Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

II Міжнародна науково-практична конференція
The second International scientific and practical conference

Кіберборотьба: розвідка, захист та протидія
Cyberwarfare: intelligence, defense and offensive security

КИЇВ - 2024

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

ІІ МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

The second International scientific and practical conference

“Кіберборотьба: розвідка, захист та протидія”

“Cyberwarfare: intelligence, defense and offensive security”

23–24.04.2024

ТЕЗИ ДОПОВІДЕЙ

Київ

Рецензенти:

Радзівілов Григорій Данилович	кандидат технічних наук, професор, заступник начальника інституту з наукової роботи
Чевардін Владислав Євгенійович	доктор технічних наук, 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
Юрченко Олег Васильович	кандидат технічних наук, заступник начальника кафедри кібербезпеки
Сілко Олексій Вікторович	кандидат технічних наук, доцент, заступник начальника інституту з навчальної роботи

Кіберборотьба: розвідка, захист та протидія: тези доповідей ІІ Міжнародної науково-практичної конференції. – Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2024. – 57 с. DOI: https://doi.org/10.61929/viti.mnpk.2.2024

У збірнику матеріалів ІІ 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 та платформ для проведення навчання фахівців з кібербезпеки.

Робочі мови конференції – українська, англійська.

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

Відповідальна за випуск О. Є. Головко

Підписано до друку 22.04.2024 р.
Друк. арк. 7,00. Ум.-друк. арк. 6,51. Обл.-вид. арк. 6,05.
Формат паперу 60×84/8. Тираж 5 прим.

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

З М І С Т

Cand. Tech. Sc., Assoc. Prof. **Humeniuk I.** (ZhMI)
Cand. Tech. Sc. **Lahodnyi O.** (ZhMI)

METHOD OF ENSURING CYBER SECURITY OF MILITARY INFORMATION AND COMMUNICATION SYSTEM

Problem statement. Timely detection, prompt counteraction to cyberthreats and unauthorized access (UaA) to components of military networks. is a necessary component of ensuring the appropriate level of cybersecurity of the information and communication system (ICS) as a whole. The necessity and importance of such a task is actualized especially in the face of armed aggression by the russian federation. Since the beginning of russia's full-scale military invasion to Ukraine, CERT-UA's Government Emergency Response Team has recorded and investigated more than 2,000 cyberattacks. Most of them – from the russian side. Among the main goals of enemy hackers is espionage (obtaining intelligence on logistics, weapons, plans and operations of the Security and Defense Forces)attempts to disable critical information infrastructure facilities, deprive citizens of access to public services and services etc., as well as information and psychological operations and disinformation "stuffing" in order to undermine confidence in the capabilities of state authorities, the Security and Defense Forces, spread panic among the population. So, based on these prerequisites, the development of new effective and improvement of known methods of countering cyberattacks and UaA is relevant and of scientific and practical interest.

Research method. Detection and counteraction of cyberattacks and UaA to the ICS of military purpose is a complex task, for the solution of which it is necessary to perform its decomposition and solve separate interrelated problems. In this scientific work, to achieve the goal of the task, a method of ensuring the cyber security of the ICS for military purposes is proposed, which consists of the following stages:

continuous monitoring of the status of network nodes and channels of military ICS;

recording the facts of cyberattacks with a detailed description of the level of danger of threats;

permanent control of user access to military ICS networks;

timely detection of UaA to the ICS for military purposes and cyberthreats, as well as operational counteraction to them.

Since the important task of network management is to maintain the functionality and reliability of each network component, at the first stage for military ICS it is necessary to use hierarchical management, distributing the network into separate clusters (zones) with the allocation of their controllers, gateway nodes and internal nodes.

Cluster controllers periodically send link status information to nodes to keep the routing tables up to date and network topology integrity. Under the conditions of a successful cyberattack on the cluster node, its physical isolation (Fig. 1).

This approach is effective for ensuring cybersecurity of internal nodes of another (non-compromised) cluster.

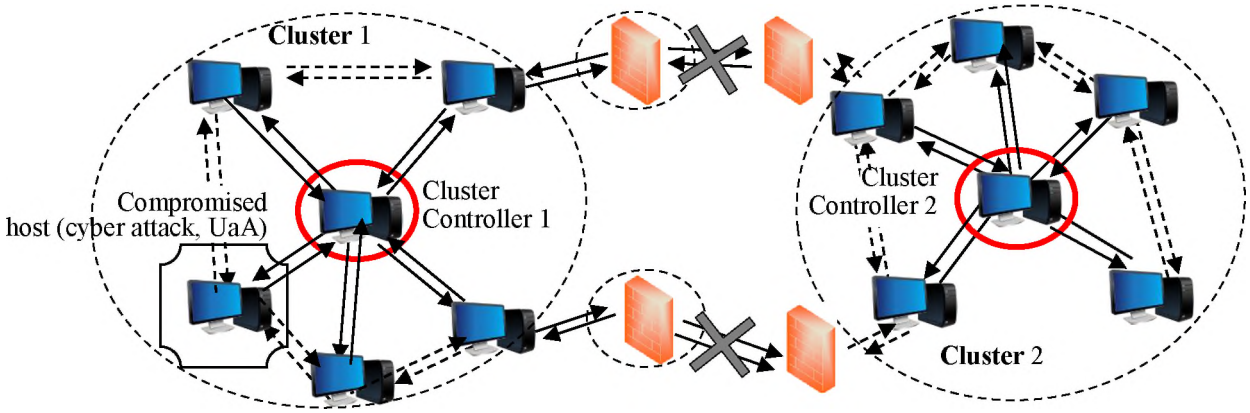


Fig. 1. Physical isolation of a potentially dangerous cluster

At the second stage, the incoming (outgoing) traffic of the network clusters is analyzed, in particular using the existing IDS intrusion detection system. As a result of the current step, the network security levels are determined: permissible (traffic contains a certain threat, but can be filtered) and unsafe (incoming traffic is blocked for further passage to the network). Cybersecurity of the ICS network will acquire its peak value provided that multi-level protection is applied.

Stage 3 – continuous control of user access to ICS networks.

Provided that cyberattacks and/or UaA have been committed, a stage of their detection and operational counteraction to these attempts and cyber threats is carried out to the ICS networks. The last stage of the methodology is based on the generalization of information about cyber threats or the commission of UaA, in particular: the very fact of cyberattacks (time, "victim component", new or repeated threat etc.); detailed description of the threat level.

Verification of the proposed method is carried out on the ICS network, which consists of 5 clustered nodes (2 clusters), each of which is conditionally taken as a critical component. The characteristics of the network are given in Table 1.

The test attack types are user-to-root (U2R) and PROBE. PROBE.

Table 1

Characteristics of the network under research

Network node number	Availability [+] and availability [-] of cybersecurity components		
	Control of nodes and channels connection	Invasion detection system	User access control
Cluster 1 (Switch 1 – Gateway; Router 1 – Cluster Controller)			
1 – PC 1	+	-	-
2 – PC 2	+	+	-
Cluster 2 (Switch 2 – Gateway; Router 2 – Cluster Controller)			
3 – PC 3	+	+	+
4 – PC 4	+	+	+
5 – PC 5	+	+	+

The results of the studies are presented in Table 2. The level of cyber security will be taken as a probabilistic normalized indicator with limits [0.1; 0.9].

Table 2

Results of verification of the proposed method

Network Component	Cybersecurity level ([0.5 and above] – sufficient; [less than 0.5] – insufficient)		
	Stage 1	Stage 2	Stage 3
Cluster 1	0,9	0,5	0,1
Cluster 2	0,9	0,9	0,9

Analysis of the obtained results suggests that each stage of the method (IDS systems, access control, etc.) is one of the technical tools for ensuring cyber security, it should not be considered separately or as a substitute for any other.

Conclusion. This paper presents the results of solving the current scientific and practical problem, which consisted in improving the existing methods of countering cyberattacks and UaA, namely in the development of a method for ensuring cyber security of the military ICS. The proposed method is based on a comprehensive application of monitoring the state of network nodes and user access to them, recording the facts of cyberattacks based on the analysis of incoming (outgoing) traffic, timely detection of cyber threats and the commission of UaA, as well as operational counteraction to these attempts.

The practical significance of the results obtained is the possibility of integrating the scientific result into military ICS to ensure the appropriate level of cybersecurity.

Kolomiiets A. (NTUU KPI)
Kovalchuk L. (PIMEE NAS of Ukraine)
Kuchynska N. (NTUU KPI)
Chevardin V. (MITIT)

PROBABILITY OF DOUBLE SPEND ATTACK ON A PROOF-OF-STAKE-BASED BLOCKCHAIN WITH CHECKPOINTS

The decentralized blockchain-based systems provide the common view on history of transaction ledger, censorship resistance and no single point of failure. There are a lot of consensus protocols, including special modifications, used in different blockchains. One can find detailed surveys in [1] and [2]. In decentralized systems, there are no trusted authority or third party, who may solve conflict and prevent fraud caused by malicious participants. Moreover, some part of network participants (we assume that this is minor part) may be malicious, therefore may break any rules and attack the system in any possible way. At the same time, honest nodes have no ability to detect the malicious behavior in advance, until the attack is finished (with some visible result). Within such conditions, a distributed system user must decide whether he accepts the transaction (and provides corresponding services or goods for the accepted value) or should wait for higher confirmation assurance. So, for given input parameters, it is important to have concrete and simple criterion when a transaction may be secure accepted with low risk of being removed from the final history of blockchain.

Thus, we need to analyze the blockchain security against the Double Spend Attack, which may be considered as the special case of persistence, one of two major ledger properties [3]. The main idea of this attack does not depend on the type of consensus protocol: the attacker tries to spend the same coin twice. Technically, it is an attack aimed at replacing one block in the blockchain with another.

In the presented work, we are also investigating security of Proof-of-Stake-based blockchain against the Double Spend Attack, but with additional condition of checkpoints. To increase the security of the blockchain, a mechanism of control points in the chain, i.e. checkpoint mechanism, is proposed, which purpose is to restrict the time of the attack. It means that in the blockchain, after a certain number of timeslots, some special blocks are created, which we call checkpoints. They are aimed to synchronize the state of the history of the chain till the previous checkpoint. Once the chain history is synced, it cannot be changed, even in case of the longer alternative chain. Using checkpoints in blockchain is described in [4].

Adding checkpoints, from the one hand, restricts the adversary in time for attack realization, and from the other hand requires more serious attack analysis. Attack probability estimations, obtained in this work, are much more complicated in compare with [5], but still may be used to obtain numerical results for block confirmation number, in dependence of adversary's ratio and distance between checkpoints. The methods of using checkpoints in blockchain are rather different, in this work we consider one definite mathematical model of blockchain with checkpoints. But proposed method may be (with slight modifications) used for different use cases of checkpoints in blockchain with Proof-of-Stake protocol, even for some Ethereum sidechains. In what follows, we get explicit formulas of the Double Spend Attack probability for Proof-of-Stake-based blockchains with checkpoints, depending on the network parameters (distance between checkpoints, ratio of malicious stakeholders) and number of confirmation blocks. Obtained formulas can also be used to define how many confirmation blocks is enough to guarantee that attack probability is less than some small preset value, like 0.001.

During the limited time of the attack, the attacker cannot build an arbitrary number of blocks. It will always be limited between checkpoints. In order to protect against the Double Spend Attack, provided that the time for its implementation is limited, it is necessary to find the number of confirmation blocks, for which the probability of the attacker's success will be negligibly small. If the number of confirmation blocks is greater than the number of timeslots between two checkpoints,

then we should not make more confirmation blocks, just the maximum number between checkpoints, because after the checkpoint, the probability of implementation of attack will be zero.

Different values of probabilities for an attack on the blockchain with checkpoints were obtained in case when the number of timeslots between checkpoints is limited. There are also blockchains with checkpoints, where the distance between checkpoints is calculated in a limited number of blocks, duration of time, number of days. In this work we do not consider blockchains with a fixed number of blocks between checkpoints, or with fixed time intervals. These partial cases of modification of the checkpoint mechanism are topics for future research.

The numerical results of probabilities of the Double Spend Attack on blockchains with different distances n between checkpoints, obtained according formulas for n = 50, 100, 150, 200, 250, 300, 350, 400, 450. For comparison, we also used the same results for blockchain without checkpoints. As we can see from obtained numbers, the difference between these two probabilities for the same number of confirmation blocks (for blockchains with checkpoints and without them) increases with increasing of adversary's ratio and decrease with increasing of difference between checkpoints, as expected. In case, when adversary's ratio is q = 0.45, the differences between these two probabilities reach more then 42-44%. For relatively small n, like n = 50, the difference becomes essential even for q = 0.25. As we can see, all these functions drop exponentially with increasing of the number of confirmation blocks, like the "classical" blockchains without checkpoints.

Using obtained analytical results, we got a large number of numerical results and built charts, which confirmed the correctness of analytical ones. The numerical results and charts, built according to corresponding analytical results, indicate that:

1) the probability of the Double Spend Attack for blockchain with checkpoints is smaller than for blockchain without them;

2) the smaller distance between checkpoints, the smaller probability of attack;

3) the larger ratio of malicious participants, the larger difference between probabilities of attack for blockchain with checkpoints and for blockchain without them;

4) the probability of the attack decreases exponentially with increasing of block confirmation number, like in classical case of blockchain without checkpoints.

Based on the analytical and numerical results of our work, for various financial transactions with cryptocurrencies, the vendor should wait for the certain number of confirmation blocks, if this number does not exceed the distance between corresponding checkpoints. In the opposite case, they should wait till the corresponding checkpoint, which makes the attack impossible.

We considered in this work only the case of Proof-of-Stake-based blockchains with checkpoints. The mathematical model for Proof-of-Work-based blockchains will be rather different and we are going to consider it in the next work.

REFERENCES

1. Nijsse, J.; Litchfield, A. A Taxonomy of Blockchain Consensus Methods. Cryptography 2020, 4, 32. https://doi.org/10.3390/cryptography40400322

2. Johar, S.; Ahmad, N.; Asher, W.; Cruickshank, H.; Durrani, A. Research and Applied Perspective to Blockchain Technology: A Comprehensive Survey. Appl. Sci. 2021, 11, 6252. https://doi.org/10.3390/app11146252

3. Garay, J.; Kiayias, A.; Leonardos, N. 2015. The Bitcoin Backbone Protocol: Analysis and Applications. 281-310. 10.1007/978-3-662-46803-6 10.

4. Chorey, P.A. 2022. Checkpoint-Based Blockchain Approach for Securing Online Transaction. In: Bhalla, S., Bedekar, M., Phalnikar, R., Sirsikar, S. (eds) Proceeding of International Conference on Computational Science and Applications. Algorithms for Intelligent Systems. Springer, Singapore. https://doi.org/10.1007/978-981-19-0863-7_12

5. Karpinski, M.; Kovalchuk, L.; Kochan, R.; Oliynykov, R.; Rodinko, M.; Wieclaw, L. Blockchain Technologies: Probability of DoubleSpend Attack on a Proof-of-Stake Consensus. Sensors 2021, 21, 6408. https://doi.org/10.3390/s21196408

Dr. Habil, prof. **Kovalchuk L.** (PIMEE NAS of Ukraine)
Koriakov I. (LLC "Crypton")
Bespalov O. (PIME NAS of Ukraine)

STATISTICAL CRITERIA OF RANDOM VARIABLES INDEPENDENCE CHECKING AND ITS APPLICATION IN CRYPTOLOGY

When a crypto-primitive, whose functions include the generation of a random/pseudo-random gamma, is admitted to operation, a necessary component of its quality control is a statistical check of the initial and intermediate gamma. This requirement should be applied, for example, to random/pseudo-random number generators (RNG/PRNG), stream ciphers, and block ciphers in "stream" modes (such as OFB, CBC, etc). There exist widely used tools for checking the statistical properties of sequences and generators, which are based on a set of statistical tests, like NIST STS set, Diehard, etc.

However, the other question, about independence of the sequences generated in such cryptoalgorithms, usually doesn't attract enough attention, though it is no less important. Indeed, the dependence of thee sequences can lead to predictability of the output gamma, which makes the cryptoprimitive vulnerable to statistical attacks.

This work is aimed at creating such a tool for checking the independence of sequences. Several statistical tests for checking the independence of bit sequences are developed in the paper. Some of them are partially empirical, so a certified PRNG was used to calculate the parameters of these tests.

Let hypothesis H_0 is formulated as "All sequences from the given set are pairwise independent". The alternative hypothesis H_1 is complex and may be formulated as "H_0 is false". Our purpose is to construct convenient, efficient, and justified tools to distinguish these two hypotheses.

As our criteria are partially empirical (like, for example, Universal Maurer Test), we calculated reference values (credential intervals) for them, using certified PRNG, described in Appendix 1 of DSTU 9041:2020.

First of all we need to make some designations and give mathematical background.

Let $m,n \in \mathbf{N}$. Define

$$\Xi = \left\{\xi^{(i)},\ i \in \overline{1,n}\right\} \tag{1}$$

the set of sequences of independent, identically distributed random variables $\xi^{(i)} = \left(\xi_1^{(i)},\dots,\xi_m^{(i)}\right)$, where $\xi_k^{(i)} \in \{0, 1\}$. Define their expectation and variance as

$$a^{(i)} = E\xi_k^{(i)} = P\left(\xi_k^{(i)} = 1\right),\ \left(\sigma^{(i)}\right)^2 = Var\left(\xi_k^{(i)}\right). \tag{2}$$

Next, introduce random variables

$$r_k^{(i,j)} = \frac{\left(\xi_k^{(i)} - a^{(i)}\right)\cdot\left(\xi_k^{(j)} - a^{(j)}\right)}{\sigma^{(i)}\cdot\sigma^{(j)}},\qquad i,j \in \overline{1,n},\ k \in \overline{1,m}, \tag{3}$$

and state some properties of these variables.

Proposition 1.

Let the sequences $\xi^{(i)}$ and $\xi^{(i)}$, defined in (1), are independent. Then the next statements are true:

1) $E\left(r_k^{(i,j)}\right) = 0$, $Var\left(r_k^{(i,j)}\right) = 1$, $i,j \in \overline{1,n}$, $k \in \overline{1,m}$;

2) if additionally $a^{(i)} = \frac{1}{2}$, $i \in \overline{1,n}$, then $\left(r_k^{(i,i)}\right)^2 = 1$.

Proposition 2.

Let $q > 0$ and $\varepsilon \in (0,1)$. Then, if the sequences $\xi^{(i)}$ and $\xi^{(i)}$, defined in (1), are independent, and additionally $m > \frac{1}{\varepsilon \cdot q^2}$, then the next inequality holds:

$$P\left(\left|R^{(ij)}\right| > q\right) \le \varepsilon . \tag{4}$$

In what follows, we also need sevaral well-known facts from Probability theory, such as *Law of iterated logarithms*, *Chebyshev's inequality*, and *Central Limit Theorem*.

Based of these statements, below we propose three statistical criteria for checking H_0 hypotheses.

Define matrix R as covariance matrix $R = \left(R^{(i,j)}\right)_{i,j=1}^{n}$ of values (3), where

$$R^{(i,j)} = \frac{1}{m}\sum_{k=1}^{m} r_k^{(i,j)} . \tag{5}$$

Criterion 1 (Based on Law of iterated logarithms)

Input: set of sequences (1); significance level α.

1. Calculate values $r_k^{(i,j)}$ according to (3) and values $R^{(i,j)}$ according to (5).
2. Calculate $\det R$ – the determinant of matrix $R = \left(R^{(i,j)}\right)_{i,j=1}^{n}$.
3. Calculate value $U_{m,n}(\alpha)$, using Table 1.
4. If $\det R \ge U_{m,n}(\alpha)$, then output « H_0 is accepted»; otherwise output « H_0 is rejected».

Criterion 2 (Based on Chebyshev's inequality)

Input: set of sequences (1); significance level α.

1. Calculate values $r_k^{(i,j)}$ according to (3) and values $R^{(i,j)}$ according to (5).
2. Calculate $\det R$ – the determinant of matrix $R = \left(R^{(i,j)}\right)_{i,j=1}^{n}$.
3. Calculate value $V_{n,m} = \left|\det R - 1 + \sum_{1 \le i < j \le n} \left(R^{(i,j)}\right)^2\right|$.
4. Calculate value $V_{n,m}(\alpha)$ using Table 2.
5. If $V_{n,m} < V_{n,m}(\alpha)$, then output « H_0 is accepted»; otherwise output « H_0 is rejected».

Criterion 3 (Based on Chebyshev's inequality)

Input: set of sequences (1); significance level α.

1. Calculate values $r_k^{(i,j)}$ according to (3) and values $R^{(i,j)}$ according to (5).
2. Calculate $\Delta = \det R$ – the determinant of matrix $R = \left(R^{(i,j)}\right)_{i,j=1}^{n}$.
3. Define the corresponding interval $\Delta(m,n,\alpha) = \left[I_0(m,n,\alpha), 1\right]$ from the Table 3.
4. If $\Delta \in \Delta(m,n,\alpha)$, then output « H_0 is accepted»; otherwise output « H_0 is rejected».

Conclusion.

Proposed criteria for independence sequences checking are convenient, useful, and necessary tool in cryptography. It should be used for checking of cryptographic quality of each RNG/PRNG, stream cipher, or block cipher in "stream" modes.

Experimental results of these criteria shows that they not only accept hypotheses H_0, if it is fair (according to chosen significance level), but also reject it in cases, when tested sequences are chosen dependent in advance.

Kulakovskyi O. (OPEN TEXT)
Cand. Mil. Sc. **Pravdyvets O.** (MITIT)

MODERN CYBERSECURITY PARADIGM

The modern globalized world is actively developing in a new paradigm of the information society, a world where global cyberspace plays a significant role in human lives, improving cybersecurity is an essential component of ensuring information security, economic development and national security. In support of this, Roger Spitz, President of the Institute for the Future, noted that the importance of cybersecurity at the moment should be at the level of national security [1].

The ongoing armed aggression of the russian federation against Ukraine has consolidated the assertion that modern wars, wars of the XXI century, are high-tech, in particular in cyberspace, which is confirmed by the practice of cyber warfare of the Defense Forces of Ukraine, which covers cybersecurity.

Such opinion on the importance of cybersecurity in modern warfare are shared by our partners, for example, Leon Panetta, former head of the CIA from 2009 to 2011 and Secretary of Defense from 2011 to 2013, emphasized in his speech that: "The potential for the next Pearl Harbor could very well be a cyber-attack" [2].

At the same time, Scott J. Shackelford, Professor, Director of the Institute for Applied Cybersecurity Research noted that "The lesson of the war is that long-proven cybersecurity standards and strategies" were not enough to "curb the ambitions of vladimir putin", who unleashed a cyber war in parallel with a conventional one" [3].

Taking into account the global views on cybersecurity, Ukraine was forced to create its own reliable and resilient lines of defense around critical infrastructure facilities and their data under conditions of limited resources and time.

A special and critical parameter in modern cyber warfare is the time for the implementation of cyber defense systems and the creation of operational protocols for responding to cyber threats, taking into account the methods of cyberattacks.

