МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

III МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

The third International scientific and practical conference

“Кіберборотьба: розвідка, захист та протидія”

“Cyberwarfare: intelligence, defense and offensive security”

06–07.05.2025

ТЕЗИ ДОПОВІДЕЙ
(Частина 2)

Київ

Рецензенти:

Радзівілов Григорій Данилович	кандидат технічних наук, професор, заступник начальника інституту з наукової роботи
Чевардін Владислав Євгенійович	доктор технічних наук, професор, старший науковий співробітник, начальник кафедри кібербезпеки
Ковальчук Людмила Василівна	доктор технічних наук, професор, доцент кафедри кібербезпеки
Хусаінов Павло Валентинович	кандидат технічних наук, професор, професор кафедри кібербезпеки
Якуб Сита	доктор філософії, заступник директора Центру морської кібербезпеки Польської військово-морської академії

Кіберборотьба: розвідка, захист та протидія: тези доповідей ІІІ Міжнародної науково-практичної конференції (Частина 2). – Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2025. – 28 с. DOI: https://doi.org/10.61929/viti.mnpk.3(2).2025.

У збірнику матеріалів ІІІ Міжнародної науково-практичної конференції **“Кіберборотьба: розвідка, захист та протидія”** опубліковано тези доповідей вчених, науково-педагогічних та наукових працівників, докторантів, ад’юнктів, здобувачів.

Метою конференції є аналіз шляхів співпраці наукових колективів європейських країн у сучасних проєктах збереження миру та безпеки та використання сучасних навчальних кіберполігонів і платформ для проведення навчання фахівців із кібербезпеки.

Робочі мови конференції – українська, англійська.

Відповідальність за точність, достовірність і зміст поданих матеріалів несуть автори.

Відповідальна за випуск І. В. Цимбал

Підписано до друку 03.06.2025. Зам. № 140
Друк. арк. 3,50. Ум.-друк. арк. 3,25. Обл.-вид. арк. 3,02
Формат паперу 60×84/8. Тираж 3 прим.

Адреса друкарні ВІТІ ім. Героїв Крут: 01011, м. Київ, вул. Князів Острозьких, 45/1

З М І С Т

UDC 621.391:519.2:519.7

Dr. Habil., prof. **Kovalchuk L.** ORCID: 0000-0003-2874-7950
Kondratenko M. ORCID: 0009-0009-0979-2626
Pukhov G. E. (Institute for Modelling in Energy Engineering, Ukraine)

SECURITY OF PROOF-OF-PROOF CONSENSUS WITH DIFFERENT TYPES OF PROTOCOLS FOR DIFFERENT LEVELS AGAINST DOUBLE SPEND ATTACK

Introduction

This work continues the research of work [1] and completes a series of studies of the security of the two-level consensus protocol Proof-of-Proof (PoP) [2; 3] against double-spend attack on a security inherited blockchain.

In our previous works, which considered the security of the PoP consensus protocol against double-spend attack, explicit formulas for the probability of the attack were obtained in the following cases:

– Proof-of-Work consensus protocols [4] (taking into account the synchronization time) in both blockchains ([5]);

– Proof-of-Stake consensus protocol [6] in both blockchains ([7]);

– Proof-of-Stake consensus protocol in the main blockchain and Proof-of-Work in the secondary blockchain ([1]).

In this paper, we obtain formulas for the probability of success of a double-spend attack for the PoP protocol in the case when the Security provided blockchain (SPB) implements the Proof-of-Work consensus protocol, and the Security Inherited blockchain (SIB) implements the Proof-of-Stake protocol. Thus, this paper completes the study of the probability of success of an attack for all cases of PoP based on the most common protocols, which are PoW and PoS.

Note that when calculating the probability of success of the attack, we also take into account the possible synchronization time in the SPB, as well as the possibility that the attacker in the SIB blockchain can ignore the blocks issue in those timeslots in which he is the slotleader. These assumptions allow us to obtain probabilities in a real model of the functioning of the blockchain, but on the other hand create significant analytical difficulties in obtaining corresponding results.

The goal of this work is to calculate the attack probability and to determine the number of confirmation blocks in the SIB that must be issued after the corresponding checkpoint in the SPB, for which the probability of a double-spend attack on the SIB is less than some predetermined value.

Mathematical model and main results.

We use the following mathematical model of a two-level blockchain. SPB uses the Proof-of-Work consensus protocol – for example, the Bitcoin network is chosen as the main blockchain. We also assume that there are malicious participants in the network who violate the rules of block creation and may try to perform various attacks on the blockchain. We also make assumptions in favor of the adversary regarding the network synchronization time: in what follows, we assume that the attacker's synchronization time is zero, and we consider the synchronization time of honest miners to be non-zero and bounded from above by some value D_H. Let's define α as the total hash rate of the network, α_M – the total hash rate of the attacker, $\alpha_H = \alpha - \alpha_M$ – the total hashrate of honest miners. Let's also define $p_H = \frac{\alpha_H}{\alpha}$ and $p_M = \frac{\alpha_M}{\alpha}$ respectively.

SIB uses the Proof-of-Stake consensus protocol, so the block creation process is divided into epochs, each of which, in turn, is divided into timeslots. Let us denote N the number of timeslots in one epoch, and τ is the duration of one timeslot. According to the slotleader selection protocol, there may be more than one slotleader in one timeslot, or there may be no slotleaders at all. In any case, the following requirement are met: *no more than one block can be added to the blockchain per one timeslot.*

Theorem 1. Let the inequality hold in our notation $p'_M < p'_H$, where $p'_M = 1 - e^{-\alpha_M D_H} \cdot p_H$, $p'_H = e^{-\alpha_M D_H} \cdot p_H$. Suppose that after the block B_{Ch} there were z confirmation blocks in the SIB. Then for any $l \in N$, such that $\tau \cdot z > l \cdot D_H$, the following upper bound for the probability Q_z of success of a double-spending attack on a block B_{Ch}:

$$Q_z \le e^{-\alpha_H \cdot (\tau \cdot z - l \cdot D_H)} \cdot \sum_{i=0}^{l-1} \frac{\left(\alpha_H \cdot (\tau \cdot z - l \cdot D_H)\right)^i}{i!} + 1 - \sum_{k=0}^{l-1} P_l(k) \left(1 - \left(\frac{p'_M}{p'_H}\right)^{l-k}\right),$$

where $P_l(k) = \frac{p_H^l}{(n-1)!} \cdot \frac{e^{-\alpha_M \cdot l \cdot D_H} \cdot (\alpha_M \cdot l \cdot D_H)^k}{k!} \cdot \sum_{i=0}^{k} \frac{(l-i+1)! \cdot C_k^i}{(\alpha \cdot l \cdot D_H)^i}$.

Numerical results

We applied Theorem 1 to calculate numerical results for the next initial data: $\tau = 60$ seconds; $D_H = 5$ seconds; $\alpha = 0.00167$.

p_M	0.1	0.15	0.2	0.25	0.3	0.35
z	183	250	339	491	750	1301

Thise numerical results indirectly confirm the correctness of corresponding analytical ones.

Conclusions

The results obtained in Theorem 1 allow us to construct a simple and transparent algorithm for determining the required number of confirmation blocks in the blockchain, for arbitrary given network parameters and a given upper limit of the permissible probability of an attack. It is interesting that the probability of an attack does not depend on the share of the attacker in the SIB. This can be explained by the fact that he does not have a significant impact on the probability of this attack, since all he can do in this case is not to release blocks in his timeslots, which will only increase the time until the required number of blocks are released in the SIB, while reducing the probability of an attack.

REFERENCES

1. Kovalchuk L. V., Kuchynska N. V., Kondratenko M. S. Determining the Number of Confirmation Blocks in a Two-Level Blockchain with Proof-of-Proof Consensus Protocol for Different Consensus Types in Mainchain/Sidechain to Prevent Double Spend Attack. I. PoS in Mainchain and PoW in Sidechain. *Cybernetics and System Analysis.* 2024. URL: https://doi.org/10.1007/s10559-024-00703-5.

2. Zhang H., Wu J., Liu Y., Yu J. VaryBlock: A Novel Approach for Object Detection in Remote Sensed Images. *Sensors.* 2019. No. 19. P. 5284. URL: https://doi.org/10.3390/s19235284.

3. Lashkari B., Musilek P. A Comprehensive Review of Blockchain Consensus Mechanisms. *IEEE Access*. 2021. Vol. 9. P. 43620–43652. URL: https://www.researchgate.net/publication/350031088_A_Comprehensive_Review_of_Blockchain_Consensus_Mechanisms.

4. Nakamoto S. A peer-to-peer electronic cash system. 2008. URL: https://bitcoin.org/bitcoin.pdf.

5. Kovalchuk L., Kostanda V., Marukhnenko O., Pozhylenkov O. Achieving Security in Proof-of-Proof Protocol with Non-Zero Synchronization Time *Mathematics*. 2022. No. 10. P. 2422. URL: https://doi.org/10.3390/math10142422.

6. Saleh F. Blockchain without Waste: Proof-of-Stake. *The Review of Financial Studies.* 2021. Vol. 34, Iss. 3. P. 1156–1190. URL: https://doi.org/10.1093/rfs/hhaa075.

7. Kondratenko M. Determining the number of confirmation blocks in the blockchain that hosts the second-level registry in the case that both blockchains use the POS-consensus protocol. Collection of materials of the XLI Scientific and technical conference of young scientists and specialists of G. E. Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine/PIMEE of NAS of Ukraine. 2023. P. 188–190. URL: https://ipme.kiev.ua/wp-content/uploads/2023/05/Матеріали-конференції-2023.pdf.

UDC 621.391

Dr. Habil., prof. **Kovalchuk L.** ORCID: 0000-0003-2874-7950
Bespalov O. ORCID: 0000-0001-7126-6752
Pukhov G. E. (Institute for Modelling in Energy Engineering, Ukraine)

PRIVACY PRESERVING PREFERENTIAL VOTING SCHEME

1. Introduction

A lot of existing blockchain, in addition to the "classic" transactions of a certain crypto asset, also provide decentralized blockchain governance through decentralized decision making. For a basic understanding of blockchain governance principles, we recommend reading the article [1], which proposes a holistic definition and a conceptual model of blockchain governance, and is a systematic literature review of 75 articles that applies systems theory to conceptualize blockchain governance as a system and parsimoniously organize its interrelated elements into a conceptual model.

