованому вигляді, що підвищує рівень її захисту від несанкціонованого доступу [1]. Додатково багато сучасних рішень пропонують генерацію стійких паролів та автоматичне заповнення форм, що сприяє підвищенню загальної кібергігієни користувачів.

Водночас менеджери паролів мають не лише переваги, але й певні ризики, зокрема пов'язані з компрометацією головного пароля або вразливостями у програмному забезпеченні. Централізація облікових даних в одному сховищі може створювати єдину точку відмови, що робить такі рішення привабливою ціллю для атак. У разі успішної атаки зловмисник може отримати доступ до значного обсягу конфіденційної інформації. Також важливим аспектом є довіра до розробника та механізмів шифрування, які використовуються у конкретному продукті. Крім того, слід враховувати ризики, пов'язані з використанням хмарної інфраструктури, зокрема можливість атак на серверну частину або перехоплення даних під час синхронізації.

Метою доповіді є здійснення порівняльного аналізу архітектури, методів шифрування та зручності сучасних менеджерів паролів (Bitwarden, 1Password та KeePassXC) для виявлення їхніх недоліків та формування базових вимог до розробки власного оптимізованого програмного рішення.

В доповіді наводяться результати аналізу обраних програмних рішень, що демонструють різні підходи до управління конфіденційними даними.

Bitwarden пропонує надійний баланс між прозорістю та зручністю. Цей продукт має відкритий вихідний код, підтримує хмарну синхронізацію та дозволяє розгортання на власному локальному сервері, що робить його привабливим як для індивідуальних, так і для корпоративних користувачів [2]. Додатково він використовує сучасні алгоритми шифрування та механізми захисту, включаючи двофакторну автентифікацію.

1Password є комерційним рішенням із закритим кодом, яке фокусується на максимальному комфорті. Програма відзначається високим рівнем

інтеграції з операційними системами, бездоганним користувацьким інтерфейсом та розширеними функціями для сімейного або командного використання [4]. Він також реалізує додаткові механізми захисту, такі як секретний ключ (Secret Key), що підвищує стійкість до атак навіть у разі компрометації основного пароля.

Водночас відсутність відкритого коду може обмежувати можливість незалежної перевірки додатку.

Натомість KeePassXC кардинально відрізняється своїм підходом до зберігання – це повністю локальна програмне рішення з відкритим кодом. Воно залишає синхронізацію та повний контроль над зашифрованим файлом бази даних виключно за користувачем [3]. Такий підхід забезпечує максимальний рівень контролю над даними, проте потребує від користувача додаткових знань для організації резервного копіювання та синхронізації між пристроями.

Основні відмінності існуючих рішень наведено у таблиці 1.

Таблиця 1 – Основні характеристики менеджерів паролів

Характеристика	**Bitwarden**	**1Password**	**KeePassXC**
Вихідний код	Відкритий	Закритий	Відкритий
Зберігання даних	Хмарне / Локальне	Хмарне	Локальне
Синхронізація	Автоматична	Автоматична	Ручна (через сторонні сервіси)
Вартість	Є безкоштовна версія	Платна підписка	Повністю безкоштовно

Порівняння цих рішень свідчить про відсутність абсолютно універсального продукту: кожен має свої обмеження щодо безпеки, контролю або зручності. Це обґрунтовує доцільність розробки нового менеджера паролів, який зможе ефективно поєднати гнучкість і безпеку локального контролю (як у KeePassXC) із сучасним інтерфейсом та зручністю автоматичної синхронізації (як у комерційних аналогах).

Список літератури

1. Рикова В. Для чого потрібен менеджер паролів і який обрати. URL: https://ms.detector.media/kiberbezpeka/post/29917/2022-07-26-dlya-chogo-potriben-menedzher-paroliv-i-yakyy-obraty/ (дата звернення: 8.03.2026).

2. Best password manager for business, enterprise & personal | bitwarden. Bitwarden. URL: https://bitwarden.com/ (дата звернення: 8.03.2026).

3. KeePassXC password manager. KeePassXC Password Manager. URL: https://keepassxc.org/ (дата звернення: 8.03.2026).

4. Passwords, secrets, and access management | 1password. Passwords, Secrets, and Access Management | 1Password. URL: https://1password.com/ (дата звернення: 8.03.2026).

МЕХАНІЗМИ ПЕРВИННОЇ ОЦІНКИ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ З ВИКОРИСТАННЯМ ПІДХОДІВ ШТУЧНОГО ІНТЕЛЕКТУ

Балагура В.О., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних умовах стрімкого зростання кількості кіберзагроз інформаційна безпека стає критично важливою складовою діяльності будь-якої організації [1, 2]. Однією з актуальних задач є оперативна первинна оцінка рівня захищеності інформаційних систем, яка дозволяє виявити потенційні вразливості без проведення повномасштабного аудиту. Така оцінка є особливо важливою для організацій, що не мають достатніх ресурсів для регулярного проведення комплексних перевірок. Традиційні підходи до оцінки безпеки часто потребують значних часових і ресурсних витрат, залучення експертів та використання спеціалізованих інструментів, тому актуальним є розроблення механізмів та інструментів, що забезпечують оперативне визначення стану інформаційної безпеки.

Метою доповіді є опрацювання концепції та механізмів застосування штучного інтелекту для проведення первинної оцінки рівня інформаційної безпеки організації.

Запропонований підхід базується на використанні структурованих опитувальників з фіксованими питаннями, що охоплюють ключові домени інформаційної безпеки:

управління доступом,
резервне копіювання,
моніторинг,
політики безпеки,
навчання персоналу, реагування на інциденти,
фізичний захист [1].

Кожен із зазначених доменів відображає окремий аспект системи захисту та дозволяє комплексно оцінити стан безпеки організації. Формування опитувальника передбачає уніфікацію питань та їх прив'язку до загальноприйнятих стандартів інформаційної безпеки, що забезпечує узгодженість та відтворюваність результатів оцінювання.

На відміну від бінарних оцінок, використовується градуйована шкала рівня впровадження контролів, що дозволяє більш точно відобразити реальний стан безпеки. Такий підхід дає змогу зменшити втрату інформації при оцінюванні та підвищити чутливість моделі до незначних відхилень у рівні захищеності. Подальша нормалізація отриманих оцінок створює основу для їх застосування у математичних моделях аналізу, забезпечуючи коректність обчислень та порівнюваність результатів між різними організаціями або підрозділами. Зокрема, для формування інтегрального показника захищеності доцільно використовувати моделі логістичної регресії [3], які добре зарекомендували себе для задач класифікації та оцінювання ризиків.

Модель логістичної регресії виконує функцію простої нейромережі з одним нейроном і дозволяє на основі множини вхідних параметрів (відповідей користувача) обчислювати інтегральний показник рівня захищеності у відсотках. Крім того, така модель дозволяє у майбутньому враховувати вагові коефіцієнти окремих ознак, що відображають їх відносну важливість для загального рівня безпеки. Це створює можливість подальшої адаптації моделі до специфіки різних організацій шляхом коригування вагових параметрів.

Запропонований підхід дає можливість оцінити рівень ризику виявлених проблем з урахуванням їх критичності, впливу та належності до певного домену безпеки [4]. Додатково може враховуватися взаємозв'язок між окремими контролами, що дозволяє більш точно оцінити сукупний ефект їх відсутності або часткової реалізації. Це дозволяє не лише отримати загальний рівень захищеності, але й ідентифікувати найбільш вразливі області, які потребують першочергового втручання. Таким чином, результати оцінювання можуть бути використані для пріоритезації заходів з підвищення безпеки.

Результатом застосування запропонованого підходу є формування аналітичного звіту, який включає інтегральний показник безпеки, оцінку за окремими доменами, виявлені слабкі місця та рекомендації щодо їх усунення [1]. Додатково звіт може містити візуалізацію результатів у вигляді графіків або діаграм, що полегшує їх інтерпретацію для керівництва організації. Такий підхід дозволяє суттєво підвищити ефективність первинної оцінки, забезпечити прозорість процесу прийняття рішень та зменшити навантаження на фахівців з кібербезпеки за рахунок автоматизації аналізу.

Таким чином, використання методів штучного інтелекту для первинної оцінки інформаційної безпеки не замінює спеціаліста, а доповнює його діяльність і є перспективним напрямом розвитку сучасних систем безпеки [5]. Воно дозволяє забезпечити швидке отримання узагальненої картини стану захищеності та своєчасно реагувати на потенційні загрози. Подальші дослідження можуть бути спрямовані на вдосконалення моделей, використання реальних даних аудиту, інтеграцію з системами моніторингу безпеки, а також розширення функціональних можливостей таких систем за рахунок застосування більш складних моделей машинного навчання.

Список літератури

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Geneva: ISO, 2022.
2. Голубничий, Д. Ю., Сєвєрінов, О. В., Коломійцев, О. В., Місюра, О. М., Третяк, В. Ф., Власов, А. В., & Крук, Б. М. (2021). Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації.
3. Goodfellow I. Deep Learning. MIT Press, 2016.
4. NIST Cybersecurity Framework (CSF) 2.0: Cybersecurity Framework. Gaithersburg, MD: National Institute of Standards and Technology, 2024.
5. Bishop C. Pattern Recognition and Machine Learning. Springer, 2006.

АНАЛІЗ ІНСТРУМЕНТІВ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Блюма К.А., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Тестування на проникнення є важливою складовою забезпечення інформаційної безпеки комп'ютерних систем та мереж [1]. Воно дозволяє виявити вразливості до того, як ними скористаються зловмисники, а також оцінити рівень захищеності системи в реальних умовах. Проведення такого тестування імітує дії потенційного атакуючого, що дає змогу виявити не лише технічні недоліки, але й організаційні проблеми безпеки, такі як неправильні налаштування доступу, відсутність політик безпеки або недостатній рівень підготовки персоналу. Таким чином, тестування на проникнення виконує як діагностичну, так і превентивну функцію в системі кіберзахисту.

У сучасній практиці кібербезпеки використовується значна кількість інструментів [2]. **Метою доповіді** є проведення базового аналізу найбільш відомих інструментів.

Одним із найпоширеніших інструментів тестування на проникнення є Nmap, який застосовується для сканування мереж та виявлення активних вузлів і відкритих портів. Даний інструмент є ефективним на етапі попередніх етапах тестування, оскільки дозволяє отримати базову інформацію про цільову систему, включаючи тип операційної системи та запущені служби та їх версії [3]. Додатковою перевагою Nmap є підтримка сценаріїв (NSE – Nmap Scripting Engine), які дозволяють автоматизувати виявлення типових вразливостей та здійснювати більш глибокий аналіз мережевих сервісів.

Metasploit Framework є потужною платформою для експлуатації вразливостей [3]. Він містить велику кількість готових експлойтів, допоміжних модулів та корисних навантажень (payloads), а також дозволяє автоматизувати процес тестування. Крім того, цей інструмент активно використовується для навчання та відпрацювання практичних навичок у сфері кібербезпеки. Важливою перевагою є також інтеграція з іншими інструментами та можливість розширення функціональності шляхом створення власних модулів.

Burp Suite широко використовується для аналізу безпеки веб-додатків. Його основною перевагою є можливість перехоплення та модифікації HTTP-запитів [3], що дозволяє досліджувати поведінку веб-додатків, знаходити вразливості типу SQL-ін'єкцій, XSS та інші. Додаткові модулі Burp Suite значно розширюють функціональність інструменту.

Wireshark застосовується для аналізу мережевого трафіку та дозволяє детально досліджувати пакети даних у режимі реального часу [1]. Це дає змогу виявляти підозрілу активність, аналізувати протоколи та знаходити потенційні точки витоку інформації. Інструмент є особливо корисним для виявлення атак типу «людина посередині» (Man-in-the-Middle), а також для аналізу некоректної роботи мережевих сервісів та протоколів.

Nessus є автоматизованим сканером вразливостей, який дозволяє швидко отримати звіт про стан безпеки системи. Він підтримує регулярні оновлення бази вразливостей, що робить його ефективним інструментом для постійного моніторингу та аудиту безпеки [1]. Крім того, Nessus дозволяє класифікувати знайдені вразливості за рівнем критичності та надає рекомендації щодо їх усунення, що значно спрощує процес прийняття рішень у сфері управління ризиками.

Кожен із розглянутих інструментів має свої особливості та сферу застосування. Виходячи з аналізу, найбільш ефективним є Metasploit Framework, оскільки він поєднує гнучкість, потужність та можливість практичної експлуатації вразливостей. Водночас найкращі результати досягаються при комплексному використанні декількох інструментів, що дозволяє отримати більш повну та об'єктивну оцінку рівня безпеки системи.

Також варто зазначити, що ефективне тестування на проникнення передбачає дотримання певної методології, яка включає етапи розвідки, сканування, експлуатації та формування звіту [4]. Якісно складений звіт є не менш важливим, ніж сам процес тестування, оскільки саме він містить рекомендації щодо усунення виявлених вразливостей. Вибір інструментів і методів тестування має здійснюватися з урахуванням специфіки досліджуваної інформаційної системи, її архітектури, критичності ресурсів та актуальних загроз [5]. Важливим аспектом є також регулярність проведення тестувань, що дозволяє своєчасно виявляти нові вразливості та підтримувати належний рівень захищеності.

Таким чином, комплексний підхід до тестування на проникнення, що включає використання різних інструментів, дотримання методології та залучення кваліфікованих фахівців, є запорукою ефективного забезпечення інформаційної безпеки сучасних систем.

Список літератури

1. Scarfone K., Souppaya M. Guide to Penetration Testing. NIST Special Publication 800-115. 2018. С. 1–25. DOI: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-115.pdf.

2. Дорофєєва, К., Сєвєрінов, О., Сидоренко, З., & СухотеплиЙ, В. (2025). Застосування інструмента аналізу безпеки для виявлення критичних вразливостей у веб-додатках. *Вісник Херсонського національного технічного університету*, *3*(4 (95)), 62-68.

3. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press. 2014. С. 25–180. https://repo.zenk-security.com/

4. Дорофєєва, К. І., Сєвєрінов, О. В., & Сидоренко, З. М. (2025). Методологія проведення тестування на проникнення веб-додатків // Проблеми інформатизації: тринадцята міжнародна науково-технічна конференція.

5. Д'якова, Н. Є., & Сєвєрінов, О. В. (2022). Тестування вразливостей сучасних веб-ресурсів // Проблеми інформатизації : десята міжнародна науково-технічна конференція.

ВИКОРИСТАННЯ ГІБРИДНОГО ШИФРУВАННЯ У СИСТЕМАХ ОБМІНУ ПОВІДОМЛЕННЯМИ (МЕСЕНДЖЕРАХ)

Цариценко І.К., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні системи обміну повідомленнями (месенджери) є невід'ємною частиною цифрової комунікації користувачів та активно використовуються як у побутовій, так і в професійній діяльності. Вони забезпечують обмін текстовими повідомленнями, мультимедійним контентом, файлами, а також підтримують голосові та відеодзвінки. Зростання обсягів переданої інформації та зростаючі вимоги до конфіденційності даних зумовлюють необхідність використання ефективних криптографічних механізмів захисту інформації під час її передачі каналами зв'язку.

Особливої актуальності набуває питання забезпечення такого рівня захисту, щоб навіть сервери, через які передаються повідомлення, не мали можливості отримати доступ до їхнього вмісту. Така модель безпеки відома як наскрізне шифрування (end-to-end encryption) і є стандартом для сучасних захищених комунікаційних платформ. Сучасні месенджери, такі як Signal, WhatsApp та Telegram, використовують гібридний підхід до шифрування для вирішення цієї проблеми, який поєднує переваги симетричних та асиметричних криптографічних алгоритмів. Такий підхід дозволяє забезпечити високу швидкість обробки даних разом із надійним механізмом розподілу криптографічних ключів між абонентами, а також зменшити обчислювальне навантаження на клієнтські пристрої.[1]

Метою доповіді є дослідження принципів застосування гібридного шифрування в системах обміну повідомленнями та формування рекомендацій щодо підвищення рівня їх криптографічного захисту. Зокрема, розглядається використання асиметричного алгоритму RSA [2] для обміну ключами та симетричного алгоритму AES [3] для шифрування даних як базового підходу до забезпечення конфіденційності.

Така комбінація дозволяє вирішити проблему безпечної доставки ключа симетричного шифру, який використовується для безпосереднього шифрування повідомлень. Додатково враховується необхідність захисту цілісності та автентичності повідомлень, що може реалізовуватися шляхом використання криптографічних геш-функцій та механізмів аутентифікації повідомлень (MAC).

Разом з тим, більшість існуючих підходів гібридного шифрування в месенджерах, що базуються на використанні RSA для обміну ключами та AES для шифрування даних, мають суттєвий недолік — відсутність або недостатню реалізацію властивості perfect forward secrecy (PFS) [5].

Це означає, що безпека попередніх сесій залежить від збереження конфіденційності довгострокових ключів.

У разі компрометації довгострокового приватного ключа користувача зловмисник отримує можливість розшифрувати раніше перехоплені

повідомлення, що створює значні ризики для конфіденційності історичних даних. Така загроза є особливо критичною в умовах тривалого зберігання зашифрованого трафіку з метою його подальшого аналізу.

Для усунення зазначеного недоліку запропоновано удосконалений підхід до організації гібридного шифрування. Він передбачає використання RSA виключно для початкового обміну ключовим матеріалом у поєднанні з генерацією ефемерних (тимчасових) сесійних ключів AES для кожного сеансу зв'язку.

Додатково пропонується механізм динамічної ротації ключів після кожного повідомлення, що забезпечує реалізацію PFS та унеможливлює розшифрування попередніх повідомлень навіть у разі компрометації довгострокових ключів, зберігаючи при цьому високу продуктивність. Такий підхід також сприяє мінімізації обсягу даних, які можуть бути скомпрометовані внаслідок однієї атаки, та підвищує загальну стійкість системи до криптографічного аналізу.

У доповіді також розглядаються загальні принципи побудови клієнт-серверної архітектури захищених месенджерів та підходи до встановлення безпечного сеансу зв'язку між клієнтами.

Моделювання запропонованого підходу доводить, що навіть за умови повного контролю над серверною інфраструктурою зловмисник не має можливості отримати доступ до вмісту переданих повідомлень без володіння закритими ключами користувачів.

Отримані результати підтверджують доцільність застосування вдосконалених підходів гібридного шифрування та можуть бути використані при формуванні рекомендацій щодо підвищення безпеки сучасних систем обміну повідомленнями [4].

Список літератури

1. Paar C., Pelzl J. Understanding Cryptography. Springer, 2010. https://gnanavelrec.wordpress.com/wp-content/uploads/2019/06/2.understanding-cryptography-by-christof-paar-.pdf

2. Zehao Tuo. A comparative Analysis of AES and RSA algorithms and their integrated application. DOI: https://doi.org/10.54254/2753-8818/25/20240893

3. Rahoul Ganesh, Burhan Ul Islam Khan,· Abdul Raouf Khan, Amirrudin Bin Kamsin A panoramic survey of the advanced encryption standard: from architecture to security analysis, key management, real-world applications, and post-quantum challenges. https://link.springer.com/article/10.1007/s10207-025-01116-x

4. Гібридне шифрування. https://www.vpnunlimited.com/ua/help/cybersecurity/hybrid-encryption

5. Colin Boyd, Kai Gellert, A Modern View on Forward Security. *The Computer Journal*, Volume 64, Issue 4, April 2021, Pages 639–652 DOI: https://doi.org/10.1093/comjnl/bxaa104

Ігор Костянтинович Цариценко, бакалавр, +380999710223, ihor.tsarytsenko@nure.ua

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ СЦЕНАРНОГО КОГНІТИВНОГО МОДЕЛЮВАННЯ ДЛЯ АНАЛІЗУ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Тютюник В. В.[1,2], Тютюник О. О.[1]
[1]Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна
[2]Харківський національний університет радіоелектроніки, Харків, України

У сучасних наукових дослідженнях значна увага приділяється проблемам захисту критичної інфраструктури (КІ), забезпечення кібербезпеки та управління ризиками. Водночас недостатньо розробленими залишаються підходи, що дозволяють комплексно враховувати взаємозалежність загроз, динаміку їх розвитку та сценарний характер впливу на інформаційну безпеку (ІБ) в умовах воєнного стану. Це обумовлює необхідність застосування методів, здатних адекватно відображати складні причинно-наслідкові зв'язки в системах із високим рівнем невизначеності. Одним із таких інструментів є когнітивне моделювання, зокрема апарат нечітких когнітивних карт (НКК), який забезпечує формалізоване представлення взаємодії факторів впливу та дозволяє здійснювати сценарний аналіз розвитку загроз [1].