In addition, the complexity of IT resources and infrastructures is constantly growing: the number of IT assets is increasing, and new technologies are being implemented that creates additional components in IT infrastructures. These new components often become the point of failure or breach of the infrastructure with the help of vulnerabilities.

This situation requires an urgent focus on the weaknesses of Ukraine's cyber defense, the implementation of the world's best practices of international institutions, the use of databases of described cyberattack methodologies and the automation of operational protocols for responding to cyber threats.

Also, there is an urgent need to minimize the impact of the human factor, due to the critical lack of qualified specialists, and the response time to cyber threats through full or partial automation of response protocols in conditions of full situational awareness and data analysis.

Thus, it is possible to identify several key trends in modern cyber warfare:

1. Cyber warfare has no geographical boundaries – it can involve resources and people from any country in the world, most often in conditions of anonymity. Along with the existing hacker groups, new ones, both separate and combined, affiliated with the russian federation, are emerging. Attacks as itself became more complex, it has to be responded much faster and more resilient.

2. Cyber warfare is not tactile – cyberattack and cyber defense activities take place in cyberspace and are not physically detected. With the beginning of a full-scale invasion, an increase in the number of cyberattacks was recorded. At the same time, the damage caused by cyber warfare can change the course of hostilities, operations, or even the war itself. In addition to conventional operations on the battlefield, there is a war in cyberspace that began in 2014. Some of its

manifestations were able to affect many Ukrainians, such as cyberattacks on Ukrainian energy companies, Kyivstar companies, or the Petya.A virus.

3. Activities in cyberspace have their own methodologies, formations, and approaches that needs to be correlated with actions at the command level.

Thus, the modern practice of performing cybersecurity tasks requires the theory to promptly solve a number of urgent scientific problems, in particular:

development (improvement) of new methods, techniques, models, algorithms of data processing;

development and implementation of new software and hardware solutions;

development of a new regulatory framework necessary for the implementation of new tasks and functions in accordance with modern challenges and threats;

standardization and study of best practices, development of science and R&D in the field of cybersecurity;

introduction of modern standards and the latest innovative technologies for the training of personnel (specialists) in cybersecurity;

and other areas.

Conclusion. Solving a number of urgent scientific problems in cybersecurity is an urgent scientific task. Prompt solving of these problems, in particular the automation of cybersecurity processes, will provide an opportunity to optimize and increase the efficiency of the cyber defense system, including the development of comprehensive systems for the protection of critical IT assets of Ukraine, etc.

REFERENCES

1. Roger Spitz, Lidia Zuin - The Definitive Guide to Thriving on Disruption: Volume I - Reframing and Navigating Disruption 2022.

2. Lawrence J. Trautman, Is Cyberattack the Next Pearl Harbor? 18 N.C. J.L. & Tech. 233 (2016). https://scholarship.law.unc.edu/ncjolt/vol18/iss2/3

3. Scott J. Shackelford - The Impact Of The War In Ukraine On The Prospects For Cyber Peace, 2022 https://www.cambridgeblog.org/2022/05/the-impact-of-the-war-in-ukraine-on-the-prospects-for-cyber-peace/

Lavryk I. (MITIT)
Pryima O. (MITIT)
Brodovskyi A. (MITIT)

NIST PQC THIRD ROUND FINALISTS STUDY

The date of the appearance of quantum computers who can break modern cryptographic systems is still unknown, but it is gnown for sure that it needs a long time to implement and standardize new cryptographic algorithms requires immediate action. In particular, existing cryptosystems must be replaced or adapted to withstand both classical cryptanalysis and attacks using quantum computers. Thus, the need of development and implemention of post-quantum (or quantum-resistant) cryptographic algorithms is obvious [1].

In 2016, NIST began the process of developing and standardizing public key cryptographic algorithms to improve the existing digital signature standard FIPS 186-4 (DSS) NIST PQC. As a result, several standardization processes rounds were conducted [2-3]. The third round, held in July 2022, completed the selection of post-quantum public-key encryption algorithms and digital signatures [4]. In general, these rounds aim to identify an algorithm capable of protecting confidential information in post-quantum period.

Crystals-Dilithium, Falcon and Sphincs+ are chosen as digital signatures candidates. Crystals-Dilithium and Falcon are based on problems from the theory and practice of algebraic lattices, with features that depend on the application context - Dilithium is easier to implement, while Falcon provides shorter signatures. Sphincs+ is slower and has larger size of signatures, as it is based on a different mathematical approach, namely hash functions.

Study of the algorithms compares two important parameters: key and signature sizes. Data on key and signature lengths are shown in Figure 1 [5,6].

The two lattice-based algorithms (Crystals-Dilithium, Falcon) have close public keys sizes, Sphincs+ has shorter public key, as shown in Figure 1. On the other hand, Sphincs+ has the longest signature length.

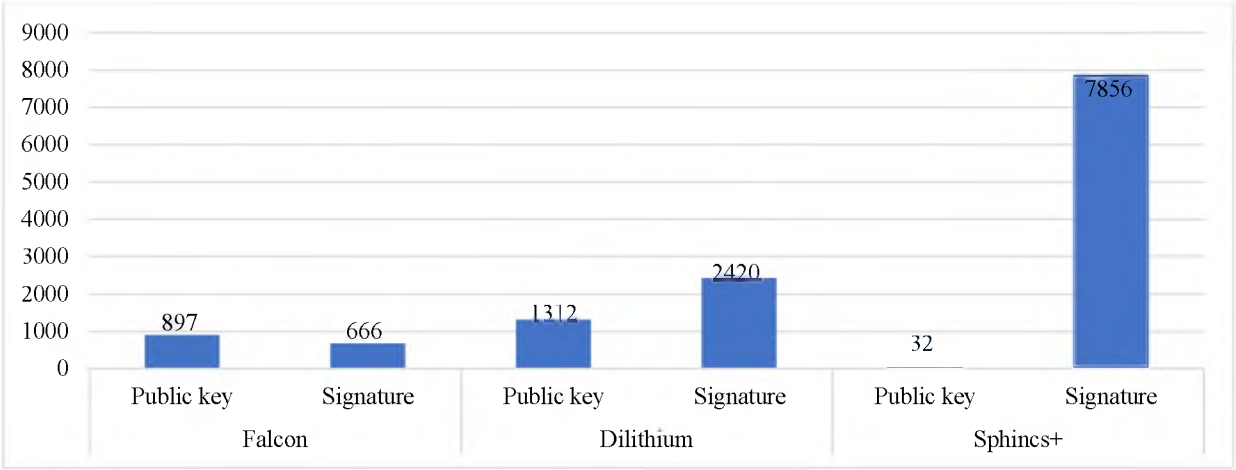


Fig. 1. Comparison of public key and signature lengths (bytes)

The data from Figure 2 shows the execution speed on the Intel Xeon Gold 63338 processor, and [7] provides execution time data for the i7 11 generation processor for Dilithium and Falcon. [8] and [9] provide data on energy consumption, concluding that energy consumption is roughly proportional to speed, i.e., execution time, since energy consumption has much smaller deviations compared to execution speed.

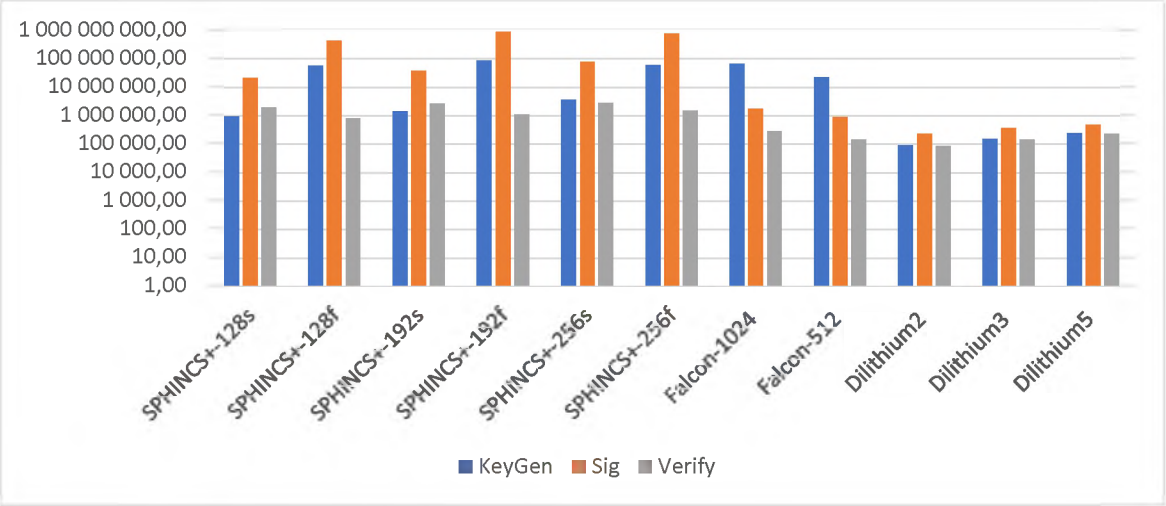


Fig. 2. Performance comparison of all candidates

Proposed candidates for the quantum-resistant electronic digital signature standard have fundamentally new structures that have not been deeply studied and ultra-long key lengths, which creates a significant burden on the computing power of existing software and hardware on which modern information systems are built.

The direction of further research is the development of new cryptographic algorithms and methods that will ensure the integrity and confidentiality of information during its transmission over unprotected channels in the transition period to the widespread use and implementation of post-quantum cryptography standards.

REFERENCES

1. NIST. Post-Quantum Cryptography. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography.

2. NIST. Post-Quantum Cryptography—Round 1 Submissions. URL: https://csrc.nist.gov/Projects/post-quantumcryptography/Round-1-Submissions.

3. NIST. Post-Quantum Cryptography—Round 2 Submissions. URL: https://csrc.nist.gov/Projects/post-quantumcryptography/round-2-submissions.

4. NIST. Post-Quantum Cryptography—Round 3 Submissions. 11 September 2023. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

5. Bai, S.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schwabe, P.; Seiler, G.; Damien, S. CRYSTALS-Dilithium–Algorithm Specifications and Supporting Documentation, 2020. URL: https://csrc.nist.gov/CSRC/media/Projects/postquantum-cryptography/documents/round-3/submissions/Dilithium-Round3.zip.

6. Fouque, P.-A.; Hoffstein, J.; Kirchner, P.; Lyubashevsky, V.; Pornin, T.; Prest, T.; Ricosset, T.; Seiler, G.; Whyte, W.; Zhang, Z. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. 2020. URL: https://csrc.nist.gov/CSRC/media/Projects/post-quantum-cryptography/documents/round-3/submissions/Falcon-Round3.zip.

7. Yokubov, B.; Gan, L. Comprehensive Comparison of Post-Quantum Digital Signature Schemes in Blockchain. In Proceedings of the 2021 IEEE International Conference on Electronic Communications, Internet of Things and Big Data, Yilan County, Taiwan, 10–12 December 2021.

8. Roma, C.A.; Tai, C.-E.A.; Hasan, M.A. Energy Efficiency Analysis of Post-Quantum Cryptographic Algorithms.

9. Dimopoulos, C.; Fournaris, A.P.; Zhao, R.K.; Sakzad, A.; Steinfeld, R. Energy Consumption Evaluation of Post-Quantum TLS 1.3 for Resource-Constrained Embedded Devices. In Proceedings of the 20th ACM International Conference on Computing Frontiers, Bologna, Italy, 9–11 May 2023.

Lohachova Y. (V. N. Karazin Kharkiv National University)
PhD **Yesina M.** (V. N. Karazin Kharkiv National University)

ANALYSIS OF THE CYBERCRIMINAL'S PERSONALITY

Introduction

In the age of digitalisation, professionals from various industries and ordinary citizens are facing the problem of cybercrime. As technology has expanded into most areas of life, such as medicine, the legal sector, banking, education and many others. In the era of large-scale digitalisation, the need to protect personal data has not only increased, but fraudsters' schemes and strategies have also evolved since the first cybercrime. An important aspect of preventing and combating cybercrime is to be aware of the psychology of criminals and which categories of people may pose the greatest threat. The main task is to analyse the personality of the cybercriminal and explore how such techniques help in practice.

1. Classification of cybercriminals

Almost everyone uses a computer every day for work, study, and entertainment, but some people are beginning to use their devices to commit cybercrime. The fact is that, depending on certain traits and characteristics, people tend to behave differently in the same situations. Thus, cybercriminals, due to a set of certain characteristics and peculiarities, are more prone to criminal activity in the technical space than ordinary users [1].

Cybercriminals can be classified in several ways. They can be divided according to their personal qualities [2]: people who commit a crime by accident; people who commit a crime for mercenary purposes; hackers; computer hooligans. The second classification includes more features of the offender and divides them into three groups [2]: professionals; fanatics; mentally ill. These classifications overlap in one way or another and cannot be assessed without each other. The most common motivation of cybercriminals is selfishness, but they can also be motivated by a desire for revenge, self-assertion, power, chaos and other feelings that have arisen as a result of certain circumstances. An example of such behaviour is the UBS Paine-Webber attack - the attacker was an employee of the company who planted a "logic bomb" that took down about 2,000 servers across the country and caused the company to be unable to conduct operations for several weeks in some of its offices [3].

Sometimes, cybercrime can be committed not by a single person, but by a group. Such groups can attack various institutions: financial institutions, hospitals, state-owned enterprises, corporations, and so on. The group always has a leader in the centre, who coordinates the attack and controls the entire branched structure of the group.

2. Psychological and personal characteristics of cybercriminals

There are many stereotypes about hackers and other criminals in the virtual space. Most people, if asked to describe such a person, will provide the same set of qualities. These stereotypes are that a cybercriminal is a person alienated from society, addicted to computers and having outstanding mental abilities, belonging to a young age group and mostly male. In order to understand what the real personal and psychological characteristics are, it is worth looking at statistics. The following conclusions can be drawn from the statistics presented in the study [2].

The majority of cybercrime offenders are indeed men, with 87.5% of them in the statistics, while women make up only 12.5%. The next characteristic is age: most cybercrime is committed by people in the 30-50 age group, with 36.2% of the total. Young people aged 18 to 25 are also one of the most common age groups, with a 34.3% participation rate. The majority of people who commit crimes using technology are single, accounting for 70% of the total number of offenders. This is largely due not only to the fact that cybercriminals are quite young, but also to the fact that married people are less likely to commit any type of crime because they are afraid of harming their family. Another remarkable feature of cybercriminals is that they are most often people with higher education or incomplete higher education. This type of criminal is characterised by good mental abilities, as they need to be on a par with those responsible for security systems when committing a

cybercrime. Approximately half of those who commit cybercrime are unemployed. Among those who do work permanently, managers are most likely to commit technical crime, while programmers are less common in statistics. Another important feature worth paying attention to is the presence of any kind of addiction. After all, people who are addicted to gambling, alcohol, drugs, etc. can get under the influence and then deliberately cause harm by committing a cybercrime. Some hackers carry out cyberattacks that they believe are beneficial to society. Such cybercriminals are mainly aimed at helping society. Such actions may be motivated by religious, political or social beliefs.

3. Using profiling in the investigation of cybercrime

Cybercrime is a crime just like physical theft or damage, but committed in the technological space. Therefore, the methods used to identify conventional criminals can also be used for cybercriminals. Criminal profiling is one of the methods actively used to identify a potential criminal (or to prevent such a person from entering an institution or enterprise under the guise of an employee or client). Profiling consists of analysing behavioural patterns that can help predict certain things about a person who has committed a crime [4]. Such analysis is aimed not only at identifying and understanding the perpetrator, but also at enabling appropriate measures to be taken. The analysis includes the study of the offender's personality traits, modus operandi, motivation and potential future steps.

It is important to understand the motive of the cybercriminal, which can vary significantly. If a hacker is motivated by the desire to get pleasure or the possibility of being recognised by the hacker community, he or she may be subject to legal measures and exposure, which can significantly complicate his or her future attempts to gain the approval of "colleagues" or close this path forever. The motives may also be the desire to have fun, excitement, obtaining benefits in the form of money, etc. [4]. Cybercriminals are human beings like everyone else, and therefore they are also driven by inherent characteristics. Humans are often prone to habits, so cybercriminals often become recognisable by the "signature" of their crimes, making them easier to detect and find. Another clue is the ultimate goal achieved by the hacker. It is important to determine what they have achieved - obtaining customer data, money, locking down a system, searching for intellectual property or installing malware, etc.

Conclusions

Cybercrime is committed by people who expect to be uncertain and unpunished, but, as with other criminals, they can be identified and exposed. An important aspect of the work of cybersecurity professionals is knowledge of the personal and psychological characteristics of cybercriminals, such as motivation, purpose, habits, etc. With this knowledge, it is possible not only to identify the offender after the crime has been committed, but also to identify potential cybercriminals and prevent cyber incidents.

REFERENCES

1. Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets / Marleen Weulen Kranenbarg, Jean-Louis van Gelder, Ard J. Barends, Reinout E. de Vries: Computers in Human Behavior, 2023.

2. Науковий вісник Міжнародного гуманітарного університету № 26, Аналіз особистості кіберзлочинця, який вчиняє злочини проти власності у кіберпросторі / М. Ю. Піцик, 2017.

3. Logic Bomb' Dropped On Brokerage / CBS News, 2002.

4. Inside the Mind of the Enemy. A Guide to Profiling Cyber Criminals. / Richard Barrell and the team at CounterCraft.

Dr. Sc., Professor **Pilkevych I.** (KZMI)
Loboda V. (KZMI)
Miroshnichenko S. (KZMI)
Ostapchuk T. (MU A0565)

CLUSTERING METHODS FOR WIRELESS INFORMATION AND TELECOMMUNICATION NETWORK

Rapid development of the IEEE 802.11 standard, designed for communication in wireless local area networks, has made it possible to build peer-to-peer local area networks based on Ad Hoc principle. Networks built on this principle are divided into stationary (Ad Hoc Networks) and mobile (Mobile Ad Hoc Networks). Their advantages are ability of the elements to self-organize into a radio network, absence a fixed architecture, and possibility a dynamic routing. Wireless information and communication networks (ICNs) are divided into clusters in order to select the optimal route.

A controller is determined in each cluster according to appropriate clustering algorithm. At the same time, for mobile devices with limited energy resources and bandwidth, an important scientific and practical task arises to effectively manage ICN resources in order to reduce transmission time with minimal energy costs and at the highest possible speed. Relevance of this important task is due to objective contradiction between requirements to increase the amount of transmitted information in a short time and fundamental impossibility to minimize energy costs to increase its speed due to existing network structure (topology).

This study aims to develop a methodology for clustering wireless ICN to reduce information transmission time with minimal energy consumption.

Methodology includes the following steps:

1. Determining a set of cluster controllers.
2. Distribution of ICN to a set of clusters. As the result of this step, we create data arrays containing numbers of graph vertices.
3. Selecting a device with a lowest value of an objective function as a cluster controller.
4. Self-organization of ICN by establishing links between nodes and controller.

At the first stage, devices transmit broadcast signals at maximum transmitter power level, which connects devices to each other. Next, the area where ICN mobile devices are located is divided by any known method into a certain number of cluster zones.

At the second stage, a cluster controller is determined in a corresponding cluster zone. This controller is a device that should provide maximum throughput in a cluster zone, is the least distant from other devices, has a large power reserve, and has a large number of connections to other devices. For this purpose, the solution of a multi-criteria problem is implemented to build an adequate objective function, which is a scalar convolution of partial criteria:

maximizing residual charge coefficient of battery of the i-th device;

minimizing bandwidth distribution coefficient of the i-th device over communication channels between devices of a cluster zone;

maximizing connectivity coefficient of the i-th device;

minimizing distance coefficient of the i-th device from other devices in a cluster zone.

As a result of this step, a data array is created that contains objective function values calculated for each device in the corresponding cluster zone. Device for which value of objective function is the smallest is selected as a cluster controller.

Performance of methodology for selecting ICN cluster controller was tested on its sample consisting on 37 devices. Four cluster zones were investigated. However, the area on which the devices are located is limited.

Therefore, the proposed methodology will increase network lifetime and reduce energy costs for transmitting information between devices in cluster zones. When choosing a cluster controller, this methodology takes into account not only energy characteristics and location of devices, but also communication channel bandwidth that can be provided by the corresponding device.

Cand. Tech. Sc. **Samoilov I.** (MITIT)
Ph.D **Storchak A.** (ISCIP)

MODEL OF CYBERSECURITY SYSTEM FOR CRITICAL INFORMATION INFRASTRUCTURE

Today, critical information infrastructure facilities face constant cyber-attacks, making the development of effective cybersecurity systems crucial for ensuring their stability and security. With the increasing number and complexity of cyber threats, an effective cybersecurity system is essential for maintaining the confidentiality, integrity, and availability of critical information resources.

The research is dedicated to developing a cybersecurity system model for critical information infrastructure facilities in response to the growing threat landscape. It focuses on improving cyber defence models to safeguard critical information infrastructure against evolving threats, providing guidance for future enhancements. The findings and recommendations can serve as a foundation for further advancements in cyber defence systems amidst the ever-evolving cyber threat landscape.

After reviewing the available literature and regulatory framework, and analyzing the history of critical information infrastructure protection, the following key features of safeguarding such facilities emerge: information security policy; user and administrator access management; identification and authentication of users and administrators; network protection of components and information resources; availability and resilience of components and information resources; determining the conditions for the use of external devices and storage media; determining the conditions of use of software and hardware; determination of conditions for the location of components of the critical information infrastructure facility.

To model the cybersecurity system for critical information infrastructure, the use of IDEF0 notation is recommended due to its logical representation of functional relationships. The functional model of cybersecurity system processes for critical information infrastructure is depicted in Fig. 1.

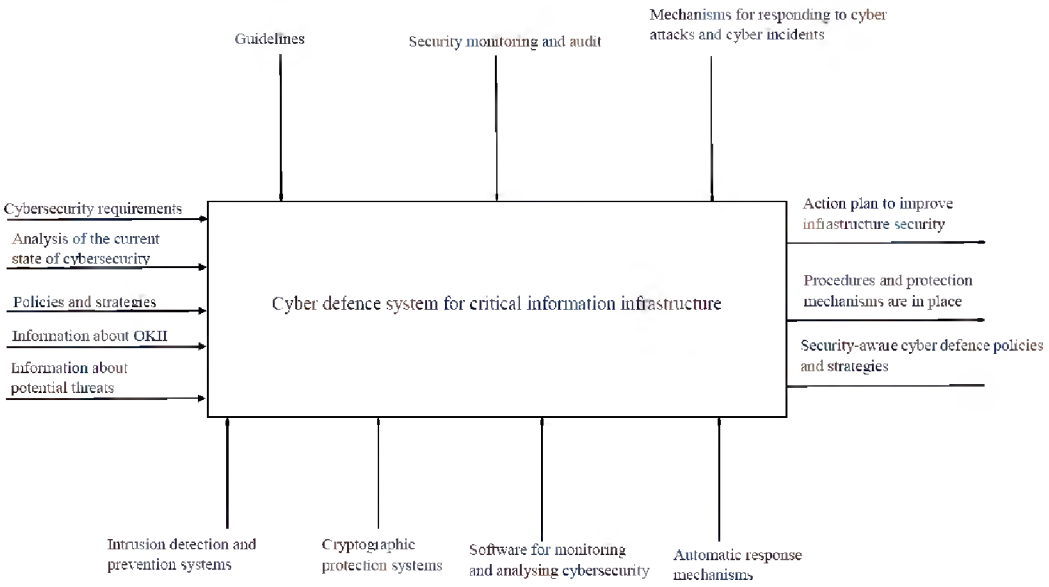


Fig. 1. Context diagram of the cybersecurity system for critical information infrastructure

The primary purpose of the model is to clearly illustrate cybersecurity system processes. The resulting model decomposition precisely identifies the following structural levels: data analysis and processing, development and planning of actions, control and monitoring, and implementation and execution of mechanisms.