One of the basic management tools is decentralized secret voting. There are a lot of real examples of using cryptographic tools to build such voting. First of all, these are digital signatures, hybrid encryption, decentralized protocols for decentralized and shared key generation, and non-interactive zero knowledge proofs (NIZK proofs). For example, such voting systems are built in the Cardano, Gitcoin, Aragon, Tezos, Polkadot, MakerDAO and many other blockchains, and a detailed description of the version of such a system can be found in the papers [2, 3]. Usually blockchain utilize different variants of multiwinner voting system, when voting for projects funding.

In this work we propose a mathematical model for privacy secure blockchain-based preferential voting. Such type of voting is essentially different from multiwinner voting schemes hence utilizes other NIZKs to provide privacy security. Because of this, we need to create new NIZK – NIZK for knowledge of exponents and there their inequalities.

Note that such type of voting may be used not only in blockchain technologies, but in different other procedures – like setting preferences for specialties when filling out entrance forms during the entrance campaign.

The purpose of the work is to create privacy secure preferential voting model, and describe and proof its properties.

2. Privacy preserving preferential voting

Let the group G be a prime-order subgroup of some cryptographically secure elliptic curve E, and $|G| = q$. Define $P, H \in G$ two base points of the curve E. The point P is used to form public keys, and the point H is used as a commitment key.

We introduce the next definitions for entities involved in voting schemes: a set of voting committee members $\mathrm{T} = \left\{T^{(1)},...,T^{(u)}\right\}$, a set of Voters $\mathrm{V} = \left\{V^{(1)},...,V^{(n)}\right\}$, a set of candidates/proposals/projects $\Pi_1,...,\Pi_m$.

We assume that committee use DKG procedure [4] to create their public key T_{pub} and use joint decryption [5] to decrypt voting results.

Next, for each voter $V^{(i)}$, $i \in [n]$, define his ballot $B^{(i)}$ as $B^{(i)} = \left(b_1^{(i)},...,b_m^{(i)}\right)$, where the values $b_j^{(i)}$ should meet the next requirements:

- $1 \le b_j^{(i)} \le m$, $i \in [n]$, $j \in [m]$;
- for a fixed $i \in [n]$, all values $b_1^{(i)},...,b_m^{(i)}$ are different.

Note that as we build privacy preserving voting, all ballots should be encrypted. It means that we can't check the correctness of ballot directly. Thus, we assume that malicious voters may create incorrect ballots, to achieve some favors. So, to check the ballot correctness, we need to have such NIZK proofs that may work with encrypted ballots and to check requirements given above, along with encryption correctness.

Each voter $V^{(i)}$, $i \in [n]$, uses lifted El-Gamal encryption [6] based on Elliptic Curve Cryptography — a cryptographic scheme with faster homomorphic operations and smaller ciphertexts – to encrypt his ballot. Such approach is usual for such situation when we need gomomorphic encryption, which allows decrypt final voting results without opening each ballot.

More precisely, each voter $V^{(i)}$, $i \in [n]$, after forming the ballot $B^{(i)} = \left(b_1^{(i)}, ..., b_m^{(i)}\right)$, does the next steps:

– chooses randomly vector $t^{(i)} = \left(t_1^{(i)}, ..., t_m^{(i)}\right)$, $t_j^{(i)} \in [q-1]$;

– forms encrypted ballot as

$$Enc_{T_{pub}}\left(B^{(i)}, t^{(i)}\right) = \left(\left[r_1^{(i)} \cdot P,\ b_1^{(i)} \cdot P + r_1^{(i)} \cdot T_{pub}\right]; ...; \left[r_m^{(i)} \cdot P,\ b_m^{(i)} \cdot P + r_m^{(i)} \cdot T_{pub}\right]\right);$$

– creates corresponding NIZK proofs to prove the ballot correctness:

– exponent equality NIZK proof $\pi_{EE}^{(i)}$, to prove that $r_j^{(i)}$ is the same for $r_j^{(i)} \cdot P$ and $b_j^{(i)} \cdot P + r_j^{(i)} \cdot T_{pub}$;

– range NIZK proof [7] $\pi_R^{(i)}$, to prove that $1 \le b_j^{(i)} \le m$, $j \in [m]$;

– exponent non-equality NIZK proof $\pi_{EN}^{(i)}$, to prove that all values $b_1^{(i)}, ..., b_m^{(i)}$ are different.

During the tally phase, the committee members firstly check the ballot correctness, then add corresponding components of encrypted ballots, and then apply shared decryption. Such approach provide security preserving and correctness of tally results.

3. Conclusion

The proposed voting scheme uses different cryptographic tools for ensuring privacy preserving in preferential voting. It also applies new NIZK for exponents non-equality to confirm ballot correctness.

REFERENCES

1. Gabriella Laatikainen, Mengcheng Li, Pekka Abrahamsson. A system-based view of blockchain governance // Information and Software Technology. 2023. Vol. 157. P. 107149. ISSN 0950-5849. URL: https://doi.org/10.1016/j.infsof.2023.107149 (https://www.sciencedirect.com/science/article/pii/S0950584923000034).

2. Bingsheng Zhang, Roman Oliynykov, and Hamed Balogun. A treasury system for cryptocurrencies: Enabling better collaborative intelligence. In *The Network and Distributed System Security Symposium (NDSS '19)*, 2019.

3. Zeyuan Yin, Bingsheng Zhang, Andrii Nastenko, Roman Oliynykov, Kui Ren. A scalable coercion-resistant voting scheme for blockchain decision-making, 2023. URL: https://eprint.iacr.org/2023/1578.pdf.

4. Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. Optimally efficient multi-authority election scheme. In *In Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques*, pages 103–118. Springer, 1997. URL: https://doi.org/10.1007/3-540-69053-0_9.

5. Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. Optimally efficient multi-authority election scheme. In *In Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques*, pages 103–118. Springer, 1997. URL: https://doi.org/10.1007/3-540-69053-0_9.

6. Gamal T. E. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theory 1985, 31, 469–472.

7. Nan Wang, Sid Chi-Kin Chau, and Dongxi Liu. Swiftrange: A short and efficient zero-knowledge range argument for confidential transactions and more, 2023. URL: https://eprint.iacr.org/2023/1185.pdf.

УДК 681.3.06

Strielnikov M. D. ORCID: 0009-0005-4928-2664
(National Technical University of Ukraine 'Kyiv Polytechnic Institute')

PROOF OF DATA POSSESSION PROTOCOL WITH HASH-BASED DETERMINISTIC CHALLENGES AND PRIVATELY VERIFIABLE PAYMENTS

1. Introduction

Existent proof-of-possession protocols surveyed are based on authentication of randomly selected number blocks within agreed number of rounds. In our work we show that, such approach implying existence of non-negligible cheating probability.

2. Cheating probability and optimal communication

The cheating probability P_{cheat} in PDP protocols depends on the number of authenticated blocks respectively to the number of all data blocks n. The P_{cheat} stated as the probability to evade authentication by certain blocks which are potentially corrupted $P_{cheat} = \frac{C_k^{n-m}}{C_k^n}$, where C_k^n is the number of combinations to chose k blocks out of n and C_k^{n-m} is the number of combinations to chose n-m correct blocks avoiding m incorrect ones.

Assume that rational data owner want to authenticate as much blocks as possible by ensuring $\epsilon = \frac{m}{n} \ll 1$, where ϵ is the fraction (or per cent) of unchecked blocks. Then cheating detection approximated to $P_{cheat} \approx \left(1 - \frac{m}{n}\right)^k$, where k is the number of random data blocks to authenticate. In practice, reasonable values for ϵ are around $10^{-2}..10^{-4}$ to allow at most 1%..0.001% unchecked blocks. It follows that probability of accurate authentication P by data owner for given small fraction ϵ trough checking k blocks is: $P \approx 1 - P_{cheat} \approx 1 - e^{-\epsilon k}$.

Consecutively, optimal data owner want to minimize number of data blocks to authenticate $k \to min$ by achieving high detection probability (confidence) $P \to 1$. This implies on practice $P \geq 1 - \delta$, where $\delta \ll 1$ is the maximum allowed but still acceptably small cheating probability (verification error) which attain bound $1 - e^{-\epsilon k} \geq 1 - \delta \Rightarrow e^{-\epsilon k} \leq \delta$, then optimal k expressed as a dependence on δ and ϵ:

$$-\epsilon k \leq ln(\delta) \Rightarrow k \geq \frac{-ln(\delta)}{\epsilon}.$$

We consider practically reasonable range for δ within $10^{-2}..10^{-4}$ which in order to tolerate targeted cheating probability $\delta \leq 1\%$ on $\epsilon \leq 1\%$ of all data blocks for the single challenge round of PDP. Such a small percentage of potentially allowed corrupted blocks can be restored with the application of error correction codes.

It's easy to see that optimal communication complexity O for probabilistic PDP is also proportional to k, but requires k to be integer rounded up: $O \sim \lceil k \rceil = \lceil \frac{-ln(\delta)}{\epsilon} \rceil$.

Observe, that optimal solution for k requires to keep both δ and ϵ as small as possible values within similar range of $10^{-2}..10^{-4}$ or smaller. Then we can express optimal communication complexity O as a dependency on the number of data blocks $O \propto n$ using approximation $\delta \approx \epsilon$:

$$O \sim \lceil k \rceil \approx \lceil \epsilon^{-1} ln(\epsilon^{-1}) \rceil = \lceil \frac{n}{m} ln\left(\frac{n}{m}\right) \rceil.$$

3. Proposed proof-of-data-possession protocol

Building on this findings, we proposed our variant of PDP protocol.

1 Setup phase:

1.a A agree on a number of challenges and rounds r with B

1.b A generates a set of random nonces $t = \{t_i \leftarrow 1^\lambda \vee i = \underline{1.r}\}$ for r round challenges with bit security of λ

1.c A computes answers v_i to each challenge as $\underline{v} = \{hash(D \vee t_i) \vee i = \underline{1.r}\}$ before any information exchange with B

1.d A signs D with $Sign(D, sk) = (Sig, pk)$ using a private key sk yielding a pair of signature Sig and public key pk

1.e A transfers funds in amount equal to agreed price to the smart-contract address (or third-party payment provider)

1.f A publishes (Sig, pk) and transfers data D to B by finishing setup phase

2 A performs r rounds of challenges for B on data D. On each i-th round while $i \leq r$:

1.a A sends t_i to B and asks him to compute $v_i' = hash(D \vee t_i)$

1.b B presents v_i' to A

1.c A check condition $v_i =^? v_i'$ by comparing v_i' with pre-computed answer v_i

1.d If the condition evaluates to $False$, A consider B cheating and aborts the protocol. Otherwise, A unlocks the portion of funds in smart-contract (made during setup phase) by making the portion of the price available for B to charge

2 If all challenges are completed successfully, then A requests back her copy D' of the data D

3 On retrieval, A verify the signature by $Verify(D', pk)$ to ensure the authenticity of the data implying $D' = D$

4 If verification is evaluated $True$, both sides conclude the end of the protocol.

4. Security analysis

The security of the protocol proposed depends on security of underlying cryptographic hash function applying to the whole data. This allowed to get a compact proof of possession with fixed size of the hash function. Such approach reduces the communication complexity for a single challenge of the data storage provider to *O(1).*

Successful forge of the data possession proof by malicious storage provider requires to find the preimage of the hash function. The probability of successful guess for a cryptografic hash function preimage is equivalent to guess an arbitrary binary string which shown to be negligible small.