Метою доповіді є дослідження та розроблення підходу до сценарного моделювання впливу загроз на ІБ об'єктів критичної інфраструктури (ОКІ) із застосуванням НКК.

У доповіді наведено результати дослідження та розроблення підходу до сценарного моделювання впливу загроз на ІБ КІ з використанням НКК. Так, когнітивне сценарне моделювання дозволяє не лише ідентифікувати ключові загрози ІБ, але й оцінити їх системний вплив на стійкість функціонування ОКІ за різних сценаріїв розвитку подій. Використання такого підходу створює підґрунтя для підтримки прийняття управлінських рішень у сфері ІБ в умовах високої невизначеності та обмеженості ресурсів. З огляду на зазначене, актуальним є дослідження, спрямоване на розроблення когнітивної моделі сценаріїв впливу загроз на ІБ ОКІ в умовах введення в державі правового режиму воєнного стану [3].

В роботі когнітивну модель подано на рис. 1 у вигляді орієнтованого зваженого графа: $G = \langle C, E, W \rangle$, де $C = \{c_1, c_2, ..., c_n\}$ – множина концептів, $E \subseteq C \times C$ – множина орієнтованих зв'язків між концептами, $W = \{w_{ij}\}$ – множина ваг зв'язків, $w_{ij} \in [-1;1]$.

З урахуванням специфіки функціонування ОКІ в умовах введення правового режиму воєнного стану множина концептів формується з чотирьох логічних груп.

Перша група – концепти-загрози (Driver-concepts): $C_D = \{c_1, c_2, c_3, c_4, c_5\}$, де c_1 – кібератаки на інформаційні системи ОКІ, c_2 – фізичне ураження об'єктів інфраструктури, c_3 – порушення телекомунікаційних каналів, c_4 – інформаційно-психологічні впливи, c_5 – інсайдерські загрози. Дані концепти є зовнішніми по відношенню до системи та ініціюють сценарії впливу.

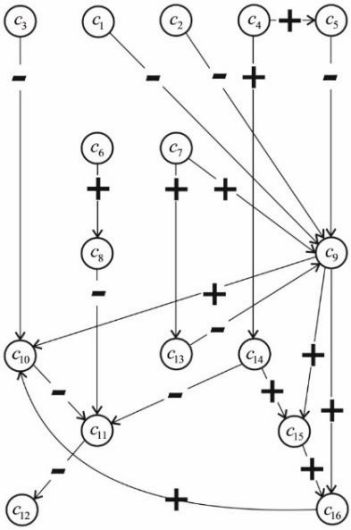


Рис. 1. Когнітивна модель сценарного впливу загроз на ІБ ОКІ в умовах запровадження правового режиму воєнного стану

Друга група – концепти умов воєнного стану (Ordinary-concepts): $C_W = \{c_6, c_7, c_8, c_9\}$ де c_6 – обмеженість ресурсів, c_7 – централізація управління, c_8 – дефіцит кваліфікованого персоналу, c_9 – підвищена інтенсивність зовнішніх загроз. Ці концепти виступають як підсилювачі або демпфери впливів.

Третя група – концепти інформаційної безпеки (Ordinary-concepts): $C_{IB} = \{c_{10}, c_{11}, c_{12}, c_{13}\}$, де c_{10} – конфіденційність інформації, c_{11} – цілісність інформації, c_{12} – доступність інформації, c_{13} – стійкість інформаційних систем.

Четверта група – концепти наслідків (Receiver-concepts): $C_R = \{c_{14}, c_{15}, c_{16}\}$, де c_{14} – порушення функціонування ОКІ, c_{15} – соціально-економічні збитки, c_{16} – зниження рівня національної безпеки.

Розроблена когнітивна модель дозволяє здійснювати сценарне моделювання розвитку ситуацій, оцінювати чутливість інформаційної безпеки до окремих загроз та обґрунтовувати пріоритетні напрями підвищення стійкості ОКІ в умовах введення правового режиму воєнного стану. Результати сценарного моделювання впливу загроз на ІБ ОКІ в умовах воєнного стану дозволяють виявити системні закономірності поширення негативних впливів, а також визначити ключові фактори, що формують стійкість або вразливість досліджуваної системи.

Так, порівняльний аналіз базового, кризового та катастрофічного сценаріїв показав, що зі зростанням інтенсивності загроз спостерігається нелінійний характер змін станів концептів. Навіть помірне підвищення активності driver-концептів за наявності несприятливих умов воєнного стану

призводить до суттєвого зниження показників доступності та стійкості інформаційних систем. У кризовому сценарії зафіксовано ефект каскадного поширення впливів, коли первинні кібернетичні або фізичні загрози через систему опосередкованих зв'язків спричиняють порушення функціонування ОКІ. Це підтверджує доцільність врахування непрямих впливів у межах когнітивного підходу. Аналіз системних показників впливу, чутливості та центральності дозволив ідентифікувати критичні вузли когнітивної моделі. Концепти, пов'язані з доступністю та стійкістю інформаційних систем, мають найвищі значення центральності, що свідчить про їх визначальну роль у забезпеченні стабільності функціонування ОКІ. Driver-концепти, що відповідають кібернетичним атакам і фізичному ураженню об'єктів, демонструють максимальні значення показника впливу. Натомість receiver-концепти, які відображають соціально-економічні наслідки та рівень національної безпеки, характеризуються високою чутливістю, що робить їх індикаторами критичного стану системи.

Отримані результати свідчать, що з точки зору управління ризиками доцільно зосереджувати захисні заходи не лише на нейтралізації окремих загроз, але й на підвищенні стійкості ключових концептів з високою центральністю. Такий підхід дозволяє зменшити системний ефект негативних впливів навіть у разі реалізації кризових сценаріїв [4, 5]. Крім того, когнітивна модель може використовуватися як інструмент підтримки прийняття рішень для оцінювання ефективності різних стратегій забезпечення ІБ ОКІ [6, 7].

Крім того, результати моделювання підтверджують, що умови воєнного стану відіграють роль підсилювальних факторів, які знижують адаптивні можливості системи ІБ. Обмеженість ресурсів, дефіцит персоналу та централізація управління зменшують ефективність реагування на загрози та прискорюють перехід системи у кризовий або катастрофічний стан. Так, навіть за однакового рівня загроз, ІБ ОКІ в умовах воєнного стану є значно вразливішою порівняно з мирним часом.

Список літератури

1. Салієва О.В., Яремчук Ю.Є. Симпліціальний аналіз структури когнітивної моделі для дослідження захищеності об'єкта критичної інфраструктури. *Реєстрація, зберігання і обробка даних.* 2020. 22. 3. 68–75. [Електронний ресурс]. Режим доступу: http://jnas.nbuv.gov.ua/article/UJRN-0001200603

2. Брежнєв Є.В., Фесенко Г.В., Харченко В.С. Методологічні засади оцінювання та забезпечення безпеки критичних інформаційних інфраструктури. *Радіоелектронні і комп'ютерні системи.* 2018. 4. 78–85. [Електронний ресурс]. Режим доступу: http://nbuv.gov.ua/UJRN/recs_2018_4_10

3. Тютюник В.В., Тютюник О.О. Сценарне когнітивне моделювання впливу загроз на інформаційну безпеку об'єктів критичної інфраструктури в умовах запровадження правового режиму воєнного стану. *Комунальне господарство міст. Серія: Інформаційні технології та інженерія*. 2026. Т. 1. Вип. 196. С. 22–33. DOI: https://doi.org/10.33042/3083-6727-2026-1-196-22-33

4. Тютюник В.В., Ященко О.А., Рубан І.В., Тютюник О.О. Особливості функціонування системи ситуаційних центрів на різних стадіях розвитку надзвичайних ситуацій. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2022. 1(43). 41–52. DOI: https://doi.org/10.33099/2311-7249/2022-43-1-41-52

ФОРМАЛІЗАЦІЯ ОПИСУ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ НА ОБ'ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Заболотний В.І., Голобородько Ю.М.
Харківський національний університет радіоелектроніки, Харків, Україна
Заболотний Д.М.
АТ «Інститут інформаційних технологій», Харків, Україна

В ході створення комплексів технічного захисту інформації (ТЗІ) на об'єкті інформаційної діяльності (ОІД) проводяться роботи по виявленню технічних каналів витоку інформації (ТКВІ) [1, 2].

Повнота та системність виявлення ТКВІ являється запорукою подальшого ефективного захисту інформації з обмеженим доступом (ІзОД), як проєктування, упровадження і супроводження розроблюваного комплексу ТЗІ. Законом України 2025р. «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» [3] запропоновані певні новації щодо реалізації скорегованих визначень на ОІД:

- "комплекс технічного захисту інформації - сукупність заходів, засобів технічного захисту інформації, призначених для захисту інформації від витоку технічними каналами в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах";
- "технічний канал витоку інформації - взаємопов'язана сукупність джерела небезпечного сигналу, середовища його поширення та засобу технічної розвідки, спрямована на забезпечення витоку інформації";
- "здійснення відповідно до законодавства підготовки, перепідготовки та підвищення кваліфікації осіб у сферах технічного захисту інформації".

Автори пропонують уточнені дії щодо виконання зазначених змін, заснованих на досвіді наукової, практичної та педагогічної діяльності в області виявлення, аналізу та захисту ТКВІ на ОІД.

Метою доповіді є пропозиція оформлення описів технічних каналів витоку інформації на ОІД в типових організаційно-розпорядчих документах, які розробляються на етапах [3]:

1) визначення й аналізу загроз інформації;
2) розроблення системи захисту інформації;
3) реалізації плану захисту інформації;
4) контролю функціювання та керування системою захисту інформації.

В доповіді наводиться досвід формалізації описів ТКВІ при їх виявленні в ході робіт при проєктуванні комплексів ТЗІ.

Запропоновано використання форми (рисунок 1) в якій наводяться графи, що дозволяють описувати основні складові технічних каналів витоку інформації в їх логічній взаємодії. Фактично така форма представляє якісну модель опису ТКВІ на основі якої можна скласти кількісну модель технічних каналів витоку інформації і проводити інженерний аналіз технічних каналів витоку інформації [2].

Це все дає можливість аналітикам, проєктантам, експлуатаційникам аргументовано відтворювати математичні співвідношення для проведення оцінок ефективності захисту інформації по обраним показникам.

№ з/п	Можливі ТКВІ					
	Назва каналу (при необхідності з визначенням ОТЗ, природи ТКВІ, засобу ТР)	Джерело ІзОД, розташування (поле, сигнал)	Середовище розповсюдження 1 (поле, сигнал)	Для складного каналу		Апаратура розвідки (АР) (Найнебезпечніше розташування) за схемою: 1) в КЗ ВП, 2) за КЗ зверху, знизу, 3) за КЗ в плані, 4) автостоянка, 5) ЗС.
				Перетворювач енергії сигналу (назва, вид)	Середовище розповсюдження 2 (поле, сигнал)	
1	2	3	4	5	6	7
1	ПЕМВ монітору ПЕОМ	Інформаційні сигнали монітору (струми)	Етера. (ПЕМВ)	-	-	2) засіб радіорозвідки (РР) поверхом вище, нижче; 3) засіб РР в за межами ВП к суміжних приміщеннях, в коридорі, за межами споруди на південь; 4) засіб РР на автостоянці; 5) засіб РР у ЗС.
2	ПЕМН монітору ПЕОМ на шину заземлення ВП	Інформаційні сигнали монітору (струми)	Етера. (ПЕМВ)	ВА (провідник заземлення)	Контур автономного заземлення ВП на зовнішній стіні споруди спуску до заземлювача (напруга небезпечного сигналу)	3) підсилювач на шині заземлення на зовнішній стіні споруди.
3	ПЕМН монітору ПЕОМ на ситему опалення ВП	Інформаційні сигнали монітору (струми)	Етера. (ПЕМВ)	ВА (труба опалення)	труби опалення (напруга небезпечного сигналу)	2) підсилювач на трубах опалення поверхом вище, нижче
…	…	…	…	…	…	…

Рис. 1. Приклад оформлення ТКВІ
у аналітичних, звітних документах на комплекси ТЗІ ОІД

Особливості оформлення колонок таблиці наступні.

1. №№ з/п. нумерація ТКВІ.
2. Назва каналу зазначається з вказівкою його природи:

1) побічне електромагнітне випромінювання (ПЕМВ),
2) побічне електромагнітне наведення (ПЕМН),
3) розвідка мовної інформації,
4) розвідка інформації, що візуалізується тощо.

При необхідності, визначається основний технічний засіб (ОТЗ) або його окремий елемент, який є джерелом ТКВІ:

1) монітор, відеокарта, підсилювач, накопичувач тощо;
2) голосовий апарат людини, гучномовець;
3) екран монітору, плакат, проекційний екран, документ на аркуші.

Засіб технічної розвідки вказується якщо він визначає назву каналу (у відповідному граматичному відмінку), наприклад:

1) лазерний засіб акустичної розвідки (ЛЗАР),
2) закладний пристрій (ЗП),
3) підсилювач,
4) контактній датчик,
5) прихована відеокамера.

3. Джерело інформації з обмеженим доступом [3], розташування, поле, сигнал, які їм породжуються.

4. Середовище розповсюдження 1 (поле, сигнал).

5. В багатьох випадках в ТКВІ здійснюється перетворення виду енергії, яка переносить сигнал. Це може бути випадкова антена (ВА), контактний датчик, акустоелектричний перетворювач, шибка вікна, мембрана тощо. В такому випадку необхідно вказати цей перетворювач енергії сигналу (назва, вид перетворення).

6. Середовище розповсюдження 2 (поле, сигнал).

7. Назва апаратура розвідки (АР). Найнебезпечніше розташування в просторі по відношенню до ОІД або виділеного приміщення (ВП) за схемою по відношенню до межі контрольованої зони (КЗ):

1) в КЗ ВП,

2) за КЗ зверху, знизу,

3) за КЗ в плані, в тому числі в межах споруди та за ними,

4) автостоянка можливого довготривалого знаходження апаратура розвідки в автомобілі.

5) зацікавлена сторона (ЗС) об’єкт, який має властивості екстериторіальності по відношенню до ОІД.

Використання даної формалізації опису ТКВІ дозволяє стандартизувати звітну документацію щодо комплексів ТЗІ при її розробці і використанню при проєктуванні, впровадженню та супроводу в життєвому циклі. Додатковим достоїнством такого формату може бути використання організаційно-розпорядної документації в ході контрольних перевірок ефективності заходів захисту ІзОД.

Також використання цього формату корисно в навчальному процесі ВНЗ та процесі підвищення професійного рівня персоналу ОІД.

Список літератури

1. Національний стандарт ДСТУ 3396.2-97. «Захист інформації. Технічний захист інформації. Терміни та визначення.

2. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації [Електронний ресурс]: навчальний посібник / С. О. Іванченко, О. В. Гавриленко, О. А. Липський [та ін.]; НТУУ «КПІ». – Електронні текстові дані (1 файл: 615 Кбайт). – Київ: НТУУ «КПІ», 2016. – 104 с. Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/930d9270-2cb1-4c62-a4ce-ab5404d9b90f/content. Дата перегляду 01.04.2026.

3. Заболотний, В. І. (2003). Класифікація технічних каналів витоку інформації // Радіотехника, 2003. Вип. 134. – С. 210-217.

4. Закон України Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури. Відомості Верховної Ради (ВВР), 2025, № 35, ст.134.

5. Національний стандарт ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні положення.

РОЛЬ МАГНІТНОЇ СКЛАДОВОЇ ПЕМВ ЗАСОБІВ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ В ОЦІНЦІ РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ

Гапіченко А.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Формування каналу витоку [1] через побічні електромагнітні випромінювання (ПЕМВ) відбувається внаслідок перехоплення апаратурою технічної розвідки електромагнітних полів. Ці поля створюються навколо струмопровідних елементів та електронних компонентів під час циркуляції інформаційних сигналів і здатні вільно поширюватися поза межами контрольованої території. Для дослідження ступеня небезпеки технічних каналів витоку інформації (ТКВІ), що виникають у відеотрактах засобів обчислювальної техніки (ЗОТ), традиційно застосовують спеціальні тестові відеосигнали, які генерують на дисплеї чергування чорних і білих пікселів. Спектр струмових імпульсів таких сигналів має вигляд дискретного набору непарних гармонік, математичний опис яких легко отримати за допомогою розкладання в ряд Фур'є. Використовуючи розв'язки рівнянь Максвелла, можна розрахувати інтенсивність компонентів ПЕМВ на будь-якій заданій відстані від випромінювача, що дає змогу оцінити рівень захищеності відповідного ТКВІ. Згідно з рішеннями рівнянь Максвелла, радіальна магнітна складова (H_r) електромагнітного поля для моделі випромінювача у вигляді елементарної рамки площею s зі струмом гармоніки I визначається як [2]:

$$H_r = jk\frac{Is}{2\pi r^2}\left[1 - j\frac{1}{kr}\right]\cos\theta,$$

де k – хвильове число, r – відстань до точки спостереження, θ – меридіальний кут на точку спостереження від осі рамки, s – площа рамки, I – комплексна амплітуда струму гармоніки струму в рамці. Пропонується для дослідження ПЕМВ використовувати передатну функцію [2]:

$$\mathrm{K}_r^H(f) = \frac{H_r}{\mathrm{I}}$$

Для дослідження ПЕМВ пропонується використовувати передатну функцію безпосередньо для магнітної складової H_r. Для оцінки загасання поля доцільно використати модуль коефіцієнта передачі. Для цього хвильове число k можна виразити через параметри середовища згідно зі співвідношенням:

$$\mathrm{k} = \frac{2\pi}{\lambda} = \frac{2\pi\mathrm{f}}{\mathrm{c}},$$

де λ – довжина хвилі, f – частота, c – швидкість світла.

Розрахувавши модуль комплексного числа, для подальшої візуалізації просторового розподілу поля виконуються відповідні математичні заміни.:

$$1 - j\frac{1}{kr} = 1 - j\frac{c}{2\pi fr} = \sqrt{1^2 + \left(\frac{c}{2\pi fr}\right)^2}.$$

В результаті:

$$K_r^H = \sqrt{\left(\frac{f}{r^2 c}\right)^2 + \left(\frac{c}{4\pi^2 r^3 f}\right)^2}\cos\theta.$$

Аналітичні оцінки проводились на діапазоні відстаней від 0.1 до 100 метрів та частот від 0.1 до 1000 МГц. В ході роботи було запропоновано три графіки:

– 3-х мірне зображення для коефіцієнта передачі,

– 2-х мірне зображення залежності коефіцієнта передачі від відстані для 3-х частот,

– 2-х мірне зображення залежності коефіцієнта передачі від частоти для 3-х відстаней.

Візуалізація виконувалась в середовищі розробки PyCharm з використанням мови програмування Python, а також допоміжних бібліотек Numpy та Matplotlib.