Ultimately, employing the model of the critical information infrastructure cybersecurity system will enable organizations to effectively protect their information resources from potential threats and ensure the stable and reliable operation of the system.

Vykhlo A. (NTUU KPI)
Dr. Habil., professor **Kovalchuk L.** (PIMEE NAS of Ukraine)

FRONTRUNNING ATTACKS DETAILED OVERVIEW AND CALCULATION OF SUCCESS PROBABILITY

The fundamental properties of blockchain networks, such as decentralization and transaction transparency, along with the time required for transaction confirmation in blocks create new challenges for protecting transactions from order execution attacks. One of the attacks that exploit these properties of the blockchain for the benefit of the malicious user is the frontrunning attack.

Frontrunning attacks are based on the illegitimate advantage gained by the attacker from knowledge about a transaction in a pending state and knowing how the creation of other transactions and the order of their execution will affect original transaction and the asset price. Decentralized exchanges and auctions are particularly vulnerable to frontrunning. These attacks are based on the principles of blockchain construction, without any necessary prerequisites or vulnerabilities in the smart contract.

The results of existing research also indicate a large-scale application of such attacks and their correlation with changes in asset prices: analyzing a sample of exchanges involving specific assets over a certain period, researchers found that prices increased on 80% of days when suspicious transactions were observed, compared to only 55% of days when no such transactions were found [1]. Such results, coupled with the increasing popularity of decentralized exchanges, confirm the necessity for detailed study of frontrunning attacks and methods of counteraction.

Before providing a detailed description of the attack, it is necessary to introduce the concept of the mempool and explain its role.

The mempool is a component of the blockchain network that serves as a temporary storage for transactions awaiting confirmation and inclusion in the next block. Typically, the priority of selecting transactions to be included from the mempool into the next block depends on the transaction fee size [2].

Information about transactions inside the mempool is public. Transparency allows users to view the status of transactions, analyze fees, determine network performance in real-time. However, this transparency also provides malicious actors with the opportunity for manipulation.

An important component of frontrunning attacks is the time a transaction spends in the mempool, which directly depends on the block generation time, typically maintained within certain timeframes. For example, Bitcoin implements a mining difficulty adjustment protocol to maintain a stable block generation time of around 10 minutes [3].

When examining the structure of the attack in more detail, depending on the manipulation of transactions and the method of gaining advantage, various types of frontrunning attacks are distinguished: displacement, insertion and suppression.

Displacement is a type of frontrunning attack where the attacker aims to precede the original transaction in the block. The attacker, by inspecting the mempool, seeks transactions that, if preempted, can yield a certain advantage. For example, winning bids in an auction, purchasing unique items, trading for a limited volume of assets, or executing transactions involving large asset volumes. The attacker, having found the transaction and analyzed potential benefits, creates a new transaction for the same asset, setting a significantly higher transaction fee than the vulnerable transaction. Consequently, two similar transactions for the same asset end up in the mempool, but the attacker's transaction has higher priority for miners due to its higher fee.

Insertion is a type of frontrunning attack whose main objective is to include two transactions in a block in such a way that the first transaction executes before the target one, and the second one executes after. After identifying a transaction that the attacker can manipulate (usually it is an asset with low liquidity and high volatility [4]), he creates two transactions: the first is a high-fee purchase transaction of the asset, which must be included by miners before the target transaction,

and the second one – a sale transaction of the purchased asset, which must be included by miners after the target transaction. Consequently, the conditions for the first transaction are optimal with, for example, negative slippage due to low demand. The target transaction receives worse conditions than expected due to the previous transaction and also increases demand for the asset. The second transaction is executed during high demand and, for example, positive price slippage. The attacker gains an advantage equal to the difference between the asset price in the buying transaction and selling transaction, which is achieved through price fluctuations and slippage.

Suppression is a type of frontrunning attack that aims to delay the execution of a specific transaction to gain illegitimate advantage from this delay. This is typically achieved by creating a certain number of transactions that are supposed to be processed before the target transaction, preventing it from being included in multiple blocks. Typically, transactions in this series not only have high fees but also high gas volumes. This way, the series will occupy a significant portion of the block or multiple blocks, delaying the execution of the original transaction for an extended period.

One way to benefit from this delay is by delaying transactions from an oracle, which often affects the conditions of other transactions. With information about such a transaction and knowledge of how it will impact asset prices, the attacker can create favorable conditions for themselves by executing transactions for these assets and including them into the block before the oracle transactions [5].

These types of frontrunning attacks are widely used in various blockchain networks. The most vulnerable to them are auctions and decentralized exchanges due to their nature and transparency of the underlying blockchain. Prevention mechanisms like Commit-Reveal and Submarine sends can significantly reduce, but not eliminate the issue [6]. Below we give two algorithms of such attack, which may be applied for different situations.

Algorithm of frontrunning attack (displacement) on an auction bid.

Input: Public information about the auction: addresses, lots, arranged timeslots, transaction structure of the bid.

1. Decide which auction lot has high potential profitability.
2. Get timeslot, bidding address and bid transaction structure for the lot.
3. Analyze how much time is required to create a transaction based on some other transaction.
4. Calculate the time range available for the attack, considering the auction timeslot and transaction creation time from step 3.
5. Start monitoring mempool in the attack time range for the related transactions.
6. Store the highest bid of the sequence filtered form mempool.
7. Create an equivalent transaction.
8. Increase transaction fee to be significantly higher than original, depending on required attack success probability.
9. Submit created bid.

Outcome: Attackers' bid winning the lot instead of another user.

Notes:

1) Considering the time malicious user requires to create a transaction should be not significant, the transaction created on step 7 should contain the highest bid. By increasing transaction fee significantly, the user increases priority of inclusion this transaction into the block by miners. Depending on the fee amount, attackers' transaction has chances to be processed before the original transaction.

2) Attack is successful if attackers' transaction included into the block before the original. As long as two transactions have the same bid amount, the winner is the transaction which was processed earlier.

Algorithm of frontrunning attack (insertion) on decentralized exchange.

Input: Public information about the asset state such as liquidity, volatility, related transaction volumes and frequencies, latest slippage percentage.

1. Decide which asset has high potential profitability.
2. Start monitoring mempool for transactions with high volumes for this asset.
3. On vulnerable transaction received – create an equivalent transaction for any amount of the asset.
4. Increase transaction fee to be significantly higher than original, depending on required attack success probability.
5. Submit the purchase transaction.
6. Create an unloading transaction that sells the asset according to step 3.
7. Submit the unloading transaction.

Outcome: Attacker yields the profit equivalent to the difference between the actual price of the purchase and sale transaction.

Notes:

1) Considering the state of chosen asset, it should have negative slippage percentage for purchase (assets actual price will be lower than expected). The transaction with high volume will increase the slippage range and, in the best-case scenario, the exchange rate [7].

2) Given such a transaction, the malicious user has an attack time range from the transaction appeared in the mempool to the time it is included into the block. Increasing the transaction fee by a significant amount on step 4, the attacker increases the probability of processing the transaction before original. The attackers' transaction will receive the negative slippage and depending on the amount, might increase the slippage percentage. Original transaction due to high volume on the asset with low liquidity guarantees increase of slippage percentage to positive and might increase the exchange rate. This creates significantly better sales terms for the unloading transaction compared to the first transaction. This difference creates profit for the attacker.

The algorithms described above mentioned "attack success probability". Based on the description of the attack, this probability should depend on the probability of inclusion attackers' transaction before the original one. In other terms, processing time of the malicious transaction should be less than the users' transaction time. The only way the attacker can manipulate the transaction processing order (time) is changing transaction fee to increase its' priority. Consequently, the attack success probability should depend on the difference of transaction fee amounts.

To calculate this probability let's consider that the transaction processing time is a random variable which follows exponential distribution with some parameter λ, which is some function on transaction fee τ: $\lambda = f(\tau)$. To obtain the main result about attack success, we need to formulate the next auxiliary result from probability theory.

Lemma 1.

Let random variables (RV) ξ_1 and ξ_2 follow exponential distributions:

$$F_i(t) = P(\xi_i \le t) = 1 - e^{-\lambda_i t}, \quad i = 1,2.$$

Then $P(\xi_1 \le \xi_2) = \dfrac{\lambda_1}{\lambda_1 + \lambda_2}$.

Lemma 2.

Let random variables (RV) ξ_1 and ξ_2 follow exponential distributions:

$$F_i(t) = P(\xi_i \le t) = 1 - e^{-\lambda_i t}, \quad i = 1,2.$$

Then $P(\xi_1 \le \xi_2 - \Delta) = e^{-\lambda_1 \cdot \Delta} \dfrac{\lambda_1}{\lambda_1 + \lambda_2}$.

Now we can formulate the main result.

Theorem 1.

Let time for transaction processing be described with some RV ξ_τ with exponential distribution as

$$F_i(t) = P(\xi_\tau \le t) = 1 - e^{-f(\tau)t},$$

where τ is transaction fee and $\lambda = f(\tau)$ is corresponding function, which describes dependence of the average time needed for transaction processing (after its creation) on transaction fee.

Next, let Δ be the time needed for adversary to find corresponding transaction and to create the alternative one.

Also assume that transaction fee for initial transaction was set as τ_1, and the fee for alternative transaction was set by adversary as τ_2.

Then the probability $P_{fr}(\tau_1, \tau_2, \Delta)$ of frontrunning attack is calculated as

$$P_{fr}(\tau_1, \tau_2, \Delta) = e^{-f(\tau_2)\cdot\Delta} \frac{f(\tau_2)}{f(\tau_1) + f(\tau_2)}.$$

The theorem given above allows adversary not only calculate transaction fee, needed for success with some desirable probability, but also to decide if such attack has some sense, depending of required expenses and possible profit.

Conclusion.

We give explicit formula to calculate the probability of frontrunning attack success, depending on transaction fee and time for transaction creation. But the open question is how to set the function f, which connects transaction fee and average time for its processing. In the simplest model it may be some linear or affine function. But it also may depend on blockchain parameters and therefore be different for different blockchains. So the question about the general view of the function and its property is the topic for further investigations. We believe that one of the way to solve it is application of statistical analysis.

REFERENCES

1. Price manipulation in the Bitcoin ecosystem, Journal of Monetary Economics / N. Gandal, JT Hamrick, T. Moore, T. Oberman, 2018.

2. Transaction Queuing Game in Bitcoin BlockChain / J. Li, Y. Yuan, S. Wang, F. Wang, 2018.

3. A Systematic Review and Empirical Analysis of Blockchain Simulators/ R. Paulavičius, S. Grigaitis, E. Filatovas, 2021.

4. The Adoption of Blockchain-based Decentralized Exchanges / A. Capponi, R. Jia, 2021.

5. Your Smart Contracts Are Not Secure: Investigating Arbitrageurs and Oracle Manipulators in Ethereum / K. Tjiam, R. Wang, H. Chen, K. Liang, 2021.

6. Blockchain-Based Distributive Auction for Relay-Assisted Secure Communications / A. S. Khan, Y. Rahulamathavan, B. Basutli, G. Zheng, B. Assadhan, S. Lambotharan, 2019.

7. Preventing Price Manipulation Attack by Front-Running / Y. Xue, X. Sun, X. Zhang, Z. Xia, E. Bertino, 2022.

Артюх С. Г. (ВІТІ ім. Героїв Крут)
д-р техн. наук **Жук О. В**. (НУОУ)
д-р іст. наук **Машталір В. В.** (НУОУ)

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ВТОРГНЕНЬ У БЕЗПРОВОДОВИХ СЕНСОРНИХ МЕРЕЖАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Безпроводові сенсорні мережі (*Wireless Sensor Network*) розподілені мережі, що складаються з маленьких вузлів (сенсорів), з інтегрованими функціями моніторингу параметрів навколишнього середовища, обробки і передачі даних.

Крім вразливостей мобільних радіомереж, в безпроводових сенсорних мережах (БСМ) існують специфічні вразливості, що пов'язані з обмеженим ресурсом мережі, відсутністю фізичного контролю вузлів (сенсорів) й особливостями безпроводового зв'язку між ними. Це створює ряд передумов для реалізації фізичних та кібернетичних атак на них та висуває вимоги до розробки ефективних систем виявлення вторгнень (СВВ) БСМ, які будуть враховувати особливості функціонування мереж даного класу.

СВВ є набором програмних й апаратних рішень, що забезпечують автоматичне виявлення спроб неавторизованого доступу до даних, ідентифікацію атак і запобігання спотворенню, знищенню або блокуванню інформації.

Метою доповіді є проведення аналізу методів виявлення вторгнень безпроводових сенсорних мереж військового призначення, визначення їх основних переваг та недоліків.

Під час досліджень було проаналізовано СВВ БСМ та запропоновано класифікацію методів виявлення вторгнень, які поділяються на чотири класи: на основі сигнатур; на основі аномалій; на основі специфікацій; гібридні. В таблиці 1 наведено основні переваги та недоліки для кожного класу.

Таблиця 1

Переваги та недоліки методів виявлення вторгнень

Тип СВВ	Переваги	Недоліки
На основі сигнатур	Висока точність та швидкість виявлення відомих атак. Простота в налаштуванні та впровадженні	Неефективні проти нових атак. Потребують постійного оновлення. Потребують великого об'єму пам'яті
На основі аномалій	Ефективність проти невідомих атак. Адаптивність. Глибокий аналіз і здатність до самонавчання	Висока складність реалізації. Велика кількість помилкових виявлень. Потребують значних обсягів даних
На основі специфікацій	Ефективність проти відомих атак. Гнучкість налаштування. Мінімальна кількість помилкових виявлень. Захист від внутрішніх загроз	Складність налаштування. Потребують більше часу для розробки правил. Потребують постійного оновлення
Гібридні	Висока точність виявлення невідомих атак. Гнучкість налаштування. Ефективність проти невідомих атак	Складність налаштування та управління. Високі вимоги до ресурсів вузлів. Потенційні конфлікти між методами

Проведений аналіз методів виявлення вторгнень дозволяє зробити висновок, що при реалізації СВВ БСМ військового призначення вибір певного методу буде залежати від місця та особливостей застосування мережі, її типу та розмірності, вибраного способу управління, характеристиками вузлів тощо. Напрямом подальших досліджень є розроблення функціональної моделі СВВ БСМ військового призначення із застосуванням технологій інтелектуальних багатоагентних систем на основі нейронних мереж.

канд. військ. наук, доц. **Бабенко О. І.** (ХНУПС)
Сізон Д. О. (ХНУПС)
Косенко В. П. (ХНУПС)

СИСТЕМНИЙ АНАЛІЗ І СИНТЕЗ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ

Якість виконання завдань забезпечення кіберзахисту в значній мірі залежить від системи підтримки прийняття рішень. Удосконалення (створення) системи підтримки прийняття рішень пропонується проводити з використанням методів системного аналізу та синтезу.

Три основні взаємопов'язані напрямки аналізу та синтезу включають синтез систем підтримки прийняття рішень, організаційне вдосконалення та автоматизацію процесів підтримки прийняття рішень.

Перший напрямок включає наступні елементи:

аналіз об'єкта управління та існуючої системи підтримки прийняття рішень;

побудова концептуальної моделі;

аналіз існуючих методів дослідження та моделювання систем підтримки прийняття рішень, їх вибір та доопрацювання;

вибір критеріїв оцінки спроможності системи підтримки прийняття рішень;

побудова та безпосередньо моделювання системи підтримки прийняття рішень;

аналіз моделі та вироблення напрямків синтезу системи підтримки прийняття рішень з урахуванням результатів забезпечення кіберзахисту.

Другий напрямок включає:

аналіз внутрішніх та зовнішніх факторів, що визначають процес удосконалення системи підтримки прийняття рішень;

розробку інформаційної моделі функціонування процесів вдосконалення системи підтримки прийняття рішень;

розробку науково-обґрунтованих принципів та методів забезпечення кіберзахисту та на їх основі синтезу системи.

Третій напрямок включає:

оцінку якості існуючих інформаційних систем та відповідності їх заданим вимогам;

розробку методології застосування нових інформаційних технологій у системах підтримки прийняття рішень з урахуванням оцінки їх достовірності та безпеки.

Для синтезу безпосередньо систем підтримки прийняття рішень доцільно застосовувати підхід, що ґрунтується на аналізі дерева завдань. Сукупність завдань, що послідовно подрібнюються відповідно до знижувального рівня підсистем формує дерево завдань, що дозволяє проводити аналіз підсистем системи підтримки прийняття рішень.

Підсистеми, які діють за умов невизначеності, вимагають використання в інформаційних системах систем підтримки прийняття рішень. Алгоритм роботи цієї системи, спосіб її функціонування залежить від конкретних підзавдань, від того, на користь якої підсистеми вона функціонує в даний момент часу.

Висновки. Алгоритм оптимізації синтезу систем підтримки прийняття рішень для забезпечення кіберзахисту:

1. *Аналіз та моделювання системи підтримки прийняття рішень.* Включає побудову концептуальної моделі системи та вибір критеріїв для оцінки її спроможності.

2. *Синтез та розвиток системи.* Базується на побудованій моделі для планування організаційного розвитку та включає створення моніторингу поточного стану системи.

3. *Оцінка та інновації.* Включає оцінку якості використовуваних і нових автоматизованих систем, аналіз можливостей застосування нових інформаційних технологій та розробку методології їх застосування у відповідності до конкретних умов функціонування системи.

д-р техн. наук **Бучма І. М.** (НУ ЛП)

ЕЛЕКТРОМАГНІТНИЙ МЕТОД ВИЯВЛЕННЯ РУХОМИХ ПРОВІДНИХ ТІЛ НА НИЗЬКИХ ВИСОТАХ

Вступ. В геофізиці давно застосовують вихрострумовий метод з використанням штучних гармонічних електромагнітних полів для розвідки родовищ поліметалічних руд, які характеризуються діамагнітними властивостями[1]. При цьому вимірюють або відношення півосей еліпса поляризації магнітного поля або відношення квадратурної компоненти вторинного (вихрострумового) магнітного поля до сумарного магнітного поля. Для розвідки родовищ руд з феромагнітними властивостями метод не застосовувався, тому що згідно із статичною моделлю мала піввісь еліпса поляризації магнітного поля або квадратурна компонента вторинного магнітного поля є меншими ніж поріг чутливості вимірювача [2]. Експериментальні дослідження рухомих повітряних вихрострумових геофізичних систем показали, що при пролітанні над провідними тілами з феромагнітними властивостями на виході вимірювача отримується сигнал на вигляд подібний до одного періоду синусоїди. Отже тут статична модель електророзвідки не працює. Автору вдалося запропонувати динамічну модель електророзвідки [3].

В роботі **поставлена задача** на основі динамічної моделі оцінити придатність статичних (наземних) вихрострумових електророзвідувальних систем без будь-якого перероблення до виявлення рухомих повітряних тіл як з діамагнітними, так і з феромагнітними властивостями в локальному повітряному просторі, що опромінюється гармонічним електромагнітним полем, порівняти сигнали на виході вимірювача системи за формою, виявнити чи їх можна відрізнити один від одного та встановити момент часу, в який тіло перебуває в точці, що є найближчою до центру збудника поля.

Метою роботи є доведення отриманих результатів до наукової спільноти, пошук зацікавлених у можливому застосуванні в галузях геофізики, вимірювальної техніки, протиповітряної оборони та визначення напрямків подальших досліджень.

Виклад основного матеріалу. На основі динамічної моделі отримано вирази для вихідних сигналів вимірювача при пролітанні через локальний повітряний простір, що опромінюється гармонічним електромагнітним полем, провідного тіла з феромагнітними властивостями та провідного тіла з діамагнітними властивостями. Встановлено, що квадратурна складова сигналу від тіла з феромагнітними властивостями виникає в результаті того, що магнітна складова вторинного магнітного поля, яка є функцією часу, множиться на синус кута, що є також функцією часу. Тому при диференціюванні магнітного потоку в приймальній петлі виникає квадратурна складова, пропорційна також і куту, який змінює знак при про літанні через точку, що є найближчою до центру збудника первинного поля. Тому обвідна цього сигналу подібна до одного періоду синусоїди.

Для тіла з діамагнітними властивостями квадратурна складова вторинного магнітного поля пропорційна косинусу кута. Тому при зміні знаку кута косинус знаку не змінює. І обвідна сигналу в цьому випадку має вигляд одиночного імпульсу.

Висновки. В роботі встановлено причини, які зумовлюють форму сигналу на виході вимірювача геофізичної системи. По формі сигналу можна судити про наявність в локальному просторі рухомого провідного тіла та його магнітні властивості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мизюк Л. Я., Поджарый В. М., Проць Р. В. Измерение инвариантов магнитного поля при электроразведке. Издательство „Наукова думка", Киев, 1976. 231 с.

2. Мизюк Л. Я. О состоянии и некоторых перспективах развития информационно-измерительных систем для наземных методов индуктивной электроразведки. В кн. Отбор и передача информации. „Наукова думка", Киев, 1970, № 26. С. 49–58.

3. Ігор Бучма. Моделі взаємодії електромагнітного поля рухомих систем низькочастотної індуктивної електророзвідки та провідних феромагнітних тіл. Фізико-математичне моделювання та інформаційні технології. № 38, 2023. С. 113–127. DOI: 10.15407/fmmit2023.38.113.

Верблюд В. О. (НДІ ВР)
Корчомний Р. О. (НДІ ВР)
Кульбачна Н. М. (НДІ ВР)
Усатенко С. О. (НДІ ВР)

ВИЗНАЧЕННЯ ДАНИХ АУДИТУ ЩОДО ПІДКЛЮЧЕННЯ ЗНІМНИХ НОСІЇВ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНІЙ СИСТЕМІ

Актуальність. Одним із джерел витоку інформації, яка обробляється в автоматизованій системі (далі – АС), є знімні носії інформації (далі – ЗНІ), які підключаються користувачами до робочих станцій обчислювальної системи АС. Під час проведення розслідувань кіберзлочинів насамперед аналізуються та досліджуються дані системи аудиту, які мають бути впроваджені в АС.

Спираючись на досвід проведення розслідувань щодо порушень політик безпеки в АС, було визначено, що в більшості систем не впроваджено комплекс засобів захисту (далі – КЗЗ), який має відповідати за контроль підключення ЗНІ та ведення аудиту роботи зі ЗНІ, або його неправильно налаштовано. Зазначене знижує рівень захищеності системи та сприяє несанкціонованому витоку інформації.