The probability P_{lookup} of success for improved guessing approach with the usage of precomputed lookup table of size $N \ll 2^n$ shown to be negligible small:

$$P_{lookup} = \left(1 - \frac{N}{2^n}\right)^r \approx e^{-\frac{rN}{2^n}} \approx e^0 \approx 1 \Rightarrow P_{lookup} \approx 0.$$

The mitigation of length extension attack on hash functions with Merkle-Damgård construction requires usage of the sponge-based hash function.

5. Conclusion

The usage of cryptographic hash functions allows to reduce communication complexity for a single challenge to the fixed size equal the size of the hash function output. The computational complexity to produce single challenge for storage provider does not depends on the size of the data by assuming random oracle access model of the hash function computation. Additional advantage of the protocol proposed is the integration of payments for successful challenge to incentivise the data storage provider.

УДК 004.056.4

Cand. Tech. Sc. **Samoilov I.** ORCID: 0000-0002-8251-9257 (ISCIP)
Cand. Tech. Sc. **Storchak A.** ORCID: 0000-0002-5267-3122 (ISCIP)
Cand. Tech. Sc. **Konotopets M.** ORCID: 0000-0002-6963-1877 (ISCIP)
Ph.D. **Lavryk I.** ORCID: 0000-0002-3433-9083 (MITIT)

APPLICATION OF ML TECHNIQUES FOR CYBER INCIDENT ANALYSIS

The analysis conducted by [1] showed that the main types of threats remain ransomware, malware, social engineering, data breaches, and availability threats. According to [2], 58.8 % of all incidents in 2024 were related to malware, including ransomware. The significant threat posed by ransomware underscores the need for new technologies to detect and neutralize it. The use of machine learning methods can reduce threat detection times and significantly improve security system efficiency [3].

The main approaches to analyzing cyber incidents and malware are signature, heuristic, static, dynamic, and neural network analysis. Machine learning addresses the challenge of polymorphic and metamorphic viruses by analyzing program behavior patterns and detecting anomalies.

The stages of applying machine learning algorithms to cyber-incident analysis are as follows:

1. Collection of input parameters.
2. Feature extraction and preprocessing.
3. Application of ML algorithms.
4. Identification of “zero-day” threats.
5. Accuracy evaluation using Precision, Recall, and F1 metrics.
6. Integration with SIEM systems (Splunk, IBM QRadar, ArcSight).

In the first stage, a comprehensive dataset is collected to detect polymorphic and metamorphic malware. The second stage extracts relevant features (API call frequency, PE‑file structure, etc.) and balances classes to reduce false positives and false negatives.

The following algorithms are used for training and threat detection:

– Random Forest (500 trees, max_depth=30) – resistant to noise and well-suited for a large number of heterogeneous features;

– Isolation Forest – for detecting anomalous patterns and uncovering unseen threats;

– Cluster Analysis – grouping similar samples to identify families of polymorphic malware.

After training, the model is evaluated on a test set to minimize false positives and false negatives. For automatic reporting of suspicious patterns and triggering correlation analysis, the method is integrated with SIEM systems.

The quality of cyber incident analysis using machine learning technologies depends on the training data. Polymorphic and metamorphic malware constantly evolves, so without regular updates and sample expansion, the method's effectiveness will degrade over time. This method should be deployed in critical infrastructure environments with large datasets and high computational resources, as its effectiveness depends on the quality of the training samples and their regular updates. The combined approach (Random Forest, Isolation Forest, clustering) can be resource-intensive, so it is most appropriate for large-scale systems.

REFERENCES

1. European Union Agency for Cybersecurity. Enisa threat landscape 2024. EUROPEAN UNION AGENCY FOR CYBERSECURITY. 2024.

2. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв’язку та захисту інформації України. Звіт системи виявлення та реагування на кіберінциденти та кібератаки за 2024 рік.

3. Zvit IBM pro vartist vytoku danykh za 2023 rik – CoreWin. (n.d.). CoreWin. URL: https://corewin.ua/news/ibm–report–2023.

УДК 004.056

Андреєв А. О. ORCID: 0000-0003-0074-0482 (ВІТІ ім. Героїв Крут)

ТЕХНОЛОГІЇ РЕЗЕРВНОГО КОПІЮВАННЯ ІНФОРМАЦІЇ ДЛЯ ПІДВИЩЕННЯ СТІЙКОСТІ ДО КІБЕРЗАГРОЗ

Актуальність теми. У сучасному цифровому середовищі питання збереження інформації є одним із ключових для організацій будь-якого масштабу. Кіберзагрози, такі як віруси, програми-вимагачі (ransomware), DDoS-атаки, внутрішні загрози від працівників або людські помилки, можуть призвести до часткової або повної втрати критично важливої інформації. В умовах гібридної війни та зростання частоти атак на інфраструктуру державних установ, підприємств і закладів освіти, забезпечення безперервного доступу до даних є критично важливим. Технології резервного копіювання стали одним із ключових інструментів підвищення інформаційної стійкості до таких загроз.

Мета роботи. Метою цієї роботи є аналіз сучасних технологій резервного копіювання інформації та визначення їх ролі в підвищенні стійкості до кіберзагроз. Також розглядаються типи резервного копіювання, принципи побудови ефективної стратегії бекапу та рекомендації щодо впровадження в організаційні структури.

Виклад основного матеріалу

Існує кілька підходів до реалізації резервного копіювання. Перший і найбільш очевидний – це повне копіювання даних, при якому створюється повна копія всіх файлів та системних налаштувань. Цей метод забезпечує максимальний рівень безпеки, але водночас потребує значного обсягу дискового простору та часу на виконання процедури. Саме тому для більшої ефективності часто використовують інкрементне копіювання – метод, при якому зберігаються лише ті зміни, що були внесені після останнього резервного збереження. Такий підхід дозволяє значно зменшити навантаження на систему та скоротити час копіювання, однак при відновленні даних необхідно мати доступ до всієї послідовності копій. Ще одним компромісним варіантом є диференціальне копіювання, при якому зберігаються всі зміни з моменту останнього повного бекапу, що спрощує процес відновлення, хоч і вимагає більше ресурсів, ніж інкрементне.

Резервні копії можуть зберігатися у різних місцях. Традиційним рішенням є локальне зберігання – на зовнішніх жорстких дисках, флеш-накопичувачах або на внутрішніх серверах організації. Такий варіант забезпечує швидкий доступ до резервних копій, проте вразливий до фізичних пошкоджень, крадіжок, пожеж чи знищення внаслідок кібератаки. З метою підвищення надійності все більше організацій переходять до використання хмарних технологій – так званих рішень Backup-as-a-Service. Завдяки використанню хмарних сховищ, таких як Google Drive, Microsoft OneDrive, Amazon S3, або спеціалізованих сервісів типу Veeam Cloud Connect, забезпечується масштабованість, географічна віддаленість збережених даних і додаткові механізми захисту. Особливо ефективним є комбіноване – гібридне рішення, при якому поєднуються локальні та хмарні ресурси, що дозволяє зменшити час відновлення та забезпечити надійний захист у разі катастроф.

Окрему увагу слід приділити побудові стратегії резервного копіювання. Ефективною вважається модель, що базується на правилі 3-2-1: мати щонайменше три копії даних, зберігати їх на двох різних носіях, причому одну з копій обов’язково за межами основної локації. Важливо також передбачити регулярне автоматичне створення копій, аби виключити людський фактор. Копії повинні бути зашифровані, щоб унеможливити їхнє викрадення у разі компрометації сховища. Ще один критичний елемент – це періодичне тестування процесу відновлення, адже лише у такий спосіб можна впевнитися, що резервні дані є придатними до використання і відновлення справді можливе.

Сучасні кіберзагрози, зокрема атаки програм-вимагачів (ransomware), становлять особливу небезпеку для організацій. У таких випадках зловмисники шифрують важливу інформацію та вимагають викуп за її розблокування. Якщо резервне копіювання здійснюється

неправильно або резервні копії зберігаються в доступному для шкідливого ПЗ середовищі, жертва може опинитися без жодної можливості відновити інформацію. Захистом від цього є використання так званих незмінних резервних копій (immutable backups), які не можуть бути змінені або видалені протягом визначеного періоду часу. Такий підхід значно знижує ризик втрати даних навіть у разі масштабної атаки.

Загалом, резервне копіювання – це не лише технічний процес, а стратегічна ініціатива, яка вимагає системного підходу, постійного оновлення та інтеграції з іншими інструментами кібербезпеки. Організації, що інвестують у створення надійної інфраструктури для збереження резервних копій, мають значно вищі шанси швидко відновити свою роботу після інциденту і мінімізувати можливі втрати.

Висновок. Технології резервного копіювання є критичним компонентом кіберзахисту в умовах постійно зростаючих загроз. Ефективна стратегія бекапу дозволяє не лише зберігати доступ до даних у випадку атаки, а й забезпечує швидке відновлення бізнес-процесів. Для досягнення високої стійкості до кіберзагроз, організаціям необхідно впроваджувати системний підхід до резервного копіювання, включаючи вибір надійних технологій, регулярне оновлення стратегій та постійний моніторинг їх ефективності.

УДК 004.056:519.1

Павликевич А. М. ORCID: 0009-0006-9216-4353
(Національний університет «Львівська політехніка»)

ПОБУДОВА ОБ'ЄДНАНОЇ ОНТОЛОГІЇ ЗАГРОЗ ТА ЗАХОДІВ ЗАХИСТУ ДЛЯ АНАЛІЗУ РИЗИКІВ КІБЕРБЕЗПЕКИ ОРГАНІЗАЦІЇ

У цій доповіді розглядається метод автоматизованої інтеграції локальних даних про ресурси підприємства (зокрема інформації із систем інвентаризації програмного забезпечення та сканування вразливостей) з базами знань (таких, як MITRE ATT&CK, D3FEND, NVD, NIST 800-53) в об'єднану онтологію. Актуальність теми зумовлена ускладненням IT-інфраструктур, зростанням кількості кібератак і, водночас, відсутністю єдиного підходу до систематичного опису способів атак і методів оборони, що ускладнює процес кількісної оцінки ризиків.