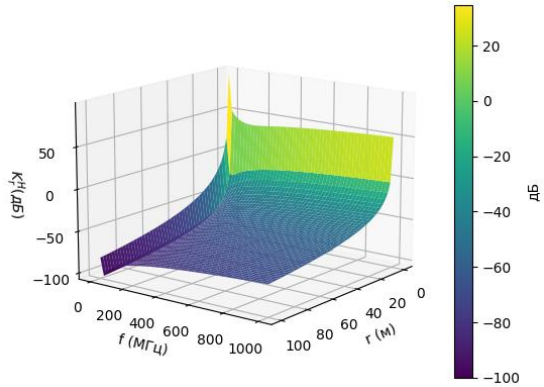


Рис. 1. Графік залежності коефіцієнта передачі від відстані та частоти

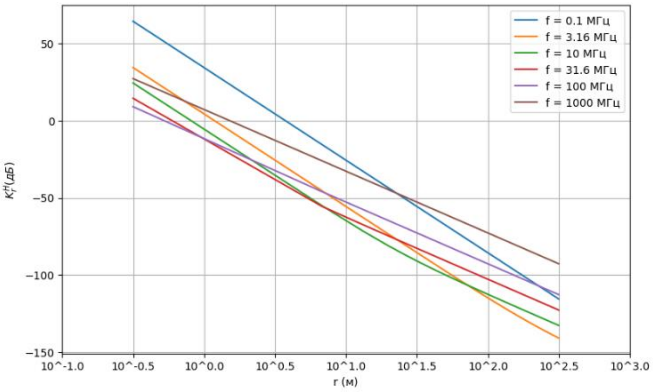


Рис. 2. Графік залежності коефіцієнта передачі від відстані для логарифмічної шкали відстаней

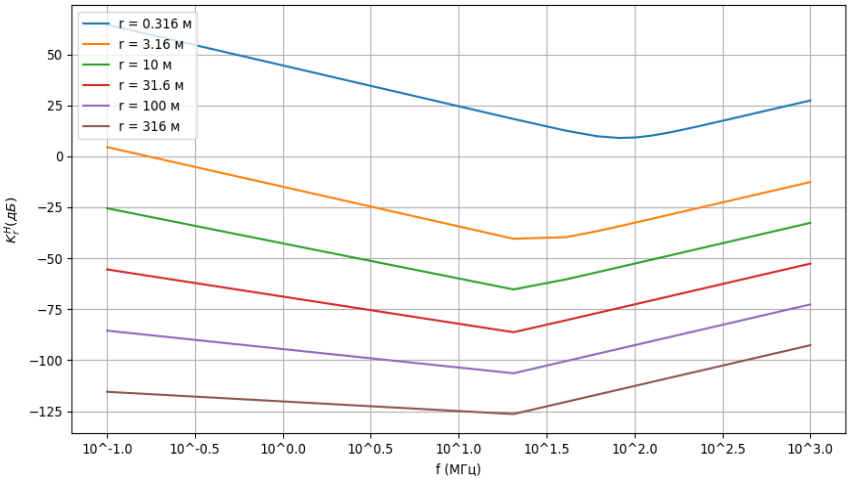


Рис. 3. Графік залежності коефіцієнта передачі
від частоти для логарифмічної шкали частот спектру

Проведене дослідження дозволило проаналізувати доцільність застосування коефіцієнта передачі для розрахунку та оцінювання параметрів побічних електромагнітних випромінювань, а також сформувати аналітичну базу для наступних наукових робіт.

На основі отриманих результатів пропонується впровадити метод екстраполяції для оцінки вразливості ТКВІ відеотрактів ЗОТ. Цей підхід дає можливість прогнозувати рівні сигналів у ймовірній точці перехоплення за межами контрольованої зони. Прогноз здійснюється шляхом перерахунку даних інструментальних вимірювань інтенсивності небезпечних гармонік, отриманих на ближній відстані контролю, із подальшим їх порівнянням із встановленими нормами технічного захисту.

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.

3. Гапіченко, А. М., & Заболотний, В. І. (2025). Математична модель коефіцієнта передачі побічних електромагнітних випромінювань відеотракту засобів обчислювальної техніки для широких діапазонів частот і відстаней. / Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доп. п'ятнадцятої міжнар. наук.-техн. конф., 24–25 квітня 2025 року: [у 4 т.]. Т. 3: секції 3, 4. – Баку; Харків ; Жиліна : [б. в.], 2025. – С. 73.

АВТОМАТИЗОВАНИЙ МЕТОД МІКРОСЕГМЕНТАЦІЇ IOT-МЕРЕЖ ДЛЯ РЕАЛІЗАЦІЇ АРХІТЕКТУРИ ZERO TRUST

Нєдєльніцев І.В., Антіпов І.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

Динамічні процеси розгортання великих і різнорідних IoT-систем, від розумних домівок до масштабних індустріальних мереж, створюють надлишкові та хаотичні канали зв'язку між вузлами. Така структурна ентропія має значний вплив на розширення поверхні атаки та створює ідеальні умови для горизонтального переміщення зловмисника після первинної компрометації одного з вузлів у середині периметру. Первинна компрометація часто відбувається через обхід застарілих заходів безпеки, експлуатацію вразливостей програмного забезпечення або використання легкодоступних пристроїв, таких як IP-камери чи сенсори. Це дозволяє зловмиснику використовувати функціонально надлишкові зв'язки та рухатися до критичних вузлів інфраструктури, таких як шлюзи чи хмарні сервіси. Тому розробка архітектурних підходів для протидії цим загрозам та впровадження парадигми Zero Trust є важливою науковою задачею [1].

Згідно зі стандартом NIST SP 800-207 [2], впровадження Zero Trust є відмова від довіри за замовчуванням, безперервна верифікація та мікросегментація системи. Мікросегментація – це сучасний метод забезпечення мережевої безпеки, який передбачає поділ центрів обробки даних та хмарних середовищ на невеликі ізольовані сегменти для впровадження детальних політик безпеки [3]. Сучасні мережі мають складну структуру взаємодії, що значно ускладнює розуміння легітимності шляхів передачі даних та ручне застосування класичних моделей сегментації або стандартних декларативних профілів, таких як MUD (Manufacturer Usage Description) [4], які хоч і задають політику за замовчуванням, але потребують адаптивної перевірки. Різноманіття пристроїв та їхні обмежені ресурси для обчислення ускладнюють перенесення традиційних механізмів ізоляції корпоративного рівня в IoT-середовище без втрати керованості саме тому є необхідність у пошуках методів та засобів автоматизації великих IoT мереж.

Метою доповіді є розробка гібридного математичного методу автоматизованої мікросегментації мережі, як один з аспектів Zero Trust архітектури, кардинально знизити ризики латерального руху та автоматично синтезувати політики безпеки на основі застосування спектральної кластеризації графів та евристичного прунінгу.

В доповіді наводяться результати застосування розробленого алгоритму, який математично моделює IoT-мережу як орієнтований зважений граф, де множина ребер $G = (V, E)$, поділяється на легітимні функціональні зв'язки E_{func} та паразитні шумові зв'язки E_{noise}. Для моделювання ентропії реального середовища генерується топологічний шум, ймовірність появи якого залежить від сумісності ролей: $P(u,v) = P_{base}(Role_u, Role_v) \times \sigma$ при цьому

враховується феномен «Rich get richer», коли центральні шлюзи мають вищу ймовірність отримати паразитні з'єднання. Мережа поділяється на 4 ієрархічні рівні:

1. L1 – сенсори, камери, актуатори;
2. L2 – агрегатори, хаби, контролери;
3. L3 – шлюзи;
4. L4 – хмарні сервіси, сервери.

Метод використовує матрицю Лапласа $L_{sym} = I - D^{-\frac{1}{2}}AD^{-\frac{1}{2}}$ [5] для знаходження власних векторів (зокрема вектора Фідлера, що кодує оптимальний розріз) та подальшого розбиття графа на ізольовані функціональні кластери.

Для усунення логічних вразливостей всередині кластерів додатково застосовується евристичний прунінг – фільтрація на основі жорстких правил. Зокрема, алгоритм блокує горизонтальну взаємодію між пристроями першого рівня – $L(u) = L(v) = 1$, забороняє зв'язки з різницею рівнів більше одиниці $|L(u) - L(v)| > 1$ – та існує $u \to w \to v$, відсікає надсилання команд до що не можуть їх приймати – $L(u) > L(v)$ та $R(v) \neq Actuator$, а також забороняє прямий доступ пристроїв рівня 1 та 2 до зовнішніх мереж в обхід проміжних вузлів.

Наведені дані експериментального моделювання, проведеного для трьох масштабів мереж (мала ~30, середня ~330, велика ~950 пристроїв) з інтенсивністю шуму σ від 0.0 до 5.0, показують, що на ефективність алгоритму безпосередньо впливають масштаб та зашумленість.

Для кількісної оцінки ефективності запропонованого методу пропонується вимірювати результати сегментації за допомогою спеціалізованих метрик:

– *wASR* (Weighted Attack-Surface Reduction) – зважене зменшення поверхні атаки;

– *wLMI* (Weighted Lateral Movement Index) – зважений індекс горизонтального переміщення;

– *FBR* (False Block Rate) – частка хибних блокувань легітимного трафіку;

– *PCR* (Policy Compression Ratio) – ефективність стиснення правил.

Зважене зменшення поверхні атаки(*wASR*), розраховується за формулою:

$$wASR = 1 - \frac{\sum_{(u,v)\in E_{policy}} Crit(v)}{\sum_{(u,v)\in E_{total}} Crit(v)},$$

де: E_{total}– множина всіх спостережуваних фізичних та логічних зв'язків у мережі до сегментації (включаючи ентропійну складову);

E_{policy} – підмножина зв'язків, дозволених синтезованою політикою;

$Crit(v) \in [0, 1]$ – коефіцієнт критичності вузла-приймача v.

Аналіз даних показує, що для середніх та великих мереж спостерігається стабільне лінійне зростання *wASR*; при $\sigma = 5$ досягається зменшення поверхні

атаки на 48%. Натомість у малих мережах показник стабілізується в межах 0.25 – 0.30 після досягнення рівня шуму $\sigma = 3$.

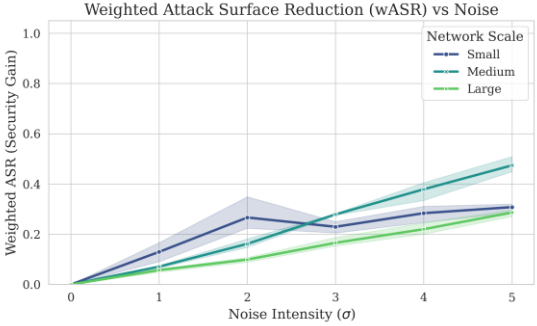


Рис. 1. Зважене зменшення поверхні атаки (wASR) відносно шуму

Для великомасштабних мереж алгоритм виявляє надзвичайно високу стійкість до зашумлення: при рівні шуму $\sigma = 2$ зважений ризик горизонтального переміщення (*wLMI*) стабільно знижується на 78.4%. Цей показник розраховується за формулою:

$$wLMI = \frac{1}{|V|} \sum_{u \in V} \frac{\sum_{v \in Reach(u, E_{policy})} Crit(v)}{\sum_{v \in V} Crit(v)}$$

де $Reach(u, E_{policy})$ представляє множину всіх вузлів, до яких існує шлях від вузла u.

Спостереження за частотою помилкових блокувань (*FBR*) свідчить про збереження високого рівня функціональної цілісності системи: для великих мереж при $\sigma = 2$ частка помилково заблокованих легітимних зв'язків становить лише 1.6%, що повністю відповідає експлуатаційним вимогам промислових середовищ (поріг < 5%).

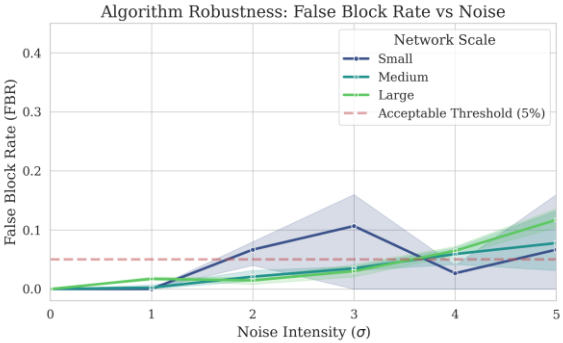


Рис. 2. Стійкість до топологічних шумів

Крім того, значення ефективності стиснення політик (*PCR*), що розраховується як $PCR = \frac{|E_{policy}|}{|E_{total}|}$, становить 0.81 для топологій з інтенсивним шумом $\sigma = 3$. Це доводить здатність системи автоматично відсікати до 19% аномальних з'єднань, оптимізуючи навантаження на мережеве обладнання, полегшуючи адміністрування та підтримку такої системи.

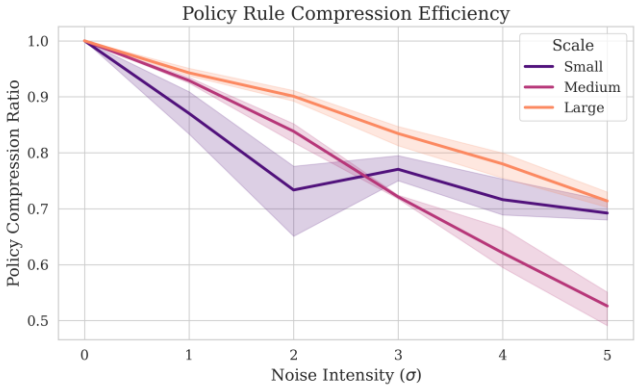


Рис. 3. Коефіцієнт стиснення політики

В зв'язку з цим актуальності набувають методи автоматизованого синтезу політик безпеки, засновані на використанні узагальнених математичних характеристик мережевої зв'язності.

Запропонований підхід забезпечує надійну локалізацію кіберінцидентів у межах однієї зони/сегменту, гарантуючи ізоляцію критичних вузлів інфраструктури від скомпрометованих периферійних пристроїв. Це дозволяє усунути операційну складність адміністрування та ефективно масштабувати парадигму Zero Trust в умовах сучасних високоентропійних IoT-систем, генеруючи компактні правила фільтрації (ACL) без ручного втручання.

Список літератури

1. Moskvin K., Sievierinov O. Zero Trust Architecture in Corporate Cybersecurity Systems // Computer and information systems and technologies : Seventh International Scientific and Technical Conference, 2024. – Kharkiv : NURE, 2024. – p. 54-55.

2. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. 2020. С. 1–50. DOI: https://doi.org/10.6028/NIST.SP.800-207.

3. What is microsegmentation in networking? вебсайт. URL: https://www.cloudi-fi.com/glossary/what-is-microsegmentation (дата звернення: 29.03.2025).

4. Lear E., Droms R., Romascanu D. Manufacturer Usage Description Specification. RFC 8520. 2019. С. 1–45. DOI: https://doi.org/10.17487/RFC8520

Wang X. Complex network security using community structure and dynamical analysis: spectral clustering and VEIP-WQU model. Complex Intelligent Systems. 2025. С. 5–7. DOI: https://doi.org/10.1007/s41109-025-00717-8

ПРОГРАМНИЙ ЗАСІБ ЗАХИСТУ ФАЙЛІВ НА ОСНОВІ XOR-ШИФРУВАННЯ

Орлов Є.К., Севостьянова О.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Забезпечення безпеки функціонування комп'ютерних систем та мереж є одним із ключових завдань сучасних інформаційних технологій. Особливої актуальності набуває захист окремих файлів, що містять конфіденційну інформацію, персональні дані або службові документи. Одним із доступних способів реалізації такого захисту є використання програмних засобів шифрування.

Метою доповіді є розробка програмного засобу для захисту окремих файлів на основі алгоритму XOR-шифрування з використанням графічного інтерфейсу користувача.

У доповіді наведено результати реалізації програмного застосунку мовою C++ із використанням бібліотеки WinAPI для операційної системи Windows. Програма забезпечує введення користувачем пароля, вибір необхідного файлу через стандартне діалогове вікно та виконання операцій шифрування або дешифрування.

Основу реалізованого методу становить побайтове XOR-шифрування, при якому до кожного байта файлу застосовується операція виключного АБО з відповідним символом пароля.

Символи ключа використовуються циклічно, що дозволяє обробляти файли довільного розміру.

Завдяки властивості симетричності операції XOR один і той самий алгоритм використовується як для шифрування, так і для відновлення початкових даних.

Реалізований програмний засіб працює з файлами в бінарному режимі, що забезпечує підтримку різних форматів даних. Наявність графічного інтерфейсу з полем введення пароля та кнопками запуску процесів шифрування і дешифрування підвищує зручність використання та дозволяє ефективно застосовувати програму для базового захисту інформації.

Результати дослідження показують можливість використання розробленого програмного засобу для забезпечення безпеки зберігання даних у комп'ютерних системах та мережах, а також як основу для подальшого вдосконалення методів захисту інформації.

Список літератури

1. Stroustrup B. The C++ Programming Language. 4th ed. Addison-Wesley, 2013.
2. Petzold C. Programming Windows. Microsoft Press, 1998.
3. Stallings W. Cryptography and Network Security: Principles and Practice. Pearson, 2020.

АНАЛІЗ ВЕБ-ІНТЕРФЕЙСІВ ВІДПОВІДНО ДО WCAG 2.2

Жорнокуй Д.Ю.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному цифровому світі дизайн веб-інтерфейсів відіграє важливу роль у забезпеченні доступності цифрових продуктів для широкого кола користувачів. Інклюзивність є важливою складовою якісного UI та UX, що зумовлює необхідність застосування міжнародних стандартів доступності. Ключовим документом у цій сфері є WCAG 2.2 (Web Content Accessibility Guidelines), який встановлює основні вимоги до доступного контенту [1].

Метою доповіді є аналіз особливостей веб-інтерфейсів з точки зору відповідності стандарту WCAG 2.2, а також встановлення ключових дизайн-принципів, що забезпечують зручність та доступність використання цифровими продуктами для різних категорій користувачів.

WCAG 2.2 базується на чотирьох принципах: сприйнятність, керованість, зрозумілість та надійність. Для дизайнерів ці принципи є практичними рекомендаціями щодо побудови інтерфейсів, які легко та швидко використовуються користувачами, включаючи людей з інвалідністю.

Сприйнятність у дизайні забезпечується правильним використанням кольору, контрасту та типографіки [2].

Керованість інтерфейсу означає доступність усіх елементів для взаємодії, також через клавіатурну навігацію. Потрібно мати чіткі фокусні стани і достатні розміри інтерактивних елементів, що є особливо важливим відповідно до вимог WCAG 2.2. З приводу зрозумілості інтерфейсу, інтерфейс має забезпечувати інтуїтивну навігацію та зрозумілі повідомлення, що є головним для користувачів із когнітивними порушеннями. І останнє - надійність, яка передбачає коректну роботу інтерфейсу з допоміжними технологіями та дотримання стандартних дизайн-патернів.

В доповіді наводяться результати аналізу сучасних підходів до проєктування доступних інтерфейсів, а також узагальнення рекомендацій щодо впровадження принципів WCAG 2.2 у практику UI/UX дизайну.

Підбиваючи підсумки, зазначу, що аналіз веб-інтерфейсів відповідно до WCAG 2.2 у контексті дизайну є комплексним процесом, що охоплює візуальні, функціональні та когнітивні аспекти взаємодії.

Застосування цих принципів дозволяє створювати інклюзивні цифрові продукти, які відповідають сучасним вимогам якості та доступності.

Список літератури

1. Loaiza-Ramírez, Isaías, and Beatriz A. González-Beltrán. "Digital accessibility guidelines for deaf and hard of hearing persons: a state-of-the-art review article." Universal Access in the Information Society 25.1 (2026): 4. doi:10.1007/s10209-025-01270-y;

2. Rizvi, Syeda Arooj Zehra. "Visual Diplomacy through Communication Design: The Revival of Basant 2026 in Lahore, Pakistan." The Critical Review of Social Sciences Studies 4.1 (2026): 3155-3172. doi: 10.59075/je71e863.