Постановка задачі. Визначення факту підключення ЗНІ до робочої станції обчислювальної системи АС під керуванням операційної системи Microsoft Windows (далі – ОС).

Мета. Отримання даних про несанкціоноване підключення ЗНІ до обчислювальної системи.

Основні положення. Після підключення USB-пристрою до комп'ютера USB-драйвер створює в ОС об'єкт пристрою. Стек функцій USB-пристрою відноситься до групи драйверів, які залежать від роботи служби Services – Plug and Paly (ім'я служби "PlugPlay"). Під час з'єднання пристрою в журналі подій Eventvwr.msc журналу Security фіксується запис із номером події 6416 (система розпізнала новий зовнішній пристрій), в якому відображається така основна інформація:

EventID – дескриптор події 6416;
TimeCreated SystemTime – системний час створення події;
Event Record – номер запису;
Computer – домен або ім'я комп'ютера;
Device ID – ідентифікатор пристрою;
Device Name – ім'я пристрою;
Class ID – клас пристрою;
Class Name – ім'я класу;
Vendor IDs – ідентифікатор розробника;
Compatible IDs – тип пристрою.

Драйвер пристрою формує ідентифікатор пристрою (Device ID) та записує його в системний реєстр у вигляді USB\VID_xxxx&PID_yyyy&MI_zz. Такий запис містить дані про тип пристрою. У дескрипторі Container ID відображається інформація про розробника пристрою та інша інформація на основі ідентифікатора PID й ідентифікатора VID, наприклад Transcend, TadaTraveler тощо. Також дескриптори містять серійний номер пристрою. Зазначені дані записуються в системному реєстрі: HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\Enum\USB\ VID_xxx, де VID_xxx – це серійний номер пристрою. Запис типу HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Enum\ USB\ VID_058F&PID_6387\VD9GDBVL містить номер пристрою (VD9GDBVL). Тип пристрою USB визначається в дескрипторі DeviceDesc, наприклад "USB Mass Storage Device". Додатково, в системному реєстрі, створюється гілка HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Enum\ USBSTOR. Ключі цієї гілки зберігають додаткові дані про ЗНІ, наприклад, у дескрипторі FrendlyName зберігається інформація про назву пристрою: "USB DISK 2.0 USB Device" тощо. При підключенні ЗНІ, драйвером Windows Driver Framework,

в системному реєстрі створюється гілка HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Enum\ SWD\ WPDBUSENUM, у ключах якої зберігаються дескриптори про маркування ЗНІ. Дескриптор FriendlyName, зазначеної гілки, може містити дані маркування, наприклад 130 НТ або 238 ДСК тощо.

Важливим джерелом даних про підключення ЗНІ є системний журнал аудиту Microsoft-Windows-Partition/Diagnostic, який зберігається в каталозі C:\Windows\System32\winevt\Logs\ у файлі Microsoft-Windows-Partition%4Diagnostic.evtx. Журнал містить дані виключно про носії інформації, які були зареєстровані в системі (USB-диски, SD-флешносії та інші зовнішні накопичувачі). Запис події має номер 1006 та містить таку основну інформацію:

EventID – дескриптор події 1006;

TimeCreated – мітка часу створення події (зазначається час останнього підключення та час останнього відключення носія);

Computer – ім'я комп'ютера;

Security – ідентифікатор безпеки облікового запису користувача;

Capacity – ємність носія;

Manufacter – розробник;

Model – модель пристрою;

SerialNumber – серійний номер носія;

ParentId – інформація про пристрій (ідентифікатор постачальника (Vendor ID), ідентифікатор пристрою (Product ID), серійний номер).

Для автоматизації процесу отримання інформації про ЗНІ, які підключалися до робочої станції, можна розробити програмне забезпечення, що зчитуватиме відповідні маркери з системного реєстру, описані вище, а також робити прив'язку із системними журналами аудиту подій.

Такої інформації буде достатньо для встановлення факту підключення користувачем відповідного USB-пристрою. Приклад інтерфейсу відповідного програмного забезпечення наведено на рис. 1.

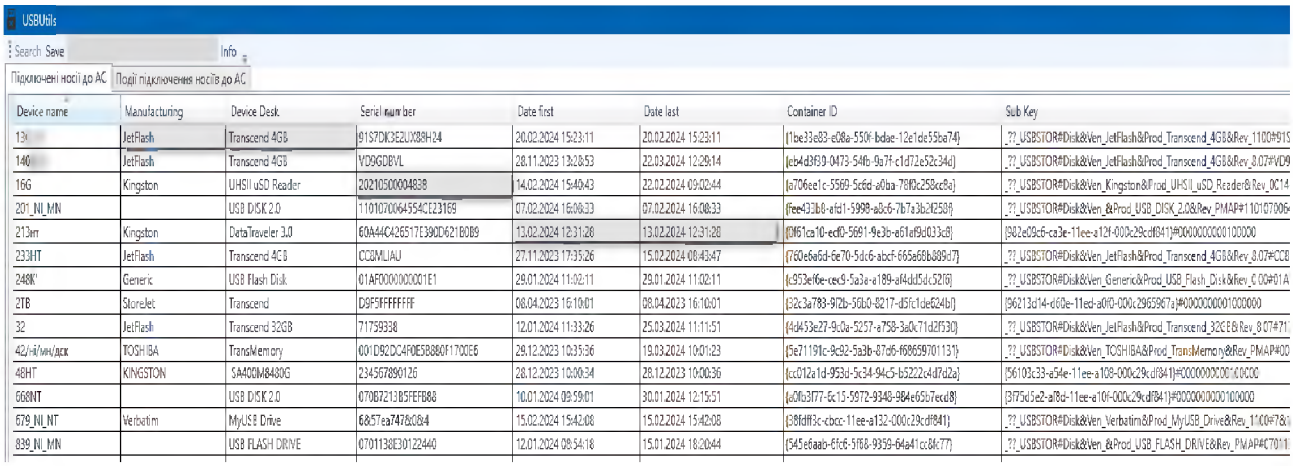


Рис. 1. Інтерфейс програмного забезпечення для встановлення факту підключення ЗНІ

Висновок. Зазначене вище можна використовувати для отримання відомостей про ЗНІ, які підключалися до робочої станції. Ці дані завжди фіксуються ОС по замовчуванню. Таким чином, коли в системі не налаштовано параметри локальної (групової) політики, а також параметри аудиту щодо ЗНІ, під час проведення розслідувань є можливість встановити факти несанкціонованого підключення носіїв інформації.

Голубничий Д. Ю. (АТ «ІІТ»)
Кандій С. О. (АТ «ІІТ», ХНУ ім. В. Н. Каразіна)
Єсіна М. В. (АТ «ІІТ», ХНУ ім. В. Н. Каразіна)
Горбенко Д. Ю. (АТ «ІІТ», ХНУ ім. В. Н. Каразіна)

МЕТОДИ ТА ЗАСОБИ ПОРІВНЯННЯ ВЛАСТИВОСТЕЙ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ТА ВИПАДКОВИХ ЧИСЕЛ

Наразі випадкові послідовності (ВП) та випадкові числа (ВЧ), що виробляються фізично справжніми (PT RNG) та нефізично справжніми (NPT RNG) генераторам, широко застосовуються на практиці – вони по суті законодавчо визначають механізми генерування ключів у криптографічних системах.

1. Джерела шуму, що можуть застосовуватися для генерації ВП та ВЧ на основі PTRNG та NPTRNG

Наразі існує значне число джерел шуму (ДШ), які можливо застосовувати для генерування ВП та ВЧ. Аналіз показав, що ДШ, які можуть задовольняти вимогам, можливо поділити на 2 класи [1-3]: фізичні та нефізичні ДШ.

2. Аналіз вимог щодо ДШ та їх ентропії

Основоположні вимоги до ДШ та їх ентропії запропоновано у [2]. Метою вимог NIST США до джерела ентропії є надання розробнику допомоги в розробці/впровадженні джерела ентропії, яке може надати вихідні дані з постійною кількістю ентропії, а також надати необхідну документацію для перевірки джерела ентропії [1; 2].

3 Методи оцінки ентропій ВП та ВЧ, що згенеровані PTRNG та NPTRNG

Ентропійні методи оцінки ґрунтуються на використанні узагальненого поняття ентропії Реньї [1]. Нехай X – випадкова змінна, що у найбільш узагальненому виді визначає ентропію Реньї. Для випадкової змінної X ентропію Реньї можливо розрахувати

$$H_\alpha(X) = \frac{1}{1-\alpha}\log_2 \sum_{i=1}^{k} (Pr[X=\omega_i])^\alpha, 0 \le \alpha < \infty. \quad (1)$$

На практиці значеннями параметра α є 1, 2 та ∞. При α є 1 із (1) отримуємо співвідношення для оцінки ентропії Шеннона, при α є 2 – для оцінки колізійної ентропії, а при α є ∞ – для оцінки мінімальній ентропії.

На рис. 1 для прикладу зображені ентропії для бінарних випадкових змінних.

Таким чином, задаючи значення ймовірностей $Pr[X=\omega_i]$, по кривим рис. 1 перевіряється, чи виконується практично співвідношення між H, H_2, H_{min}. Якщо так, то приймається рішення, що послідовність відповідає ентропійним критеріям випадковості.

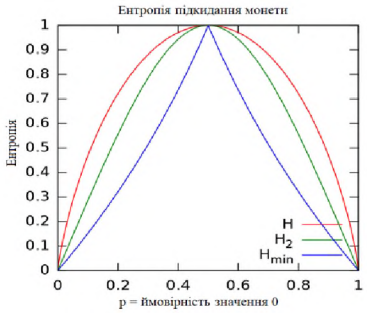


Рис. 1. Мінімальна, колізійна та ентропія Шеннона для випадкових бінарних змінних

На рис. 2 наведено експериментальні дані оцінки мінімальної ентропії бінарних послідовностей для $p=\{0.5, 0.6, 0.7, .0.8, 0.9\}$ на послідовності довжини 10^6 біт.

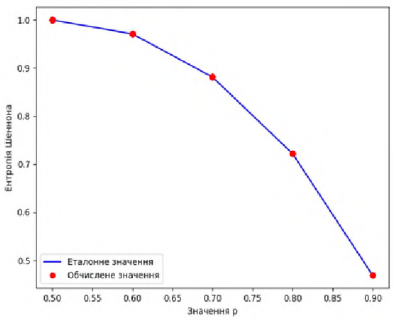


Рис. 2. Експериментальна оцінка ентропії Шеннона

На рис. 3 наведено експериментальні дані оцінки колізійної ентропії бінарних послідовностей для $p = \{0.5, 0.6, 0.7, .0.8, 0.9\}$ на послідовності довжини 10^6 біт.

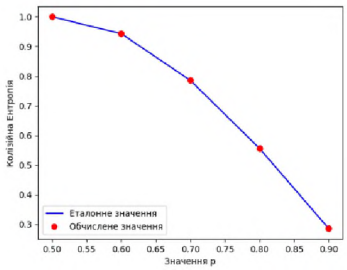


Рис. 3 – Експериментальна перевірка оцінки колізійної ентропії

На рис. 4 наведено експериментальні дані оцінки колізійної ентропії бінарних послідовностей для $p = \{0.5, 0.6, 0.7, .0.8, 0.9\}$ на послідовності довжини 10^6 біт.

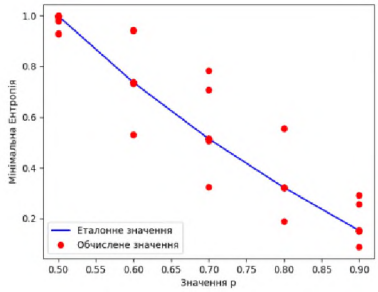


Рис. 4. Експериментальна перевірка оцінки мінімальної ентропії

З отриманих даних випливає, що ентропію Шеннона та колізійну ентропію можливо оцінити доволі точно, у той час як мінімальну ентропію оцінити складніше. Проте, мінімальна ентропія є важливим показником для багатьох практичних застосувань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. BSI AIS 31. A Proposal for Functionality Classes for Random Number Generators, September 2022. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/Interpretations/AIS_31_Functionality_classes_for_random_number_generators_e.pdf?__blob=publicationFile&v=7.

2. NIST SP 800-90 B: M. Turan, E. Barker, J. Kelsey, K. McKay, M. Baish, M. Boyle: Recommendation for the Entropy Sources Used for Random Bit Generation. January 2018. – URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf.

3. NIST SP 800-90 C, Third Draft: E. Barker, J. Kelsey: Recommendation for Random Bit Generator (RBG) Constructions. September 2022. URL: https://nvlpubs.nist.gov/nistpubs/pecialPublications/NIST.SP.800-90C.3pd.pdf.

Горбенко І. Д. (АТ ІІТ, ХНУ ім. В. Н. Каразіна)
Дерев'янко Я. А. (АТ ІІТ)
Горбенко Д. Ю. (ХНУ ім. В. Н. Каразіна)

ДНК – ДЖЕРЕЛО ШУМУ ТА НЕФІЗИЧНИХ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ. ОСНОВНІ ПОЛОЖЕННЯ ПРАКТИЧНИХ ДОСЛІДЖЕНЬ

В криптографічних застосунках захищеність криптоперетворень та криптопротоколів забезпечується використанням в якості ключів та загальних параметрів надійних (псевдо)випадкових послідовностей (ВП). Такі послідовності обчислюються (генеруються) на основі фізичних та нефізичних джерел шуму (ДШ). На наш погляд, можливим є використання у якості ДШ та відповідно джерела ВП ДНК. Попередній аналіз вказує на те, що якість ВП обов'язково повинна бути експериментально підтверджена на основі стохастичних та статистичних досліджень. Стохастичні дослідження, як правило, виконуються на основі аналізу ентропії Реньї [1], а статистичні на основі, наприклад, стандарту NIST 800-22 [2].

Метою цієї доповіді є обґрунтування у якості моделі нефізичного ДШ – ДНК, а також попереднє визначення практичних застосувань таких ВП на основі екстракції [3].

Дезоксирибонуклеїнова кислота (ДНК) – природна нуклеїнова кислота, забезпечує зберігання, передавання і впровадження генетичної інформації живих організмів. Основним її призначенням є довготривале зберігання відомостей про структуру РНК і білків. ДНК складається з 4 видів азотистих основ (аденін, гуанін, тимін і цитозин). Зважаючи на це ДНК можна представити у вигляді послідовності азотистих основ наступним чином (рис. 1):

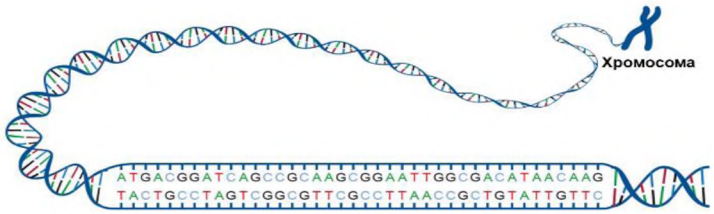


Рис. 1. Представлення ДНК у вигляді послідовності азотистих основ

Експериментальні дослідження виконані у такій послідовності:

1. Аналіз теоретичної та практичної можливості отримання двійкових послідовностей або послідовностей довільного алфавіту з послідовностей ДНК.

2. Вибір 6 зразків ДНК різних організмів. Послідовності ДНК було взято з DNA Data Bank of Japan [4], оскільки пошук там є більш зручним. Так можна шукати за організмом, його типом, довжиною ДНК послідовності і т.д.

3. Аналіз відомостей про обрані послідовності ДНК за критеріями: організм; опис; довжина послідовності ДНК (кількість азотистих основ), що буде використовуватись.

4. Детальне дослідження та розробка різних методів отримання двійкових послідовностей та послідовностей довільного алфавіту з ДНК: метод прямого перетворення, метод транскрипції послідовності ДНК у РНК, з подальшою трансляцією у білкову послідовність без урахування «старт» та «стоп» кодонів та подібний метод, але з урахуванням «старт» та «стоп» кодонів.

5. Вибір кращого з методів на основі аналізу отриманих двійкових послідовностей та послідовностей довільного алфавіту (Метод транскрипції з урахуванням «старт» та «стоп» кодонів).

6. Представлення ДНК у вигляді білків і подальше перетворення послідовностей білків на двійкові послідовності (рис. 2):

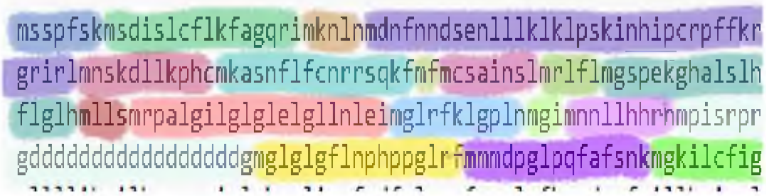


Рис. 2. Послідовність білків з урахуванням «старт» та «стоп» кодонів

7. Дослідження статистичних та стохастичних «сирих» послідовностей з ДНК, наприклад послідовностей з ДНК Homo Sapiens.

8. Оскільки «сирі» послідовності не повністю задовольняють вимогам – виконання екстракції послідовностей на основі стандарту ДСТУ 7624:2014.

9. Результати статистичного дослідження з використанням NIST 800-22, а також стохастичного тестування методами ентропій підтвердили випадковість та рівномірність послідовностей з екстрактора.

Усі згенеровані послідовності успішно пройшли статистичне тестування. Найкращий результат для більш жорсткого критерію показала послідовність з ДНК людини, для неї успішно пройдено 143 тести (76 %). Для більш послабленого критерію найкращою є послідовність з ДНК калини, оскільки проходить всі 189 тестів (100 %). Приклад статистичного портрету однієї з послідовностей (рис. 3):

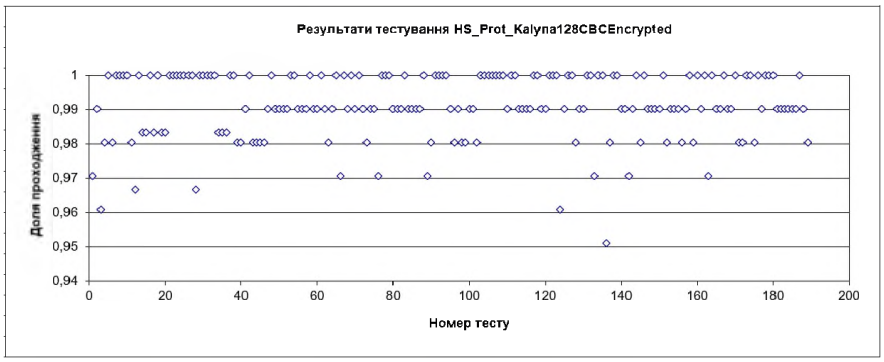


Рис. 3. Статистичний портрет HS_Prot_Kalyna128CBCEncrypted

Подібність послідовностей з одного ДШ можливо оцінити через колізійну ентропію. Колізійна ентропія дозволяє перевірити ймовірність того, що дві незалежні випадкові величини, які є однаково розподіленими, приймуть однакове значення. Для перевірки цього досліджувались послідовності з ДНК людини, каламоїхта калабарського, калини, кота, тощо. Дослідження дають обнадійливі результати, з них можна зробити висновок щодо необхідності проведення подальших оцінок методами ентропії Реньї – ентропії Шеннона, колізійної та мінімальної ентропій – та порівняння їхніх результатів [1]

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Matthias Peter, Werner Schindler. A Proposal for Functionality Classes for Random Number Generators. 2022. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/Interpretations/AIS_31_Functionality_classes_for_random_number_generators_e.pdf?__blob=publicationFile&v=7.

2. NIST SP 800-22 Rev. 1. 2010. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf.

3. L. Trevisan, S. Vadhan. Extracting randomness from samplable distributions. 2000. URL: https://people.seas.harvard.edu/~salil/research/samplable-Apr00.pdf.

4. ДНК банк Японії. URL: https://ddbj.nig.ac.jp/arsa/quick_search?lang=en;jsessionid=5FC7A34BD7FA0826284A6619E85BCA97.

УДК 681.35

Денисюк М. В. ORCID: 0009-0007-7735-4615 (ВІТІ ім. Героїв Крут)
канд. техн. наук **Хусаінов П. В.** ORCID: 0000-0002-0675-0369 (ВІТІ ім. Героїв Крут)

ІНФОРМАЦІЙНА ПІДГОТОВКА РІШЕНЬ ЩОДО КОМПРОМЕТАЦІЇ СИСТЕМИ ОБ'ЄКТА КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Об'єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури. Компрометація системи об'єкта критичної інформаційної інфраструктури є порушенням її сталого, надійного та штатного режиму функціонування, конфіденційності, цілісності, доступності інформації, що обробляється. Перевірка ефективності заходів захисту об'єкта критичної інформаційної інфраструктури здійснюється шляхом виконання періодичних (не рідше одного разу на рік) тестів на проникнення (Penetration Tests) на основі пошуку та виявлення потенційної вразливості. Під час пошуку потенційної вразливості системи дослідник може здійснювати аналіз алгоритмів штатного режиму функціонування системи, нагляд за порядком, результатами виконання завдань, пошук ознак відомих вразливостей (на підставі досвіду експлуатації інших аналогічних систем). Сукупність методів та способів одержання інформації про потенційну вразливістьоб'єкту дослідження розглядається в контексті тактик Reconnaissance, Discovery, Credential Access, Collection, Exfiltration [1–4].

Процес застосування вектору компрометації системи під час тестування на проникнення на основі пошуку та виявлення потенційної вразливості доцільно досліджувати у термінах науково-методичного апарату систем підтримки прийняття рішень. Складовими процесу прийняття рішень є послідовність етапів інформаційної підготовки, вибору та реалізації рішення. Інформаційна підготовка рішення зазвичай складає до 50–80 % від загальної тривалості процесу прийняття рішень.

Цілеспрямована діяльність щодо компрометації системи під час тестування на проникнення реалізується за схемою: мета – план дій – необхідні програмно-апаратні засоби – результат. Мета, в контексті цілеспрямованої діяльності, відображає певну уяву про стан або результат, який має вагому цінність або корисність для суб'єкта. Планування дій стає необхідним коли відсутня їх передбачувана послідовність для конкретної ситуації, особливо, при забезпечення виконання складних або у повній мірі невизначених завдань з багатьма факторами та обмеженнями. Необхідні програмно-апаратні засоби обумовлені контекстом здійснення процедур Reconnaissance, Discovery, Credential Access, Collection, Exfiltration. В якості базового елементу організації знань про предметну область пропонується використання поняття гіпотези про можливе рішення.

Висновки. Ефективність вибору вектору компрометації системи при виконанні завдань тестування на проникнення для об'єкта критичної інформаційної інфраструктури може бути суттєво покращена шляхом оперативного синтезу можливих варіантів дій щодо пошуку та виявлення потенційної вразливості за результатами Reconnaissance, Discovery, Credential Access, Collection, Exfiltration.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 3 липня 2023 року "Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі".