Основна ідея полягає у створенні семантичної моделі, яка дає змогу об'єднати декілька масивів даних, що традиційно існують окремо. З боку глобальних баз знань застосовуються MITRE ATT&CK, що описує техніки й тактики атакуючих, та D3FEND, що каталогізує оборонні дії; у поєднанні з NVD (де зберігаються дані про вразливості CVE, відповідні CPE та рівні ризику CVSS) і стандартом NIST 800-53 (що містить рекомендації й контролі безпеки). Ці знання доповнюються специфічною інформацією підприємства – передусім даними інвентаризації ПЗ та результатами сканування вразливостей, для створення бази знань про безпеку підприємства. Таким чином, у єдиному просторі опису можна пов'язати: конкретні вразливості (CVE) зі станом серверів чи робочих станцій (зокрема, яка версія ПЗ встановлена, чи містить вона відомі CVE), а також з'ясувати, які саме техніки ATT&CK може застосувати зловмисник для експлуатації цих вразливостей, і які оборонні дії (D3FEND чи заходи з NIST) варто реалізувати, щоби знизити ризики.

Для досягнення такої інтеграції пропонується екосистема RDF/OWL2, яка забезпечує формальну семантику моделі, що дозволяє однозначно визначати взаємозв'язки між сутностями (наприклад, вразливість CVE-2023-XXXX може бути пов'язана з технікою T1059, а техніка T1059 пом'якшується певною дією з D3FEND; при цьому NIST 800-53 описує загальний контроль, який реалізує цю дію).

У пропонованій семантичній моделі всі ці зв'язки можуть бути записані у вигляді триплетів (RDF), з використанням унікальних URI для кожного CVE, техніки, контролю тощо. Внаслідок цього аналітик може за допомогою SPARQL-запиту миттєво з'ясувати, які хости (з локальної інвентаризації) мають вразливість, що відповідає певній техніці ATT&CK і, зважаючи на це, підібрати релевантні контрзаходи D3FEND чи NIST. Більше того, у семантичному просторі логічні вивідники (reasoner) здатні генерувати нові факти: якщо певна вразливість і техніка, а також певний контрзахід пов'язані, модель може в автоматичному режимі вказувати, що впровадження цього контрзаходу потенційно нівелює загрозу.

У доповіді показується, як згадана семантична модель може використовуватися під час побудови дерева атак (Attack Defense Tree або ADT). Оскільки у моделі вже є інформація про CVE, відповідні Exploitability Score чи EPSS, і вона пов'язана з ATT&CK-технікою, що експлуатує ці вразливості, формування зовнішніх вузлів (leaf nodes) у ADT стає майже автоматичним: кожен такий вузол отримує власну ймовірність (близьку до exploitability), а дії оборони (за D3FEND чи NIST 800-53) можуть відображатися як «вузли захисту» ("defense nodes"). Семантична модель дозволяє логічно виводити такі факти й оперативно відображати зміни у стані безпеки (коли інвентаризація чи сканери вразливостей виявляють нові факти). Існує також можливість систематичного контролю якості даних, що надходять із різних джерел.

Таким чином, вибір об'єднаної семантичної онтології (D3FEND, ATT&CK, NVD, NIST 800-53, локальні ресурси), описаної за допомогою RDF/OWL2, дає змогу поєднувати методи аналізу ризиків (ADT) із даними про конфігурації та вразливості, отриманими

з автоматизованих систем управління, що мінімізує суб'єктивізм у прийнятті рішень з ефективності системи безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Akbar K. A., Rahman F. I., Singhal A., Khan L., Thuraisingham B. The Design and Application of a Unified Ontology for Cyber Security. In V. Muthukkumarasamy, S. D. Sudarsan, R. K. Shyamasundar (Eds.) // Information Systems Security. 2023. Vol. 14424. P. 23–41. Springer Nature Switzerland. URL: https://doi.org/10.1007/978-3-031-49099-6_2.

2. Hu X., Cheng D., Chen J., Jin X., Wu B. Multiontology Construction and Application of Threat Model Based on Adversarial Attack and Defense Under ISO/IEC 27032 // IEEE Access. 2022. Vol. 10. P. 117955–117972. IEEE Access. URL: https://doi.org/10.1109/ACCESS.2022.3220637.

3. Huang C.-C., Huang P.-Y., Kuo Y.-R., Wong G.-W., Huang Y.-T., Sun Y. S., Chang Chen M. Building Cybersecurity Ontology for Understanding and Reasoning Adversary Tactics and Techniques. 2022 IEEE International Conference on Big Data (Big Data), 4266–4274. URL: https://doi.org/10.1109/BigData55660.2022.10021134.

4. Kougioumtzidou A., Papoutsis A., Kavallieros D., Mavropoulos T., Tsikrika T., Vrochidis S., Kompatsiaris I. An End-to-End Framework for Cybersecurity Taxonomy and Ontology Generation and Updating. 2024 IEEE International Conference on Cyber Security and Resilience (CSR), 247–254. URL: https://doi.org/10.1109/CSR61664.2024.10679346.

5. Maunero N., De Rosa F., Prinetto P. Towards Cybersecurity Risk Assessment Automation: An Ontological Approach. 2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 0628–0635. URL: https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361456.

6. Rafiey P., Namadchian A. Mapping Vulnerability Description to MITRE ATT&CK Framework by LLM. 2024. URL: https://doi.org/10.21203/rs.3.rs-4341401/v1.

УДК 004.5

канд. техн. наук **Сколоздра М. М.** ORCID: 0009-0004-4559-0101
студент **Куриляк А. І.**
(Національний університет «Львівська політехніка»)

МОДЕЛЮВАННЯ ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ ДЛЯ ПІДВИЩЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНІЗАЦІЯХ

Розглянуто підходи до моделювання професійної компетентності працівників як інструменту підвищення рівня інформаційної безпеки в організаціях. Обґрунтовано необхідність інтеграції психофізіологічних моделей у систему управління інформаційною безпекою відповідно до вимог міжнародних стандартів ISO/IEC 27001. Запропоновано модель аналізу та оцінювання функціонального стану працівників, що дозволяє прогнозувати їхню компетентність в інформаційній безпеці підприємства. Наведено практичні рекомендації щодо впровадження адаптивних методів управління персоналом у контексті системи управління інформаційною безпекою, що забезпечують зменшення ризиків, пов'язаних із впливом людського фактору.

Вивчення системи управління інформаційною безпекою (СУІБ) в Україні та підкріплення її практичним досвідом дозволяють зробити висновок, що людський фактор і науковий підхід до його вивчення вимагають ретельних досліджень. Аналіз літературних джерел свідчить, що сучасні методи менеджменту персоналу у рамках СУІБ в Україні ще не знайшли широкого використання.

У сучасному цифровому суспільстві інформаційна безпека є критичним компонентом ефективної діяльності будь-якої організації. Через це виникає потреба у всебічному аналізі людського фактору в рамках СУІБ. Зокрема, увага зосереджується на оцінці та оптимізації параметрів працездатності персоналу, особливо в дослідних лабораторіях, де інтелектуальна праця відіграє вирішальну роль.

Ефективність СУІБ значною мірою залежить від людського ресурсу. Підвищення вимог до професіоналізму, здатності до навчання, командної роботи та творчого мислення працівників є необхідною умовою захисту інформаційних активів організації. Професійний відбір, постійний та періодичний контроль функціонального стану персоналу повинні базуватись на стандартизованих, системних підходах, що відповідають вимогам ISO/IEC 27001 [0] та супутнім нормативам.

Функціональний стан працівника можна визначити як багатовимірний образ психофізіологічного стану людини, що впливає на діяльність людини. Він має багаторівневу природу і тут можна оцінювати наступних три його рівні [2; 3]:

- загальний – генетично визначений, який зумовлює принципову придатність людини до певної професії;
- віковий – визначає зміни динаміки професійно важливих психофізіологічних якостей, які є результатом професійного старіння працівника, сезонних впливів, хвороб тощо;
- поточний (оперативний) – визначає короткотермінові (щоденні, щотижневі) зміни, які забезпечують готовність до конкретної діяльності, включають щоденні й більш швидкоплинні зміни стану чи навіть настрою працівника.

Відповідно до функціонального стану психофізіологічний профіль людини можна описати наступною моделлю [4; 5]:

$$PPS = f\,(C, T, Fl, St), \tag{1}$$

де $C = C(p)$ – множина психологічних і фізіологічних параметрів (метаболізм, сила й рухливість нервових процесів);

$T = T(p)$ – множина психофізіологічних параметрів, які залежать від статі, рівня освіти, тренування, старіння, хвороб тощо;

Fl = Fl(*p*) – множина передбачуваних коливань психофізіологічних показників на середніх інтервалах часу (щоденні, упродовж робочого дня);

St = St(*p*) – стохастичні параметри, які швидко замінюються на коротких інтервалах часу (хвилини, секунди) і вимагають безперервного контролю в реальному часі, щоб оцінити й передбачити зміни працездатності працівника. Можна сказати, що *St*(*p*) визначає рівень ризику небажаних змін функціонального стану перед виконанням певних завдань.

Методи аналізу можуть відрізнятися залежно від напряму діяльності підприємства. На практиці інформація щодо функціонального стану може використовуватися з метою ретроспективного аналізу причин подій, а прогноз – це нечітка величина, тому може бути оцінений лише як імовірність зміни чи виникнення того чи іншого функціонального стану, тоді як інформація щодо працездатності, яка є проявом реалізації працівником свого психофізіологічного профілю у зовнішньому світі, може бути корисною і практично досяжною для поточної оцінки та прогнозу ефективності інформаційного захисту на підприємстві.

Застосування математичних моделей дозволяє не лише контролювати, але й прогнозувати компетентність персоналу в інформаційній безпеці підприємства. Це особливо важливо для запобігання інцидентам інформаційної безпеки. Оцінка ефективності моделі базується на оптимізації функціонала якості, що дозволяє адаптувати управлінські рішення у реальному часі.

Висновки

На підставі результатів проведеного дослідження зроблено висновки щодо сутності кадрової політики персоналу організації, методологічних, методичних і концептуальних засад її формування та реалізації.

Формуванню системи оціночних характеристик кадрової політики персоналу підприємства сприяє уточнення її класифікаційної бази, зокрема, вибір параметрів та інформаційних потоків.