МЕТОД ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО ДОСТУПУ ДО РОЗПОДІЛЕНОГО СХОВИЩА ДАНИХ З ВИКОРИСТАННЯМ ПРОТОКОЛУ BITTORRENT

Чепурна І.С., Жинжиков Д.Д.
Харківський національний університет радіоелектроніки, Харків, Україна

Стрімке зростання обсягів цифрового контенту та розвиток розподілених інформаційних систем формують нові підходи до організації зберігання даних, удосконалення методів їх обробки та ефективної передачі великих масивів інформації. У таких умовах актуалізується потреба в забезпеченні надійного розподіленого зберігання даних і розробці ефективних методів передачі інформації відповідно до підвищених вимог щодо забезпечення цілісності та конфіденційності даних на тлі зростання кількості кіберзагроз, ризиків несанкціонованого доступу та витоків інформації.

Використання піринговых мереж дозволяє сформувати децентралізовану мережу з територіально розподіленими сховищами даних, що забезпечують зберігання великих обсягів інформації.

Застосування протоколу BitTorrent забезпечує високу швидкість передачу даних, масштабованість та відмовостійкість децентралізованої мережі [1]. Водночас специфіка функціонування піринговых мереж не забезпечує належного рівня захисту конфіденційних даних, що зумовлює необхідність впровадження додаткових механізмів безпеки, спрямованих на забезпечення цілісності інформації, а також її захисту від несанкціонованої модифікації та перехоплення [2].

Метою доповіді є огляд та систематичний аналіз існуючих методів організації захищеного доступу до ресурсів комп'ютерної мережі та обґрунтування методу реалізації доступу до інформаційних ресурсів розподіленого сховища даних із забезпеченням високого рівня цілісності та конфіденційності даних з мінімізацією ризиків несанкціонованого доступу та витоку інформації.

В доповіді наводяться результати аналізу сучасних методів організації доступу до розподілених сховищ даних корпоративних комп'ютерних мереж організацій, що базуються на впровадженні технологічних рішень з використанням віртуальних приватних мереж (VPN) [3]. Наведені дані показують, що застосування віртуальних тунелів VPN при організації доступу до розподілених сховищ даних дозволяє забезпечити диференційований доступ на основі ролей та прав користувачів до інформаційних ресурсів корпоративних комп'ютерних мереж організації. Використання протоколу тунелювання OpenVPN та криптографічних алгоритмів на основі AES забезпечує цілісність і конфіденційність даних під час доступу до інформаційних ресурсів розподіленого сховища даних [4]. Перспективи подальших досліджень спрямовані на вдосконалення методу організації захищеного доступу до інформаційних ресурсів розподіленого сховища даних з використанням протоколу обміну даних BitTorrent, що забезпечує одночасно

високу швидкість передачі даних, їх цілісність і конфіденційність та мінімізує ризики несанкціонованого доступу та витоку інформації.

Список літератури

1. Кренцін, М., & Куперштейн, Л. (2024). Метод захищеного обміну та зберігання файлів у пірингових мережах. *Herald of Khmelnytskyi National University. Technical Sciences*, *337*(3(2), 461-466 https://doi.org/10.31891/2307-5732-2024-337-3-69

2. Лужецький, В., & Савицька, Л. (2024). Механізми забезпечення захисту даних у пірингових мережах. *Herald of Khmelnytskyi National University. Technical Sciences*, *339*(4), 503-508. https://doi.org/10.31891/2307-5732-2024-339-4-74

3. Верховський, Ігор; Ткачов, Віталій. Методи побудови віртуальних тунелів extranet-систем. Scientific review, 2023, 4.89: 22-40.

4. Чепурна, І. (2025). Метод організації захищеного сегмента приватних SDN-мереж на основі протоколу bittorrent. *Вісник Херсонського національного технічного університету*, *2*(3 (94)), 515-525.

МЕТОДИ ПОБУДОВИ ЗАХИЩЕНИХ СЕГМЕНТІВ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ МЕДИЧНОЇ УСТАНОВИ

Чепурна І.С., Ларін Т.І.
Харківський національний університет радіоелектроніки, Харків, Україна

Впровадження цифрових технологій у сфері охорони здоров'я, зокрема розвиток державної електронної системи охорони здоров'я eHealth в Україні та перехід до застосування електронних медичних записів (ЕМЗ) зумовлює необхідність розробки технологічних рішень для захисту цифрових медичних архівів від ризиків несанкціонованого доступу та витоків конфіденційної медичної інформації, зокрема даних пацієнтів. Сучасна парадигма доступу до медичної інформації пацієнтів базується на дотриманні вимог Закону України «Про захист персональних даних» та європейського регламенту General Data Protection Regulation (GDPR), що гарантують конфіденційність даних пацієнтів [1, 2]. Водночас зі зростанням кіберзагроз та ризиків витоку конфіденційних даних нагальною проблемою стає забезпечення балансу між оперативним та безпечним доступом до таких даних, що зберігаються в локальних електронних сховищах медичних установ.

Метою доповіді є огляд та систематичний аналіз існуючих методів побудови захищених сегментів корпоративної комп'ютерної мережі медичної установи та обґрунтування методу реалізації контрольованого доступу до інформаційних ресурсів із забезпеченням високого рівня цілісності та конфіденційності медичних даних та мінімізацією ризиків несанкціонованого доступу та витоку інформації.

В доповіді наводяться результати аналізу сучасних методів побудови захищених сегментів корпоративних комп'ютерних мереж установ та організацій, що базуються на впровадженні технологічних рішень із

використанням віртуальних приватних мереж (VPN) [3]. Наведені дані показують, що застосування віртуальних тунелів VPN дозволяє забезпечувати захищену передачу даних між територіально розподіленими підрозділами, здійснювати диференційований доступ на основі ролей та прав користувачів до ресурсів корпоративних комп'ютерних мереж організації. Використання протоколів тунелювання, зокрема OpenVPN, WireGuard, IPsec, та криптографічних алгоритмів на основі AES забезпечує цілісність і конфіденційність даних під час передачі відкритими мережами [4]. Перспективи подальших досліджень спрямовані на розробку методу організації захищеного доступу до інформаційних ресурсів корпоративної комп'ютерної мережі медичної установи з використанням програмно-конфігурованого VPN-шлюзу на базі маршрутизатора MikroTik, що відповідає високим вимогам до забезпечення цілісності та конфіденційності даних та мінімізує ризики несанкціонованого доступу та витоку інформації.

Список літератури

1. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 07.04.2026).

2. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : станом на 20 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 07.04.2026).

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): 299-308.*

4. Верховський, Ігор; Ткачов, Віталій. Методи побудови віртуальних тунелів extranet-систем. Scientific review, 2023, 4.89: 22-40.

МЕТОДИ ОРГАНІЗАЦІЇ ЗАХИЩЕНОГО ДОСТУПУ ДО ЦИФРОВИХ РЕСУРСІВ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОСВІТНЬОЇ УСТАНОВИ

Корх О.С., Чепурна І.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Цифровізація науково-освітньої галузі зумовлює перехід від фізичних носіїв даних до цифрових сховищ на базі розподілених інформаційних систем, що забезпечують віддалений доступ користувачів до науково-освітніх ресурсів [1].

Водночас розширення відкритого доступу до наукових даних актуалізує потребу у забезпеченні високого рівня захисту корпоративних ресурсів наукових та освітніх установ на тлі зростання кількості кіберзагроз, ризиків витоку даних та несанкціонованого доступу [2].

Традиційні засоби безпеки, що базуються на довірі до внутрішнього середовища та зорієнтовані переважно на захист периметра корпоративної

мережі, поступово втрачають ефективність та виявляються вразливими до внутрішніх загроз [3].

Застосування технологій віртуалізації та контейнеризації дозволяє реалізувати надійні програмні засоби захисту інформаційних ресурсів освітніх установ. Використання віртуальних приватних мереж (VPN), сегментації мереж та програмно-конфігурованих засобів контролю трафіку дозволяють підвищити рівень захисту інформації, забезпечити цілісність і конфіденційність даних та ефективно керувати доступом до інформаційних ресурсів [4].

Метою доповіді є огляд та систематичний аналіз існуючих методів організації захищеного доступу до ресурсів корпоративної комп'ютерної мережі освітніх установ та обґрунтування методу реалізації контрольованого доступу до інформаційних ресурсів із забезпеченням ефективної фільтрації зовнішнього та внутрішнього трафіку.

В доповіді наводяться результати аналізу сучасних методів організації захищеного доступу до інформаційних ресурсів освітніх установ, що базуються на впровадженні технологічних рішень із застосуванням технології контейнеризації.

Отримані результати підтверджують, що використання розподіленого файрвола, що розгорнуто в ізольованих контейнерах Docker, дозволяє забезпечити контрольований доступ до інформаційних ресурсів корпоративної комп'ютерної мережі освітньої установи, мінімізуючи ризики несанкціонованого доступу та витоку даних.

Перспективи подальших досліджень спрямовані на вдосконалення методів управління доступом до ресурсів корпоративних комп'ютерних мереж освітніх установ та їх інтеграцію в чинні інформаційні системи.

Список літератури

1. Віротченко С. ЦИФРОВІЗАЦІЯ В ОСВІТІ: ПОРІВНЯННЯ ПІДХОДІВ УКРАЇНСЬКИХ І БАЛТІЙСЬКИХ ДОСЛІДНИКІВ ДО ВИЗНАЧЕННЯ ПОНЯТТЯ ТА ЗАВДАНЬ. *Наукові праці Міжрегіональної Академії управління персоналом. Педагогічні науки*. 2024. № 2(61). С. 5–9. URL: https://doi.org/10.32689/maup.ped.2024.2.1 (дата звернення: 07.04.2026).

2. *Poberezhnyk V., Balatska V., Opirskyy I. Development of the learning management system concept based on blockchain technology. CEUR Workshop Proceedings. 2023. Vol. 3550. URL: https://ceur-ws.org/Vol-3550/*

3. ZERO TRUST CONCEPT: MODERN METHODS OF ENSURING CYBERSECURITY IN CORPORATE NETWORKS / T. I. Korobeinikova et al. *Bulletin of Lviv State University of Life Safety*. 2024. No. 30. P. 67–77. URL: https://doi.org/10.32447/20784643.30.2024.07 (date of access: 07.04.2026).

4. Chepurna, I. і Frolov, D. (2025) «Метод підвищення продуктивності розподіленого брандмауера на базі Proxmox у корпоративних комп'ютерних мережах», *СУЧАСНИЙ СТАН НАУКОВИХ ДОСЛІДЖЕНЬ ТА ТЕХНОЛОГІЙ В ПРОМИСЛОВОСТІ*, (3(33), с. 180–188. doi: 10.30837/2522-9818.2025.3.180.

ВИБІР ОПТИМАЛЬНОЇ КОНФІГУРАЦІЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ З ДОВІРЕНИМИ ВУЗЛАМИ ЗА ДОПОМОГОЮ УНІФІКОВАНОЇ МОДЕЛІ ПРОГНОЗУВАННЯ ВИТРАТ ЕНЕРГІЇ

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

У розподілених обчислювальних мережах на основі персональних мобільних пристроїв актуальною науковою задачею є забезпечення належного рівня інформаційної безпеки без суттєвого зниження енергоефективності системи [1, 2]. Використання довірених вузлів дає змогу зменшити ризики викрадення даних, фальсифікації результатів обчислень і порушення цілісності обчислювального процесу, однак одночасно призводить до появи додаткових енергетичних витрат [2, 3]. За недостатньої кількості довірених вузлів знижується рівень захищеності та надійності мережі, а за їх надмірної кількості погіршується загальна енергетична ефективність обчислень. У зв'язку з цим виникає необхідність формалізованого підходу, який дозволить ще на етапі проектування оцінити вплив кількості довірених вузлів на сумарне енергоспоживання мережі та обрати раціональну конфігурацію [4].

Метою доповіді є застосування розробленої уніфікованої моделі прогнозування витрат енергії для вибору оптимальної конфігурації обчислювальної мережі з довіреними вузлами. Підхід базується на прогнозуванні сумарних енергетичних витрат для різної кількості довірених вузлів з урахуванням характеристик мобільних пристроїв, параметрів мережевої взаємодії, особливостей розподілу задач і накладних витрат, пов'язаних із забезпеченням безпеки [5]. На відміну від підходів, у яких кількість довірених вузлів задається емпірично, у даному випадку вона визначається на основі результатів моделювання як параметр. Доцільність такого підходу підтверджується сучасними дослідженнями мобільних volunteer та edge-середовищ, у яких питання довіри, конфіденційності, доступності та безпечної взаємодії розглядаються як ключові обмеження для практичного використання персональних мобільних пристроїв у розподілених обчисленнях [6]. У доповіді розглядається виконання серії прогнозних експериментів для мереж із різною кількістю довірених вузлів та аналіз характеру зміни сумарного енергоспоживання. Це дає змогу виявити область раціональних конфігурацій, у межах якої досягається компроміс між рівнем інформаційної безпеки та енергетичною ефективністю [7]. Таким чином, основна ідея роботи полягає в тому, що розроблена уніфікована модель може бути використана як інструмент підтримки прийняття рішень для прогнозування витрат енергії за різної кількості довірених вузлів і подальшого підбору їх оптимального числа. Такий підхід створює підґрунтя для енергоорієнтованого проектування захищених обчислювальних мереж на основі персональних мобільних пристроїв.

Список літератури

1. Мамчич О. О., Волк М. О. A unified model and method for forecasting energy consumption in distributed computing systems based on stationary and mobile devices.

Radioelectronic and Computer Systems. 2024. № 2(110). DOI: https://doi.org/10.32620/reks.2024.2.10

2. Мамчич О. О., Волк М. О. Model and methodology of measuring and forecasting of energy impact of security risks mitigation approaches in distributed computing systems on personal mobile devices. Вісник ХНТУ. 2025. № 3(94), Ч. 2. DOI: https://doi.org/10.35546/kntu2078-4481.2025.3.2.42

3. Ma P., Garg S., Barika M. Research allocation in mobile volunteer computing system: Taxonomy, challenges and future work. Future Generation Computer Systems. 2024. Vol. 154. P. 251–265. DOI: https://doi.org/10.1016/j.future.2024.01.015

4. Alsenani Y. VonEdgeSim: A Framework for Simulating IoT Application in Volunteer Edge Computing. Electronics. 2024. Vol. 13, No. 20. Art. 4124. DOI: https://doi.org/10.3390/electronics13204124

5. Alsubhi K. A Secured Intrusion Detection System for Mobile Edge Computing. Applied Sciences. 2024. Vol. 14, No. 4. Art. 1432. DOI: https://doi.org/10.3390/app14041432

6. Jia R., Ma J., You Z., Zhang M. Transparent and Privacy-Preserving Mobile Crowd-Sensing System with Truth Discovery. Sensors. 2025. Vol. 25, No. 7. Art. 2294. DOI: https://doi.org/10.3390/s25072294

7. Bashir S. R., Raza S., Misic V. A Narrative Review of Identity, Data and Location Privacy Techniques in Edge Computing and Mobile Crowdsourcing. Electronics. 2024. Vol. 13, No. 21. Art. 4228. DOI: https://doi.org/10.3390/electronics13214228

АНАЛІЗ ПОВЕРХНІ АТАКИ СИСТЕМИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ ЯК ОСНОВА ПОБУДОВИ ЦИФРОВОЇ ІМУННОЇ СИСТЕМИ

Товкун Ю.І., Хаханова Г.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Стрімка цифровізація державних сервісів супроводжується зростанням вимог до їхньої безпеки, надійності та стійкості до цілеспрямованих кіберзагроз. Особливої уваги в цьому контексті потребують системи електронного голосування, оскільки вони поєднують технічну, організаційну та суспільну складові й мають забезпечувати не лише коректність оброблення голосів, а й довіру до результатів виборчого процесу. Для таких систем критичними є гарантії цілісності бюлетеня, таємниці голосу, перевірюваності підрахунку та безперервності функціонування в умовах зовнішнього впливу [1].

Однією з базових передумов побудови стійкої архітектури захисту є аналіз поверхні атаки. Під поверхнею атаки доцільно розуміти сукупність інтерфейсів, сервісів, каналів взаємодії, компонентів і довірчих меж, через які потенційний порушник може вплинути на функціонування системи [2]. На відміну від підходу, зосередженого лише на окремих вразливостях, аналіз поверхні атаки дає змогу досліджувати систему комплексно, з урахуванням її архітектурних зв'язків, залежностей і можливих багатокрокових сценаріїв компрометації [3].

Метою доповіді є аналіз поверхні атаки системи електронного голосування та обґрунтування її ролі як основи побудови цифрової імунної системи, здатної забезпечити проактивне виявлення, локалізацію та

стримування кіберзагроз. Для систем електронного голосування доцільно виділити кілька основних контурів поверхні атаки. Перший контур пов'язаний із взаємодією користувача із системою та охоплює механізми автентифікації, веб інтерфейс, сесії доступу, клієнтське середовище голосування, а також канали доставлення посилань, токенів чи інших засобів доступу. У межах цього контуру актуальними є ризики фішингу, викрадення облікових даних, підміни сесій, використання шкідливого програмного забезпечення на кінцевому пристрої та маніпуляцій із діями виборця [3]. Другий контур становить прикладно-криптографічний рівень. Він охоплює створення електронного бюлетеня, його шифрування, передавання, зберігання, підрахунок та перевірюваність результатів. Саме цей рівень визначає можливість забезпечення цілісності голосу, неможливості несанкціонованої модифікації бюлетенів і прозорості виборчої процедури. Водночас навіть наявність криптографічних гарантій не усуває повністю ризики компрометації, якщо інші частини системи залишаються вразливими. Тому криптографічні механізми мають розглядатися як складова загальної архітектури безпеки, а не як самодостатній захист [2]. Третій контур формує інфраструктурно-інтеграційний рівень. До нього належать серверні компоненти, бази даних, журнали подій, API, механізми адміністрування, мережеві сервіси, а також інтеграції із зовнішніми системами ідентифікації, моніторингу чи сповіщення. Саме на цьому рівні виникають ризики несанкціонованого доступу до серверного середовища, ескалації привілеїв, компрометації адміністративних облікових записів, підміни конфігурацій, порушення доступності сервісу або використання вразливостей суміжних компонентів. Для структурованого опису таких сценаріїв доцільно використовувати матрицю MITRE ATT&CK, яка дозволяє зіставляти потенційні дії порушника з відповідними тактиками і техніками, зокрема Initial Access, Credential Access, Privilege Escalation, Discovery, Collection та Impact [4].

Такий поділ поверхні атаки дозволяє перейти від фрагментарного переліку загроз до цілісного представлення можливих векторів компрометації. Для систем електронного голосування це особливо важливо, оскільки реальна атака зазвичай не обмежується одним кроком, а розвивається як послідовність взаємопов'язаних дій. Порушник може починати з компрометації користувацького середовища, далі використовувати слабкі місця в логіці автентифікації, а потім переходити до інфраструктурного рівня або намагатися вплинути на цілісність оброблення виборчих даних [5].

У цьому контексті аналіз поверхні атаки є базовим етапом побудови цифрової імунної системи. Під цифровою імунною системою доцільно розуміти сукупність архітектурних, аналітичних та організаційних механізмів, що забезпечують безперервний цикл спостереження за станом системи, виявлення аномалій, інтерпретації інцидентів, локалізації впливу та адаптивного реагування. На відміну від статичних моделей захисту, такий підхід орієнтований не лише на запобігання компрометації, а й на збереження працездатності системи в умовах інциденту та на адаптацію до нових і комбінованих загроз [6]. Для систем електронного голосування це має

принципове значення, оскільки їхній захист не може зводитися лише до запобігання проникненню. Необхідно також забезпечити виявлення підозрілої активності, ізоляцію уражених сегментів, підтримання контролю над критичними компонентами та збереження довіри до результатів голосування навіть у разі часткової компрометації окремих елементів системи. Саме тому аналіз поверхні атаки слід розглядати не як допоміжний етап, а як концептуальну основу подальшого проектування механізмів цифрового імунітету. Отже, аналіз поверхні атаки системи електронного голосування створює підґрунтя для побудови цифрової імунної системи, орієнтованої на проактивний захист державних цифрових сервісів. Його застосування дає змогу структуровано визначити архітектурні контури ризику, виявити ключові вектори компрометації та сформувати основу для подальшого моделювання сценаріїв атак і вибору адаптивних механізмів захисту.