2. Постанова Кабінету Міністрів України від 19 червня 2019 року № 518 "Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури".

3. Постанова Кабінету Міністрів України від 16 травні 2023 року № 497 "Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж".

4. Adversarial Tactics, Techniques & Common Knowledge (https://attack.mitre.org).

канд. техн. наук **Залужний О. В.** (ВІТІ ім. Героїв Крут)
д-р техн. наук, ст. наук. співр. **Чевардін В. Є.** (ВІТІ ім. Героїв Крут)
канд. техн. наук **Юрченко О. В.** (ВІТІ ім. Героїв Крут)

ДОСЛІДЖЕННЯ СЦЕНАРІЇВ КОНКУРЕНТНИХ АТАК НА МОДЕЛІ МАШИННОГО НАВЧАННЯ СИСТЕМ КІБЕРЗАХИСТУ

В наш час активно застосовуються технології машинного навчання в системах кіберзахисту. Разом з тим зловмисники шукають способи обходу таких систем, використовуючи при цьому атаки, що орієнтовані, виключно, на протидію штучному інтелекту, – конкурентні атаки (adversarial attacks). Тому актуальним науково-технічним завданням є дослідження існуючих сценаріїв реалізації конкурентних атак.

Метою досліджень є визначення напрямків підвищення стійкості моделей машинного навчання систем кіберзахисту до впливу конкурентних атак.

Підчас досліджень було проаналізовано відомі сценарії здійснення конкурентних атак на моделі машинного навчання (ML-моделі) та наведено приклади їх раелізації, а саме:

сценарій 1 – атака на основі відгуку ML-моделі (Inference Attack);

сценарій 2 – атака на ML-модель під час її навчання (Training Time Attack);

сценарій 3 – атака на ML-модель клієнта або периферійному пристрою (Attack on Edge/Client).

Перший сценарії є найпоширенішим, при його реалізації зловмисник може лише надсилати запити до моделі і спостерігати за її відповіддю. У випадку використання другого сценарію зловмисник контролює навчальні дані, отримавши попередньо доступ до них. Третій сценарій передбачає, що ML-модель встановлена у клієнта (наприклад, у телефоні) або використовується на периферійному пристрої (наприклад, IoT пристрій). Зловмисник може оцінити алгоритми функціонування моделі шляхом застосування методів реверс-інжинірингу до служби, встановленої у клієнта. За цими сценаріями можуть бути реалізовані конкурентні атаки ухилення (Evasion), отруєння (Poisoning), функціонального вилучення моделі (Functional Extraction model), інверсії (Inversion), атака на приналежність (membership inference attack). В таблиці 1 наведено узагальнену класифікацію конкурентних атак на ML-моделі систем кіберзахисту та сценарії за якими вони здійснюються.

Таблиця 1

Класифікація конкурентних атак на ML-моделі систем кіберзахисту

Атака	Опис атаки	Сценарій
Ухилення	Зловмисник змінює запит до моделі, щоб отримати бажаний результат (обійти захист). Для цього йому потрібно вивчити функціонування моделі, навіть не знаючи її алгоритмів. Такі атаки виконуються шляхом надсилання різних за змістом запитів до моделі та спостереження за результатом (відгуком моделі)	Сценарій 1
Отруєння	Зловмисник отримує доступ та змінює навчальні дані ML-моделі або саму модель, щоб отримати бажаний результат її роботи. Модель може бути «перепрограмована» для виконання нового непередбаченого розробниками завдання. Доступ до навчальних даних також може призвести до компрометації особистих даних користувачів	Сценарій 2
Функціональне вилучення моделі	Зловмисник створює (відтворює) функціонально еквівалентну модель (офлайн-копію моделі) шляхом ітераційних запитів до моделі ML та оцінки відгуків. Це дозволяє зловмиснику перевірити створену офлайн-копію моделі перед подальшою атакою на онлайн-модель (робоча модель)	Сценарій 3

У доповіді розглянуто декілька прикладів успішних конкурентних атак, які здійснювались за різними сценаріями.

Атаки ухилення. Дослідницька група Palo Alto Networks Security AI змогла обійти детектор, який здійснює виявлення доменних імен, що створені з використанням Domain Generation Algorithm (DGA). Для цього вони провели пошук наукових праць та технічних

рішень на основі штучного інтелекту, що пов'язані з виявленням DGA. Далі – протестували загальнодоступну модель виявлення DGA. На наступному кроці, скориставшись результатами наукових публікацій, – розробили техніку «мутації» доменних імен. Запропонована техніка «мутації» дозволила уникати виявлення DGA.

Дослідники компанії SkylightCyber змогли знайти універсальний спосіб обходу антивірусного програмного засобу (АВПЗ) «Cylance», який функціонує на основі штучного інтелекту. Спочатку вони зібрали та проаналізували інформацію про об'єкт атаки з відкритих джерел (аналіз наукових публікацій, препринтів). Далі було здійснено емпіричне тестування різних нешкідливих і шкідливих файлів та проаналізовано журнали подій АВПЗ. Наступним кроком було здійснення реверс інжинірингу коду програми для визначення особливостей формування вектору ознак. На основі проведених досліджень вдалось сформувати список рядків, які необхідно додати до шкідливого файлу для того, щоб значно зменшити ймовірність його детектування.

Атака отруєння. Дослідниками компанії McAfee було помічено незвичне збільшення кількості звітів про відоме сімейство програм-вимагачів. Під час розслідування було виявлено, що зловмисники використали зразок шкідливого програмного забезпечення з поширеного сімейства програм-вимагачів, як основу для створення «мутантних» варіантів, які вони завантажили на популярну платформу обміну вірусами. Як наслідок, системи захисту почали класифікувати файли, як сімейство програм-вимагачів, хоча більшість із цих файлів, навіть, не запускались. Зразки «мутантів» отруїли набір даних, які ML-модель використовує для ідентифікації та класифікації цього сімейства програм-вимагачів.

Атака функціонального вилучення. Дослідницька група Palo Alto Networks Security AI випробувала Deep Learning модель (DL-модель) для виявлення трафіку контролю та управління (C2-трафік) шкідливим програмним забезпеченням у HTTP-трафіку (робоча модель). Спочатку вони провели збір та аналіз інформації з відкритих джерел про об'єкт здійснення атаки. На основі проведеного аналізу створили функціонально-еквівалентну модель (ФЕМ). Протестували її на відомих наборах даних та провели коригування параметрів. З використанням ФЕМ створили зразки ухилення. Далі вони протестували зразки ухилення на робочій моделі, які були визначені, як доброякісні.

Випадок CVE-2019-20634 описує, як було здійснено ухилитися від системи захисту електронної пошти ProofPoint, яка використовує заголовки електронних листів для детектування шкідливого вмісту. Для цього було надіслано велику кількість електронних листів та зібрано оцінки моделі ML Proofpoint. Визначено, яка змінна в оцінці відповідає за безпеку електронної пошти. Використовуючи ці оцінки, побудовано ФЕМ. З її використанням, створено шкідливі електронні листи, які змогли обійти системи захисту електронної пошти ProofPoint.

За результатами досліджень було встановлено, що для підвищення стійкості систем кіберзахисту зі штучним інтелектом до впливу конкурентних атак необхідно:

забезпечувати збір та агрегацію навчальних даних кожною системою окремо, а не отримувати їх із загально-доступних джерел;

обмежувати кількість інформації у відкритих джерелах про особливості функціонування робочих моделей систем кіберзахисту;

у випадку розгортання систем кіберзахисту на об'єктах критичної інфраструктури використовувати спеціально розроблені ML-моделі, яких немає в загальному доступі, що ускладнить можливість створення їх ФЕМ;

здійснювати розробку алгоритмів детектування конкурентних атак, які виявляють аномалії в поведінці ML-моделей систем кіберзахисту або вхідних даних і надають можливість реагувати на них.

використовувати технології шифрування та електронного підпису, щоб забезпечити цілісність та автентифікацію навчальних даних.

Напрямком подальших досліджень є аналіз ефективності існуючих методів підвищення стійкості систем кіберзахисту зі штучним інтелектом до впливу конкурентних атак.

Кондратюк М. А. (НАУ)
Кондратюк А. Г. (ВІТІ ім. Героїв Крут)

ВЕКТОРИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В СФЕРІ КІБЕРБЕЗПЕКИ

У зв'язку із хвилеподібним зростанням обсягів цифрової активності та загроз кібербезпеці й ускладненням тактик і методик проведення кібератак актуальним постає питання вдосконалення методів виявлення та протидії кіберзагрозам. Це важко уявити без застосування технологій штучного інтелекту (ШІ) які стають одним із центральних інструментів захисту від кіберзлочинності та активно використовуються в проведені кібероперацій в сучасних кібервійнах.

Існує велика кількість рішень з кібербезпеки, що використовують технології ШІ і можуть застосовуватися в різних напрямках. Визначення векторів використання технологій штучного інтелекту в сфері кібербезпеки дозволить побудувати більш ефективну систему інформаційної безпеки. Розглянемо основні з них:

1. Виявлення та класифікація кіберзагроз. В сучасному цифровому світі кіберзагрози стають все більш небезпечними та розповсюдженими, зокрема через поширення шкідливого програмного забезпечення (ШПЗ), використання при проведенні атак методів соціальної інженерії (СІ) таких як фішинг та ін. Алгоритми машинного навчання (МН) виявляються надзвичайно корисними інструментами в цьому контексті, оскільки вони можуть аналізувати великі обсяги даних та виявляти складні патерни, які вказують на наявність кіберзагроз.

Одним з головних аспектів використання алгоритмів МН для розпізнавання та класифікації кіберзагроз є їхній потенціал у виявленні нових, раніше невідомих загроз, які можуть виникнути в майбутньому. Ще одна перевага полягає у здатності цих алгоритмів до навчання на великій кількості даних, що дозволяє їм постійно адаптуватися до нових типів кіберзагроз та покращувати свою ефективність.

Отже, сучасні інструменти що використовуються в розвідці кіберзагроз здатні: вилучати та узагальнювати інформацію щодо індикаторів компрометації; отримувати знання щодо нових тактик, технік та процедур (ТТП) проведення атак; здійснювати прогнозування та розвідку загроз в реальному часі; визначати пріоритети та сортувати загрози на основі впливу, терміновості або серйозності; генерувати оповіщення про загрози. Сьогодні відомі наступні рішення в цьому напрямку на основі технологій ШІ: Trellix Global Threat Intelligence (https://www.trellix.com), IBM Watson (https://www.ibm.com), TCPWave (https://www.tcpwave.in), Palo Alto Networks WILFIRE (https://www.paloaltonetworks.com), ThreatConnect (https://threatconnect.com), Dynatrace (https://www.dynatrace.com).

2. Поведінковий аналіз. Розвиток систем штучного інтелекту для аналізу великих обсягів даних стає необхідністю в контексті постійного зростання обсягів інформації, що генерується в цифровому світі. Системи штучного інтелекту, такі як нейронні мережі та алгоритми МН, можуть аналізувати великі масиви даних з швидкістю та точністю, недосяжними для людського аналізу. Це особливо актуально в контексті кібербезпеки, де фіксується розвиток алгоритмів ШІ які здатні виявляти аномалії мережевого трафіку та поведінки користувачів, що потребує обробки великої кількості даних.

Сучасні рішення для кібербезпеки збирають дані з усіх можливих джерел що розташовані в мережі, на кінцевих точках та хмарних ресурсах. Обробка цих даних разом з існуючими даними аналітики загроз дозволяє проводити інтелектуальне групування аномалій для розуміння підозрілої поведінкової активності та автоматизувати виявлення загроз. Серед відомих рішень з використанням ІІІ можна виділити для: аналізу мережевої поведінки - Cisco Secure Network Analytics (https://www.cisco.com), NetWitness Detect AI (https://www.netwitness.com); для аналізу поведінки користувачів – Userlytics (https://www.userlytics.com), ManageEngine Log 360 (https://www.manageengine.com).

3. Автоматизація процесів реагування на кібератаки. Впровадження автоматизації процесів реагування на кібератаки за допомогою ШІ дозволить відстежувати мільйони подій

безпеки за короткий проміжок часу, що суттєво відрізняється від традиційних стратегій реагування на інциденти. Автоматизація цих процесів скорочує час на управління інцидентами, що призводить до швидкого виявлення загроз і швидкого відновлення. У порівнянні з ручними методами, системи реагування на інциденти безпеки на основі ІІІ та МН працюють швидше і менш схильні до людських помилок. Отже однією з основних переваг автоматизації процесів реагування є здатність знизити час від реакції на виявлення кібератаки до прийняття відповідних заходів для запобігання або мінімізації її наслідків. Інтеграція штучного інтелекту в процес реагування на кібератаки дозволяє автоматизувати не лише виявлення, але й класифікацію атак з метою визначення їхнього типу та потенційного рівня небезпеки.

Відомі рішення для управління подіями та інформацією з безпеки (Security information and event management – SIEM) на основі ШІ аналізують різні події безпеки, виявляючи закономірності та аномалії, щоб поліпшити виявлення загроз і оповіщення про них та навіть організовувати складні робочі процеси реагування – IBM QRadar (https://www.ibm.com).

Ще одним з рішень даного вектору є утиліти для оркестрування, автоматизації та реагування на інциденти безпеки (Security orchestration, automation, and response – SOAR) які інтегрують ІІІ в автоматизацію робочих процесів, яскравим представником якого є Splunk AI (https://www.splunk.com/en_us/solutions/ splunk-artificial-intelligence.html), Swimlane SOAR (https://swimlane.com).

Сьогодні вже неможливо уявити застосування засобів виявлення та реагування на кібератаки на кінцевих точках (Endpoint detection and response – EDR) без технологій ШІ – Symantec Endpoint Protection (https://www.broadcom.com), Coro Endpoint Security (https://www.coro.net).

Все більш популярними стають рішення розширеного виявлення та реагування (XDR) які використовують розширену аналітику, включаючи МН та ШІ, для аналізу зібраних даних на предмет виявлення закономірностей, аномалій та індикаторів компрометації, що допомагає виявляти загрози на ранніх стадіях і підвищує точність – Cynet auto XDR (https://www.cynet.com), Trend Micro Vision One (XDR) (https://www.trendmicro.com), Microsoft XDR (https://www.microsoft.com).

4. Програмні системи для організації роботи та підготовки фахівців кіберзахисту. Chatbot GPT (Generative Pre-trained Transformer) відноситься до типу програми що використовує технології ІІІ, призначеної для імітації спілкування з людьми. Він використовує вдосконалені методи обробки природньої мови та МН, що дозволяє генерувати текстові відповіді, схожі на відповідь людини. Ця технологія використовується в різних програмах, включаючи віртуальних помічників, ботів для обслуговування користувачів та систем інтерактивного навчання. Моделі GPT навчаються генерувати текст на основі великих наборів даних людської мови, що дозволяє їм відповідати на широкий спектр тем і запитів. На теперішній час відомо більш ніж п'ятдесят GPT-агентів що використовуються в сфері кібербезпеки (https://chat.openai.com).

Проаналізувавши вектори використання ШІ можна зробити висновки що основною відмінністю інструментів кібербезпеки де використовуються технології ШІ від традиційних полягає в їх адаптивності та гнучкості. Тоді як традиційні засоби працюють з використанням чітко визначених правил, котрі потрібно з часом оновлювати, інструменти з ШІ виявляють загрози та реагують на них у реальному часі. Здатність таких застосунків обробляти великі обсяги даних під час прийняття рішень є дуже корисною та впливає на швидкість реакції на кіберзагрози. Кіберзлочинці також відстежують розвиток технологій ШІ та використовують їх для створення нових типів кібератак та виявлення вразливостей систем захисту. Це є ще одною причиною застосування даних технологій для побудови ефективного кіберзахисту.

Порівняння алгоритмів та технологій ШІ щодо ефективності їх застосування за різними векторами використання в сфері кібербезпеки є метою подальших досліджень.

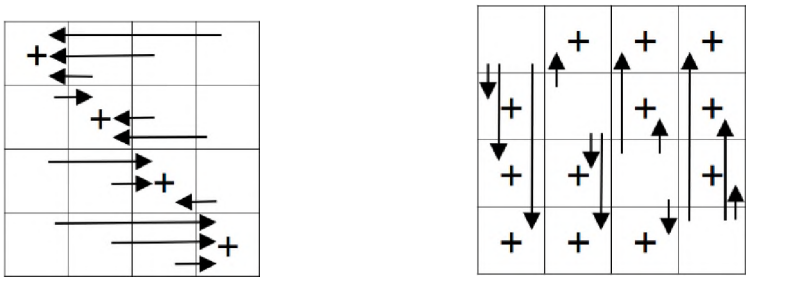
Недождій М. А. (КПІ ім. Ігоря Сікорського)
канд. техн. наук **Яковлєв С. В.** (ВІТІ ім. Героїв Крут)

ПОБУДОВА ДИФЕРЕНЦІАЛЬНОЇ АТАКИ ЗБОЇВ НА МОДИФІКОВАНИЙ ШИФР QALQAN

Симетричний блоковий шифр Qalqan [1] був запропонований у 2021 році як кандидат на національний стандарт шифрування Республіки Казахстан. Даний шифр орієнтований на байтову архітектуру. Розмір блоку складає 128 бітів, довжина ключа може варіюватись від 256 до 1024 бітів з кроком у 128 бітів. Залежно від довжини ключа, схема шифрування містить від 17 до 23 раундів.

Шифр Qalqan побудовано на основі архітектури SP-мережі. Кожен раунд, окрім останнього, складається з 3 операцій: накладання раундового ключа, застосування нелінійного перетворення (S-блоку) та лінійного перетворення L, яке має унікальну структуру; останній раунд містить тільки операцію накладання ключа. У лінійному перетворенні шифру використовується побайтове додавання (тобто додавання за модулем 256 з переносом без виходу за межі байту). Ключі на усіх раундах, окрім першого і останнього, накладаються додаванням за модулем 2^{128}; у першому та останньому раундах накладання ключа відбувається побітовим додаванням $\oplus$.

Блоки відкритого тексту, проміжні шифротексти та раундові ключі представляються матрицями 4×4 байтів. Лінійне перетворення $L: V_{128} \to V_{128}$ складається з фаз «всмоктування» і «розповсюдження». Схему обчислення перетворення L наведено на рис. 1.



а) фаза «всмоктування» б) фаза «розповсюдження»

Рис. 1. Схема роботи лінійного перетворення L

Попередній аналіз криптографічної стійкості шифру Qalqan наведено у [2, 3]. Зокрема, у [2] було показано, що структура шифру має уразливості до диференціальних та лінійних атак, головними з яких є низьке значення індексу розгалуження лінійного перетворення L та велика кількість його нерухомих точок.

У цій роботі розглядаються диференціальні атаки збоїв — атаки на реалізацію криптосистеми у певному обчислювальному середовищі. Основним інструментом таких атак є внесення збоїв у виконання криптографічних операцій для одержання інформації про ключі шифрування на основі відмінностей між коректним та збитим шифротекстами. Для цього збої (випадкові спотворення) вносяться у біти проміжних шифротекстів перед певною операцією раундової функції; аналітику при цьому доступні тільки результати шифрування, тобто фінальні шифротексти, обчислені правильно та зі збоями.

Ми розглядаємо модифіковану версію шифру Qalqan із 17 раундами шифрування та довжиною ключа 256 бітів. Ключі будуть накладатись, як у модифікації, запропонованій [2], побайтовим додаванням $\boxplus$ без переносу за межі байту (тобто так, як додаються у перетворенні L). Відповідно, структура модифікованого шифру Qalqan стає повністю байт-орієнтованою, тому доцільно розглядати усі збої як випадкові спотворення на рівні окремих байтів проміжних шифротекстів.

Атака на останній раунд шифрування визначається такою послідовністю дій:

внесення збою у певний байт матриці;

накладання ключа $K^{(r-1)}$ побайтовим додаванням $\boxplus$;
застосування нелінійного перетворення S-блоку;
застосування лінійного перетворення L;
накладання ключа $K^{(r)}$ побітовим додаванням $\oplus$ (фінальне маскування).

Як приклад, наведемо схему атаки на останній раунд, у якій збій вноситься у діагональний елемент матриці. Накладання ключа побайтовим додаванням, S-блок та маскування ніяк не впливають на розповсюдження збою. Лавинний ефект виникає виключно при застосуванні лінійного перетворення L. При цьому значення збою поширюється на увесь стовпчик (рис. 2), і всі байти стовпчика спотворюються однаково.

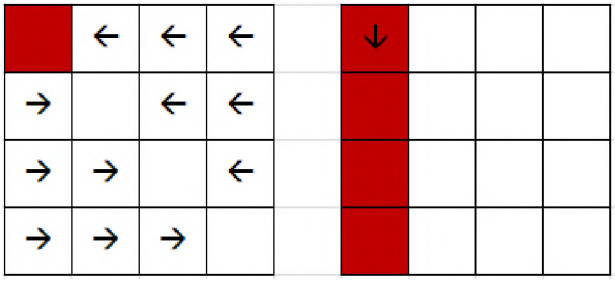


Рис. 2. Лавинний ефект при збитті байту $a_{1,1}$

Позначимо різницю між звичайним і збитим байтами шифротекстів через β. Позначимо лівий стовпчик нормального шифротексту через y_1, y_2, y_3, y_4, тоді лівий стовпчик збитого шифротексту дорівнює $y_i' = y_i \boxplus \beta$. Перебираючи усі можливі значення байтів ключа $K_1^{(r)}$ та $K_2^{(r)}$ (2^{16} варіантів пар ключів) знаходимо усі значення, для яких виконується рівність

$$\left(y_1 \oplus K_1^{(r)}\right) - \left(y_1' \oplus K_1^{(r)}\right) = \left(y_2 \oplus K_2^{(r)}\right) - \left(y_2' \oplus K_2^{(r)}\right)$$

Фіксуємо ці значення, повторюємо для y_3, y_3' та y_4, y_4' і отримуємо кандидати у пари байтів ключа $K_3^{(r)}$, $K_4^{(r)}$. Якщо виявиться, що кандидатів у потенційні пари байтів ключа, для яких виконується співвідношення буде більше, ніж одна, перевіряємо це рівняння на інших четвірках. Перебрати окремо усі можливі розв'язки цих рівнянь значно легше за перебір усіх можливих ключів. Повторюючи збої в інших діагональних комірках, можна аналогічним чином відновити усі байти останнього раундового ключа. Якщо збій виникне в недіагональному байті, то через структуру L він все одно поширюється на окремий стовпчик вихідної матриці, що дозволить провести атаку.

Таким чином, використання різних операцій додавання у лінійному перетворенні та ключовому суматорі дозволяє побудувати ефективну атаку збоїв на шифр Qalqan. В подальшому планується описати детальні атаки на більшу кількість раундів шифрування оригінального шифру Qalqan, із урахуванням впливу бітів переносу у ключовому суматорі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. L. Gorlov, R. Ibrayev, G. Ospanov, R. Itemirov, and I. Kiyashko, "Алгоритм шифрования Qalqan," in Proceedings of VI International Scientific Conference "Computer Science and Applied Mathematics" (September 29 – October 2, 2021, Almaty, the Republic of Kazakhstan), pp. 458–463, 2021. Available at: https://conf.iict.kz/wp-content/uploads/2021/11/6th_csam.29.09-02.10.21_sbornik.pdf.