Аналіз природи людини як фахівця показує, що її складність призводить до надзвичайної диференціації здібностей сприймати, пізнавати й оцінювати якість як на професійному, так і на побутовому рівнях. У формуванні «нової свідомості», нової філософії, індивідуальної та суспільної діяльності сучасної людини, який відповідатиме високим моральним вимогам, істотно сприятиме інтеграції у світовий простір. Необхідні оригінальні технології виховання професійних якостей, здатності до творчого, цілеспрямованого мислення, можливості ретельно і плідно аналізувати нестандартні ситуації.

У перспективі концептуальною основою сучасної кадрової політики підприємств України може виступити маркетинг персоналу. Його використання призведе до демократизації кадрової політики та розроблення передумов відтворення на практиці актуальних принципів економічного зростання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27001:2022 – Система Менеджменту Інформаційної Безпеки.

2. Сколоздра М, Байцар Р. Роль особистості у професійній діяльності // Психологія і суспільство. № 4 (30). 2007. С. 132–137.

3. Буров О. Ю. Ергономічні основи розробки систем прогнозування працездатності людини-оператора на основі психофізіологічних моделей діяльності / Автореф. дисс. докт. техн. наук. Харківська національна академія міського господарства. Харків. 2007. 44 с.

4. Юзевич В. Моделювання кваліфікації персоналу / В. Юзевич, Р. Байцар, М. Сколоздра // Стандартизація, сертифікація, якість. 2008. № 4. С. 65–69.

5. Сколоздра М. Оптимізація параметрів професійного відбору персоналу дослідних лабораторій / М. Сколоздра, Л. Сопільник, Р. Байцар // Вісник Національного технічного університету «ХПІ». 2010. № 46. С. 215–220.

УДК 355/359
д-р техн. наук, професор **Сніцаренко П. М.** ORCID: 0000-0002-6525-7064 (ЦВСД НУОУ)
канд. техн. наук, ст. наук. співроб. **Саричев Ю. О.** ORCID: 0000-0003-1380-4959 (ЦВСД НУОУ)
д-р філософії **Грицюк В. В.** ORCID: 0000-0002-3146-1956 (ЦВСД НУОУ)
Зубков В. П. ORCID: 0009-0008-5755-2339 (ЦВСД НУОУ)
Піщанський Ю. А. ORCID: 0000-0003-4392-3318 (ЦВСД НУОУ)

ПРОБЛЕМНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІБЕРПРОСТОРУ В ІСНУЮЧІЙ СИСТЕМІ КІБЕРОБОРОНИ УКРАЇНИ

Вступ. У цей час, поряд із традиційними сферами "Земля", "Море", "Повітря" та "Космос", інформаційний простір став ареною активного протиборства. Державами світу здійснюється цілеспрямоване опанування цього простору в інтересах реалізації своїх національних інтересів. Це стало можливим завдяки бурхливому розвитку протягом останніх кількох десятиліть інформаційних технологій та інформаційних систем на їх основі, що призвело до утворення потужного сегмента загального інформаційного простору – простору електронних інформаційних ресурсів, який отримав назву "кіберпростір".

Виконання завдань у кіберпросторі воєнної сфери сьогодні здійснюють відповідні підрозділи збройних сил та спецслужб провідних країн світу. При цьому їх діяльність може бути реалізована шляхом нанесення негативного впливу по об'єктах інформаційної сфери противника або ментальності його соціального середовища. Таким чином, виникає конфліктна ситуація у кіберпросторі, яка, зокрема, може мати, у тому числі й воєнний характер.

З цієї причини, а також в умовах повномасштабної збройної агресії, виникла загальнодержавна проблема кібероборони України як один із необхідних механізмів протидії гібридним воєнним загрозам та агресії у кіберпросторі.

Постановка задачі. Вперше питання щодо кібероборони України було визначено у Стратегії кібербезпеки України (2016 рік) як відбиття воєнної агресії у кіберпросторі [1]. У цьому документі Міністерству оборони (МО) України та Генеральному штабу (ГШ) Збройних Сил (ЗС) України доручалося, серед іншого, здійснювати заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі. Проте таке формулювання завдання виглядало занадто узагальненим, принаймні з огляду на те, що у цьому документі не розкрито поняття "воєнна агресія у кіберпросторі", а також що таке її "відбиття". Такий стан не дозволяє належним чином розуміти подальші практичні дії щодо удосконалення системи кібероборони держави та провокує довільне трактування цього завдання.

Отже, чинне законодавство України не дозволяє у повному обсязі окреслити сучасний обрис системи, яка має забезпечити реалізацію перспективної моделі кібероборони держави.

У Законі України "Про основні засади забезпечення кібербезпеки України" [2] від 2017 року наведено значення терміну "кібероборона". Крім того, МО України, ГШ ЗС України, відповідно до компетенції, визначено перелік завдань щодо забезпечення кібербезпеки, зокрема щодо здійснення заходів із підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони). Це завдання безпосередньо вказує на те, що кібероборона є складовою забезпечення кібербезпеки держави та зобов'язує МО України і ГШ ЗС України здійснювати заходи з питань кібероборони держави.

Водночас, цього ж року в Закон України "Про оборону України" [3] від 1991 року було внесено наступні зміни, зокрема:

здійснення заходів з кібероборони (активного кіберзахисту) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройної агресії.

Із цього Закону випливає, що *кібероборона – це активний кіберзахист*, що є третім варіантом для розуміння сутності кібероборони.

Таким чином, маємо три варіанти визначень, що містяться в законодавстві України, за якими сутність кібероборони держави у повному обсязі зрозуміти неможливо. При цьому, неможливо також уявити шляхи реалізації у кіберпросторі більшості перелічених заходів.

Отже, поняття “кібероборона” в законодавстві України виписане недосконало, що потребує невідкладного усунення.

Заразом, при вирішенні питань створення та функціонування перспективної системи кібероборони України виникає потреба уточнення переліку заходів такої системи з урахуванням особливостей національного законодавства у сфері оборони, кібербезпеки та, зокрема, кібероборони, що залишилися поза межами як Стратегії кібербезпеки України [4] від 2021 року, так і Плану її реалізації [5] від 2022 року. Це спричиняє потребу коригування цього Плану у питанні кібероборони.

Метою доповіді є огляд ключових положень з аналізом існуючої системи кібероборони України як складової національної системи кібербезпеки.

Викладення основного матеріалу. Загальне поняття системи, за даними різних словникових і енциклопедичних джерел, зводиться до того, що це множина взаємопов’язаних елементів, що утворюють єдине ціле, взаємодіють із середовищем та між собою, і мають єдину мету.

Систему визначають також як сукупність елементів та їх властивостей, взаємодія між якими зумовлює появу якісно нової цілісності. Наявність істотних стійких зв’язків (відношень) між складовими системи або (та) їхніми властивостями є важливим її атрибутом [6]. При цьому різновидів систем за ознаковими чинниками є чимало. Водночас, і варіантів реалізації системи кібероборони України, зокрема залежно від змісту чинних законодавчих актів, відповідно до представленої схеми на рисунку 1, може бути декілька.

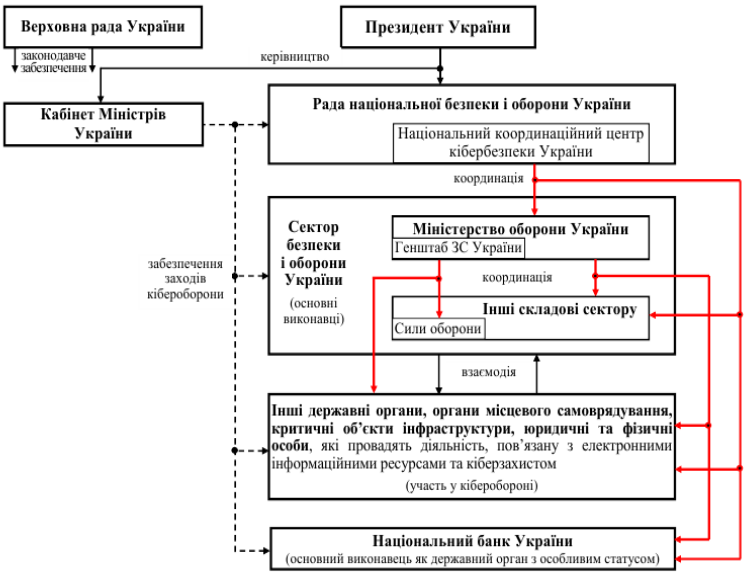

Рис. 1. Загальна схема існуючої системи кібероборони України

Проте важливо зрозуміти сутність та рівень дієздатності системи кібероборони держави, яка відповідає чинному національному законодавству України. Тому зосередимо увагу на розгляді логіко-описового варіанту існуючої системи кібероборони України (рис. 1).

Із формальної точки зору система на рисунку 1 виглядає переконливо, але є ряд принципових особливостей, які перешкоджають гармонійній та однозначній її реалізації на практиці. Відмічаючи певні особливості, що характеризують цю загальну структурну схему системи кібероборони України, окреслимо ряд проблемних питань, які потребують відповіді для здійснення адекватних практичних заходів як на рівні держави, так і локальному рівні.

1. У цій схемі має місце дублювання функції координації у спільному виконанні завдань кібероборони з боку Ради національної безпеки і оборони України (через Національний координаційний центр кібербезпеки) та МО України. Крім цього, значна роль у питанні координації щодо кібероборони належить ГШ ЗС України, що в сукупності з попереднім призводить до додаткового дублювання цієї функції по відношенню до суб’єктів, задіяних

у цей процес. Але у виконанні цієї функції координації повноваження названих державних органів чинне законодавство не розділяє, відповідного установленого порядку дій не визначає.

На наш погляд, невдалою спробою усунення зазначених недоліків було внесення окремим Законом України [7] змін до Законів України "Про Державну службу спеціального зв'язку та захисту інформації України" [8] та "Про основні засади забезпечення кібербезпеки України" [2].

Тепер одним із завдань Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку України) є "активна протидія агресії у кіберпросторі", для чого у цьому відомстві запроваджується відповідна структура та окремий Центр активної протидії агресії у кіберпросторі.

Звернемо увагу на зміни, застосовані в законі [2] в редакції:

система активної протидії агресії у кіберпросторі – сукупність організаційних, правових, наукових і технічних заходів, спрямованих на підвищення рівня кіберзахисту держави шляхом здійснення впливу на інформаційні (автоматизовані), електронно-комунікаційні, інформаційно-комунікаційні системи держави-агресора, джерела походження кіберзагроз та кібератак.

По-перше, це визначення суперечить поняттю кіберзахисту, визначеному Законом України "Про основні засади забезпечення кібербезпеки України" [2], відповідно призначенню та повноваженням Держспецзв'язку України.