Список літератури

1. Adida B. Helios*: Web-based Open-Audit Voting. Proceedings of the 17th USENIX Security Symposium*. 2008. P. 335–348. URL: https://www.usenix.org/legacy/event/sec08/tech/full_papers/adida/adida.pdf

2. Kremer S., Ryan M., Smyth B. *Election Verifiability in Electronic Voting Protocols.* In: ESORICS 2010. Lecture Notes in Computer Science. Vol. 6345. Springer, 2010. P. 389–404. DOI: 10.1007/978-3-642-15497-3_24.

3. Heinl M. P., Haines T., Teague V. *Remote Electronic Voting in Uncontrolled Environments: A Survey of Failures and Threats*. ACM Computing Surveys. 2022. Vol. 55, No. 8. Article 167. DOI: 10.1145/3551386.

4. MITRE ATT&CK. *Enterprise Matrix*. MITRE Corporation. URL: https://attack.mitre.org/matrices/enterprise/

5. TovkunY., Personal data protection in context of cyberwarfare, *DIVA portal*. 2023. URL: https://www.diva-portal.org/smash/get/diva2:1773044/FULLTEXT02

6. Tovkun Y., Semerenska V., Adamov A. *An overview of cyber attacks on critical cyber-physical systems and government infrastructures*. Security and Safety. 2026. Vol. 5. Article 2026002. DOI: 10.1051/sands/2026002.

МЕХАНІЗМ САМОВІДНОВЛЕННЯ В СІТЧАСТІЙ АРХІТЕКТУРІ КІБЕРБЕЗПЕКИ КРИТИЧНИХ КІБЕРФІЗИЧНИХ СИСТЕМ

Семеренська В.В., Хаханова Г.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Критичні кіберфізичні системи відрізняються від звичайних інформаційних систем тим, що кібератака в них впливає не лише на дані чи цифрові сервіси, а й на фізичний процес керування. Наслідком інциденту можуть бути порушення телеметрії, деградація контурів керування, втрата синхронізації між вузлами, зупинка окремих функціональних модулів або перехід системи в небезпечний стан. Саме тому для таких систем недостатньо моделей захисту, орієнтованих лише на запобігання або детекцію атак. Після виявлення інциденту система повинна зберегти керованість, локалізувати

вплив компрометації та відновити мінімально необхідний рівень функціонування [4, 6]. Як архітектурну основу для розв'язання цієї задачі доцільно розглядати сітчасту архітектуру кібербезпеки. Її перевага для критичних кіберфізичних систем полягає в тому, що захист не концентрується в одному центральному вузлі, а розподіляється між окремими доменами, сегментами, сервісами та вузлами системи. У такій моделі рішення щодо безпеки можуть прийматися ближче до джерела події, а сама архітектура краще пристосована до роботи в середовищі з кількома довірчими межами, неоднорідними компонентами та частково ізольованими контурами [1]. Для критичної системи це означає, що компрометація одного сегмента не повинна автоматично призводити до втрати працездатності всієї системи.

У межах CSMA механізм самовідновлення доцільно розглядати не як зовнішній сервіс реагування, а як нативну властивість самої архітектури. Це принципове положення для критичних кіберфізичних систем. Якщо процес відновлення критично залежить від хмарної інфраструктури, зовнішнього центру координації або постійно доступного каналу зв'язку, то в умовах реальної атаки така залежність сама перетворюється на точку відмови. При порушенні мережевої зв'язності, перевантаженні каналів, затримках або цілеспрямованій атаці на зовнішній контур система може втратити не лише функції моніторингу, а й саму можливість відновлення. Тому для критичних CPS механізм self-healing має бути локальним, автономним і реалізованим у межах довіреного середовища системи [2, 3]. У такому підході самовідновлення включає не одну дію, а послідовність координованих етапів. Першим етапом є локальне виявлення аномалії або атаки на основі змін стану вузла, сервісу чи фізичного процесу. Другим етапом є оцінювання впливу інциденту, тобто визначення, чи зачіпає він допоміжну функцію, чи безпосередньо впливає на критичний контур керування. Третій етап полягає в локалізації ураженого сегмента шляхом ізоляції вузла, обмеження його взаємодії з іншими компонентами або переключення трафіку й командного обміну на довірений маршрут. Четвертим етапом є відновлення, яке може реалізовуватися у формі реконфігурації, переведення системи у деградований, але безпечний режим, активації резервної логіки або заміщення скомпрометованого компонента функціональним аналогом [2, 3]. У цьому контексті важливо, що метою самовідновлення не обов'язково є повне повернення системи до початкового стану в той самий момент. Для критичної кіберфізичної системи першочерговим є збереження критичних функцій, навіть якщо частина другорядних сервісів тимчасово відключається. Тобто механізм повинен забезпечувати не "ідеальне відновлення", а кероване збереження працездатності. Наприклад, система може тимчасово відмовитися від неосновних аналітичних або сервісних модулів, але зберегти базовий контур прийняття рішень, канал телеметрії, локальний контроль стану та можливість безпечного завершення операції. Саме така логіка краще відповідає природі критичних CPS, ніж класична модель централізованого after-incident recovery. У сітчастій архітектурі це означає, що рішення про ізоляцію, реконфігурацію та підтримання функціональності

приймаються розподілено. Окремі захисні компоненти архітектури мають не лише виявляти відхилення, а й обмінюватися між собою контекстом інциденту, щоб не допустити його каскадного поширення. Така координація є однією з ключових переваг CSMA, оскільки дозволяє поєднати локальну автономність із загальною узгодженістю захисної реакції [1]. У результаті архітектура підтримує логіку detect–assess–isolate–recover, причому етап recover не виноситься за межі системи, а закладається в її внутрішню організацію. З цієї точки зору самовідновлення слід розглядати як складову кіберстійкості, а не лише як окремий технічний механізм. Кіберстійка система повинна бути здатною витримувати порушення, зберігати ядро функціональності та адаптуватися до нових умов після інциденту [5]. Для критичних кіберфізичних систем це означає, що архітектура захисту має оцінювати не лише факт виявлення атаки, але й те, наскільки швидко система локалізувала збій, який рівень функціональності зберегла під час інциденту та чи змогла перейти в безпечний робочий режим без зовнішньої допомоги.

Саме тому ефективність механізму самовідновлення доцільно оцінювати не загальними деклараціями, а конкретними показниками. До них належать час відновлення, глибина втрати функціональності, мінімально збережений рівень працездатності після атаки, а також здатність системи виконувати критичні функції в режимі деградації [6]. Для критичної системи це значно важливіше, ніж проста наявність факту детекції. Якщо атака виявлена, але система втратила контроль над фізичним процесом, така детекція не вирішує основної задачі безпеки. Отже, у критичних кіберфізичних системах механізм самовідновлення має проєктуватися як нативний елемент сітчастої архітектури кібербезпеки. Його функція полягає не лише у відновленні після інциденту, а в забезпеченні безперервності критичних операцій за рахунок локального виявлення, ізоляції, реконфігурації та переходу до безпечного режиму функціонування. Саме поєднання розподіленої логіки CSMA з автономним self-healing створює практичну основу для побудови архітектур, які не просто фіксують атаку, а зберігають керованість і працездатність системи в умовах реального порушення.

Список літератури

1. Ramos-Cruz B., Andreu-Perez J., Martínez L. The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research. *Neurocomputing*. 2024. Vol. 581. 10.1016/j.neucom.2024.127427.

2. Johnphill O., Sadiq A. S., Al-Obeidat F., Al-Khateeb H., Taheir M. A., Kaiwartya O., Ali M. Self-Healing in Cyber-Physical Systems Using Machine Learning: A Critical Analysis of Theories and Tools. *Future Internet*. 2023. Vol. 15, No. 7. Art. 244. DOI: 10.3390/fi15070244.

3. Ratasich D., Höftberger O., Isakovic H., Shafique M., Grosu R. A Self-Healing Framework for Building Resilient Cyber-Physical Systems. In: *2017 IEEE 20th Int. Symposium on Real-Time Distributed Computing (ISORC)*. 2017. P. 133–140. DOI: 10.1109/ISORC.2017.7.

4. Tovkun Y., Semerenska V., Adamov A. *An overview of cyber attacks on critical cyber-physical systems and government infrastructures*. Security and Safety. 2026. Vol. 5. Article 2026002. DOI: 10.1051/sands/2026002.

5. Segovia-Ferreira M., Cavalli A. R., Garcia-Alfaro J. A Survey on Cyber-Resilience Approaches for Cyber-Physical Systems. *ACM Computing Surveys*. 2024. DOI: 10.1145/3652953.

6. Aghazadeh Ardebili A., Boscolo M., Longo A., Pourmadadkar M., Ficarella A., Padoano E. Resilience in Cyber-Physical Infrastructures: R-KPI prioritization, framework development, and case study insights. *Journal of Safety Science and Resilience*. 2025. Vol. 6, No. 3. Art. 100194. DOI: 10.1016/j.jnlssr.2024.12.005.

ДОСЛІДЖЕННЯ СУЧАСНИХ АРХІТЕКТУР В МОБІЛЬНІЙ РОЗРОБЦІ

Пашков Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

У контексті забезпечення безпеки функціонування комп'ютерних систем та мереж питання вибору архітектури програмного забезпечення і застосування дизайн-патернів набуває особливої важливості. Із зростанням складності інформаційних систем підвищуються вимоги не лише до їх продуктивності та масштабованості, але й до надійності, захищеності та передбачуваності поведінки в умовах потенційних загроз. У зв'язку з цим дослідження підходів до побудови безпечної програмної архітектури є актуальним завданням.

Метою доповіді є аналіз впливу архітектурних рішень і дизайн-патернів на рівень безпеки комп'ютерних систем та мереж, а також визначення підходів, що сприяють підвищенню захищеності, контрольованості та стійкості програмного забезпечення до потенційних загроз. В доповіді розглянуто значення класичних патернів проєктування, таких як Delegate, Observer та Singleton, у контексті забезпечення безпеки. Їх використання сприяє чіткому розмежуванню відповідальностей між компонентами системи, зменшенню зв'язності модулів та підвищенню контрольованості потоків даних, що є важливим для запобігання несанкціонованому доступу та витокам інформації. Окрему увагу приділено принципам SOLID як основі побудови надійних і захищених систем, де кожен компонент виконує чітко визначену функцію, що спрощує аудит та тестування безпеки. Проаналізовано архітектурні підходи з точки зору їх впливу на безпеку. Зокрема, класична архітектура MVC, незважаючи на свою простоту, у практичному застосуванні часто призводить до надмірної концентрації логіки в контролерах (так звані Massive View Controller), що ускладнює контроль за обробкою даних і підвищує ризики виникнення вразливостей. Це стимулювало розвиток альтернативних підходів, таких як MVP, VIPER та інші, які забезпечують кращу ізоляцію компонентів і, відповідно, вищий рівень контролю над безпекою.

Список літератури

1. Design Patterns: Elements of Reusable Object-Oriented Software / E. Gamma, R. Helm, R. Johnson, J. Vlissides. — Boston : Addison-Wesley, 1994. — 395 p.

2. Clean Architecture: A Craftsman's Guide to Software Structure and Design / R. C. Martin. — Boston : Prentice Hall, 2017. — 432 p.

ОПТИМІЗАЦІЯ МЕТОДІВ МАРШРУТИЗАЦІЇ В КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ ДЛЯ ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ ТА ПРОДУКТИВНОСТІ

Гордійко В.Р., Єрошенко О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Ефективна організація потоків даних у межах корпоративної комп'ютерної мережі є фундаментом стабільного функціонування сучасних бізнес-процесів, що вимагають високої швидкості доступу до сервісів та надійності каналів зв’язку.

Маршрутизація як процес вибору оптимального шляху передачі пакетів між сегментами мережі стає складним завданням через багаторівневу ієрархічну структуру корпоративних систем, наявність віддалених філій та інтеграцію хмарних технологій [1, 2].

Метою дослідження є аналіз та розробка підходів до вибору методів маршрутизації, які здатні динамічно адаптуватися до змін топології та навантаження, забезпечуючи при цьому мінімальні затримки та раціональне використання мережевих ресурсів.

Розглянуто особливості функціонування протоколів стану каналів, зокрема OSPF, що базується на алгоритмі Дейкстри для побудови найкоротшого шляху, та їх переваги перед дистанційно-векторними протоколами в умовах великих мереж.

Математичний апарат проєктування таких систем включає розрахунок метрик, що базуються на пропускній здатності, затримках та надійності інтерфейсів, що дозволяє формувати таблиці маршрутизації з урахуванням пріоритетності критично важливих бізнес-додатків та трафіку реального часу.

Алгоритми інтелектуального вибору шляху дозволяють не лише оптимізувати трафік, а й захистити внутрішню інфраструктуру від атак типу «відмова в обслуговуванні» та несанкціонованого перехоплення даних.

Результати роботи підтверджують, що вибір методу маршрутизації має безпосередній вплив на масштабованість корпоративної мережі та її здатність підтримувати зростаючі обсяги мультимедійного та корпоративного трафіку.

Список літератури

1. Єрошенко О. А., Піняєв Є. В., Пивоварова Д. І., Кравченко П. О. Метод оптимізації publish-subscribe архітектур для інтелектуального інформування в умовах обмежених ресурсів IoT, *Системи управління, навігації та зв’язку. Збірник наукових праць*, Т. 1. № 83. 2026. С. 69-76. DOI: 10.26906/SUNZ.2026.1.069

2. Fedorchenko V., Yeroshenko O., Shmatko O., Kolomiitsev O., Omarov M. Password hashing methods and algorithms on the .Net platform. *Advanced Information Systems*. №8(4). 2024. Pp. 82–92. DOI: 10.20998/2522-9052.2024.4.11

АНАЛІЗ ВІДМОВОСТІЙКОСТІ СИСТЕМ ПОТОКОВОЇ ОБРОБКИ ДАНИХ НА ОСНОВІ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ

Тухтаров В.Б., Міхаль О.П.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасний стан розвитку інформаційних технологій характеризується стрімким зростанням обсягів даних, що генеруються в режимі реального часу, зокрема від пристроїв GPS, сенсорних мереж та Інтернету речей. Ефективна обробка таких потокових даних потребує розподілених систем з високим рівнем відмовостійкості. Мікросервісна архітектура пропонує гнучкість та незалежність компонентів, проте її здатність забезпечувати стійкість до збоїв у великомасштабних потокових обчисленнях потребує ґрунтовного дослідження. Паралельно, платформа Apache Flink надає вбудовані механізми для забезпечення відмовостійкості через контрольні точки та узгоджені знімки стану [1]. Виникає науково-практичне завдання порівняльного аналізу цих двох підходів в контексті забезпечення надійності обробки потокових даних. Крім того, сучасні тенденції до децентралізації обчислень та впровадження технологій периферійних обчислень висувають додаткові вимоги до забезпечення надійності в умовах нестабільних мережевих з'єднань та гетерогенного апаратного забезпечення. Відсутність систематизованих підходів до оцінки відмовостійкості мікросервісних рішень у порівнянні з класичними платформами потокової обробки ускладнює вибір оптимальної архітектури для критичних застосунків, що й зумовлює необхідність проведення дослідження.

Метою доповіді є представлення результатів порівняльного дослідження відмовостійкості двох типів систем: системи, побудованої на мікросервісній архітектурі з використанням мови Python, та системи на основі платформи Apache Flink, з акцентом на їхню продуктивність та здатність до відновлення після збоїв в умовах високого навантаження. В рамках роботи було розроблено два експериментальних стенди, що імітують обробку потокових даних від GPS-пристроїв у реальному часі. Перший стенд реалізовано з використанням мікросервісної архітектури на Python, де кожен мікросервіс відповідав за окремий етап обробки даних: фільтрацію, збагачення, матчинг та агрегацію. Для забезпечення базової відмовостійкості застосовано патерни повторних спроб та тайм-аутів [2]. Другий стенд реалізовано на платформі Apache Flink з використанням її вбудованого механізму відмовостійкості через періодичне створення узгоджених контрольних точок стану. Експерименти проводилися при різних рівнях навантаження (від 10^4 до 10^7 подій на секунду) з імітацією відмов окремих вузлів обчислювального кластера. Основними метриками оцінки були: пропускна здатність системи, середня затримка обробки та час відновлення після збою.

Експериментальні дослідження показали, що Apache Flink демонструє кращу стабільність та масштабованість при високих навантаженнях. Механізм асинхронних контрольних точок у Flink дозволяє досягти гарантії обробки "рівно один раз" (exactly-once) без суттєвого впливу на продуктивність. Час

відновлення системи після збою на платформі Flink виявився передбачуваним та лінійно залежав від обсягу стану операторів [3]. Натомість, мікросервісна реалізація на Python продемонструвала більшу гнучкість та простоту впровадження в менш вимогливих середовищах. Однак при масштабуванні понад 50 мікросервісів виникли проблеми з управлінням станом та координацією відновлення після збоїв. Час відновлення в такій системі зростав непередбачувано через необхідність повторної обробки накопичених даних. Крім того, у мікросервісній реалізації спостерігався ефект "каскадного поширення" збоїв, коли відмова одного мікросервісу призводила до ланцюжкової реакції через мережеві тайм-аути, що потребувало впровадження додаткових патернів стійкості, таких як "автоматичний вимикач" та "перегородка". Проведене порівняльне дослідження дозволяє стверджувати, що вибір архітектури для побудови відмовостійких систем потокової обробки даних має визначатись специфічними вимогами до продуктивності та складністю середовища експлуатації. Для високонавантажених систем з жорсткими вимогами до часу відновлення та консистентності даних більш доцільним є використання спеціалізованих платформ, таких як Apache Flink, з їхніми вбудованими механізмами відмовостійкості. Для систем з помірним навантаженням та високими вимогами до гнучкості розробки мікросервісна архітектура на Python залишається привабливою альтернативою, за умови ретельного проєктування механізмів стійкості на рівні архітектурних патернів. Результати роботи можуть бути використані як практичні рекомендації при проєктуванні систем обробки потокових даних в задачах моніторингу транспортних потоків та інших сферах, що використовують GPS-трекінг.

Список літератури

1. Apache Flink Documentation: Data Streaming Fault Tolerance. – Apache Software Foundation. – URL: https://nightlies.apache.org/flink/ /

2. Beereddy, K. R. Self-Healing Streaming Architecture: Resilience Patterns for Event-Driven Microservices. *Journal of Computing and Scientific Technological Studies*. 2025. Vol. 7, no. 8. DOI: https://doi.org/10.32996/jcsts.2025.7.8.30

3. Fragkoulis, M., Carbone, P., Kalavri, V. et al. A survey on the evolution of stream processing systems. *The VLDB Journal*. 2024. Vol. 33, p. 507–541. DOI: https://doi.org/10.1007/s00778-023-00819-8.