2. N. Seilova, A. Kungozhin, R. Ibrayev, L. Gorlov, Z. Ospanov, R. Itemirov, and I. Kiyashko, "About Cryptographic Properties of the Qalqan Encryption Algorithm," in CEUR Workshop Proceedings "Cybersecurity Providing in Information and Telecommunication Systems II" — CPITS-II'2021 (October 26, 2021, Kyiv, Ukraine), pp. 206–215, 2021. Available at: https://ceur-ws.org/Vol-3187/paper19.pdf.

3. S. Yakovliev, M. Stolovych. "On the Security of Qalqan Cipher against Differential Cryptanalysis", Theoretical And Applied Cybersecurity, Vol. 4, No. 1, 2022. Available at: https://doi.org/10.20535/tacs.2664-29132022.1.274112.

УДК 681.35

Нещерет В. О. ORCID: 0009-0004-7940-141X (ВІТІ ім. Героїв Крут)
канд. техн. наук **Хусаінов П. В.** ORCID: 0000-0002-0675-0369 (ВІТІ ім. Героїв Крут)

НАДІЙНІСТЬ ПРИХОВАНОГО КАНАЛУ ЗВ'ЯЗКУ БЕКДОРА

Бекдор – технологія, метод та/або засіб обходу засобів захисту з метою несанкціонованого доступу до системи об'єкта кіберзахисту з використанням засобів приховування (каналу) такого обходу та доступу. Прихований канал – спосіб одержання інформації за рахунок використання шляхів передачі інформації, що не контролюється комплексом засобів захисту або шляхом спостереження за існуючими потоками інформації. Розрізняють прихований канал з пам'яттю та з часовим порядком подій. Перший тип реалізується шляхом прямого або непрямого запису інформації в певну область пам'яті одним процесом і прямим чи непрямим читанням даної області пам'яті іншим процесом. Другий тип – шляхом модулювання першим процесом часових характеристик системи, що спостерігаються іншим процесом. Програма з функціями бекдор відноситься до класу шкідливого програмного забезпечення, що передбачає реалізацію несанкціонованих або неавторизованих процесів, які мають прямий або опосередкований вплив на сталий, надійний та штатний режим функціонування системи об'єкта кіберзахисту та порушення властивосте інформації. Сукупність методів та способів створення каналів прихованого каналу зв'язку бекдора у складі об'єкта кіберзахисту розглядається в контексті тактик Command and Control, Exfiltration [1–3].

Надійність включає безвідмовність, довговічність, пристосованість до ремонту. Нерідко, при цьому, вирішальне значення має лише перша характеристика. Безвідмовність – властивість системи безперервно зберігати працездатність. Основним поняттям надійності є поняття відмови тобто поступової або раптової втрати працездатності функціональним елементом. Кількісні і якісні показники надійності (ймовірність відмови, тривалість безвідмовної роботи, тривалість ремонту, вартість відновлення і т. ін.) випадкові.

Для збільшення надійності використовуються таки прийоми як резервування, профілактичні огляди і ремонти, експлуатація при зменшеному навантаженні. Під резервуванням розуміється метод підвищення надійності шляхом внесення надлишковості того чи іншого роду. Розрізняють структурне (додаткові елементи), часове (додатковий час), інформаційне (додаткове копії даних), функціональне (додаткові функції елементів), навантажувальне (додатковий ресурс) резервування.

Апріорний аналіз надійності здійснюється на стадії проектування пристрою (системи, каналу зв'язку), коли намічено кілька можливих варіантів будови. Дозволяє виявити на стадії проектування слабкі з точки зору надійності місця в конструкції і прийняти необхідні заходи щодо їх усунення, а також відкинути деякі незадовільні варіанти побудови системи. На практиці апріорні (ймовірні) кількісні характеристики надійності функціональних елементів пристрою (системи, каналу зв'язку) можуть бути визначені лише для тих, що вже довгий час знаходилися на експлуатації.

Висновки. Апріорний аналіз надійності використання загальнодоступних (відкритих, соціально значущих) інформаційних ресурсів для прихованого каналу зв'язку з бекдором показав, що таки варіанти побудови мають найкращу безвідмовність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України "Про основні засади забезпечення кібербезпеки України".

2. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 3 липня 2023 року "Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі".

3. Adversarial Tactics, Techniques & Common Knowledge (https://attack.mitre.org).

канд. техн. наук. **Остапчук В. М.** ORCID: 0000-0001-5686-0198 (ВІТІ ім. Героїв Крут)
д-р техн. наук, ст. наук. співр. **Чевардін В. Є.** ORCID: 0000-0002-1070-4568 (ВІТІ ім. Героїв Крут)
Бешевець М. О. ORCID: 0009-0001-4793-4789 (ВІТІ ім. Героїв Крут)

ПРОГРАМНИЙ МОДУЛЬ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ КІБЕРАНАЛІТИКОМ

Інформація про вразливості є життєво необхідною для захисту інформаційно-комунікаційних систем в корпоративних підприємствах та особливо в сфері критичної інфраструктури країни. Аналізуючи набір відомих вразливостей, стає можливим їх своєчасне усунення і значне зменшення поверхні кібератаки на організацію, що в свою чергу мінімізує ризики для ексфільтрації даних чи відмови в обслуговуванні відповідного сервісу. Для підвищення обізнаності про вразливості, їх аналізу, ефективної та своєчасної протидії, відмінною та зручною практикою є збір та структурування інформації про вразливості в єдиному централізованому сховищі. Прикладами таких баз знань є такі електронні вебресурси, як cvedetails.com, vulners.com, exploit-db.com.

CVEdetails є широкою відкритою базою даних, яка збирає та систематизує відомості про вразливості, що були ідентифіковані у програмному забезпеченні чи операційних системах. CVEdetails включає розгорнуті бази даних метасплойтів та рекомендації щодо забезпечення кіберзахисту, RSS-канали для отримання інформації про нові вразливості, що в свою чергу значно підвищує її актуальність. CVEdetails спрощує розробку стратегій протидії та формування моделей кіберзахисту.

Розроблений програмний застосунок з вебінтерфейсом, виступає як логічний та необхідний крок до синтезу та оптимізації існуючих даних. Синтез даних щодо CVE, який надається відкритими ресурсами, передбачає структуризацію інформації з різних джерел у єдину, ієрархічно організовану базу, що стане централізованим сховищем відомостей для надійного захисту інформаційних активів. Такий підхід дозволить розробити та впровадити ефективні заходи захисту, підвищуючи рівень кібербезпеки структур. Розроблене програмне рішення має таку архітектуру:

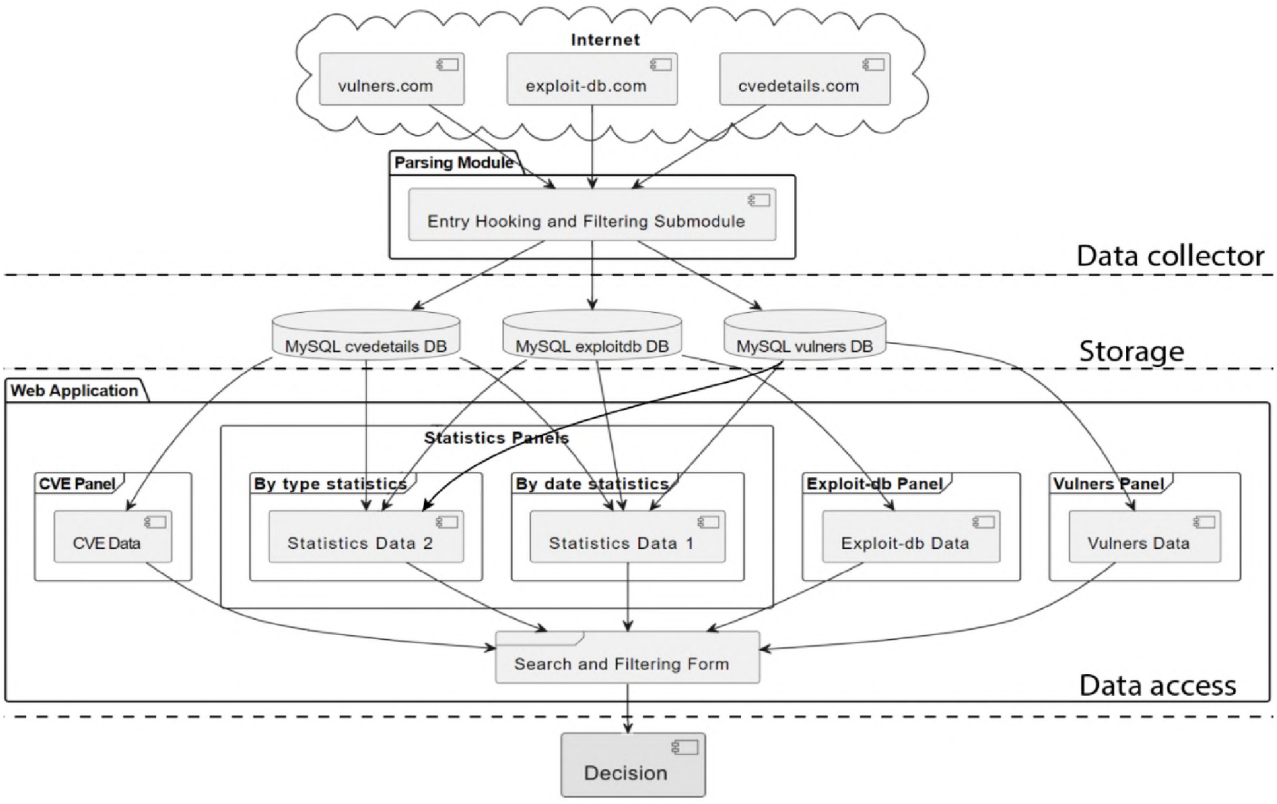


Рис. 1. Модуль надання рекомендацій щодо реагування на виявлену вразливість

Програмне рішення розбите на 3 основних рівні:

1) Data collector – модуль парсингу, який збирає дані про вразливості з загальнодоступних ресурсів з мережі Інтернет. Цей модуль являє собою програму, написаною мовою C# з використанням бібліотеки Html Agility Pack (HAP). Для обробки сотень тисяч записів з зовнішніх ресурсів використовуються максимально оптимізовані запити, весь модуль адаптований під роботу в багатопотоковому режимі. Для збору інформації використовується три основних вебресурси: cvedetails.com, exploit-db.com та vulners.com. Додатково, для підтримки актуальності інформації про вразливості, були написані модулі, які забезпечують автоматичне оновлення баз даних;

2) Storage – сховище інформації. У якості системи управління базою даних було обрано MySQL, яка має велику кількість перевірених інструментів для керування та бібліотек під мову програмування C#;

3) Data access – рівень доступу до даних. Основна мета цього рівня – надання зручного та інтуїтивно зрозумілого інтерфейсу для кінцевого користувача, забезпечення інтерактивності роботи з базою даних, фільтрацію та групування за відповідно вказаними параметрами. Цей модуль представляє собою вебдодаток написаний на мові C# з використанням Active Server Pages Network Enabled Technologies (ASP.NET). Для доступу до другого рівня рішення (бази даних) використовується техніка object–relational mapping (ORM) Entity Framework, яка значно спрощує побудову запитів для роботи з набором даних. Цей рівень включає наступні компоненти графічного інтерфейсу:

- CVE panel – сторінка, яка містить інформацію, статистику та користувацькі елементи пошуку для взаємодією з базою даних ресурсу cvedetails.com;
- Exploit-db panel – сторінка, яка забезпечує взаємодію користувача з базою даних ресурсу exploit-db.com, дозволяє завантажити експлойт та відповідну вразливу версію програмного забезпечення до нього;
- Vulners panel – сторінка, яка призначена для відображення та управління інформацією з ресурсу vulners.com;
- By date – сторінка, де інформація згрупована та структурована з усіх трьох джерел. Вона містить графіки та діаграми, завдяки яким можна простежити тенденції розвитку та появи вразливостей за кількістю і датою виникнення;
- By type – сторінка, де інформація про всі зібрані вразливості згупована за типом та відображена на відповідному графіку. Для забезпечення зручності управління графіком був доданий модуль Java Script, який надає змогу зручно відображати тільки необхідні типи вразливостей;
- Search and filtering form – узагальнена форма для пошуку та фільтрації даних зі всіх баз даних. Імплементовані функції пошуку вразливостей за назвою, датою, оцінкою, типами вразливості, вектором атаки та іншими параметрами.

Така архітектура сприяє зручності управління та простоти подальшого розширення програмного рішення, а реалізовані функції забезпечують зручний та гнучкий користувацький інтерфейс.

Висновки. Розроблене рішення служить важливим інструментом для оперативного збору, аналізу та управління даними про уразливості в інформаційно-комунікаційних системах корпоративних підприємств, особливо в секторі критичної інфраструктури. Модуль забезпечує централізоване зберігання інформації про уразливості, дозволяючи прискорити процес ідентифікації та реагування на вразливі місця в IT-інфраструктурі, тим самим мінімізуючи ризики кібератак та потенційні збитки. Основним завданням програмного модулю є формування додаткової інформації для прийняття рішення кібераналітиком щодо обраної стратегії реагування на виявлені вразливості інформаційної системи.

Острянська Є. В. (ХНУ ім. В. Н. Каразіна, АТ «ІІТ»)
Горбенко Ю. І. (АТ «ІІТ»)

МОДЕЛІ ДЖЕРЕЛ ШУМУ ДЛЯ ГЕНЕРАЦІЇ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ PTRNG ТА NPTRNG

Актуальність.

Програми для криптографії та безпеки широко використовують випадкові числа та випадкові біти. Однак генерування випадкових бітів є проблематичним у багатьох практичних застосуваннях криптографії. Саме тому метою даної роботи є аналіз моделей джерел шуму для генерації випадкових послідовностей на основі PTRNG та NPTRNG.

Джерело шуму є основою безпеки для джерела ентропії та для ГВБ в цілому. Це компонент, який містить недетермінований процес забезпечення ентропії, який остаточно відповідає за невизначеність, пов'язану з бітовими рядками, виведеними джерелом ентропії.

Постановка задачі

Нижче розглядаються та пояснюються моделі джерел шуму для генерації випадкових послідовностей (випадкових чисел) на основі PTRNG та NPTRNG. Пояснюється сутність, опис, вимоги, попередня оцінка та проводиться порівняння. Також розглядається вирішальне питання при оцінці випадкових генераторів: які властивості складають безпечний RNG для досягнення бажаних результатів?

Основні положення

Джерело шуму (ДШ) є основою безпеки для джерела ентропії та для генераторів випадкових бітів (ГВБ) в цілому. Це компонент, який містить недетермінований процес забезпечення ентропії, який остаточно відповідає за невизначеність, пов'язану з бітовими рядками, виведеними джерелом ентропії.

Взагалі ГВБ прийнято поділяти на детерміновані (DRNG) та не детерміновані (TRNG) [2]. Схематично дану класифікацію зображено на рисунку 1 нижче. В цій роботі ми будемо розглядати недетерміновані ГВБ.

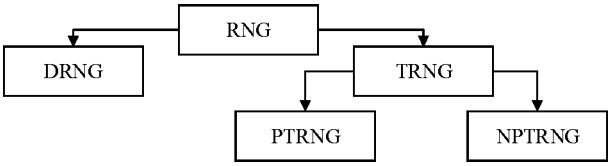


Рис. 1. Класифікація генераторів випадкових бітів

Ключовою властивістю TRNG є їх здатність видавати випадкові числа, які перед тим, як покинути пристрій ще містять певну кількість ентропії. Це означає, що будь-який суб'єкт, який спостерігає за TRNG ззовні, незалежно від своїх знань про конструкцію TRNG, його обчислювальну потужність або криптоаналітичні здібності, не може бути впевненим щодо значення наступного випадкового числа до ступеня, визначеного заявленою ентропією. Ця перевага перед DRNG з'являється ціною того, що TRNG, загалом, складніше оцінити.

Недетерміновані джерела шуму можна розділити на дві категорії:

фізичні джерела шуму (PTRNG);

нефізичні джерела шуму (NPTRNG).

PTRNG – фізичні джерела шуму, в основі яких лежить деяке непередбачуване явище. Такі ДШ використовують спеціальне обладнання для генерування випадковості. PTRNG виробляють випадкові біти з високою ентропією з джерела фізичного шуму на основі фізичного явища, що демонструє випадковість. Це явище можна реалізувати за допомогою фізичного експерименту або електронної схеми. Зазвичай це дозволяє отримати точні оцінки ентропії. Приклади PTRNG включають конструкції на основі кільцевих осциляторів, випадкову поведінку яких можна простежити до теплового шуму, або конструкції на основі діодів Зенера.

NPTRNG – нефізичні джерела шуму, в основі яких лежать достатньо передбачувані явища, які, тим не менш, містять певну кількість ентропії. Такі ДШ використовують системні дані (такі як вихід функцій інтерфейсу прикладного програмування (API), дані оперативної пам'яті (RAM) або системний час) або вхідні дані людини (наприклад, рухи миші, тощо) для створення випадковості. NPTRNG також передають по-справжньому випадкові біти, але збирають їх ентропію з нефізичних джерел шуму, для яких точна оцінка ентропії зазвичай неможлива, оскільки NPTRNG може працювати на зовсім інших платформах, які не контролюються розробником.

Центральним завданням оцінок як PTRNG, так і NPTRNG є перевірка того, що (середня) ентропія на один біт внутрішнього випадкового числа перевищує задану нижню межу.

Безпека RNG. Розглянемо які властивості складають безпечний RNG [1]. Природною вимогою було б наступне: RNG має виводити всі допустимі значення з однаковою ймовірністю та незалежно від попередників і наступників. Це характеризує ідеальний RNG. Однак це суто математична конструкція. У реальному світі практично неможливо побудувати ідеальний RNG, принаймні в строгому математичному сенсі. Крім того, навіть якби існував ідеальний RNG, було б неможливо довести чи перевірити ідеальну випадковість.

Натомість найкраще, що можна зробити – це прагнути до RNG, які в певному сенсі «наближені» до ідеального RNG. Обґрунтування полягає в тому, що застосунки IT-безпеки зазвичай вимагають «захищених» випадкових чисел, які неможливо ані передбачити, ані визначити пізніше. Для TRNG цю «безпеку» можна виміряти в термінах ентропії, тоді як для DRNG потрібен обчислювальний еквівалент.

Висновки

1) ГВБ прийнято поділяти на два класи: детерміновані (DRNG) та не детерміновані (справжні) (TRNG). В свою чергу TRNG поділяють на фізичні (PTRNG) та не фізичні генератори (NPTRNG).

2) Центральним завданням оцінок як PTRNG, так і NPTRNG є перевірка того, що середня ентропія на один біт внутрішнього випадкового числа перевищує задану нижню межу.

3) Важливою відмінністю між PTRNG і NPTRNG, яка впливає на глибину оцінювання, є те, що джерело фізичного шуму в PTRNG знаходиться «під контролем» розробника RNG, а джерело нефізичного шуму NPTRNG зазвичай не може контролюватися розробником RNG.

4) Наразі, у більшості випадків застосування, перевага надається джерелам шуму на основі PTRNG аніж на основі NPTRNG. Взагалі кажучи, наприклад, BSI має меншу довіру до NPTRNG, ніж до PTRNG [2]. По-перше, джерела шуму, які використовують NPTRNG, часто працюють добре лише за певних обставин, а NPTRNG часто не в змозі перевірити, чи виконуються ці умови. По-друге, оцінка ентропії зазвичай базується на складних припущеннях щодо знань і можливостей зловмисника і оперативного середовища. І також слід зазначити, що NPTRNG зазвичай мають більше експлуатаційних вимог до безпеки, ніж PTRNG і ці вимоги є сильнішими.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. M. S. Turan, E. Barker, J. Kelsey, Kerry A. McKay, Mary L. Baish, M. Boyle. Recommendation for the Entropy Sources Used for Random Bit Generation. NIST Special Publication 800-90B. Available online: https://doi.org/10.6028/NIST.SP.800-90B.

2. Killmann, W.; Schindler, W. A Proposal for Functionality Classes for Random Number Generators. In Proceedings of BSI, September 2022. Available online: https://www.bsi.bund.de/AIS_31_Functionality_classes_for_random_number_generators_e.pdf.

3. Barker, E.; Kelsey, J.; McKay, K.; Roginsky, A.; Turan, M.S. Recommendation for Random Bit Generation (RBG) Constructions. NIST Special Publication 800-90C Revision 3, September 2022. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90C.3pd.pdf.

4. Bikos, A.; Nastou, P.E., Petroudis, G.; Stamatiou, Y.C. Random Number Generators: Principles and Applications. Cryptography October 2023, 7, 54. Available online: https://www.mdpi.com/2410-387X/7/4/548.

канд. техн. наук **Охрімчук В. В.** (ЖВІ)
Охрімчук І. А. (ЖВІ)

НЕОБХІДНІСТЬ ІНТЕГРАЦІЇ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ В СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Кіберзахист в сучасному світі стає все більш актуальною проблемою. Аналіз останніх інцидентів у кіберпросторі, що відбулися в Україні та світі свідчить не тільки про збільшення кількості кібератак, а й про зростання їх технологічної складності. Тому, на сьогоднішній день одним з найбільш пріоритетних напрямків наукових досліджень у галузі забезпечення кібербезпеки є удосконалення існуючих та створення нових та дієвих методів, засобів виявлення кібератак. Але нажаль постійне вдосконалення або модернізація діючих систем інформаційної безпеки не може сьогодні гарантувати повноцінного захисту від кібератак.

Здебільшого це пов'язано з тим, що прийняття рішення про виявлення кібератаки системою інформаційної безпеки (СІБ) здійснюється на основі даних, які були отримані в результаті аналізу раніше виявлених кібератак. При цьому кожна така система використовує інформацію виключного від свого вендору. Це, в свою чергу, може призвести до ситуації коли в базі даних про кібератаки вендора СІБ, що здійснює захист системи буде відсутня інформація про певну кібератаку, а у іншого вендора ця інформація в базі може бути. Проте, оскільки СІБ працює з базою виключного свого вендора, може відбутися ситуація пропуску кібератаки, що в свою чергу є неприйнятним.

На даний час існує велика кількість баз даних про відомі кібератаки. Всі вони містять в собі відомості про вразливості програмного забезпечення, шаблони мережевого трафіку, шаблони нормальної поведінки, сигнатури відомих кібератак, шаблони дій зловмисника при проведенні кібератак тощо. Нині як бази даних шаблонів кібератак досить широко застосовуються бази KDD-99, CAPEC, CVE, NVD тощо. Але ці бази заповнюються різноманітною інформацією незалежно одна від одної. Це призводить до дисбалансу форматів подання первинних даних. Крім того інформація, яка міститься в цих базах має значний об'єм. Як наслідок, ускладняються технології їх спільного використання в СІБ.

