МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
УНІВЕРСИТЕТ БЕЛЬСЬКО-БЯЛА (ПОЛЬЩА)
КАСПІЙСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕХНОЛОГІЙ ТА ІНЖИНІРИНГУ ІМ. Ш. ЕСЕНОВА (РЕСПУБЛІКА КАЗАХСТАН)

I Міжнародна науково-практична конференція «БЕЗПЕКА РЕСУРСІВ ІНФОРМАЦІЙНИХ СИСТЕМ»

(м. Чернгів, 16-17 квітня 2020 р.)

Збірник тез

I International scientific-practical conference «SECURITY OF INFORMATION SYSTEMS RESOURCES»

(Chernihiv, April, 16-17, 2020)

The collection of abstracts

Чернігів, 2020

УДК 004.05
Б40

Рекомендовано до друку за рішенням вченої ради
Національного університету «Чернігівська політехніка»
(протокол № 3 від 27.04.2020 р.)

Безпека ресурсів інформаційних систем : збірник тез
Б40 І Міжнародної науково-практичної конференції (м. Чернігів 16-17 квітня 2020 р.). – Чернігів : НУЧП, 2020. – 214 с.

ISBN 978-617-7571-83-3

У збірнику представлені тези доповідей учасників І Міжнародної науково-практичної конференції «Безпека ресурсів інформаційних систем», яка відбулася 16–17 квітня 2020 р. на базі Національного університету «Чернігівська політехніка» (м. Чернігів). Розглянуто результати теоретичних і практичних досліджень, а також проблемні пита ння кібербезпеки та захисту інформації. Збірник призначений для науково-технічних працівників, викладачів вищих навчальних закладів, докторантів, аспірантів та студентів.

УДК 004.05

Доповіді та тези доповідей друкуються мовою оригіналу в редакції авторів.

ISBN 978-617-7571-83-3

ЗМІСТ

UDC 004.75

Ivan Burmaka
Ph.D. Student dept. of information technologies and software engineering
Chernihiv National University of Technology, Chernihiv, Ukraine
Ivan.Bourmaka@stu.cn.ua

CONSENSUS ALGORITHM COMPARISON FOR BLOCKCHAIN BASED INTRUSION DETECTING SYSTEM

Introduction

To protect modern networks from intrusion distributed and collaborative intrusion detecting systems are used. The main reason for this is a huge amount of traffic in most of modern corporate networks. But in a big networks it's hard to setup a trust between a huge amounts of nodes, because some of the nodes can be modified and can sent some untrusted and irrelevant data then all distributed nodes can work incorrectly.

Classical solution for setting up a trust between the nodes in the distributed system is using a trusted third party, usually server. This server becomes a central node, which is trusted by all other participants, and the main task of this server is to set up trusted data exchange between nodes. But this approach has few disadvantages, the main one it that the central node is the single point of failure - if the central node fails all other nodes will lose the communication and all system will stop working. Another problem is that the huge of nodes in network will increase the CPU load on the central node.

As another solution of problem of setting trust between nodes in distributed system researchers proposed to use a blockchain technology to set up trusted data exchange between nodes[1]. The blockchain, as a continiously growing list of linked records can help to prevent the modification of already accepted data. One more feature of blockchain is that all information is distributed between all nodes. That’s why every node can check information correctness. To keep trust between the nodes blockchain is using consensus algorithms. This algorithm are used to decide which node will generate the next block in the blockchain. But it’s very important to choose correct consensus algorithm for such specific purpose blockchain, to achieve good performance and make system efficient.

Consensus algorithms

Distibuted blockchain based systems don't have any central node (central authority) which will be fully trusted by all other nodes. Information exchange between nodes in blockchain based system is implemented by broadcasting information (transaction) to all available nodes. Each node then rebroadcast this information to another available nodes. This way information becomes distributed via all blockchain network. But information is still stored only in memory pool. Information becomes stored in blockchain only when one of the nodes will write it into the block, and this block will be accepted by the network. So all nodes in a blockchain system have possibility to generate next block, that's why the system needs some protocols to achieve a consensus between the nodes and to be sure that all nodes work with the same consistent information. It also helps to resolve conflicts in chain of blocks which can appear sometimes when few nodes are trying to create block simultaneously. In case of this kind of conflicts blockchain can become forked for some time. Then consensus algorithm will be used to choose a correct branch of the forked blockchain. Another branch will be marked as invalid and dropped.