МЕТОД ВИЯВЛЕННЯ АНОМАЛІЙ ДЛЯ МЕРЕЖ ІОТ

Сгібнєв В.І., Бабич К.Ф.
Харківський національний університет радіоелектроніки, Харків, Україна

Динамічні процеси в мережах Інтернету речей (IoT) суттєво впливають на якість передачі даних, затримки, пропускну здатність та загальну надійність функціонування розподілених кіберфізичних систем. Велика кількість гетерогенних пристроїв, обмежені обчислювальні ресурси, енергетичні обмеження та використання різнорідних протоколів обміну даними формують

складне середовище функціонування мереж. Це, у свою чергу, ускладнює забезпечення стабільності мережевих з'єднань і підвищує вразливість до аномальних станів та кіберзагроз. У зв'язку з цим дослідження методів виявлення аномалій у мережах IoT є важливою науково-практичною задачею [1]. Із завданнями підвищення ефективності та безпеки IoT-мереж пов'язана необхідність розробки нових підходів до аналізу потоків даних, що генеруються великою кількістю пристроїв у режимі реального часу. Такі дані характеризуються високою варіативністю, нестаціонарністю, наявністю шумів і складною часовою структурою. Зокрема, застосування автоенкодерів, рекурентних нейронних мереж та алгоритмів кластеризації дозволяє виявляти приховані закономірності та ідентифікувати аномальні відхилення у поведінці мережевих вузлів [2].

Метою доповіді є розробка методу виявлення аномалій у мережах IoT, який базується на комбінованому використанні статистичних характеристик трафіку та моделей глибинного навчання. Метод передбачає попередню обробку даних, виділення інформативних ознак (інтенсивність трафіку, затримки, варіації пакетів), формування навчальної вибірки та побудову моделі нормальної поведінки мережі. Виявлення аномалій здійснюється шляхом оцінки відхилення поточних параметрів від сформованого еталонного стану. У доповіді наведено результати аналізу реального та змодельованого трафіку IoT-мереж, які демонструють, що на локальні флуктуації інтенсивності трафіку впливають типи пристроїв, протоколи передачі (MQTT, CoAP), мережева топологія, щільність вузлів та рівень навантаження. Дослідження показують, що поведінка мережі має виражений нестаціонарний характер, що проявляється у змінності статистичних характеристик у часі та появі короткочасних аномальних відхилень [3]. Запропонований метод дозволяє ефективно виявляти такі аномалії, як перевантаження вузлів, відмови пристроїв, а також аномалії, пов'язані з кіберзагрозами (наприклад, DDoS-атаки або несанкціонований доступ). Порівняльний аналіз показує, що використання комбінованого підходу забезпечує підвищення точності виявлення аномалій та зниження кількості хибних спрацьовувань у порівнянні з класичними методами. Таким чином, запропонований метод може бути використаний для побудови інтелектуальних систем моніторингу та забезпечення кібербезпеки IoT-мереж у реальному масштабі часу.

Список літератури

1. Ahmed, Mohiuddin, Abdun Naser Mahmood, and Jiankun Hu. "A survey of network anomaly detection techniques." Journal of network and computer applications 60 (2016): 19-31. DOI: https://doi.org/10.1016/j.jnca.2015.11.016

2. Sahu, Nilesh Kumar, and Indrajit Mukherjee. "Machine learning based anomaly detection for IoT network:(Anomaly detection in IoT network)." 2020 4th ICOEI (48184). IEEE, 2020. DOI: https://doi.org/10.1109/ICOEI48184.2020.9142921

3. Мартовицький, ВО, et al. "Дослідження методів виявлення аномалій у арі журналах для забезпечення безпеки та надійності програмних систем." Вісник ХНТУ 2.1 (92) (2025): 142-148. DOI: https://doi.org/10.35546/kntu2078-4481.2025.1.2.19

АВТЕНТИФІКАЦІЯ КОРИСТУВАЧА НА ПЕРИФЕРІЙНОМУ РІВНІ В РОЗПОДІЛЬНИХ КІБЕР-ФІЗИЧНИХ СИСТЕМАХ

Радченко І.А., Міхаль О.П.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні розподілені кібер-фізичні системи (КФС) поєднують обчислювальні компоненти з фізичними процесами, забезпечуючи моніторинг і керування об'єктами критичної інфраструктури [1]. Розвиток IIoT і віддаленого доступу значно розширив поверхню атаки, зробивши системи вразливими до несанкціонованого втручання.

Однією з найсерйозніших загроз є слабка автентифікація користувачів при виконанні критичних команд (зміна уставок, аварійне вимкнення, активація обладнання).

Традиційні методи захисту вже недостатньо надійні [2, 3].

Метою доповіді є представлення розробленого механізму багатофакторної автентифікації на периферійному рівні з використанням Time-based One-Time Password (TOTP), який дозволяє значно підвищити безпеку критичних операцій у розподілених кібер-фізичних системах.

Запропонована архітектура розміщує механізм багатофакторної автентифікації безпосередньо на периферійному рівні у вигляді програмного middleware на IoT-шлюзі.

Це дозволяє виконувати перевірку автентичності користувача локально, перед передачею будь-яких критичних команд на виконавчі пристрої кібер-фізичних систем, і мінімізує залежність від централізованої хмарної інфраструктури.

Основні компоненти архітектури:

- Edge IoT-шлюз – основний елемент, що діє як маршрутизатор і ізолює внутрішню мережу управління від зовнішнього доступу. Зв'язок із хмарою відбувається через захищений канал, а внутрішній зв'язок з КФС – через дротові з'єднання;

- Edge-платформа – Node-RED як легковаговий flow-based рушій, що дозволяє візуально проектувати потоки даних і логіку безпеки без складного кодування;

- протоколи інтеграції – повна підтримка MQTT/MQTT, Modbus та BACnet. У разі відсутності підтримки MQTT шлюз може безпосередньо записувати команди через Modbus Write або BACnet-вузли;

- механізм TOTP – другий фактор аутентифікації. Використовується алгоритм SHA256, 6-значний код, період дії 30 секунд. Секретний ключ задається через payload.

Така архітектура є мультипротокольною, малозалежною від апаратного забезпечення і легко інтегрується як у нові, так і в існуючі КФС без суттєвої модернізації обладнання.

Ефективність запропонованої системи Edge MFA була перевірена на реальному апаратному стенді, зібраному на базі Raspberry Pi 3 Model B з встановленим Node-RED та MQTT-брокером Mosquitto. Тестування проводилося в умовах, максимально наближених до реального промислового середовища, шляхом імітації надсилання критичних команд з хмарної платформи на периферійний шлюз з подальшою необхідністю підтвердження через TOTP.

У ході експериментів моделювалися типові сценарії виконання критичних операцій у кібер-фізичних системах. Кожна команда проходила повний цикл: надходження на Edge-шлюз, генерація одноразового пароля, надсилання його користувачеві через SMS, введення коду назад у систему та остаточне прийняття або відхилення команди.

Особлива увага приділялася перевірці стійкості механізму до типових атак, таких як:

повторне використання коду,

введення прострочених паролів,

спроби несанкціонованого доступу,

перевищення допустимого часу очікування.

Результати експериментів продемонстрували високу надійність запропонованого рішення. Система коректно розпізнавала правильні коди та дозволяла виконання команди лише у разі успішної автентифікації.

Проведене тестування також підтвердило стабільність роботи рішення під тривалим навантаженням.

Навіть при інтенсивному потоці команд система зберігала стабільну продуктивність без втрати продуктивності та збоїв. Локальна обробка TOTP безпосередньо на периферійному рівні дозволила суттєво знизити залежність від постійного з'єднання з хмарою, що підвищує відмовостійкість усієї системи в разі тимчасової втрати інтернет-з'єднання.

Отримані експериментальні дані свідчать про те, що запропонований механізм Edge MFA забезпечує значне підвищення рівня безпеки критичних операцій при збереженні прийнятної затримки та мінімальних апаратних вимог. Рішення демонструє добру масштабованість і може бути ефективно інтегроване як у нові, так і в уже розгорнуті кібер-фізичні системи.

Список літератури

1. Kotzanikolaou P. et al. An Edge Multi Factor Authentication System for Cyber Physical Systems Based on OTP // IEEE Symposium on Computers and Communications (ISCC). 2024.

2. Alcaraz C., Zeadally S. Critical infrastructure protection: Requirements and challenges for the 21st century // International Journal of Critical Infrastructure Protection. 2015. Vol. 8. P. 53–66.

3. Sadeghi A.-R., Wachsmann C., Waidner M. Security and privacy challenges in industrial Internet of Things // Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference (DAC). 2015.

АВТОНОМНА СИСТЕМА КЕРУВАННЯ ДРОНАМИ ДЛЯ НАВІГАЦІЇ У ПРИМІЩЕННЯХ

Кліменко А.В., Литвиненко Г.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Динамічні процеси навігації безпілотних літальних апаратів (БПЛА) у закритих приміщеннях характеризуються високим рівнем невизначеності, обмеженою доступністю сигналів глобальних навігаційних систем та складною геометрією середовища. У таких умовах традиційні методи позиціонування, засновані на використанні GPS, є неефективними або недоступними. Це обумовлює необхідність розробки автономних систем керування дронами, здатних забезпечувати точну навігацію, уникнення перешкод і стабільність польоту в умовах обмеженого простору [1]. Із завданнями підвищення ефективності автономної навігації пов'язана необхідність інтеграції різнорідних сенсорних даних, таких як дані камер, лідарів, інерціальних вимірювальних блоків (IMU) та ультразвукових датчиків. Обробка цих даних у режимі реального часу дозволяє формувати карту середовища та визначати положення дрона відносно перешкод. Для цього широко використовуються методи одночасної локалізації та побудови карти (SLAM), а також алгоритми комп'ютерного зору та глибинного навчання [2].

Метою доповіді є розробка автономної системи керування дроном для навігації у приміщеннях на основі поєднання методів сенсорного злиття, алгоритмів SLAM та інтелектуальних методів прийняття рішень. Запропонований підхід передбачає використання візуально-інерціальної одометрії для оцінки положення, побудову карти середовища та планування траєкторії руху з урахуванням перешкод. У доповіді наведено результати експериментальних досліджень, які показують, що використання комбінованого підходу дозволяє досягти високої точності позиціонування та стабільності польоту навіть у складних умовах. Зокрема, встановлено, що інтеграція даних з різних сенсорів дозволяє зменшити накопичення похибок та підвищити надійність навігації. Крім того, застосування алгоритмів планування траєкторії забезпечує ефективне уникнення перешкод у режимі реального часу [3]. Особливістю запропонованої системи є її адаптивність до змін умов середовища, що досягається за рахунок використання методів машинного навчання для корекції параметрів керування. Це дозволяє підвищити ефективність роботи системи у різних типах приміщень, включаючи складські, виробничі та офісні середовища. Таким чином, розроблена автономна система керування дроном забезпечує ефективну навігацію у приміщеннях без використання GPS та може бути використана для вирішення широкого кола прикладних задач, зокрема інспекції, моніторингу та логістики.

Список літератури

1. Cadena, Cesar, et al. "Past, present, and future of simultaneous localization and mapping: Toward the robust-perception age." IEEE Trans. on robotics 32.6 (2017): 1309-1332.

2. Scaramuzza, Davide, and Zichao Zhang. "Visual-inertial odometry of aerial robots." arXiv preprint arXiv:1906.03289 (2019).

3. Qin, Tong, Peiliang Li, and Shaojie Shen. "Vins-mono: A robust and versatile monocular visual-inertial state estimator." IEEE transactions on robotics 34.4 (2018): 1004-1020.

ГІБРИДНА МОДЕЛЬ МОНІТОРИНГУ СТАНУ ПРОМИСЛОВОГО ОБЛАДНАННЯ НА ОСНОВІ БАЙЄСІВСЬКОЇ МЕРЕЖІ ТА АНСАМБЛЕВОГО МЕТОДУ XGBOOST

Зібаров О.В., Знайдюк В.Г.
Харківський національний університет радіоелектроніки, Харків, Україна
Ляшенко С.О.
Державний біотехнологічний університет, Харків, Україна

Сучасна парадигма Індустрії 4.0 передбачає перехід від традиційних стратегій реактивного та планово-попереджувального обслуговування до систем прогнозного обслуговування, заснованих на інтелектуальному аналізі даних моніторингу стану [1]. Незважаючи на високу точність методів глибокого навчання (ГН) у задачах виявлення аномалій та прогнозування залишкового ресурсу, їх широке впровадження у виробничі процеси стримується проблемою «чорної скриньки» – відсутністю прозорої інтерпретації прийнятих моделлю рішень [2]. У контексті експлуатації складних технічних об'єктів, зокрема високошвидкісного текстильного обладнання, виникає об'єктивна потреба в архітектурах, здатних забезпечити компроміс між дискримінаційною здатністю та інтерпретованістю прогнозів, що є критичним для довіри оперативного персоналу та відповідності стандартам управління активами [3].

Метою доповіді є розробка та верифікації гібридної моделі прогнозування несправностей, яка поєднує структурне навчання байєсівської мережі (БМ) із градієнтним бустингом XGBoost, орієнтованої на підвищення надійності та моніторингу стану технологічного обладнання в умовах реального виробництва.

Об'єктом дослідження виступила багатоголкова квілтингова машина, що експлуатується в безперервному циклі та схильна до поступової деградації механічних вузлів. Для реєстрації фізичних параметрів було розгорнуто периферійну платформу збору даних на базі архітектури ESP-32 та хмарної інфраструктури [4]. Мультимодальний потік даних включав показники тривимірної вібрації, температури, електричного струму та концентрації твердих частинок. Протягом трьох місяців експлуатації було акумульовано понад 220000 синхронізованих записів, що зберігаються в часовій базі даних InfluxDB.

Важливим етапом підготовки даних стало формування цільової змінної – міток стану деградації. На противагу використанню виключно порогових

значень, у роботі застосовано підхід до семантичного маркування на основі кореляції часових рядів із записами комп'ютеризованої системи управління технічним обслуговуванням. Відповідно до часової близькості до задокументованих відмов, кожному вимірюванню присвоювався один із трьох класів: «Справний» (нормальна робота), «Середня деградація» (24-годинний інтервал до незначної несправності) та «Висока деградація» (безпосереднє передування критичній відмові). Для підвищення достовірності розмітки виконано верифікацію з операторами змін та застосовано гібридні методи імпутації пропущених значень. Запропонована гібридна архітектура прогнозування ґрунтується на синергії двох математичних апаратів.

Структура БМ не задавалася експертами апріорно, а була вивчена автоматично з емпіричних даних за допомогою алгоритму пошуку сходженням до вершини, оптимізованого за байєсівським інформаційним критерієм. Це дозволило ідентифікувати стійкі причинно-наслідкові зв'язки між латентними ознаками вібрації, тепловим навантаженням та електричними флуктуаціями, забезпечивши прозору ймовірнісну логіку діагностики першопричин. Для підвищення точності класифікації в умовах зашумлених даних та нелінійних залежностей застосовано ансамблевий метод градієнтного бустингу. На вхід моделі подавалися статистичні характеристики сигналів, вилучені після попередньої низькочастотної фільтрації.

Експериментальна валідація на тестовій вибірці підтвердила комплементарність підходів. Модель XGBoost продемонструвала високу предикативну ефективність, досягнувши F1-оцінки 0,967 при класифікації стану «Висока деградація», що перевершує результати ізольованої БМ за показниками чутливості до передвідмовних станів. Водночас байєсівська мережа забезпечила можливість візуалізації ймовірностей та аналізу шляхів поширення впливу, що надає інженеру з технічного обслуговування обґрунтовані докази для прийняття рішення про зупинку обладнання або позачергову інспекцію. Інтеграція обох моделей у єдиний конвеєр даних SmartFlow дозволяє не лише з високою достовірністю детектувати ранні ознаки механічних дисбалансів або критичного зносу, але й відповідати принципам пояснюваного штучного інтелекту, що регламентуються сучасними вимогами до кіберфізичних систем.

Список літератури

1. Mobley R. K. An Introduction to Predictive Maintenance. 2nd ed. Amsterdam: Elsevier, 2002. 438 p.

2. Barredo Arrieta A. et al. Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges // Information Fusion. 2020. Vol. 58. P. 82-115.

3. Van Horenbeek A., Pintelon L. Development of a maintenance performance measurement framework // International Journal of Production Economics. 2014. Vol. 153. P. 324-337.

4. Poursabzi-Sangdeh F. et al. Manipulating and measuring model interpretability // Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. 2021. P. 1–18.

АРХІТЕКТУРА ТРАСФОРМЕРА ДЛЯ БЕЗПЕРЕРВНОЇ АВТЕНТИФІКАЦІЯ НА ОСНОВІ ДИНАМІКИ КЛАВІАТУРНОГО НАБОРУ

Довгаль В.С., Ляшенко О.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Механізми статичної авторизації забезпечують перевірку автентичності лише в один конкретний момент часу. Однак після відкриття сеансу пристрої, залишені без нагляду, стають вразливими до захоплення сеансу, перехоплення даних або повторного використання облікових даних. Для вирішення цієї проблеми використовується безперервна авторизація, яка в режимі реального часу базується на аналізі поведінкової біометрії користувача [2]. Серед неінвазивних підходів виділяється метод динаміки натискань клавіш - це аналіз часу між натисканнями клавіш, послідовностей натискань та загального ритму, який є апаратно-незалежним, конфіденційним і підходить як для настільних, так і для мобільних пристроїв.

Метою доповіді є розробка архітектури на основі трасформера, яка інтегрує попередньо навчені мовні моделі для роботи зі символами, доповнені інформацією про час натискання клавіш. Модель обробляє послідовності натискань клавіш у вільнотекстових сценаріях, дозволяючи проводити двійкову класифікацію: справжній користувач проти самозванця. Навчання включало використання як відкритих баз даних із натисканнями клавіш, так і даних зібраних протягом тривалого часу на основі вільного тексту. Було протестовано чотири варіанти реалізації: обробка на серверній стороні, обробка на стороні клієнта, двоетапна автентифікація та персоналізований підхід на стороні клієнта, коли модель спочатку тренується на сервері, а потім довчається безпосередньо на пристрої користувача.

Архітектура трасформера для безперервної автентифікація на основі динаміки клавіатурного набору поєднує послідовності символів з інформацією про час натискання клавіш. Для мінімізації ризику витоку чутливих даних про натискання клавіш впроваджено гібридну клієнт-серверну архітектуру. Часовий кодер проходить попереднє навчання на централізованих даних самозванців, тоді як дані справжнього користувача зберігаються виключно на пристрої для цілей персоналізації двійкового класифікатора [2]. Таким чином, необроблені послідовності натискань клавіш не передаються через мережу, зберігаючи безпосередній доступ до переваг масштабного попереднього навчання без шкоди для приватності користувача.

Експерименти показали, що модель надійно розпізнає самозванців, яких ніколи не бачила під час навчання. Крім того, модель, тренована на послідовностях завдовжки 384 символи, демонструють прийнятний рівень EER навіть під час оцінки на значно коротших фрагментах (до ≈100 символів) [3]. Це свідчить про потенціал для впровадження безперервної автентифікації в реальному часі з мінімальною затримкою, забезпечуючи оптимальний баланс між безпекою та зручністю використання.

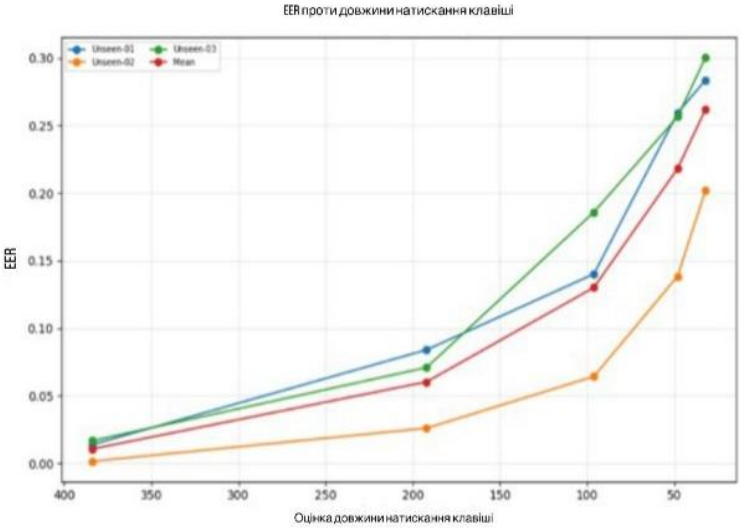


Рис. 1. Рівний коефіцієнт помилок як функція довжини натискання клавіші для моделей, навчених на послідовностях із 384 символів.