По-друге, власне кіберзахист за визначенням є лише одним з елементів активної протидії агресії у кіберпросторі, тому наведене в законі [2] визначення є невдалою спробою узагальнення.

І по-третє, якщо в Держспецзв'язку України створюється така система та профільний структурний підрозділ з метою і правом здійснення впливу на інформаційні системи в кіберпросторі держави-агресора, то функціонально – це аналог кібервійськ, і тоді створення в системі МО України кібервійськ для стримування збройної агресії у кіберпросторі та надання відсічі агресору (як головний напрям досягнення стратегічної цілі С.1 "Дієва кібероборона" [10]) вбачається зайвим державним заходом.

Таким чином, таке дублювання щодо координації без уточнення повноважень та установлення порядку відповідних дій є принциповим системним недоліком існуючої структурної схеми системи кібероборони України, що дестабілізує зазначену систему та створює окрему проблему, яка потребує невідкладного усунення.

2. Відсутнє нормативно-правове тлумачення положення (яке випливає із Закону України "Про національну безпеку України" [9]) щодо взаємодії інших державних органів та органів місцевого самоврядування, що здійснюють свої функції у спільному виконанні завдань кібероборони з органами, які входять до складу сектору безпеки і оборони. Іншими словами, потребує уточнення: хто, з ким, за яких умов, на якій підставі, в якому обсязі та протягом якого часу має взаємодіяти в інтересах виконання завдань кібероборони. Цей недолік невизначеності спричиняє іншу проблемну ситуацію, яка також перешкоджає реалізації системи кібероборони держави та потребує її усунення (відповідно до Плану реалізації Стратегії кібербезпеки України [5]).

3. Принциповий проблемний характер мають питання термінологічного блоку щодо кібероборони як понятійної основи цієї нової предметної галузі діяльності, без чого неможливо ні розвивати її теоретичні основи, ні розумітися в практичних заходах. Особливість цього проблемного питання полягає в тому, що оскільки кібероборона є складовою загального процесу як забезпечення кібербезпеки України, так і оборони держави, то теорія і практика кібероборони має ґрунтуватися на раціональному синтезі термінологічних баз кібербезпекової та оборонної галузей. Зважаючи на новизну ситуації, розробка такої синтетичної бази на сьогодні першочергово є актуальним науковим завданням.

У Законі України "Про основні засади забезпечення кібербезпеки України" [2] визначено:

кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії.

Із приводу законодавчого визначення поняття кібероборони виникає багато запитань для його розуміння.

По-перше, в наведеному визначенні ставиться широка мета: забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії, у чому криється перший сумнів щодо коректності такого визначення.

Для розкриття цього розпишемо спрямованість заходів (завдань) кібероборони роздільно:

на забезпечення захисту суверенітету держави;

на забезпечення захисту обороноздатності держави;

на запобігання виникненню збройного конфлікту;

на відсіч збройній агресії.

Поняття захисту суверенітету держави (самостійності, повної незалежності держави від інших держав у її внутрішніх справах та зовнішній політиці), "поглинає", поряд з іншим, справи захисту обороноздатності держави, запобігання виникненню збройного конфлікту, відсічі збройній агресії, оскільки останні є елементами захисту суверенітету держави. Тому у тексті визначення ці три напрями формально є зайвими, або має бути інша інтерпретація змісту, що звужує та конкретизує мету кібероборони.

По-друге, незрозуміло, яким чином можуть бути реалізовані у кіберпросторі усі види перерахованих у наведеному визначенні заходів.

По-третє, доповнення статті 3 Закону України "Про оборону України" [3] контекстно визначає кібероборону як "активний кіберзахист" без необхідної деталізації цього словосполучення, що не додає ясності до основного визначення.

По-четверте, доповнення статті 4 Закону України "Про оборону України" [3] (щодо відсічі збройній агресії проти України) визначає: "На підставі відповідного рішення Президента України ЗС України разом з іншими військовими формуваннями розпочинають воєнні дії, у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі". Це доповнення тільки додатково "розмиває" основне визначення, оскільки у діючій військовій термінології поняття "розвідувальна операція" відсутнє, інформаційно-психологічна операція до виду "спеціальних операцій" не відноситься, а додаток "тощо" дає привід для вільного застосування будь-яких заходів у кіберпросторі, що не завжди допустимо.

По-п'яте, завдання щодо кібербезпеки для МО України, ГШ ЗС України відповідно до законодавства [2] в редакції: "здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони)" контекстно означає, що кібероборона – це відбиття воєнної агресії у кіберпросторі. Така формула відповідає розумінню відповідно до вже скасованої Стратегії кібербезпеки України [1] та суттєво відрізняється від вищенаведеного основного визначення. Також, маємо невідповідність змісту визначення в [2] поняття кібероборони, зокрема як складової оборони держави, сутності оборони України, визначеної Законом України "Про оборону України" [3] в редакції: оборона України – система політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних, інших заходів держави щодо підготовки до збройного захисту та її захист у разі збройної агресії або збройного конфлікту. Як видно, на відміну від цього поняття, у наведеному в [2] визначенні відсутні фази підготовки кібероборони та відсічі агресії проти України у кіберпросторі, тобто логіка зазначеного раціонального термінологічного синтезу належним чином не спрацювала, а тому за чинним законодавчим визначенням неможливо адекватно структурувати послідовність необхідних для кібероборони дій та заходів.

Наведене засвідчує, що поняття кібероборони в Законі України “Про основні засади забезпечення кібербезпеки України” [2] виписане некоректно.

Інші положення законодавства України не додають належного роз’яснення його сутності, достатнього для однозначного розуміння. Такий стан цього питання у сукупності призводить до суб’єктивізму як окремої проблеми в шляхах практичної реалізації необхідних заходів в межах структури системи кібероборони держави (рис. 1).

Щодо інших термінів та словосполучень зазначимо наступне. Найбільш часто вживаними у публікаціях стосовно кібероборони є такі словосполучення як “воєнна агресія у кіберпросторі” та “відбиття воєнної агресії у кіберпросторі”.

Поняття “воєнна агресія у кіберпросторі” на рівні законодавства України визначене в Стратегічному оборонному бюлетені України [10] в редакції:

воєнна агресія в кіберпросторі – здійснення системних та масштабних дій проти України в кіберпросторі іноземними державами (групами держав), зокрема із залученням кіберпідрозділів військових формувань, розвідувальних та спеціальних служб, включаючи використання кіберозброєння та інших спеціальних засобів впливу в кіберпросторі (зокрема, опосередковано шляхом приховування джерел їх походження).

Але таке визначення в його ознаковій частині викликає принципові питання:

по-перше, не усі “масштабні дії проти України в кіберпросторі іноземними державами (групами держав)” можуть вважатися воєнною агресією – “здійснення …” іноземними державами (групами держав) або “масштабність” не є ознакою “воєнної агресії” (той самий вірус NotPetya зовнішнього впливу, що призвів до масштабних збитків в Україні та інших країнах, не визнано воєнною агресією);

по-друге, “розвідувальні та спеціальні служби” можуть бути цивільними службами, що діють проти цивільних об’єктів України, тоді де тут ознака “воєнної агресії”?

по-третє, невизначеним, отже незрозумілим, є вжитий термін “кіберозброєння”, принаймні це не тільки “засіб впливу в кіберпросторі”.

Тому наведене визначення потребує уточнення. Інше поняття “відбиття воєнної агресії у кіберпросторі” в законодавстві України не визначене. Не зустрічається його тлумачення і в доступних фахових наукових виданнях. У цій ситуації, на перший погляд, можна посилатися на статтю 4 Закону України “Про оборону України” [3], де міститься положення (на яке вище вже посилалися), що у разі збройної агресії ЗС України розпочинають воєнні дії, у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі. Якщо так, тоді виходить, що “відбиття воєнної агресії у кіберпросторі” (як варіант, це також сутність кібероборони, що зазначалося вище) означає проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі. За цією логікою відбиття воєнної агресії у кіберпросторі (кібероборону) мають здійснювати Сили спеціальних операцій ЗС України, оскільки, відповідно до ряду законів України [3; 11; 12], лише вони проводять спеціальні операції, включно зі спеціальною розвідкою та інформаційно-психологічними діями. Через це знову, як і у випадку з Держспецзв’язком України, виникає питання щодо доцільності створення в системі МО України кібервійськ (відповідно до Указів Президента України про Стратегію кібербезпеки України [4] та про невідкладні заходи з кібероборони держави [13]), що суперечить положенням цих законів.

Отже, для виправлення стану цієї законодавчої колізії в реалізації системи кібероборони України має бути виважене законодавче визначення поняття “відбиття воєнної агресії у кіберпросторі”.

Висновки

1. Аналіз схеми існуючої системи кібероборони України засвідчив наявність її головної системної вади – дублювання державними органами функції координації без законодавчого уточнення їх повноважень та установлення порядку відповідних дій. Це дестабілізує систему та створює окрему проблему невизначеності, без усунення якої неможливо досягти гармонійності реалізації системи кібероборони України.

2. Інше проблемне питання в системі кібероборони України полягає в неочевидності порядку взаємодії інших державних органів та органів місцевого самоврядування, що здійснюють свої функції в спільному виконанні завдань кібероборони з органами, які входять до складу сектору безпеки і оборони, без окремого нормативно-правового тлумачення.

3. Результати аналізу термінологічного блоку законодавства, що впливає на розуміння сутності кібероборони України, вказують на його недосконаліть. Це дозволяє стверджувати, що існуючий стан теоретичних засад як щодо кібербезпеки, так і складової кібероборони, основу чого закладає понятійно-категорійний апарат (термінологія), є незадовільним. У цьому є одна із головних причин невисокої якості відповідної нормативно-правової бази, що в практиці реалізації моделі кібероборони держави призводить до суб'єктивності, хаотичності та ситуативного характеру дій.

4. Термінологічну базу галузі кібербезпеки, у тому числі кібероборони, і її належні теоретичні засади слід невідкладно розвивати та удосконалювати, та на цій основі покращувати законодавство України задля реалізації кращих практик, зокрема щодо кібероборони.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від 15.03.2016 № 96/2016. URL: http://president.gov.ua.

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: http://zakon2.rada.gov.ua.

3. Про оборону України: Закон України від 06.12.1991 № 1933-XII (зі змінами). URL: http://zakon.rada.gov.ua.

4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 № 447/2021. URL: http://president.gov.ua.

5. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про План реалізації Стратегії кібербезпеки України": Указ Президента України від 01.02.2022 № 37/2022. URL: http://president.gov.ua.

6. Поняття системи та її властивості. URL: http://lib-net.com/content/11017_Ponyattya_sistemi_ta_ii_vlastivosti.html.