Одним із перспективних шляхів вирішення цієї проблеми може стати інтеграція в СІБ систем підтримки прийняття рішення (СППР) про кібератаки. Впровадження таких систем в СІБ має особливу важливість, оскільки допомагає ефективно виявляти, аналізувати та реагувати на потенційні загрози безпеки. Існує декілька позитивних рис від такого впровадження, серед яких слід виокремити:

1. *Прогнозування загроз.* СППР дозволяють аналізувати великі обсяги даних, виявляти аномалії, що може вказувати на потенційні загрози безпеці. Це допомагає організаціям прогнозувати та уникати можливих атак або інцидентів з порушенням безпеки.

2. *Оптимізація реагування на інциденти.* СППР автоматизують процес виявлення та реагування СІБ на інциденти з порушенням безпеки, забезпечуючи швидке виявлення та аналіз атак або інших випадків.

3. *Підвищення ефективності захисту.* Завдяки аналітичним інструментам СППР, СІБ можуть ідентифікувати кіберзагрози за рахунок розширення баз знань та приймати ефективні заходи для їх усунення.

4. *Адаптація до змін в загрозах.* Оскільки загрози безпеці постійно еволюціонують, СППР дозволяють організаціям швидко адаптуватися до нових видів атак та інших потенційних загроз.

Висновки. Система підтримки прийняття рішень є ключовим елементом в забезпеченні ефективного кіберзахисту. Її впровадження та оптимізація вимагає комплексного підходу, включаючи технології, аналітику, навчання персоналу та стратегічне планування. Наукові дослідження в цій області спрямовані на розробку нових методів та підходів до забезпечення кібербезпеки, враховуючи постійно зростаючі загрози та виклики.

Потій О. В. (ДССЗЗІ)
Качко О. Г. (АТ «ІІТ»)
Кандій С. О. (АТ «ІІТ»)
Каптьол Є. Ю. (АТ «ІІТ»)

ДОСЛІДЖЕННЯ ВПЛИВУ ПЛАВАЮЧОЇ ТОЧКИ НА БЕЗПЕКУ АЛГОРИТМУ ЕЛЕКТРОННОГО ПІДПИСУ FALCON

Схема електронного підпису Falcon є фіналістом конкурсу NIST PQC. Однією з особливостей ЕП Falcon є використання обчислень з плаваючою точкою. У нашій роботі ми пропонуємо атаку спеціального вигляду, що використовує шум обчислень з плаваючою крапкою у ЕП Falcon та потребує близько $3 \cdot 10^5$ підписів для відновлення таємного ключа. Атака використовує дві реалізації ЕП Falcon, у яких порядок обчислень вектора з вибірки Гауса відрізняється. При цьому необхідною умовою проведення атаки є однакові seed при виробленні підпису. Ця умова робить атаку скоріш теоретичною, ніж практичною, проте, можливість використання шуму обчислень з плаваючою крапкою показує, що для ЕП Falcon існують додаткові вектори атак, що мають враховуватися в моделях безпеки та потребують детальних досліджень. Процедуру підпису, згідно специфікації (спрощено) можливо описати наступним чином:

Вхідні дані: повідомлення m у форматі бітового рядка, базис NTRU-решітки B.

Вихідні дані: підпис (s_1, nonce), де s_1 - поліноми у $\mathbb{Z}_q[X]/(x^n+1)$, nonce – випадковий бітовий рядок, що використовувався для рандомізації повідомлення.

1. Отримати *nonce* з рівномірного розподілу
2. Обчислити випадковий поліном c як геш значення від $m \| nonce$
3. Обчислити $\hat{t} = (\hat{c}, \hat{0}) \cdot B^{-1}$
4. Обчислити вектор $\hat{z} = (\hat{z}_0, \hat{z}_1)$ за допомогою алгоритму вибірки *ffSampling* (і $T = T(B)$) для цільової точки $\hat{t}$.
5. Обчислити $\hat{s} = (\hat{s}_0, \hat{s}_1) = (\hat{t} - \hat{z})B$ у Фур'є базисі та відповідний вектор $s = (s_0, s_1)$ за допомогою зворотного перетворення Фур'є.
6. Якщо норма вектора s є достатньо малою, то повернути підпис (s_1, nonce), інакше – повернутися до кроку 4.

З кроків 3 та 5 у алгоритмі підпису випливає, що:

$$\hat{s} = (\hat{t} - \hat{z})B = \hat{t}B - \hat{z}B = (\hat{c}, \hat{0})B^{-1}B - \hat{z}B = \begin{pmatrix} \hat{c} \\ \hat{0} \end{pmatrix} - \begin{pmatrix} \hat{z}_0 g + \hat{z}_1 G \\ -\hat{z}_0 f - \hat{z}_1 F \end{pmatrix} = \begin{pmatrix} \hat{c} - \hat{z}_0 g - \hat{z}_1 G \\ \hat{z}_0 f + \hat{z}_1 F \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \end{pmatrix} \quad (1)$$

Припустимо, що існує дві реалізації ЕП Falcon, що при однакових значеннях *seed* (випадкове значення, що використовується у *ffSampling*) та *nonce* для однакових ключей дають різні підписи. Надалі позначатимемо верхніми індексами відповідні змінні. Наприклад, (s_0^0, s_1^0) – вектор s у першому підписі та (s_0^1, s_1^1) – вектор s у другому підписі. Використовуючи формулу (1), маємо рівність:

$$\begin{cases} s_0^0 + s_1^0 h = c \\ s_0^1 + s_1^1 h = c \end{cases} \Rightarrow h = \frac{s_0^0 - s_0^1}{s_1^1 - s_1^0} \quad (2)$$

Тобто, h можливо виразити через (s_0^0, s_1^0) та (s_0^1, s_1^1).

Підставляючи (1) у (2) для h, отримуємо:

$$h = \frac{c - z_0^0 g - z_1^0 G - c + z_0^1 g + z_1^1 G}{z_0^1 f + z_1^1 F - z_0^0 f - z_1^0 F} = \frac{g(z_0^1 - z_0^0) + G(z_1^1 - z_1^0)}{f(z_0^1 - z_0^0) + F(z_1^1 - z_1^0)} = \frac{g\delta_0 + G\delta_1}{f\delta_0 + F\delta_1} \quad (3)$$

Ідея атаки полягає у тому, щоб підібрати повідомлення m таким чином, щоб $\delta_1 = 0$, а δ_0 було деяким достатньо малим для використання алгоритму пошуку найбільшого спільного дільника поліномом (в ідеалі - $\delta_0 \in \square$). Тоді, можливо буде обчислити таємний ключ f, g як:

$$f = (s_1^1 - s_1^0) / \gcd(s_1^1 - s_1^0, s_0^0 - s_0^1)$$
$$g = (s_0^0 - s_0^1) / \gcd(s_1^1 - s_1^0, s_0^0 - s_0^1) \quad (4)$$

Де gcd – найбільший спільний дільник поліномів. Зауважимо, що ситуація, коли $\delta_0 = 0$, а $\delta_1 \neq 0$ є не можливою через структуру алгоритму вибірки.

Еталонна реалізація ЕП Falcon надає два інтерфейси для користувачів. Перший інтерфейс обчислює структуру даних $T = T(B)$ у процедурі вироблення підпису. Другий інтерфейс передбачає передачу $T = T(B)$ у якості аргумента. В реалізаціях це призводить до зміни порядку обчислень і відповідно до виникнення ситуацій, де виконуються умови атаки. Перший інтерфейс реалізований функцією sign_dyn, другий інтерфейс функцією sign_tree. Обидва інтерфейси замість повідомлення приймають вже поліном c.

Для виявлення різниць у підписах ми запустили 10^6 разів для 10 випадкових ключових пар генерацію підпису функціями sign_dyn та sign_tree для випадкового 33-байтного повідомлення з рівномірного розподілу. У середньому атака працює у 76 % випадків для Flacon512 та у 70 % випадків для Falcon1024. Аналіз конкретних випадків показав, що усі випадки $(\delta_0, \delta_1) \neq (0,0)$ можливо поділити на наступні класи:

Випадок I. $\delta_1 \neq 0$. Відповідно, до структури алгоритму вибірки також $\delta_0 \neq 0$, тож формула (12) не буде давати коректний результат. Таких випадків близько 24% для Falcon512 і близько 29 % для Falcon1024.

Випадок II-a. Коли $\delta_1 = 0$ і $\delta_0 = a, a \in \square$. У цьому випадку формула (12) працює. При чому, значення a є не великим числом (менше 10). Таких випадків для Falcon512 складає близько 29 % від загальної кількості і близько 26 %.

Випадок II-b. Коли $\delta_1 = 0$ і $\delta_0 = a \cdot x^{n/2}$, a $\in \square$. У цьому випадку формула (12) працює. При чому, значення a є не великим числом (менше 10). Таких випадків для Falcon512 складає близько 38 % від загальної кількості і близько 35 %.

Випадок II-c. Коли $\delta_1 = 0$ і $\delta_0 = a + b \cdot x^{n/2}$, де a, b $\in \square$. Цей випадок є комбінацією попередніх випадків і формула (12) також буде працювати, але цей випадок цікавий тим, що δ_0.є поліномом. Така ситуація трапляється близько у 7% випадків для Falcon512 та у 9 % випадків для Falcon1024.

Висновки

В роботі була запропонована атака ЕП Falcon з використанням властивостей обчислень з плаваючою крапкою. Атака потребує близько $3 \cdot 10^5$ підписаних повідомлень для реалізації. Хоча атака є можливою тільки при неправильному використанні ЕП Falcon, проте вона показує, що обчислення з плаваючою крапкою можуть призводити до векторів атак, які раніше були не можливими. До того ж, стандартна модель безпеки не враховує можливість побудови таких атак. Необхідні додаткові дослідження для повного розуміння впливу обчислень з плаваючою крапкою на безпеку криптографічних перетворень.

д-р техн. наук **Сніцаренко П. М.** (ЦВСД НУОУ)
канд. техн. наук **Саричев Ю. О.** (ЦВСД НУОУ)
канд. військ. наук **Передрій О. В.** (ЦВСД НУОУ)
Зубков В. П. (ЦВСД НУОУ)
Піщанський Ю. А. (ЦВСД НУОУ)

ОСНОВНІ ЕТАПИ СТВОРЕННЯ ПЕРСПЕКТИВНОЇ СИСТЕМИ КІБЕРОБОРОНИ УКРАЇНИ

Актуальність проблеми. Інформаційні системи і технології, які утворюють кіберпростір, дозволяють синтезувати між собою різні види електронних інформаційних ресурсів (EIP) – це електронна кодограма для їх створення, зберігання, обробки або передачі (представлення) споживачу. Цей формат є технічною основою і одночасно умовою для інформаційної взаємодії між різними елементами глобального кіберпростору. При цьому взаємодія, поряд з іншим, може бути реалізована і з метою шкідливого впливу шляхом кібератаки (або їх сукупності) для нанесення уразливого кіберудару інформаційній інфраструктурі противника (суперника) або ментальності його соціального середовища. Таким чином виникає ситуація агресії у кіберпросторі, яка, зокрема, може мати воєнний характер.

З метою виконання завдань в кіберпросторі, що мають воєнний характер, сьогодні все більш активно діють відповідні підрозділи збройних сил та спецслужб провідних держав світу. Зважаючи на можливість надзвичайно прихованого характеру різноманітних агресивних дій у кіберпросторі, включно з генерацією спеціальних медіа-продуктів маніпулятивно-підступного змісту, кіберпростір сьогодні виступає як базова платформа забезпечення реалізації гібридних воєнних дій. 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. Питання кібероборони України вперше окреслене в 2016 році у Стратегії кібербезпеки України як відбиття воєнної агресії у кіберпросторі [1], а з цього приводу Міністерству оборони (МО) України та Генеральному штабу (ГШ) Збройних Сил (ЗС) України доручалося, відповідно до компетенції, здійснювати заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі. Таке формулювання завдання виглядало як надто узагальнене, принаймні з огляду на те, що у цьому документі не розкрито поняття "воєнна агресія у кіберпросторі", а також що таке її "відбиття". Це не дозволяло належним чином розуміти подальші практичні дії щодо удосконалення системи кібероборони держави та провокувало довільне сприйняття цього завдання.

Аналіз останніх досліджень та публікацій. Законом України "Про основні засади забезпечення кібербезпеки України" [2] у 2017 році уточнено сутність кібероборони. Цим же Законом МО України, ГШ ЗС України відповідно до компетенції визначено перелік завдань щодо забезпечення кібербезпеки, зокрема, щодо здійснення заходів з 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.

Разом з тим, у 2017 році в Закон України "Про оборону України" [3] внесено зміни наступного змісту:

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

З цього положення: *кібероборона – це активний кіберзахист*, що є третім варіантом для розуміння сутності кібероборони.

Отже, розглядаючи разом зазначені варіанти визначень, що містяться в законодавстві України, сутність кібероборони держави зрозуміти неможливо, а до цього ж, (у прямому

визначені) неможливо також уявити шляхи *реалізації у кіберпросторі* більшості перелічених заходів. Отже, поняття "*кібероборона*" в законодавстві України виписане недосконало.

Разом з тим, при вирішенні питань створення та функціонування перспективної системи кібероборони України викликає потреба уточнення переліку заходів та визначення основних етапів створення перспективної системи кібероборони України з урахуванням особливостей національного законодавства у сфері оборони, кібербезпеки та, зокрема, кібероборони, що залишилися поза межами як Стратегії кібербезпеки України [4], так і Плану її реалізації [5]. Це спричиняє потребу коригування частини цього Плану у питанні кібероборони та створення відповідної перспективної системи.

Метою доповіді є огляд ключових положень зі створення перспективної системи кібероборони України як складової національної системи кібербезпеки з визначенням основних етапів її реалізації.

Викладення основного матеріалу. У новій Стратегії кібербезпеки України [4] (чинна з 2021 року) йдеться про те, що для формування потенціалу стримування першою серед стратегічних цілей значиться ціль С.1 "Дієва кібероборона", яка має бути реалізована відповідно до Плану реалізації Стратегії кібербезпеки України [5].

На перший погляд, основні етапи створення перспективної системи кібероборони України означені цим Планом із терміном завершення основних робіт щодо досягнення стратегічної цілі С.1 у 2024 році. Між тим, судячи із реалій, пов'язаних у першу чергу із російсько-українською війною, цей План належним чином не виконується, зокрема, кібервійська у системі МО України не створено і перспективи цього неочевидні. Вже ця обставина спричиняє потребу коригування частини цього Плану щодо здійснення кібероборони та створення відповідної перспективної системи.

Крім цієї формальної причини, також коригування перспектив створення та функціонування системи кібероборони України викликає потреба уточнення ряду дій з урахуванням тонкощів національного законодавства України у сфері оборони, кібербезпеки та, зокрема, кібероборони, які залишилися поза межами як Стратегії кібербезпеки України [4], так і Плану її реалізації, але враховані у вищевикладених результатах досліджень. Звернемо увагу на такі особливості.

По-перше, у системі МО України створити кібервійська адміністративно відносно просто. Але без участі розвідувальних органів України, які за Законом України "Про розвідку" [6] координуються Радою національної безпеки і оборони України чи координаційним органом з питань розвідки при Президентові України, ці війська не зможуть проводити воєнні кібероперації на законних підставах, оскільки не мають права самостійно вести розвідку у кіберпросторі, зокрема спеціальні заходи розвідки. Таким чином, має бути запропоновано відповідний механізм взаємодії та координації, а також необхідне для цього нормативно-правове підґрунтя. Наведена на рис. 1 загальна схема перспективної системи кібероборони України передбачає потребу та можливість такого механізму, створення якого поряд з іншим, має бути окремим етапом досягнення стратегічної цілі С.1 та побудови перспективної системи кібероборони України.

По-друге, і Стратегія кібербезпеки України [4], і План її реалізації [5] неоднозначно означують участь суб'єктів в частині спільного виконання завдань кібероборони: в одному пункті значиться "суб'єктів національної системи кібербезпеки та сил оборони", а в іншому "суб'єктів сектору безпеки і оборони", що не є еквівалентом. При тому, що у Законі України "Про основні засади забезпечення кібербезпеки України" [2] визначається, що *суб'єкти забезпечення кібербезпеки у межах своєї компетенції, зокрема, "розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері ... кібероборони ..."*. А суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки у цьому законі є [2]:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

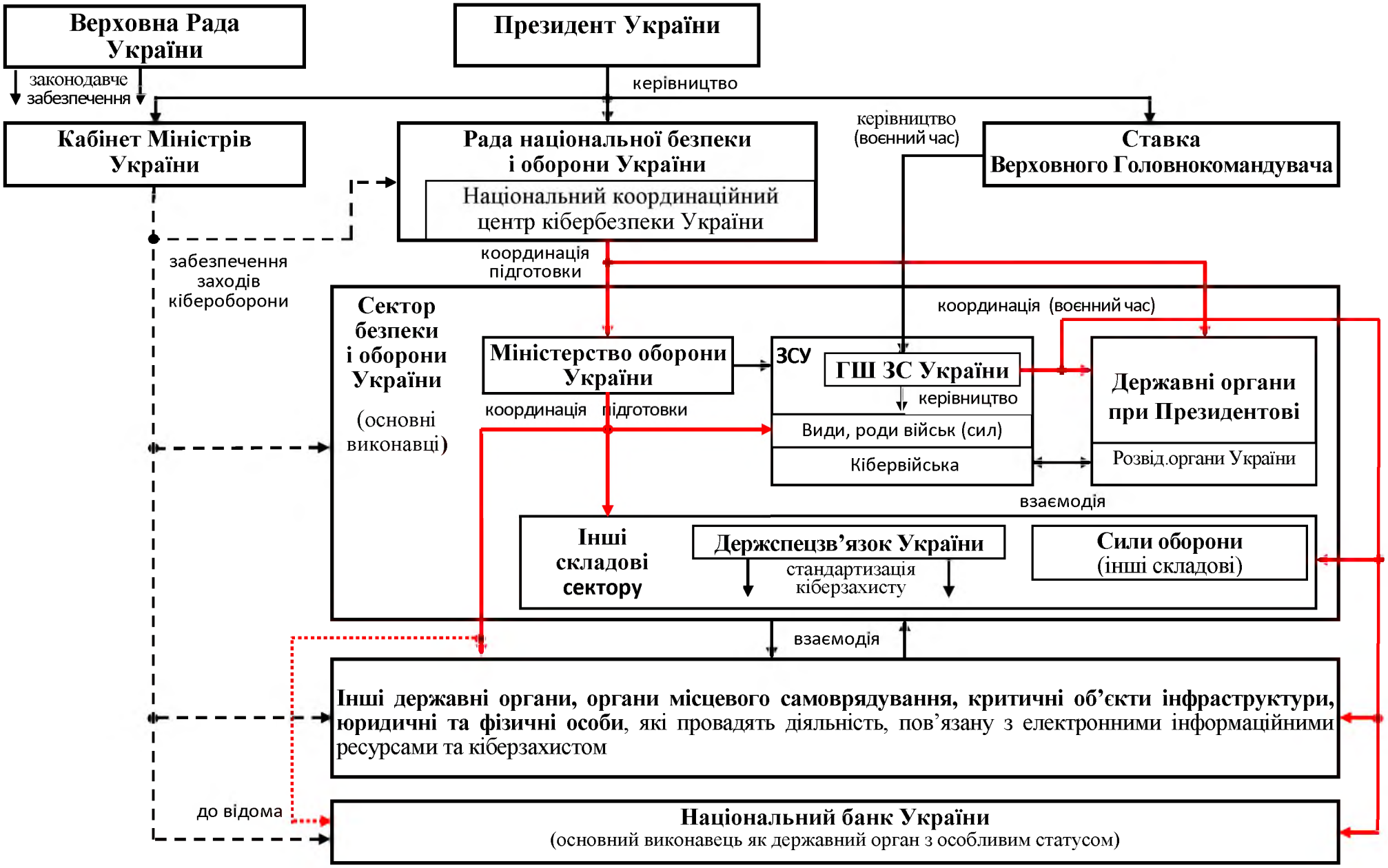


Рис. 1. Структурно-логічна схема перспективної системи кібероборони України

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

5) ЗС України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;

8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Як видно, за законом перелік суб'єктів, що мають здійснювати заходи щодо кібероборони, значно ширший, ніж закріплюється у чинній Стратегії кібербезпеки України [4] та Плані її реалізації [5]. Водночас, це вказує на спрощений характер цих нормативно-правових актів. Крім того, це свідчить про необхідність удосконалення існуючої системи кібероборони України, зокрема у відповідності до сутності функціонування цієї системи згідно загальної схеми на рис. 1.

По-третє, в питанні кібероборони, на жаль, ще не звучить тема інформаційно-психологічного впливу через кіберпростір (Інтернет, соціальні мережі, електронні медіа) на когнітивну сферу суспільства з метою формування індивідуальної та колективної свідомості у напрямі, потрібному для ініціатора такого впливу. Зважаючи на активізацію користування переважної більшості різних верств населення Інтернет-кіберпростором, питання кібероборони держави на цьому напрямі стають принципово актуальними для практичної діяльності та реагування на різноманітні кіберзагрози. Вищенаведені результати проведених досліджень на цьому акцентують увагу, наголосивши, що це питання має бути частиною як державної оборонної політики, так і практичної діяльності у сфері оборони, у першу чергу при створенні системи кібероборони держави.

По-четверте, має бути єдине і просте розуміння кіберпростору як середовища ЕІР, поєднаних між собою засобами комунікації. При цьому слід брати до уваги, що Інтернет-середовище ЕІР є серйозно вразливим в умовах воєнних дій, що підтверджено фактами російсько-української війни. Тому при формуванні споживацького кіберпростору, особливо кіберпростору воєнної сфери, також мають бути задіяні мережі ЕІР поза межами Інтернету. У першу чергу, це стосується середовищ ЕІР військових систем зв'язку, автоматизованого управління військами (силами) та зброєю, радіоелектронної розвідки, радіонавігації, радіоелектронної боротьби, автоматизованого управління технологічними процесами важливих (критичних) інфраструктурних об'єктів економіки держави. Цілком очевидно, що з одного боку саме існування таких систем спричиняє потребу кібероборони, а з іншого – ЕІР, які продукують такі системи, відіграють значну роль власне у заходах кібероборони. Тому в інтересах кібероборони мають створюватися та розвиватися чимало елементів інформаційної інфраструктури держави, а не лише кібервійськ, які повинні і будуть діяти у взаємодії та з використанням спроможностей цих елементів. При цьому, раціональне поєднання, зокрема задля практики кібероборони, обох напрямів (Інтернет та середовища ЕІР поза ним) має бути важливим принципом та завданням подальшого розвитку інформаційної інфраструктури держави.

По-п'яте, має бути чітке розуміння того, що за умови розвитку інформаційної інфраструктури держави на достатньому для споживачів ЕІР рівні головні завдання усіх суб'єктів системи кібероборони держави полягають в кіберзахисті власних ЕІР, а також дотриманні настанов (правил) кібергігієни. І лише суб'єкти цієї системи, яким державою надано виключне право, мають проводити воєнні дії (акції та операції) у кіберпросторі (кібервійська та розвідувальні органи України).