Використання синтетичних зразків натискань клавіш, створених шляхом контрольованої модифікації часових розподілів, суттєво покращує продуктивність системи порівняно з результатами, які базуються на невеликій вибірці даних [1]. Такий підхід допомагає зменшити потребу в об'ємному зборі даних під час реєстрації, при цьому зберігаючи важливі часові характеристики, які є критичними для ідентифікації користувачів.

Водночас виявлено суттєве обмеження моделі за умов зміни мови або контексту вводу навіть у межах однієї мови, що є ключовим бар'єром для практичного застосування в багатомовних середовищах.

Таким чином, запропонований підхід до динаміки клавіатурного набору демонструє високу точність, стійкість до обробки коротких послідовностей і ефективне забезпечення конфіденційності завдяки персоналізації на стороні клієнта. Основним напрямком подальших досліджень залишається покращення саме міжмовних та міжконтекстних узагальнень.

Список літератури

1. Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2017, October). A Survey on Homomorphic Encryption Schemes: Theory and Implementation. https://doi.org/10.48550/arXiv.1704.03578

2. Alsultan, A., Warwick, K., & Wei, H. (2018). Improving the performance of free-text keystroke dynamics authentication by fusion. Applied Soft Computing, 70, 1024–1033. https://doi.org/10.1016/j.asoc.2017.11.018

3. Ayeswarya, S., & Singh, K. J. (2024). A Comprehensive Review on Secure Biometric-Based Continuous Authentication and User Profiling. IEEE Access, 12, 82996–83021. https ://doi.org/10.1109/ACCESS .2024.3411783

ФЕДЕРАТИВНЕ НАВЧАННЯ В УМОВАХ ГЕТЕРОГЕННОСТІ ПРИСТРОЇВ

Башилов В.С., Ляшенко О.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Федеративне навчання (ФН) є частиною розподіленого машинного навчання, що забезпечує конфіденційність даних за рахунок децентралізованого тренування моделей без передачі локальних даних на центральний сервер.

Ця властивість робить ФН особливо привабливим для систем граничного інтелекту, де велика кількість різноманітних пристроїв генерує дані, чутливі до витоку або централізованої обробки.

Проте практичне впровадження ФН у реальних граничних середовищах стикається з низкою суттєвих перешкод, серед яких найбільш критичними є статистична гетерогенність (non-IID розподіли даних між клієнтами), апаратна гетерогенність (суттєві відмінності в обчислювальних ресурсах пристроїв) та наявність зашумлених або некоректних міток у навчальних даних.

Ці фактори призводять до дрейфу локальних моделей, сповільнення збіжності глобальної моделі, збільшення комунікаційних витрат та загального зниження точності [1, 2].

Сучасні дослідження у галузі ФН виокремлюють три ключові виклики, що потребують комплексного вирішення.

По-перше, проблема non-IID даних виникає, коли локальні набори даних на різних клієнтах мають суттєво різні статистичні розподіли. Це спричиняє неузгодженість напрямків оновлення локальних моделей та перешкоджає формуванню узагальненої глобальної моделі [3].

По-друге, гетерогенність пристроїв, що проявляється у значних відмінностях обчислювальної потужності, обсягу пам'яті, енергоспоживання та пропускної здатності каналів зв'язку, унеможливлює використання єдиної архітектури моделі для всіх учасників навчання. Це ускладнює агрегацію параметрів та створює ризик відставання «повільних» клієнтів [4].

По-третє, у реальних сценаріях граничних обчислень мітки даних часто є неточними або зашумленими внаслідок помилок анотування, збоїв сенсорів чи людського фактору. Навчання на таких даних призводить до перенавчання моделі та погіршення її узагальнювальної здатності [5].

Метою доповіді є аналіз сучасних методів удосконалення федеративного навчання, спрямованих на подолання проблем гетерогенності пристроїв, non-IID даних та зашумлених міток у контексті систем граничного інтелекту, а також окреслення перспективних напрямів подальших досліджень у цій галузі.

Для вирішення проблеми не-IID даних запропоновано метод кластеризації клієнтів на основі подібності їхніх моделей. Підхід FLIS (Federated Learning by Inference Similarity) передбачає динамічне групування клієнтів за ознакою подібності векторів виведення, що дозволяє формувати кластери зі статистично узгодженими розподілами даних. Експериментально

підтверджено, що така кластеризація дозволяє підвищити точність персоналізованих моделей до 40% порівняно з існуючими методами, зберігаючи при цьому конфіденційність локальних даних. Додатково розроблено стандартизований застосунок оцінювання для non-IID ФН, що включає структуровані метрики, уніфікований дизайн експериментів та практичні рекомендації щодо оптимізації навчання в умовах статистичної гетерогенності.

Для мінімізації впливу некоректних міток у навчальних даних запропоновано метод відсікання клієнтів федеративного навчання (ВКФН), що ідентифікує та виключає «зашумлених» клієнтів на основі їхньої продуктивності на чистому валідаційному наборі даних. Метод використовує показник кандидатності на шум та складається з трьох фаз: попереднє оцінювання клієнтів для виявлення потенційно зашумлених, виключення клієнтів із найвищим показник та фінальне додаткове налаштування глобальної моделі на «чистих» клієнтах. Емпіричні дослідження свідчать, що ВКФН забезпечує точність виявлення зашумлених клієнтів понад 80% та дозволяє скоротити комунікаційні витрати на 17% порівняно з існуючими стійкими до шуму ФН-методами.

Проведений аналіз демонструє, що комплексне вирішення проблем гетерогенності даних, апаратної різнорідності пристроїв та зашумлених міток є критично важливим для ефективного впровадження федеративного навчання в системах граничного інтелекту.

Розглянуті методи забезпечують суттєве покращення точності моделей, зменшення комунікаційних витрат та підвищення робастності ФН-систем у реальних умовах експлуатації.

Список літератури

1. Jimenez G. D.M., Anagnostopoulos A., Chatzopoulos D., et al. Non-IID data in Federated Learning: A Survey with Taxonomy, Metrics, Methods, Frameworks and Future Directions. arXiv preprint arXiv:2411.12377, 2024. https://doi.org/10.48550/arXiv.2411.12377

2. Pfeiffer K., Rapp M., Khalili R., Henkel J. Federated Learning for Computationally Constrained Heterogeneous Devices: A Survey. ACM Computing Surveys, 2023, Vol. 55, No. 14s, Article 334. https://doi.org/10.1145/3596907

3. Ye M., Fang X., Du B., Yuen P.C., Tao D. Heterogeneous Federated Learning: State-of-the-art and Research Challenges. ACM Computing Surveys, 2023, Vol. 56, No. 3, Article 79. https://doi.org/10.1145/3625558

4. Al-Quraan M., Mohjazi L., Bariah L., Centeno A., Zoha A., Muhaidat S., Debbah M., Imran M.A. Edge-Native Intelligence for 6G Communications Driven by Federated Learning: A Survey of Trends and Challenges. arXiv preprint arXiv:2111.07392, 2023.

5. Li Y., Wang Z., Zhang Y. Federated learning with noisy labels: A comprehensive and concise review of current methodologies and future directions. Neural Networks, 2026, Vol. 201, Article 108889. https://doi.org/10.1016/j.neunet.2026.108889

МЕТОД ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ У СИСТЕМНОМУ ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ НА ОСНОВІ АДАПТИВНОЇ МОБІЛЬНОСТІ КОДУ

Амосов Д.О., Знайдюк В.Г., Ляшенко Г.Є.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасний розвиток високопродуктивних обчислень, штучного інтелекту та edge-систем характеризується масовим переходом до гетерогенних many-core архітектур [1]. Такі платформи поєднують десятки або сотні CPU-ядер з GPU-акселераторами, тензорними ядрами та RISC-V прискорювачами. Однак зростання обчислювальної потужності супроводжується глибокими проблемами на рівні системного програмного забезпечення. Традиційні моделі паралелізму та runtime-системи базуються на підході переміщення даних, що в умовах many-core призводить до катастрофічного зростання комунікаційних накладних витрат, ефекту «memory wall» та нелінійного збільшення енергоспоживання. Додатковим критичним недоліком є семантичні прогалини в I/O-стеку [2]: велика кількість інформації про колективний доступ, шаблони даних, залежності та життєвий цикл втрачається при переході від прикладного рівня до ядра операційної системи та апаратного забезпечення, що унеможливлює глибокі оптимізації.

Метою доповіді є представлення нового методу Adaptive Code-Mobility Runtime System (ACMRS) для організації паралельних обчислень у системному програмному забезпеченні гетерогенних many-core архітектур, який комплексно вирішує проблеми надмірного переміщення даних, адаптивності до динамічного навантаження та семантичної цілісності I/O.

Запропонований метод ACMRS базується на трьох ключових компонентах. Перший – динамічна мобільність коду, яка замінює переміщення великих обсягів даних на міграцію компактних обчислювальних ядер. Розмір коду зазвичай на кілька порядків менший за обсяг даних, що дозволяє суттєво знизити трафік між'ядерних з'єднань, покращити просторову та часову локальність обчислень і зменшити енергоспоживання. Для кожної задачі обчислюється коефіцієнт вигоди міграції коду, який враховує розмір даних, вартість комунікації, розмір коду, вартість міграції та коефіцієнт енергоефективності цільового домену. Міграція виконується, якщо цей коефіцієнт перевищує адаптивний поріг. Другий компонент – ієрархічний адаптивний шедулінг з елементами машинного навчання [3]. Система організована у три рівні: глобальний, локальний та ядерний. Ймовірність крадіжки задачі між кластерами визначається адаптивно на основі поточного навантаження, а саме навантаження прогнозується легкою нейронною мережею (LSTM або Gradient Boosting), яка на вхід отримує телеметрію апаратного забезпечення, довжину черги задач та історію продуктивності. Такий підхід дозволяє динамічно перерозподіляти ресурси з урахуванням гетерогенності та енергетичного стану системи. Третій компонент – семантично-усвідомлений I/O-bridging, який усуває семантичні прогалини в стеку введення-виведення. Кожна I/O-операція подається у вигляді

розширеного кортежу: тип операції, шаблон доступу, семантика доступу, залежності від інших задач, очікуваний життєвий цикл даних та додаткові підказки. Ця інформація зберігається в Semantic Context Token (SCT), який супроводжує задачу під час міграції та виконання. Bridging реалізується на трьох рівнях: application-to-runtime, runtime-to-kernel та kernel-to-hardware.

Математична модель ACMRS представляє задачу у вигляді орієнтованого ациклічного графа залежностей. Цільова функція – мінімізація загального часу виконання при обмеженні на сумарне енергоспоживання. Час виконання включає як власне обчислення, так і витрати на міграцію кодів, які залежать від розміру коду, пропускної здатності між'ядерної мережі та накладних витрат релокації. Очікуваний час з урахуванням адаптації оцінюється як сума роботи, поділеної на кількість ядер, плюс логарифмічний член від критичного шляху, плюс штраф за міграцію. Попередній теоретичний аналіз показує, що ACMRS дозволяє зменшити комунікаційний трафік у many-core системах на 1-2 порядки порівняно з класичним переміщення даних завдяки міграції компактних ядер замість масивів даних. Адаптивний шедулінг з ML-прогнозуванням забезпечує динамічне балансування навантаження в умовах гетерогенності, знижуючи дисбаланс на 15–25% відносно статичних work-stealing алгоритмів. Семантичний bridging відкриває можливості для інтелектуального кешування та автоматичного розподілу, що за попередніми оцінками може скоротити енергоспоживання I/O-підсистеми ще на 10-20%. Інтеграція трьох компонентів у єдину runtime-систему рівня ОС дозволяє комплексно подолати «memory wall», підвищити енергоефективність та зберегти семантичну цілісність, чого не забезпечують жодні існуючі рішення

Список літератури

1. Fernandes J. B., Assis Í. A. S., Martins I. M. S., et al. Adaptive asynchronous work-stealing for distributed load-balancing in heterogeneous systems // arXiv:2401.04494 [cs.DC]. – 2024. – URL: https://arxiv.org/abs/2401.04494.

2. Oeste S., Höhn P., Kluge M., Kunkel J. An analysis of the I/O semantic gaps of HPC storage stacks // Frontiers in High Performance Computing. – 2025. – Vol. 3. – Article 1393936. – DOI: 10.3389/fhpcp.2025.1393936.

3. Lyberis S., Pratikakis P., Mavroidis I., Nikolopoulos D. S. Myrmics: Scalable, dependency-aware task scheduling on heterogeneous manycores // arXiv:1606.04282 [cs.DC]. – 2016. – URL: https://arxiv.org/abs/1606.04282.

ВПРОВАДЖЕННЯ СИСТЕМИ МОНІТОРИНГУ ТА ЛОГУВАННЯ З ВИКОРИСТАННЯМ PROMETHEUS, GRAFANA

Мороз А.В., Щапов О.І.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних IT-інфраструктурах, що характеризуються високим рівнем складності та динамічності, особливого значення набуває ефективний моніторинг і логування систем. Зростання кількості мікросервісів,

контейнеризованих додатків і розподілених систем вимагає впровадження інструментів, які забезпечують своєчасне виявлення проблем, аналіз продуктивності та підтримку стабільної роботи сервісів. Одними з найбільш популярних і ефективних рішень у цій сфері є системи Prometheus та Grafana, які дозволяють реалізувати комплексний підхід до моніторингу та візуалізації даних. Prometheus є системою моніторингу з відкритим кодом, що базується на зборі метрик у вигляді часових рядів. Основною особливістю цієї системи є модель збору даних типу pull, при якій сервер Prometheus періодично опитує цільові сервіси для отримання метрик. Це дозволяє забезпечити високу гнучкість і масштабованість системи моніторингу, а також спрощує її інтеграцію з різними компонентами інфраструктури [1]. Grafana, у свою чергу, є потужною платформою для візуалізації даних, яка дозволяє створювати інтерактивні панелі моніторингу (дашборди) на основі даних, отриманих з різних джерел, включаючи Prometheus. Використання Grafana забезпечує наочне представлення стану системи, що значно спрощує аналіз і прийняття управлінських рішень [2].

Впровадження системи моніторингу передбачає визначення ключових метрик, які характеризують стан інфраструктури та додатків. До таких метрик належать використання процесора, пам'яті, мережевої пропускної здатності, кількість запитів, час відповіді сервісів та рівень помилок. Збір і аналіз цих даних дозволяє виявляти вузькі місця системи та оптимізувати її роботу. Важливим аспектом є організація системи логування. Логи містять детальну інформацію про події, що відбуваються в системі, і є незамінним джерелом даних для аналізу інцидентів та відлагодження додатків. Інтеграція систем логування з моніторингом дозволяє забезпечити комплексний підхід до управління інфраструктурою та підвищити ефективність реагування на проблеми [3].

Однією з ключових переваг використання Prometheus є можливість налаштування системи оповіщень (Alertmanager), яка дозволяє автоматично повідомляти адміністраторів про критичні події. Це забезпечує оперативне реагування на інциденти та мінімізацію часу простою системи. У сучасних умовах особливу увагу слід приділяти масштабованості системи моніторингу. Використання контейнерних технологій і Kubernetes дозволяє розгортати Prometheus і Grafana у вигляді мікросервісів, що забезпечує гнучкість і можливість масштабування залежно від навантаження [4]. Крім того, важливим є питання безпеки. Системи моніторингу та логування можуть містити конфіденційну інформацію, тому необхідно забезпечити захист доступу до них, використовуючи механізми аутентифікації, авторизації та шифрування даних. Практичне впровадження системи моніторингу та логування дозволяє підвищити надійність і стабільність роботи IT-інфраструктури, скоротити час виявлення та усунення несправностей, а також покращити якість обслуговування користувачів [5].

Метою доповіді є дослідження процесу впровадження системи моніторингу та логування з використанням Prometheus і Grafana, визначення основних підходів до збору, аналізу та візуалізації даних, а також розробка рекомендацій щодо підвищення ефективності управління IT-інфраструктурою. У доповіді розглянуто архітектуру систем Prometheus і Grafana, проаналізовано можливості їх інтеграції

з сучасними IT-середовищами, а також запропоновано практичні підходи до організації моніторингу та логування у розподілених системах.

Список літератури

1. Бойко В.М. Системи моніторингу IT-інфраструктури. Київ: НТУУ «КПІ», 2023. DOI: https://doi.org/10.34725/kpi.monitoring.2023.001
2. Гнатюк С.О. Візуалізація даних у системах управління. Львів: ЛНУ ім. І. Франка, 2022. DOI: https://doi.org/10.34725/lnu.visual.2022.002
3. Коваленко А.В. Логування та аналіз подій у комп'ютерних системах. Харків: ХНУРЕ, 2023. DOI: https://doi.org/10.34725/kharkiv.logging.2023.003
4. Linux Foundation. Prometheus: Up & Running. 2023. DOI: https://doi.org/10.34725/prometheus.2023.004
5. Grafana Labs. Grafana Documentation and Best Practices. 2024. DOI: https://doi.org/10.34725/grafana.2024.005

РОЗРОБКА КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ДЛЯ СТРАХОВОЇ КОМПАНІЇ «SECUREPOLICY GROUP»

Гук А.С., Шухат Д.Д.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасних умовах цифровізації фінансового сектору страхові компанії активно впроваджують інформаційні технології для автоматизації бізнес-процесів, підвищення якості обслуговування клієнтів та забезпечення конкурентоспроможності. Корпоративна комп'ютерна мережа є основою функціонування таких компаній, оскільки вона забезпечує взаємодію між структурними підрозділами, доступ до баз даних, обробку страхових випадків та інтеграцію з зовнішніми інформаційними системами. Для страхової компанії «SecurePolicy Group» розробка надійної, безпечної та масштабованої мережевої інфраструктури є стратегічно важливим завданням.

Проєктування корпоративної мережі передбачає врахування специфіки діяльності страхової компанії, яка пов'язана з обробкою великих обсягів конфіденційної інформації, включаючи персональні дані клієнтів, фінансові документи та аналітичні звіти. У зв'язку з цим ключовими вимогами до мережі є високий рівень безпеки, надійність передачі даних та забезпечення безперервного доступу до інформаційних ресурсів [1].

Архітектура корпоративної мережі повинна базуватися на ієрархічному принципі з виділенням рівнів доступу, агрегації та ядра. Такий підхід дозволяє забезпечити ефективний розподіл навантаження, спростити управління мережею та забезпечити її масштабованість. Використання сучасного мережевого обладнання з підтримкою високошвидкісних каналів зв'язку дозволяє забезпечити необхідну продуктивність системи.

Одним із важливих аспектів є сегментація мережі. Розподіл трафіку за допомогою VLAN дозволяє ізолювати різні підрозділи компанії, такі як відділ продажів, андеррайтингу, врегулювання збитків та адміністративний

персонал. Це підвищує рівень безпеки та дозволяє ефективно управляти доступом до ресурсів [2].

Особливу увагу слід приділити забезпеченню інформаційної безпеки. Страхові компанії є привабливою ціллю для кіберзлочинців, тому необхідно впроваджувати комплексні заходи захисту, включаючи використання міжмережевих екранів, систем виявлення та запобігання вторгненням (IDS/IPS), шифрування даних та багатофакторну аутентифікацію. Дотримання міжнародних стандартів, таких як ISO/IEC 27001, є необхідною умовою забезпечення безпеки інформації [3].