7. Про внесення змін до деяких законів України щодо забезпечення формування та реалізації державної політики у сфері активної протидії агресії у кіберпросторі: Закон України від 28.07.2022 № 2470-IX. URL: http://zakon2.rada.gov.ua.

8. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV. URL: http://zakon2.rada.gov.ua.

9. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: http://zakon.rada.gov.ua.

10. Про рішення Ради національної безпеки і оборони України від 20 травня 2021 року "Про Стратегічний оборонний бюлетень України: Указ Президента України від 17.09.2021 № 473/2021. URL: http://president.gov.ua.

11. Про розвідку: Закон України від 17.09.2020 № 912-IX. URL: http://zakon.rada.gov.ua.

12. Про Збройні Сили України: Закон України від 06.12.1991 № 1934-XII (зі змінами). URL: http:// zakon.rada.gov.ua.

13. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави: Указ Президента України від 26.08.2021 № 446/2021. URL: http:// president.gov.ua.

УДК 004.8:351.78:623.4

канд. техн. наук, доцент **Чесановський І. І.** ORCID: 0000-0002-8161-3276
(НАДПСУ ім. Богдана Хмельницького)
Площик А. С. ORCID: 0000-0002-7034-1930 (НАДПСУ ім. Богдана Хмельницького)

ВПРОВАДЖЕННЯ МУЛЬТИАГЕНТНИХ МОДЕЛЕЙ В СИСТЕМІ МОНІТОРИНГУ ДЕРЖАВНОГО КОРДОНУ

Сучасні загрози в галузі безпеки державного кордону (нелегальна міграція, контрабанда) вимагають пошуку інноваційних підходів до побудови систем моніторингу, що в сучасних умовах утворюють основу системи інженерно-технічного контролю. Традиційні підходи побудови систем моніторингу схиляються до максимального насичення зони контролю різного типу засобами (сенсори, датчики, радари, засоби відеоспостереження, тощо), які часто не повною мірою реалізують свої потенційні можливості через відсутність дієвих моделей інтеграції даних, обмежену гнучкість системи управління та недосконаліть аналітичних інструментів. Це обумовлено тим, що традиційні системи, які ґрунтуються на централізованому управлінні та фіксованих алгоритмах, не здатні адаптуватися до динамічних змін, що значно обмежує їхню ефективність. Альтернативою в цьому контексті є мультиагентні системи (МАС), що стають ключовим інструментом для побудови розподіленого (децентралізованого) управління. На відміну від традиційних систем МАС базуються на розподілених автономних агентах – алгоритмічних (інформаційних) сутностях, здатних самостійно аналізувати дані, взаємодіяти з оточуючим середовищем і між собою та приймати рішення в реальному часі.

Для реалізації МАС необхідна потужна інформаційно-комунікаційна інфраструктура, що містить велику кількість обчислювальних вузлів та достатню пропускну здатність комунікаційної платформи для розгортання моделей розподілених обчислень, оскільки основою МАС є ціла мережа спеціалізованих агентів, кожен з яких виконує унікальну роль. Наприклад, у системі моніторингу державного кордону агенти спостереження (дрони, сенсори радари, відеокамери тощо), що забезпечують безперервний збір даних із контрольованих територій. Вони фіксують відео, теплові зображення, радіосигнали та інші типи інформації, формуючи первинний шар даних. Другий клас агентів відповідає за аналітику: завдяки технологіям машинного навчання вони ідентифікують аномалії, виявляють підозрілі об’єкти або незвичайні шаблони поведінки, наприклад, нетипову поведінку людей в пункті пропуску, рух транспорту поза встановленими маршрутами тощо. Наступний рівень – агенти прийняття рішень, які перетворюють зібрані і систематизовані дані на певні дії – аналізують та сигналізують про підвищений рівень загрози, формують рекомендації для прикордонних нарядів або автоматично активують додаткові ресурси (засоби фізичного впливу або блокування). Важливу роль відіграють комунікаційні агенти, які забезпечують синхронізацію між всіма компонентами системи, а також інтеграцію з зовнішніми структурами, такими як міжвідомчі та міждержавні бази даних, GIS-системи або інші міжнародні платформи безпеки.

Головна перевага концепції МАС – це здатність поєднувати швидкість, гнучкість і масштабованість. На відміну від централізованих систем, де збір і обробка даних залежать від єдиного вузла, МАС розподіляють навантаження між агентами, що в поєднанні з моделями розподілених обчислень дає змогу аналізувати інформацію паралельно та зменшує час реакції на загрози. Наявність в агентів власних моделей глибокого навчання дає змогу системі постійно вдосконалюватись, оскільки агенти адаптуються до нових даних (ознак загроз, тактик, реакцій). Крім того, архітектура системи є гнучкою і дає змогу легко (без технічної модернізації) додавати нових агентів будь-якого рівня в існуючу інфраструктуру. Це не лише підвищує ефективність системи моніторингу, але й знижує операційні витрати.

Таким чином, впровадження мультиагентних моделей у системі інженерно-технічного контролю державного кордону може бути стратегічним кроком до створення “розумного кордону”, який поєднує технології, людський потенціал і міжнародну співпрацю для протидії транскордонній злочинності.

канд. техн. наук **Яковлєв С. В.** (ВІТІ ім. Героїв Крут, КПІ ім. Ігоря Сікорського)
Кобець Д. С. (КПІ ім. Ігоря Сікорського)

RA-АНАЛІЗ СКЛАДНИХ ARX-ПЕРЕТВОРЕНЬ

ARX-криптосистеми будуються на основі простих операцій, доступних на рівні інструкцій процесорів: модульного додавання, побітового додавання, циклічних зсувів та, у розширеному розумінні, інших операцій логіки (ТА, АБО, нециклічних зсувів тощо). Через просту реалізацію та надвисоку швидкість роботи такі криптосистеми стали важливою частиною так званої «легкої криптографії» — напрямку, присвяченому розробці надійних алгоритмів для малоресурсних пристроїв та Інтернету речей. На ARX-дизайні побудовані такі широко розповсюджені криптопримітиви, як шифр ChaCha, геш-функції BLAKE2 та Skein, автентифікований шифр Ascon тощо.

Основними інструментами криптографічного аналізу ARX-криптосистем є диференціальний криптоаналіз, який у цьому контексті можна розглядати як за операцією побітового додавання [1], так і за операцією модульного додавання [2], а також обертальний криптоаналіз [3], який досліджує особливості зміни пар текстів, які відрізняються циклічним зсувом під час виконання обчислень. Через структурні та алгебраїчні особливості ARX-криптосистем обертальний криптоаналіз дозволяє будувати ефективні атаки розпізнавання, тому захищеність від нього наразі є однією з обов'язкових умов для надійних криптосистем цього типу. Втім виявилось, що підвищити стійкість до обертального криптоаналізу можна відносно простим шляхом – внесенням у схему додавань із константами, які мають нерегулярний вид.

У роботі [4] було запропоновано диференціально-обертальний криптоаналіз, який комбінує ідеї диференціального та обертального криптоаналізу і дозволяє оминути додавання із константами під час аналізу. Диференціально-обертальний криптоаналіз досліджує проходження через криптосистему пар текстів, які відрізняються одночасно і циклічним зсувом, і деякою різницею, яка в оригінальній роботі розглядалась відносно операції побітового додавання.

У цій роботі буде розвинуто запропонований авторами раніше підхід до диференціально-обертального криптоаналізу, у якому різниці між текстами розглядаються за додаванням за модулем 2^n [7]. Буде проаналізовано ARX-перетворення, які складаються з декількох послідовних операцій, та побудовано аналітичні вирази для оцінок імовірностей узагальнених диференціалів таких перетворень відносно модульного додавання.

Нехай $F: V_n \times V_n \to V_n$ – довільне відображення. *RA-диференціалом* $(r;\ \alpha, \beta \to \gamma)$ будемо називати трійку векторів $\alpha, \beta, \gamma \in V_n$ та ціле число r, $0 \le r < n$, які описують подію

$$F(x^r + \alpha, y^r + \beta) = \big(F(x, y)\big)^r + \gamma,$$

де u^r позначає циклічний зсув вектору u: $u^r = u <<< r$, а + позначає додавання $mod\ 2^n$.

Імовірність RA-диференціалу $arp^F(r;\ \alpha, \beta \to \gamma)$ – це імовірність наведеної події при випадковому виборі значень $x, y \in_R V_n$. Імовірності RA-диференціалів подібні до імовірностей звичайних диференціалів за модульним додаванням adp^F:

$$arp^F(r;\ \alpha, \beta \to \gamma) = \Pr_{x,y}\{F(x^r + \alpha, y^r + \beta) = \big(F(x, y)\big)^r + \gamma\},$$
$$adp^F(\alpha, \beta \to \gamma) = \Pr_{x,y}\{F(x + \alpha, y + \beta) = F(x, y) + \gamma\}.$$

У попередній роботі [7] було знайдено аналітичні вирази для RA-диференціалів базових ARX-перетворень; зокрема було показано, що:

1) $arp^+(r;\ \alpha, \beta \to \gamma) \neq 0$ тоді та тільки тоді, коли $\gamma \in \alpha + \beta + \mathbb{D}_{n,r}$, де $\mathbb{D}_{n,r}$ – так звана *множина Даума*: $\mathbb{D}_{n,r} = \{0, -1, 2^{n-r}, 2^{n-r} - 1\}$;

2) $arp^{<<<s}(r;\ \alpha \to \beta) \neq 0$ тоді та тільки тоді, коли $\beta \in \mathbb{B}_{n,s}(\alpha)$, де $\mathbb{B}_{n,s}(\alpha)$ – так звана *множина Берсона для вектора* α: якщо $\alpha = \alpha_{n-s} \parallel \alpha_s$, то

$$\mathbb{B}_{n,s}(\alpha) = \{\alpha_s \parallel \alpha_{n-s}, (\alpha_s - 1) \parallel \alpha_{n-s}, \alpha_s \parallel (\alpha_{n-s} + 1), (\alpha_s - 1) \parallel (\alpha_{n-s} + 1)\};$$

зокрема імовірність $arp^{<<<s}$ не залежить від значення r;

3) $arp^{\oplus}(r;\ \alpha, \beta \to \gamma) = adp^{\oplus}(\alpha, \beta \to \gamma)$ і так само не залежить від значення r.

Оскільки базові перетворення в ARX-системах зазвичай не є незалежними (наприклад, не розділяються рандомізованими ключами), для оцінки імовірності проходження RA-диференціалу через складне перетворення не можна просто перемножувати імовірності по кожній компоненті. У цій роботі ми наведемо аналітичні вирази для імовірностей RA-диференціалів або їх верхніх оцінок для найбільш вживаних ARX-конструкцій. Ці результати сформульовано у наступних двох теоремах.