There are few popular consensus algorithms which are used in most of blockchain base systems (mostly cryptocurrencies):

Proof of work - was the first consensus algorithm which was used in the Bitcoin network. This algorithm helps to select in decentralized permissionless blockchain network a node for saving the records into a block. Random selection is not suitable here, because it has few vulnerabilities. For example malicious node can try to make a blocks with wrong information. So by using proof of work algorithm each node which wants to publish the block needs to do a loot of work to prove that it does not want to attack the network. In most of cases the work is to calculate cryptographic hashes to find one which meets some requirements. The block header contains a nonce and miners would change the nonce frequently to get different hash values. The consensus requires that the calculated value must be equal to or smaller than a certain given value. The difficulty of work is regulated automatically to achieve a stable block generation speed by changing that value. When one node reaches the target value, it would broadcast the block to other nodes and all other nodes must

mutually confirm the correctness of the hash value. If the block is validated, other miners would append this new block to their own blockchains. Nodes that calculate the hash values are called miners and the PoW procedure is called mining[2].

In the decentralized network with PoW, valid blocks might be generated simultaneously when multiple nodes find the suitable nonce nearly at the same time. As a result, parallel branches may be generated. However, it is unlikely that two competing forks will generate next block simultaneously. In PoW protocol, a chain that becomes longer thereafter is judged as the authentic one. Consider two forks created by simultaneously validated blocks. Miners keep mining their blocks until a longer branch is found. Then all miners would switch to the longer branch.Miners have to do a lot of computer calculations in PoW, yet these works waste too much resources. To mitigate the loss, some PoW protocols in which works could have some side-applications have been designed. For example, Primecoin[3] searches for special prime number chains which can be used for mathematical research.

Proof of stake - energy efficient alternative to Proof of work algorithm. In proof of stake miners need to prove the ownership of some amount of currency.It is believed that people with more currencies would be less likely to attack the network. Selection can be based on different rules, for example based on amount of currency. But the selection based on account balance is quite unfair because the single richest person is bound to be dominant in the network. As a result, many solutions are proposed with the combination of the stake size to decide which one to forge the next block.In particular, Blackcoin [4] uses randomization to predict the next generator. It uses a formula that looks for the lowest hash value in combination with the size of the stake. Peercoin[5] favors coin age based selection. In Peercoin, older and larger sets of coins have a greater probability of mining the next block. Compared to PoW, PoS saves more energy and is more effective. Unfortunately, as the mining cost is nearly zero, attacks might come as a consequence. Many blockchains adopt PoW at the beginning and transform to PoS gradually.

Proof of elapsed time - algorithm based on Intel trusted computing platform SXG. The basic idea is that each node generates a random number to determine how long it has to wait before it is

allowed to generate a block. The generation of random numbers is based on certain distribution specified by the system in advance.When a new block is submitted to the system, SGX helps the node creating the block to generate a proof of the waiting time. This proof can be easily verified by other nodes with SGX technology. A statistical test is used to determine whether the waiting time indeed follows the specified distribution[6].

DPOS(Delegated proof of stake). The major difference between PoS and DPOS is that PoS is direct democratic while DPOS is representative democratic. Stakeholders elect their delegates to generate and validate blocks. With significantly fewer nodes to validate the block, the block could be confirmed quickly, leading to the quick confirmation of transactions. Meanwhile, the parameters of the network such as block size and block intervals could be tuned by delegates. Additionally, users need not to worry about the dishonest delegates as they could be voted out easily. DPOS is the backbone of Bitshares [7].