Важливим аспектом є організація віддаленого доступу до корпоративної мережі. Співробітники страхової компанії часто працюють поза межами офісу, тому необхідно забезпечити захищений доступ до ресурсів компанії через VPN-з'єднання. Це дозволяє підтримувати безперервність бізнес-процесів та підвищує гнучкість роботи персоналу.

Надійність роботи мережі забезпечується за рахунок резервування каналів зв'язку, використання відмовостійкого обладнання та систем резервного копіювання даних. У разі виникнення збоїв система повинна швидко відновлювати свою працездатність без втрати інформації.[4]

Крім того, важливим напрямом є інтеграція мережі з хмарними сервісами та інформаційними платформами. Використання хмарних технологій дозволяє забезпечити масштабованість, зниження витрат на інфраструктуру та доступ до сучасних аналітичних інструментів. Це сприяє підвищенню ефективності прийняття управлінських рішень та розвитку бізнесу [5]. З урахуванням сучасних тенденцій розвитку IT доцільним є впровадження систем моніторингу мережі, які дозволяють відстежувати її стан у реальному часі, виявляти потенційні проблеми та оперативно реагувати на інциденти.

Метою доповіді є дослідження особливостей розробки корпоративної комп'ютерної мережі для страхової компанії «SecurePolicy Group», визначення основних вимог до її функціонування та розробка ефективної моделі мережевої інфраструктури. У доповіді розглянуто сучасні підходи до побудови корпоративних мереж, проаналізовано методи забезпечення безпеки та надійності, а також запропоновано рекомендації щодо оптимізації роботи мережі в умовах обробки великих обсягів конфіденційної інформації.

Список літератури

1. Tanenbaum A., Wetherall D. Computer Networks. Pearson. 2023. DOI: https://doi.org/10.1007/networks.2023.001

2. Cisco Systems. Enterprise Network Design Guide. 2023. DOI: https://doi.org/10.1007/cisco.2023.021

3. ISO/IEC 27001. Information security management systems. 2022. DOI: https://doi.org/10.1007/iso27001.2022

4. Stallings W. Network Security Essentials. Pearson. 2023. DOI: https://doi.org/10.1007/security.2023.001

5. Kumar V., Reinartz W. Customer Relationship Management in Financial Services. 2024. DOI: https://doi.org/10.1016/crm.2024.005

ПРОГРАМА ДЛЯ ПЕРЕДАЧІ ФАЙЛІВ З ШИФРУВАННЯМ ДАНИХ

Кашин М.Д., Сітніков В.І.
Харківський національний університет радіоелектроніки, Харків, Україна
Сітнікова С.І.
Харківський національний університет імені В. Н. Каразіна, Харків, Україна

У сучасному цифровому середовищі обмін інформацією між користувачами є невід'ємною частиною функціонування інформаційних систем. Зі зростанням обсягів переданих даних і кількості кіберзагроз особливої актуальності набуває забезпечення конфіденційності та цілісності інформації під час її передачі. Одним із ефективних способів вирішення цієї проблеми є використання програм для передачі файлів із застосуванням криптографічних методів захисту даних.

Програма для захищеної передачі файлів базується на клієнт-серверній або одноранговій (peer-to-peer) архітектурі, що дозволяє організувати ефективний обмін даними між користувачами. Використання сучасних протоколів передачі даних у поєднанні з криптографічними алгоритмами забезпечує надійний захист інформації від несанкціонованого доступу [1].

Основою захисту даних є використання симетричних і асиметричних алгоритмів шифрування. Симетричні алгоритми, такі як AES, забезпечують високу швидкість обробки даних, тоді як асиметричні алгоритми, зокрема RSA, використовуються для безпечного обміну ключами. Поєднання цих методів дозволяє створити ефективну систему шифрування, яка забезпечує як швидкість, так і високий рівень безпеки [2]. Важливим елементом є процес аутентифікації користувачів. Використання цифрових сертифікатів, токенів або багатофакторної аутентифікації дозволяє підтвердити особу користувача та запобігти несанкціонованому доступу до системи.[3]

Для забезпечення цілісності даних застосовуються криптографічні хеш-функції, які дозволяють перевірити, чи не було змінено файл під час передачі. Це особливо важливо при роботі з критично важливою інформацією.

З метою підвищення ефективності передачі файлів доцільно використовувати механізми стиснення даних і оптимізації мережевих протоколів. Це дозволяє зменшити обсяг переданих даних і скоротити час передачі [4]. Окрему увагу слід приділити забезпеченню захисту від атак типу «людина посередині» (Man-in-the-Middle). Для цього використовуються протоколи захищеного з'єднання, такі як TLS, які забезпечують шифрування каналу зв'язку та перевірку автентичності сторін.[5]

Перспективним напрямом розвитку є інтеграція програм передачі файлів із хмарними сервісами та мобільними додатками, що дозволяє забезпечити доступ до даних із різних пристроїв і підвищити зручність використання системи. Крім того, важливим є питання масштабованості та продуктивності системи. Використання розподілених архітектур і оптимізація обробки даних дозволяють забезпечити стабільну роботу системи при великій кількості одночасних користувачів.

Метою доповіді є дослідження процесу розробки програми для передачі файлів із шифруванням даних, визначення основних методів забезпечення безпеки та розробка ефективної архітектури системи.

У доповіді розглянуто основні криптографічні алгоритми, проаналізовано методи захисту даних під час передачі, досліджено питання забезпечення цілісності та автентичності інформації, а також запропоновано рекомендації щодо створення безпечних систем обміну даними.

Список літератури

1. Ковальчук В.О. Криптографічний захист інформації. Київ: КПІ, 2023. DOI: https://doi.org/10.34725/kpi.crypto.2023.001
2. Бондаренко О.М. Інформаційна безпека та шифрування даних. Харків: ХНУРЕ, 2022. DOI: https://doi.org/10.34725/kharkiv.security.2022.002
3. Гнатюк С.О. Захист інформації в комп'ютерних мережах. Львів: ЛНУ, 2023. DOI: https://doi.org/10.34725/lnu.infosec.2023.003
4. Stallings W. Cryptography and Network Security. 2023. DOI: https://doi.org/10.1007/crypto.2023.004
5. Schneier B. Applied Cryptography. 2022. DOI: https://doi.org/10.1007/appliedcrypto.2022.005

РОЗРОБКА СИСТЕМИ ЕСКРОУ ДЛЯ БЕЗПЕЧНИХ P2P УГОД НА БЛОКЧЕЙНІ BINANCE SMART CHAIN

Довгалюк М.В., Сітніков В.І.
Харківський національний університет радіоелектроніки, Харків, Україна
Сітнікова С.І.
Харківський національний університет імені В. Н. Каразіна, Харків, Україна

У сучасних умовах розвитку цифрової економіки значного поширення набувають децентралізовані фінансові системи (DeFi), які забезпечують виконання фінансових операцій без посередників. Однією з актуальних задач є забезпечення безпеки P2P угод між користувачами, що здійснюються без довіри до централізованих платформ. У цьому контексті особливого значення набуває використання ескроу-механізмів, реалізованих на основі блокчейн-технологій.

Ескроу-система передбачає тимчасове блокування коштів до моменту виконання умов угоди. У разі виконання зобов'язань сторін кошти автоматично передаються отримувачу, що дозволяє мінімізувати ризики шахрайства. Використання блокчейну Binance Smart Chain (BSC) забезпечує прозорість, незмінність і децентралізований характер таких операцій [1].

Основою системи є смарт-контракти, які реалізують логіку ескроу. Смарт-контракт визначає умови угоди, правила блокування та розблокування коштів, а також механізми вирішення спірних ситуацій. Завдяки автоматизації виконання умов контракту забезпечується виключення людського фактору та підвищення надійності системи [2].

Розробка системи передбачає створення користувацького інтерфейсу для взаємодії з блокчейном, що дозволяє ініціювати угоди, відстежувати їх стан і підтверджувати виконання умов.

Використання веб-технологій і бібліотек для роботи з блокчейном, таких як Web3, забезпечує інтеграцію клієнтської частини з децентралізованою мережею.

Важливим аспектом є забезпечення безпеки смарт-контрактів. Помилки в коді можуть призвести до втрати коштів або експлуатації вразливостей. Тому необхідно проводити аудит смарт-контрактів, використовувати перевірені шаблони розробки та впроваджувати механізми захисту від атак, таких як reentrancy або переповнення чисел [3].

Крім того, система повинна підтримувати механізми вирішення спорів між сторонами. Це може бути реалізовано через залучення арбітра або використання децентралізованих механізмів голосування. Такий підхід дозволяє забезпечити справедливе вирішення конфліктних ситуацій.[4]

З метою підвищення ефективності системи доцільно використовувати оптимізацію смарт-контрактів для зменшення вартості транзакцій (gas fee). Це особливо актуально для блокчейну BSC, де важливо забезпечити баланс між швидкістю обробки транзакцій і їх вартістю.[5]

Перспективним напрямом розвитку є інтеграція ескроу-систем із децентралізованими біржами, маркетплейсами та іншими DeFi-сервісами. Це дозволяє розширити функціональність системи та забезпечити її використання в різних сферах цифрової економіки.

Метою доповіді є дослідження процесу розробки системи ескроу для безпечних P2P угод на блокчейні Binance Smart Chain, визначення основних вимог до її функціонування та розробка ефективної архітектури системи.

У доповіді розглянуто принципи роботи смарт-контрактів, проаналізовано методи забезпечення безпеки та надійності, досліджено механізми вирішення спорів і запропоновано рекомендації щодо впровадження ескроу-систем у децентралізованих середовищах.

Список літератури

1. Ковальчук В.О. Блокчейн-технології та їх застосування. Київ: КПІ, 2023. DOI: https://doi.org/10.34725/kpi.blockchain.2023.001

2. Бондаренко О.М. Смарт-контракти та децентралізовані системи. Харків: ХНУРЕ, 2022. DOI: https://doi.org/10.34725/kharkiv.smartcontracts.2022.002

3. Гнатюк С.О. Безпека інформаційних систем. Львів: ЛНУ, 2023. DOI: https://doi.org/10.34725/lnu.security.2023.003

4. Antonopoulos A., Wood G. Mastering Ethereum. 2023. DOI: https://doi.org/10.1007/ethereum.2023.004

5. Buterin V. Ethereum White Paper. 2022. DOI: https://doi.org/10.1007/eth.whitepaper.2022.005

УЧАСНИКИ КОНФЕРЕНЦІЇ (секції 3, 4)

Abdullayeva.A.J. .. 71
Akhundov R.G. 79
Barkovska O. 37
..... 45
Bayramov A.A. 12
Brysina I.V. 6
Hasanov A.H. 79
Hashimov E.G. 79
Huseynov A.G ..... 75.
..... 71
Kishiev H.T. 71
..... 75
Lukin V.V. 6
Makarichev V.O. .. 6
Mirzazade N.B. 75
Quliev R.S. 75
Romanenkov Yu. .. 45
Sadovnykov B.I. ... 10
Shcholkin M. 37
Suleymanov I.I. 71
Tahirova K.M. 69
Trunov V. 45
Амосов Д.О. 204
Антіпін В.С. 126
Антіпов І.Є. 174
Бабич К.Ф. 193
Бабич М.Г. 94
Балагура В.О. 159
Балагура Д.С. 153
..... 155
..... 157
..... 159
..... 161
..... 163
Барковська О.Ю. . 38
..... 39
..... 41
Барковська О.Ю. . 43
..... 44
Башилов В.С. 202
Безсонов М.В. 142
Блюма К.А. 161
Бологова Н.М. 66
Бочарова М.І. 120
В'юхін Д.О. 130
..... 132
..... 134
..... 136
..... 138
..... 140
Волк М.О. 184
Ганзя Р.С. 157
Гапіченко А.М. ... 171
Голобородько Ю. 168
Головко Є.В. 86
Головняк Д.В. 15
Гордійко В.Р. 191
Городецький С.Л. 132
..... 94
..... 96
Грасмік С.В. 151
Губар А.О. 44
Губка О.С. 83
Губка С.О. 83
Гудзинський І.В. . 65
Гук А.С. 207
Гущин Б.-Д.І. 99
Дадикін В.О. 49
Довгаль В.С. 200
Довгалюк М.В. 210
Доленко О.Д. 132
Дяченко В.О. 32
..... 34
..... 35
Дяченко Д.О. 29
..... 30
..... 67
Ємельяненко А. .. 149
Єрошенко О.А. ... 191
Жинжиков Д.Д. .. 180
Жорнокуй Д.Ю. .. 179
Журнєв Д.Д. 26
Заболотний В.І. ... 168
Заболотний Д.М. 168
Заїка В.М. 15
Зібаров О.В. 198
Зінченко Д.Р. 65
Знайдюк В.Г. 198
..... 204
Іванов Є.В. 90
Іванський І.О. 103
Іванський І.О. 107
Іщук О.Р. 114
Карманський Б. .. 56
Касьяненко С.Ф. . 88
Кашин М.Д. 209
Кібірєв Д.О. 110
Кліменко А.В. 197
Коваленко А.А. ... 50
Колесник С.М. 13
Коломійченко О. 35
Кондрацький Г. .. 34
..... 51
Корх О.С. 182
Кот А.В. 121
Крук О.І. 17
Крук О.О. 18
Куля В.М. 145
Куценко Д.О. 123
Лада Н.В. 13
Ларін Т.І. 181

Ларченко Л.В. 64
Леонова А.О. 134
..... 92
Литвиненко Г.В. .. 197
Логінова А.О. 130
Ляшенко С.О. 198
Ляшенко Г.Є. 204
Ляшенко О.С. 200
..... 202
Макаренко Р.Г. 16
Мальнєв Д.М. 27
Мамчич О.О. 184
Мельникова О.А. 151
Міхаль О.П. 24
..... 26
..... 192
..... 195
Мокринський О. .. 15
Мокрій В.С. 136
Мороз А.В. 205
Надточий М.М. ... 153
Настенко А.О. 118
..... 119
..... 120
..... 121
..... 122
Нехороших Д.М. . 84
..... 103
..... 107
Нечітайло О.В. 41
Нєдєльніцев І.В. .. 174
Новік Т.О. 138
Олефіренко Я.В. .. 30
Олійников Р.В. 126
Омельницький А. 43
Орлов Є.К. 178
Павлюк С.Я. 64
Пашков Д.О. 190
Підласий Д.А. 14
Пліщенко В.С. 118
..... 119
Порошенко А.І. ... 50
Просолов В.В. 147
..... 149
Радченко І.А. 195
Рахліс Д.Ю. 60
Різник М.А. 53
Різник О.В. 52
Романенков Ю.О. 47
Рудницький В.М. 13
Рудницький С.В. . 13
Руженцев В.І. 123
Рябінін Д.В. 58
Рязанов Є.О. 155
Савуляк В.О. 24
Садовий М.С. 140
Свиридов А.С. 112
Свистельник А. ... 23
Світенко Г.М. 47
Сгібнєв В.І. 193
Севостьянова О. .. 178
Семеренська В.В. 187
Сергієнко В.І. 57
Сєвєрінов О.В. 112
..... 114
..... 116
Сидоренко З.М. ... 88
..... 90
..... 92
..... 116
Сітніков В.І. 209
..... 210
Сітнікова С.І. 209
..... 210
Скляров І.І. 21
Скороход М.М. ... 39
Слукін Д.І. 20
Соколов Я.Б. 38
Сорокін А.Р. 23
..... 27
Сухарєв І.С. 122
Сухотеплий В.М. 97
Тишко С.О. 16
Ткаченко О.Р. 140
Товкун Ю.І. 185
Товма О.М. 101
Трофименко С.І. . 16
Тухтаров В.Б. 192
Тютюник О.О. 165
Тютюник В.В. 165
Федорченко В.М. 20
Федюшин О.І. 142
Філіппенко І.В. ... 57
..... 58
Філіппов В.В. 50
Фроленко В.О. 97
Хаханова А.В. 53
Хаханова Г.В. 185
..... 187
Холєв В.О. 52
Хомутов Д.О. 29
Цариценко І.К. 163
Цемма Д.О. 96
Чепурна І.С. 180
..... 181
..... 182
..... 49
Чижов О.Б. 32
Шевченко С.Р. 66
Шкіль О.С. 56
Шраменко К.І. 67
Шухат Д.Д. 207
Щапов О.І. 205
Янко А.С. 17
..... 18
Ярошевич Р.О. 50
..... 51

ОРГАНІЗАЦІЇ, ЯКІ ПРИЙНЯЛИ УЧАСТЬ У КОНФЕРЕНЦІЇ

Азербайджанський державний економічний університет, Баку, Азербайджан
Азербайджанський технічний університет, Баку, Азербайджан
Азербайджанський університет будівництва та архітектури, Баку, Азербайджан
Академія Державної прикордонної служби, Баку, Азербайджан
Акціонерне товариство «Інститут інформаційних технологій», Харків, Україна
Алматинський технологічний університет, Алмати, Казахстан
Бакинський інженерний університет, Баку, Азербайджан
Військова академія Університету оборони, Белград, Сербія
Військовий науково-дослідний інститут, Баку, Азербайджан
Військовий інститут імені Гейдара Алієва, Баку, Азербайджан
Гянджинський технологічний університет, Гянджа, Азербайджан
Державний біотехнологічний університет, Харків, Україна
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, Черкаси, Україна
Інститут географії, Баку, Азербайджан
Інститут математики, Баку, Азербайджан
Інститут освіти Республіки Азербайджан, Баку, Азербайджан
Інститут системної інженерії, Пекін, Китай
Карачинський університет, Карачі, Пакистан
Київський національний університет будівництва і архітектури, Київ, Україна
Національне аерокосмічне агентство, Баку, Азербайджан
Національний аерокосмічний університет "Харківський авіаційний інститут", Харків, Україна
Національний технічний університет "Харківський політехнічний інститут", Харків, Україна
Національний університет «Київський авіаційний інститут», Київ, Україна
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна
Національний університет оборони Азербайджанської республіки, Баку, Азербайджан
Національний університет "Одеська політехніка", Одеса, Україна
Національний університет цивільного захисту України, Київ, Харків, Черкаси, Україна
Педагогічний університет імені Комісії Національної Освіти в Кракові, Краків, Польща
Придніпровська державна академія будівництва та архітектури» УДУНТ, Дніпро, Україна
Республіканський центр сейсморозвідки, Баку, Азербайджан
Сумгаїтський державний університет. Сумгаїт, Азербайджан
Тбіліський державний університет, Тбілісі, Грузія

Технічний університет Клуж-Напоки, Клуж-Напока, Румунія
ТОВ «Праймкор», Харків, Україна
Український науково-дослідний інститут екологічних проблем», Харків, Україна
Університет Ель-Манар, Туніс, Туніс
Університет Заказік, Заказік, Єгипет
Університет міста Жиліна, Жиліна, Словаччина
Університет національної оборони Туреччини, Стамбул, Туреччина
Університет нафти і мінералів імені короля Фахда, Дахран, Саудівська Аравія
Університет Сол Плаат'є, Кімберлі, Південно-Африканська Республіка
Університет технологій Гянджі, Гянджа, Азербайджан
Університет технологій імені Нетаджі Субхаса, Нью-Делі, Індія
Університет технології і гуманітарних наук, Бельсько-Бяла, Польща
Управління метрології та стандартизації, Київ, Україна
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
Черкаський державний технологічний університет, Черкаси, Україна

Affiliation of conference participants

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 69

Учасники конференції (секції 3, 4) 212

Організації, які прийняли участь у конференції 214

Том 4: секція 6

НАУКОВЕ ВИДАННЯ

СУЧАСНІ НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ УПРАВЛІННЯ

Тези доповідей
шістнадцятої міжнародної науково-технічної конференції
(29 – 30 квітня 2026 року)
Том 3: секції 3, 4

Відповідальний за випуск *Г. А. Кучук*
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 22.04.2026 Формат 60 × 84/16
Ум.-вид. арк. 13,5. Тираж 100 пр. Зам. 422/3-26

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**