Теорема 1. Нехай $f_s(x, y) = x^s \oplus y$, $F_s(x, y, z) = (x + y)^s \oplus z$; тоді

$$arp^{f_s}(r;\ \alpha, \beta \to \gamma) = adp^{f_s}(\alpha, \beta \to \gamma);$$
$$arp^{F_s}(r;\ \alpha, \beta, \delta \to \gamma) \leq \max_{\xi \in \mathbb{D}_{n,r}} \{adp^{f_s}(\alpha + \beta + \xi, \delta \to \gamma)\};$$

Теорема 2. Нехай $g_s(x, y) = x^s + y$, $G_s(x, y, z) = (x \oplus y)^s + z$; тоді

$$arp^{g_s}(r;\ \alpha, \beta \to \gamma) = \max_{\xi \in \mathbb{D}_{n,r}} \{adp^{<<<s}(\alpha \to \gamma - \beta - \xi)\};$$
$$arp^{G_s}(r;\ \alpha, \beta, \delta \to \gamma) \leq \max_{\substack{\xi \in \mathbb{D}_{n,r} \\ \eta \in \mathbb{B}_{n,s}(\gamma - \delta - \xi)}} \left\{adp^{\oplus}(\alpha, \beta \to (\gamma - \delta - \xi)^{-s} + \eta)\right\};$$

Бачимо, що в загальному випадку вдається звести аналіз складних ARX-перетворень до аналізу більш простих відображень, а імовірності RA-диференціалів оцінюються імовірностями звичайних диференціалів за модульним додаванням, для яких існують ефективні алгоритми обчислення (див. [2]). Побудовані оцінки використовують не більш ніж 16 різних складових, відповідно, легко будуються та перевіряються. Більш того, принципи виведення таких аналітичних оцінок можуть бути застосовані й до інших перетворень ще більш складної структури. Це дозволяє в сукупності одержувати обґрунтовані оцінки стійкості до RA-аналізу для ARX-криптосистем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lipmaa H., Moriai S. Efficient Algorithms for Computing Differential Properties of Addition // Fast Software Encryption. Springer Berlin Heidelberg. 2002. P. 336–350.

2. Lipmaa H., Wallén J., Dumas P. On the Additive Differential Probability of Exclusive-OR // Fast Software Encryption. 2004. P. 317–331.

3. Khovratovich D., Nikolic I. Rotational Cryptanalysis of ARX // Lecture Notes in Computer Science. 2010. P. 333–346.

4. Ashur I., Liu Y. Rotational Cryptanalysis in the Presence of Constants. Cryptology ePrint Archive, Report 826/2016. URL: https://eprint.iacr.org/2016/826.pdf.

5. Daum M. Cryptanalysis of Hash Functions of the MD4-Family (PhD thesis). 2005.

6. Berson T. Differential cryptanalysis mod 2^{32} with applications to MD5 // Advances in Cryptology – Eurocrypt'92. 1992. P. 71–80.

7. Кобець Д. С., Яковлєв С. В. Диференціально-обертальний криптоаналіз ARX-криптосистем за операцією модульного додавання // Теоретичні і прикладні проблеми фізики, математики та інформатики: матеріали XXII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (13−17 травня 2024 р., м. Київ, Україна). 2024. С. 213–215.

УДК 004.052.4: 006.3

аспірант **Яцина Д. Ю.** (ХНУ ім. В. Н. Каразіна)

ІННОВАЦІЇ В МУЛЬТИБІОМЕТРІЇ: ПОЄДНАННЯ КВАНТОВИХ ГЕНЕРАТОРІВ КЛЮЧІВ ТА МАШИННОГО НАВЧАННЯ

Вступ. Нині в умовах стрімкої цифровізації зростає потреба в забезпеченні надійності систем безпеки, котрі здатні ефективно забезпечувати захист персональних даних і протидіяти дедалі складнішим кіберзагрозам. Зокрема особливої актуальності набуває проблема ідентифікації особи на основі біометричних характеристик, зокрема у контексті мультимодальної біометрії – технології, що поєднує декілька типів біометричних ознак задля підвищення точності та стійкості систем автентифікації [1]. Однак традиційні біометричні системи мають низку вразливостей, пов'язаних із ризиками фальсифікації даних, недостатньою адаптивністю до змін середовища та обмеженою здатністю до самонавчання [2]. Зокрема в цій області одним із перспективних напрямів є інтеграція квантових генераторів ключів у мультимодальні біометричні системи. Тому, зважаючи на вищезазначене, виникає нагальна потреба щодо проведення дослідження, яке буде присвячене розвитку інноваційних методів забезпечення безпеки в мультимодальній біометрії на основі квантових генераторів ключів і машинного навчання, є своєчасним і суспільно значущим, так як його результати можуть мати як теоретичну цінність, так і прикладне значення для впровадження новітніх технологій захисту інформації.

Метою роботи є розробка та оцінка ефективності запропонованого підходу до підвищення захисту біометричних систем шляхом використання генераторів квантових ключів і глибоких нейронних мереж.

Основна частина. Запропонована в дослідженні методика передбачає використання квантового генератора випадкових чисел (QRNG) для створення криптостійких сесійних ключів і багатошарових нейронних мереж для обробки біометричних даних (відбитки пальців, райдужка, голос тощо). Вихідні дані нейромережі використовуються як захищені біометричні шаблони, що унеможливлює відновлення оригінальних даних. Для оцінки ефективності застосовується метрика точності, яка враховує рівні хибного прийняття (FAR) та відхилення (FRR). Оптимізація архітектури нейромереж, зокрема шляхом додавання додаткових шарів, дозволяє підвищити точність, стійкість до помилок та загальну безпеку системи автентифікації.

Ключ K, згенерований за допомогою квантового генератора випадкових чисел, забезпечує високий рівень криптографічної стійкості. У цьому випадку використовуються властивості квантової випадковості для створення повністю непередбачуваних ключів, що робить їх значно більш захищеними від атак порівняно з класичними генераторами випадкових чисел. Для побудови мультимоделі біометричної автентифікації застосовується багатошарова нейронна мережа.

У дослідженні брали участь 500 учасників, кожен з яких надає 10 біометричних зразків, зосереджуючись на ЕКГ та розпізнаванні облич. 6-шарова нейронна мережа обробляє біометричні дані, навчається на 5000 зразках та тестується на 2000 зразках. Довжина вектора ознак становить 256, а квантові ключі довжиною 1024 біти підвищують безпеку.

Система підтримує максимальний час обробки 15 мс на зразок, досягаючи мінімальної точності автентифікації 98 %, з коефіцієнтом помилкових прийняття (FAR) обмеженим 0,1 % та коефіцієнтом помилкових відхилень (FRR) на рівні 1,5 %. Прийнятні варіації забезпечують адаптивність до різних біометричних умов.

На рисунку 1 представлено результати: ЕКГ з однаковим коефіцієнтом помилок (%).

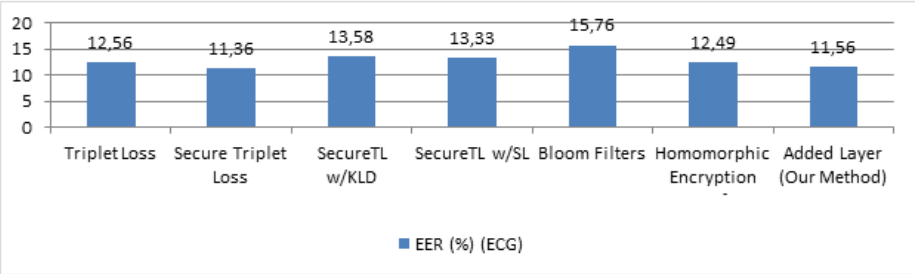

Рис. 1. ЕКГ з однаковим коефіцієнтом помилок (%)

На рисунку 2 представлено результати: рівний коефіцієнт помилок (%) (обличчя).

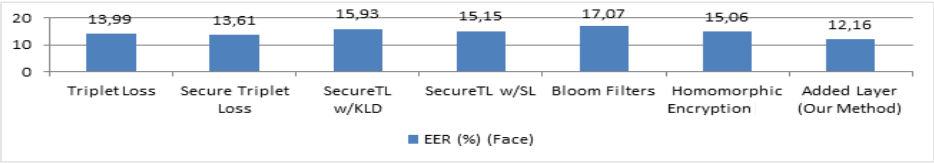

Рис. 2. Рівний коефіцієнт помилок (%) (обличчя)

Дослідження показало, що інтеграція генераторів квантових ключів із методами машинного навчання суттєво підвищує ефективність мультимодальних біометричних систем безпеки. Запропонований підхід дозволив знизити середню помилку рівності (EER) до 11,56 % для біометрії на основі ЕКГ та до 12,16 % для розпізнавання обличчя, що забезпечило вищу точність класифікації порівняно з традиційними методами. Досягнута точність автентифікації становить 98 %, що свідчить про високу надійність розпізнавання. При цьому рівень хибної відмови залишався на рівні 1,5 %, а хибного прийняття – лише 0,1 %, що мінімізує ризики несанкціонованого доступу та необґрунтованих відмов. Модель також підвищує захищеність біометричних шаблонів, знижуючи ризики їх скасування та зв’язності, що робить її придатною для застосування у сферах із підвищеними вимогами до безпеки.

Висновки. Дослідження показує, що поєднання генераторів квантових ключів із методами машинного навчання суттєво підвищує ефективність багатофакторних біометричних систем безпеки. Запропонований підхід дозволяє знизити коефіцієнт рівної помилки (EER) до 11,56 % для біометрії на основі ЕКГ та до 12,16 % для розпізнавання обличчя, демонструючи кращу точність класифікації порівняно з традиційними методами. Загальна точність автентифікації досягла 98 %, що свідчить про високу надійність розпізнавання. Крім того, рівень хибної відмови залишався на рівні 1,5 %, а хибного прийняття – лише 0,1 %, що знижує ризики несанкціонованого доступу та помилкових відмов.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Asoke Nath, Shreya Maity, Soham Banerjee, Rohit Roy. Quantum key distribution (QKD) for symmetric key transfer. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. 2024. № 10 (3). P. 270–280. URL: https://doi.org/10.32628/cseit24103105.

2. Begimbayeva Y. Approaches to developing key distribution protocols based on quantum key distribution. *Journal of Electrical Systems*. 2024. № 20 (7s). P. 2323–2330. URL: https://doi.org/10.52783/jes.3968.