PBFT(Practical byzantine fault tolerance) is a replication algorithm to tolerate byzantine faults [8]. Hyperledger Fabric utilizes the PBFT as its consensus algorithm since PBFT could handle up to 1/3 malicious byzantine replicas. A new block is determined in a round. In each round, a primary would be selected according to some rules. And it is responsible for ordering the transaction. The whole process could be divided into three phase: pre-prepared, prepared and commit. In each phase, a node would enter next phase if it has received votes from over 2/3 of all nodes. So PBFT requires that every node is known to the network. Like PBFT, Stellar Consensus Protocol (SCP) [9] is also a Byzantine agreement protocol. There are also few other algorithms which are based on PBFT, like Simplified Byzantine Fault Tolerance and Delegated Byzantine Fault Tolerance, but all this algorithms can be used only in permissioned blockchain.

IDS and consensus algorithms

Now we need to compare advantages and disadvantages of the different consensus algorithms for blockchain based intrusion detecting system. Consensus algorithms comparison is shown in Table 1. First of all we need to take a look at hardware requirements for using consensus algorithms, because most of proof of work consensus algorithms require specific hardware like GPUs or ASIC chips to make a stable and secure system. Proof of elapsed time also requires specific hardware platform which supports Intel SGX technology.

Table 1

Consensus algorithms comparison

Property	PoW	PoS	PoET	DPoS	PBFT
Blockchain type	Permissi-onless	Permissi-onless	Permissi-oned	Permissi-onless	Permissi-oned
Energy consumption	High	Low	Low	Low	Very low
Fault tolerance	50%	50%	-	50%	33%
Scalability	Good	Good	Bad	Good	Bad
Suitable for IDS	Not suitable	Suitable	Not suitable	Suitable	Suitable

So proof of work consensus algorithm is not suitable for using in blockchain based intrusion detecting system because of it's low energy efficiency and specific hardware requirements. Proof of work mining will use a lot of computational resources (and of course electricity) which will make IDS too expensive to keep.

Proof of stake and delegated proof of stake are two algorithms which are based on stacking, so they don't require high computational power and can be adopted for IDS case.

Proof of elapsed time also can be a good solution, but for now this algorithm has a vulnerability so this solution is not secure.

Intrusion detecting system can be built on both permissioned and permissionless blockchain, so PBFT algorithms are also suitable. But this algorithms will make blockchain system hard to scale.

Conclusion

Blockchain can be a good solution for building distributed intrusion detecting system, but for this case we have limited choice of consensus algorithms, because some algorithms have high computational resources usage (and of course energy consumption) and some algorithms still are not secure. After analyzing advantages and disadvantages of different consensus algorithms we can see that the most suitable algorithms for building blockchain based IDS are PoS based and PBFT, depends on type of blockchain and system scalability. For systems which does not require scaling better to use permissioned blockchain with PBFT algorithm, because its better to keep all nodes known in IDS. For large and scalable distributed IDS better to use permissionless blockchain with PoS algorithm. It will make system more open for new nodes and

much more easier to scale. Also permissionless blockchain with PoS algorithm has much higher fault tolerance, which is important for using IDS in unsafe environment.

Abstract. Modern corporate networks need distributed intrusion detecting system. But big distributed systems need a mechanism of setting trust between the nodes. A blockchain can be used as such kind of mechanism, but one of the main problems in building blockchain based IDS is to choose correctly blockchain type and consensus algorithm.Our goal here is to compare the most popular consensus algorithms by few parameters such a scalability and energy consumption, and choose which one can help to achieve optimal performance in distributed blockchain based intrusion detecting system.

Keywords*: intrusion detecting system, blockchain, consensus algorithm, PoW, PoS*

References

1. Li, W., Tug, S., Meng, W., Wang, Y.: Designing collaborative blockchained signature-based intrusion detection in IoT environments. Future Generation Computer Systems 96, 481{489 (Jul 2019), http://www.sciencedirect.com/science/article/pii/S0167739X18327237

2. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.[Online]. Available: https://bitcoin.org/bitcoin.pdf

3. S. King, "Primecoin: Cryptocurrency with prime number proof-of-work,"July 7th, 2013

4. P. Vasin, "Blackcoins proof-of-stake protocol v2," 2014. [Online]. Avail-able: https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

5. S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," Self-Published Paper, August, vol. 19, 2012.

6. Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., Shi, W.: On security analysis of proof-of-elapsed-time (PoET) (full version) (2017). http://i2c.cs.uh.edu/tiki-
downloadwikiattachment.php?attId=70&download=y

Bitshares - your share in the decentralized exchange." [Online]. Available: https://bitshares.org/

7. C. Miguel and L. Barbara, "Practical byzantine fault tolerance," inProceedings of the Third Symposium on Operating Systems Design andImplementation, vol. 99, New Orleans, USA, 1999, pp. 173–186.