Нами означено найбільш принципові особливості в системному розумінні перспектив забезпечення кібероборони України, що слід вважати головним у розвитку відповідної

системи. Все інше, що, зокрема, наведено в чинній Стратегії кібербезпеки України [4] та Плані її реалізації [5], є наслідком головного та є технічними деталями нижчого рівня значимості:

виконання плану кібероборони;

тематичні кібернавчання;

взаємодія із відповідними підрозділами держав-членів НАТО;

запровадження CERT-UA-взаємодії на різних рівнях;

навчання заходам кібергігієни у сфері кібербезпеки;

перманентне оцінювання спроможностей суб'єктів системи в частині спільного виконання завдань кібероборони.

Необхідність реалізації запропонованого підходу в організації кібероборони України спричиняє етапність створення перспективної системи кібероборони держави [7].

Етап 1. *Сформувати належну правову основу організації кібероборони України, шляхом внесення необхідних змін до національного законодавства*, при цьому враховуючи оновлену термінологічну базу, а також, що необхідно вважати об'єктами кібероборони (середовище ЕІР критичних об'єктів інфраструктури України; розвиток цифрового комунікативного середовища України (розвиток національного кіберпростору України); когнітивна сфера України (соціальна свідомість суспільства); когнітивна сфера держави-противника (свідомість, ментальний стан населення та збройних сил); середовище ЕІР критичних об'єктів інфраструктури противника), а здійснення кібероборони держави – це справа усього Українського народу з урахуванням можливостей та ролі кожного із суб'єктів у системі кібероборони.

Етап 2. З урахуванням оновлених положень національного законодавства *уточнити Стратегію кібербезпеки України та План її реалізації в частині питань кібероборони*.

Етап 3. *Створити у Збройних Силах України кібервійська* із повноваженнями ведення збройного протиборства в кіберпросторі для стримування збройної агресії проти України шляхом надання відсічі агресору у кіберпросторі або через кіберпростір, забезпечивши їх належними фінансовими, кадровими та технічними ресурсами.

Етап 4. *Створити в Україні єдину мережу галузевих (регіональних, місцевих) ситуаційних центрів кібербезпеки (кіберзахисту)*, що здатна забезпечити оперативне реагування на кіберзагрози на рівні, який відповідає потребам кібероборони держави та стандартам НАТО.

Етап 5. *Уточнити План кібероборони України* як керівництво щодо підготовки кібероборони держави та її здійснення у випадку воєнної (збройної) агресії проти України, в тому числі у кіберпросторі зі складовими:

розвиток цифрового комунікативного середовища України (розвиток національного кіберпростору України);

когнітивна безпека України у кіберпросторі (безпека соціальної свідомості суспільства при використанні кіберпростору);

кіберзахист ЕІР в національному кіберпросторі України (впровадження організаційно-технічної моделі кіберзахисту Держспецзв'язку України);

воєнні дії у кіберпросторі (мережеві акції та операції, радіоелектронна боротьба);

ресурсне забезпечення системи кібероборони України (кадрове, матеріальне, фінансове).

Етап 6. *Нормативно встановити механізми (порядок) реалізації комплексу взаємопов'язаних дій суб'єктів перспективної системи кібероборони України* (керівництво, координація, взаємодія) з метою ефективного функціонування системи відповідно до запропонованої структурно-логічної схеми.

Етап 7. *Використання спроможностей перспективної системи кібероборони України* у визначених ситуаціях та умовах відповідно до Плану кібероборони України.

Така етапність носить системний характер та визначає новий підхід до сутності

побудови перспективної системи кібероборони України на відміну від тих, що визначено Планом реалізації Стратегії кібербезпеки України [5].

Висновки

1. Проведений аналіз загальної 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 (хто, з ким, за яких умов, на якій підставі, в якому обсязі та протягом якого часу має взаємодіяти в інтересах виконання завдань кібероборони).

3. Результати аналізу термінологічного блоку законодавства, що впливає на розуміння сутності кібероборони України, вказують на його недосконалість. 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. Тому і термінологічну базу галузі кібербезпеки, у тому числі кібероборони, і належні теоретичні засади слід невідкладно розвивати та удосконалювати, та на цій основі покращувати законодавство України задля реалізації кращих практик, зокрема, щодо кібероборони.

4. Реалізація запропонованих етапів створення системи кібероборони України дозволить створити перспективну систему національного рівня, яка має забезпечити надійну безпеку інформації (інформаційних ресурсів), в тому числі у кіберпросторі воєнної сфери держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Стратегія кібербезпеки України**:** Указ Президента України від 15 березня 2016 року № 96/2016 Про рішення РНБО України від 27 січня 2016 року "Про Стратегію кібербезпеки України". – [Електронний ресурс]. – Режим доступу: http://president.gov.ua.

2. Закон України "Про основні засади забезпечення кібербезпеки України" від 05 жовтня 2017 року № 2163-VIII. – [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua.

3. Закон України "Про оборону України" від 6 грудня 1991 року № 1933-XII (зі змінами). – [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

4. Стратегія кібербезпеки України**:** Указ Президента України від 26 серпня 2021 року № 447/2021 Про рішення РНБО України від 14 травня 2021 року "Про Стратегію кібербезпеки України". – [Електронний ресурс]. – Режим доступу: http://president.gov.ua.

5. План реалізації Стратегії кібербезпеки України**:** Указ Президента України від 01 лютого 2022 року № 37/2022 Про рішення РНБО України від 30 грудня 2021 року "Про План реалізації Стратегії кібербезпеки України". – [Електронний ресурс]. – Режим доступу: http://president.gov.ua.

6. Закон України "Про розвідку" від 17 вересня 2020 року № 912-IX. – [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

7. Звіт про науково-дослідну роботу "Обґрунтування обрису системи кібероборони України" (проміжний). – Київ, НУОУ, 2023. – 107 с. – № держреєстрації 0123U101426.

УДК 681.35

канд. техн. наук **Хусаінов П. В.** ORCID: 0000-0002-0675-0369 (ВІТІ ім. Героїв Крут)
Андреєв А. О. ORCID: 0000-0003-0074-0482 (ВІТІ ім. Героїв Крут)
Нестеренко Д. В. ORCID: 0009-0001-2635-0055 (ВІТІ ім. Героїв Крут)

ДЕРЕВО ПЕРЕВІРОК ЕЛЕМЕНТІВ МЕРЕЖНОЇ ДОСТУПНОСТІ ОБ'ЄКТІВ ПОШУКУ ТА ВИЯВЛЕННЯ ПОТЕНЦІЙНОЇ ВРАЗЛИВОСТІ

Пошук та виявлення потенційної вразливості здійснюється з метою запобігання порушення штатному режиму функціонування, несанкціонованому втручанню, загрозам безпеки електронних інформаційних ресурсів інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (далі – об'єкти пошуку та виявлення потенційної вразливості). Дослідник потенційної вразливості – фізична або юридична особа, яка здійснює пошук потенційної вразливості. Один з аспектів пошуку потенційної вразливості полягає у здійснення сканування мережі, хостів і сервісів (об'єктів пошуку та виявлення потенційної вразливості) без подолання систем логічного захисту. Сканування мережної доступності між робочою станцією дослідника (потенційної вразливості) та хостами цільових об'єктів (пошуку та виявлення потенційної вразливості) має результатом створення деревоподібної схеми маршрутів доступу. Елементам гілок дерева маршрутів ставиться у відповідність середній час одержання реакції на тестові повідомлення процедур Active Scanning [1–2].

Перша фаза перевірки мережної доступності (підготовча) здійснюється для кожного елемента всіх можливих варіантів маршрутів між засобами дослідника та множиною цільових об'єктів з додаванням відповідних значень середніх часових витрат. Друга фаза перевірки (робоча) – здійснюється на підставі повної інформації про дерево маршрутів. Гілки дерева маршрутів можна прийняти ізоморфними дереву перевірок працездатності елементів маршруту, що також надає можливість перейти до мінімального остовного дерева.

Наступний крок зменшення часових витрат при періодичному характері робочих перевірок мережної доступності полягає у переході до застосування групового пошуку на відміну від послідовного (притаманний першій підготовчій фазі). Метод послідовного пошуку розпочинає програму перевірок з елементу, що має найбільшу величину показника абсолютної чи відносної значущості за певним критерієм. Наступна чергова перевірка виконується для елемента меншої значущості ніж попередній і т. д. за порядком зменшення величини цього показника тобто послідовно. Завершення перевірок відбувається в момент знаходження першого непрацездатного елементу в їх впорядкованій множині (за величиною абсолютної чи відносної значущості). Метод групового пошуку розпочинає програму перевірок з елементу, працездатність якого забезпечує функціональний зв'язок між двома впорядкованими підмножинами (групи) елементів. Обов'язковою умовою застосування методу є функціональна зв'язність елементів як першої, так і другої впорядкованої підмножині (групами) елементів. Тоді, висновок про працездатність для першої або другої групи функціонально-зв'язаних елементів може бути зроблений на підставі оцінки працездатності останнього порядкового елементу, відповідно, у кожній з них.

Висновки. Перспективним напрямом зменшення часу робочої фази перевірки елементів мережної доступності цільових об'єктів слід вважати оперування мінімальним остовним деревом перевірок із застосуванням методу групового пошуку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Постанова Кабінету Міністрів України від 16 травні 2023 року № 497 "Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж".

2. Adversarial Tactics, Techniques & Common Knowledge (https://attack.mitre.org).

УДК 681.35

Череушенко В. Б. ORCID: 0009-0006-2839-3637 (ВІТІ ім. Героїв Крут)
Андреєв А. О. ORCID: 0000-0003-0074-0482 (ВІТІ ім. Героїв Крут)
канд. техн. наук **Хусаінов П. В.** ORCID: 0000-0002-0675-0369 (ВІТІ ім. Героїв Крут)

ОЦІНКА ВАРІАНТІВ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ЗА МЕТОДОМ МЕРЕЖНОГО ПЛАНУВАННЯ

Компрометація системи об'єкта кіберзахисту – порушення сталого, надійного та штатного режиму функціонування системи об'єкта кіберзахисту та/або порушення конфіденційності, цілісності, доступності інформації (інших властивостей інформації), що обробляється. Сукупність методів та способів компрометації системи на основі експлуатації деякої вразливості об'єкта кіберзахисту розглядається в контексті тактик Initial Access, Execution, Privilege Escalation. Перевірка ефективності заходів кіберазахисту здійснюється шляхом виконання періодичних (не рідше одного разу на рік) тестування на проникнення на основі використання методів та способів Initial Access, Execution, Privilege Escalation. Кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [1–4].

Процес тестування на проникнення являє собою деяку сукупність окремих взаємопов'язаних операцій. Вироблення варіанту тестування на проникнення передбачає, перш за все, узгодження окремих операцій за часом і порядком виконання в умовах часових обмежень, різної кваліфікації дослідника та повноти знань про систему об'єкта дослідження. Дослідник – фізична або юридична особа, яка здійснює пошук та експлуатацію вразливості у контексті тестування на проникнення. Залежно від того, як формулюється завдання, потрібно відшукати порядок виконання робіт або час початку, завершення, тривалості операцій. Вибір варіанту тестування на проникнення здійснюється за методом мережного планування.

Основою метода мережного планування є орієнтований граф мережного графіку послідовності операцій та відношень порядку між ними. Граф будується з позначенням вершин операцій у формі кружечків (прямокутників, ромбів) та дуг – суцільними, (пунктирними, штрих-пунктирними) стрілками. Мережний графік надає можливість оцінювати та здійснювати контроль за ходом виконання операцій, вносити необхідні зміни. Відмінності мережевих графіків визначаються інформацією про предметну область та комплекс операцій. В якості критеріїв аналізу мережних графіків використовується імовірність, математичне очікування часу виконання операції, загальна та гарантована найменша тривалість процесу.

Висновки. Застосування науково-методичного апарату мережного планування є одним з центральних аспектів раціональної організації тестування на проникнення. Він дозволяє оперативно сформувати множину варіантів виконання послідовності операцій для заданої тривалості процесу, кваліфікації та обізнаності дослідника про об'єкт тестування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 3 липня 2023 року "Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі".

2. Постанова Кабінету Міністрів України від 16 травні 2023 року № 497 "Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж".

3. Adversarial Tactics, Techniques & Common Knowledge (https://attack.mitre.org).

4. Закон України "Про основні засади забезпечення кібербезпеки України".

канд. техн. наук **Штаненко С. С.** (ВІТІ ім. Героїв Крут)
Бокій О. В. (ВІТІ ім. Героїв Крут)

КОНТРОЛЬ ТА ДІАГНОСТУВАННЯ МІКРОПРОЦЕСОРНИХ СИСТЕМ У КОНТЕКСТІ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ СУЧАСНИХ СИСТЕМ УПРАВЛІННЯ

Сучасні системи управління різного функціонального призначення в якості основних елементів містять засоби обчислювальної техніки – процесори, блоки пам'яті, програмне забезпечення, різного роду перетворювачі, датчики, вимірювальні та виконавчі прилади тощо.

Останнім часом в якості основи проєктування сучасних систем управління почали застосовуватись обчислювальні засоби, реалізовані на новітній елементній базі – універсальних і спеціалізованих мікропроцесорних системах, які являють собою систему на одній платі (кристалі) – System-on-Chip або вбудовану систему – Embedded system.

Слід зазначити, що сучасні обчислювальні засоби характеризуються великою різноманітністю функціональних можливостей, ступенем складності та специфікою технологій, що застосовуються для їхньої розробки та виготовлення. Крім цього, кожна зі складових обчислювального засобу (апаратна або програмна частина) має свої особливості та характерні властивості, які зумовлюють існування досить специфічних різновидів несправностей її стану в цілому. Перераховані вище специфічні особливості сучасних обчислювальних засобів викликали значні зміни, як у процесі їхнього проєктування, так і розробки методів та засобів контролю і діагностування з метою виявлення та локалізації несправностей (апаратної та програмної складової), пов'язаних із хіміко-фізичними процесами, а також із навмисними чи ненавмисними несприятливими впливами (радіоелектронне подавлення та кіберінциденти/кібератаки).

Так, новим поштовхом у проєктуванні сучасних систем управління стала поява програмованих логічних інтегральних схем (ПЛІС), які являють собою матрицю програмованих логічних елементів з SPLD (Simple Programmable Logic Devices), CPLD (Complex Programmable Logic Device), FPGA (Field-Programmable Gate Array), FLEX (Flexible Logic Element MatriX) структурами. За допомогою даних структур, застосовуючи на нижньому рівні (рівень регістрових передач) мови опису апаратури AHDL, VHDL, Verilog, на середньому (блочному) – бібліотечні програмоподібні IP-ядра (intellectual property) та верхньому – високорівневі мови програмування C/C++, System C, Python, Java, ми отримуємо можливість проєктувати не лише комбінаційні та послідовні пристрої, а й універсальні та спеціалізовані мікропроцесорні системи.

Якщо розглядати мікропроцесорну систему як об'єкт контролю та діагностування, то вона являє собою складну обчислювальну структуру з шинною організацією, яка складається з чотирьох основних підсистем: процесора, пам'яті, контролерів введення-виводу та контролерів зв'язку з об'єктами. При цьому кожна з цих функціональних підсистем, у свою чергу, є також досить складною з точки зору контролю та діагностування. Тому при визначенні технічного стану (справний, працездатний та правильно функціонуючий) мікропроцесорних систем використовується декомпозиційний підхід, при якому в якості об'єкту контролю та діагностування виступають окремі функціональні пристрої: арифметико-логічний пристрій, процесор, оперативно-запам'ятовуючий пристрій, пристрій введення-виводу, програмне забезпечення тощо.

Зазначимо, що на сьогодні питанням контролю та діагностування мікропроцесорних систем, а саме апаратної складової, присвячено багато наукових праць на відміну від програмної складової, яка потребує більш ретельного вивчення за умови, що сучасні мікропроцесорні системи функціонують в умовах несприятливого впливу, пов'язаного на рівні програмного забезпечення з кіберінцидентами/кібератаками [1].

Так, згідно з [2] під контролем правильності виконання програм розуміють програмно-логічний контроль, до якого входять: контроль тривалості та послідовності виконання програм, метод контрольних функцій та контроль гладкості.

Контроль тривалості виконання програм заснований на тому, що для кожної програми відома максимальна тривалість виконання і будь-яке перевищення тривалості означає, що програма зациклилася, зупинилася або виконана неправильно. Перевищення тривалості виконання обов'язково пов'язане з помилками у програмі, часто причиною може бути спотворення адресної інформації збоями.

Метод контрольних функцій ґрунтується на тому, що результати роботи програми мають відповідати певним функціональним співвідношенням. Наприклад, рішення системи диференціальних рівнянь можуть бути перевірені за критерієм задоволення контрольного рівняння, утвореного у вигляді рівнянь вихідної системи.

Контроль гладкості заснований на тому, що якщо ряд результатів обчислень являє собою більш-менш гладку функцію, то будь-які різкі відхилення результату від екстрапольованого значення свідчать про помилку.

У свою чергу під діагностуванням, в класичній теорії, будемо розуміти процедуру локалізації несправності об'єкта, тобто встановлення того, яка частина об'єкта, що діагностується, несправна. При діагностуванні проводиться встановлення несправності об'єкта на більш нижчому ієрархічному рівні, ніж під час контролю. У деяких випадках контроль технічної систем сприймається як окремий випадок діагностування.

На сьогодні за характером взаємодії між об'єктом та засобами діагностування розрізняють тестове та функціональне діагностування. Однак якщо розглядати програмну складову мікропроцесорної системи як об'єкт діагностування, то найбільш коректною є процедура тестування програм, під якою будемо розуміти перевірку роботи програми за результатами її виконання на спеціально підібраних наборах вихідних даних – тестах. При цьому згідно з [3] тестування програми поділяють на тестування чорної, білої та сірої скриньок.

Тестування чорної скриньки є стратегією, в якій тестування засноване виключно на вимогах і специфікаціях, при цьому не потрібні знання щодо внутрішніх шляхів, структури або реалізації програми, що перевіряється.

Тестування білої скриньки являє собою стратегію, в якій тестування засноване на внутрішніх зв'язках, структурі та реалізації програми, що перевіряється, а також детальних знань у галузі програмування.

Додатковим видом тестування є тестування сірої скриньки. При такому підході відбувається процес вивчення «скриньки» настільки, щоб зрозуміти, як вона була реалізована, а також обираються найефективніші тести чорної скриньки.

Слід зазначити, що тестування є невід'ємною частиною загальної методології розробки програмного забезпечення та характеризується високою трудомісткістю та відповідно вартістю. Серед багатьох проблем і завдань з тестування побудова тестів є одним із найскладніших інтелектуальних завдань, оскільки якість тестових послідовностей та трудомісткість їхньої побудови дуже впливають на розробку програмного забезпечення.

Зауважимо, що тести як важливий допоміжний елемент програмного забезпечення повинні будуватися на підставі деякої інформації, яка містить: структуру програми та/або вихідний код; специфікацію програмного забезпечення та/або моделі його проєктування; інформацію про простір даних вводу/виводу та інформацію, що динамічно отримується внаслідок виконання програми.

Так, згідно з [4] найбільш розповсюдженими методами тестування програм є:

Метод символьного виконання заснований на аналізі коду програми для автоматичного генерування тестових даних програми та реалізує концепцію білої скриньки, тобто аналізує програму шляхом її вихідного коду чи двійкового коду. При цьому символьне виконання використовує символьні значення замість конкретних значень вхідних даних і представляє значення програмних змінних як символьні вирази цих вхідних даних.

Побудова тестів на основі моделі є формальною методологією, яка використовує різні моделі програмних систем для отримання тестових наборів. За такого підходу акцент робиться на поведінковий рівень програм, реалізуючи концепцію чорної скриньки, за якої тестується програма згідно з її поведінкою. Різновидом такої моделі є:

аксіоматичний підхід побудови тестів, який використовує моделі, що базуються на певній формі логічного обчислення;

підхід із використанням моделей кінцевих автоматів.

У рамках аксіоматичного підходу розроблено різні поняття тестових гіпотез, зокрема регулярності та однорідності. Відповідно до гіпотези про регулярність, всі можливі значення X для вхідних тестових впливів до певної складності N вважаються достатніми для досягнення необхідної ефективності тесту. Відповідно до гіпотези однорідності одне значення для кожного класу вхідних даних вважається достатнім для досягнення необхідної повноти покриття тесту.

Основою методів побудови тестів відповідно до їхніх моделей є кінцеві автомати та різні їхні модифікації. Кінцевий автомат являє собою систему з кінцевою множиною станів, серед яких виділяються початковий стан і кінцеві множини стимулів (вхідних даних), що сприймаються ззовні, а також реакцій, що формуються (вихідних даних). Крім цього, в кінцевому автоматі визначено набір переходів між станами, причому кожен перехід позначений його вхідним значення (стимулом), що викликається, та вихідною реакцією, що генерується.

Комбінаторне тестування. Суть цього методу полягає в виборі вхідних параметрів чи реконфігурацій настройки, які охоплюють задану підмножину комбінацій елементів програм, які підлягають тестуванню.

Адаптивне ймовірнісне тестування. Цей метод реалізує концепцію чорної скриньки та є альтернативою ймовірнісному тестуванню. За таких умов структура та функціональність об'єкта тестування приймається невідомою або вважається, і ніяк не враховується при формуванні тестових наборів. Крім цього, ймовірнісне тестування не використовує інформацію, яка доступна в процесі генерування чергового тестового набору. Ця інформація може бути отримана з попередніх тестових наборів та в подальшому використана для формування чергового тактового впливу.

Пошукове тестування. В основі цього методу лежить використання програмного забезпечення, в якому застосовуються алгоритми оптимізації для автоматичного пошуку тестових даних, що максимізують досягнення цілей тестування, одночасно зводячи до мінімуму витрати на побудову тестів.

Таким чином, розглянуті методи контролю та діагностування (тестування) програмного забезпечення сучасних обчислювальних систем дають можливість не тільки зберігати протягом необхідного інтервалу часу здатність системи управління правильно виконувати задані специфікацією правила переробки інформації в реальних умовах експлуатації, але також можуть бути в сукупності з програмованою елементною базою основою для проєктування кіберстійких сучасних систем управління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Толюпа С. В. Самодіагностування як спосіб підвищення кіберстійкості термінальних компонентів технологічної системи / С. В. Толюпа, Ю. Я. Самохвалов, П. В. Хусаінов, С. С. Штаненко // Електронне фахове наукове видання. Кібербезпека: освіта, наука, техніка, 2023. № 2 (22). С. 134–147.

2. Иыуду К. А. Надежность, контроль и диагностика вычислительных машин и систем. М.: Высшая школа, 1989. 216 с.

3. L. Copeland. A Practitioner's Guide to Software Test Design. Artech House. Publishers, 2003. P. 300.

4. Ярмолик В. Н. Контроль и диагностика вычислительных систем / В. Н. Ярмолик. Минск: Бестпринт, 2019. 387 с.