8. D. Mazieres, "The stellar consensus protocol: A federated model forinternet-level consensus,"Stellar Development Foundation, 2015.

UDC 323:351

Kryvoruchko Olena
Kyiv National University of Trade and Economics,
Professor of Department of Software Engineering and Cybersecurity,
Doctor of Engineering sciences
ORCID: 0000-0002-2675-6514
e-mail: ev_ryvoruchko@ukr.net

Desyatko Alona
Kyiv National University of Trade and Economics,
Senior Lecturer of Department of Software Engineering and Cybersecurity
ORCID: 0000-0003-3270-4494
e-mail: desyatko@knute.edu.ua

Shestak Yaroslav
Kyiv National University of Trade and Economics,
Director of Information Technologies Main Center
ORCID: 0000-0001-6599-0808
e-mail: shestak@ knute.edu.ua

CYBERSECURITY AS A PART OF BUSINESS

Nowadays way people share knowledge, process and manage business, create value is heavily dependent on the Internet[1]. In the 21st century, business owners use computer systems and the Internet to compete in the technology-infused markets. Improvements in global wi-technology (wired and wireless) provide businesses benefits, in the same time expose companies to potential vulnerabilities[2]. In 2019, victims of cyber incidents reported an estimated loss due to cyber attacks at $400 billion a year [3].

Small and medium-sized enterprise owners often lack important information technology means and capabilities required to implement emerging cyber security activities [4]. Specifically, small and medium-sized enterprise owners regularly lack the proper means to control rapidly increasing cybersecurity risks and information systems security threats[5]. Theft or loss of private information can be an expensive incident at any business. Nevertheless, for small and medium-sized enterprise owners, losses from cyber attacks might be unrecoverable. The loss of customers, income, and in some instances forfeiture of business due to expensive litigation costs are among the potential negative effects on small and medium-sized enterprise owners.

Managing cyber risks requires organizations to implement modern security strategies focused on prediction, prevention, mitigation, and reaction while concentrating on people, processes, and systems.

Each day more than 2.3 billion people use online technologies to work, learn, bank and shop. Cyber criminals want access to computers, tablets and phones because they contain valuable information, and they are always developing new ways to attack networked technologies. Cyber criminals use exactly the same devices: mobile phones, tablets, laptops, and server computers, to commit crimes.

In 2018, cyber attackers were responsible for 49% of data breach attacks all over the world, and SMEs were the primary targets of cyber attacks. In 2019, cyber attacks against small and medium-sized enterprises continued to increase. However, many of these attacks were directed to fewer organisations. Business owners must be aware of and active in implementing new security strategies in a way to protect their corporate and personal client information. New and innovative hardware and software technologies are essential for business systems and critical infrastructure are resilient [6].

Security hackers pose a continuous and unrelenting threat to organizations by exploiting their computer systems. Moreover, importance of effective cyber security practices are critical factors to ensure Internet communications remain protected, and that individuals of every organization should have security awareness [7,8]. Cyber crimes are diversified and broad reaching. Owners cyber security awareness and active actions can potentially limit future cyber crimes and increase small business cyber survivability [9,10].

Cyber attacks are increasing, and victimization of individuals, businesses, and governments will regularly continue to occur. In 2019, estimated cyber crime losses exceeded $67.2 billion in European companies. That is because of 60% of all targeted cyber attacks struck small and medium-sized enterprises whose owners were disadvantaged in protecting their infrastructures. small and medium-sized enterprise owners often do not view themselves as targets for cyber attacks due to their small size or the perception they have nothing worth stealing. The general business problem is 80% of small and medium-sized enterprise owners do not use adequate processes to protect against cyber attacks [11]. The specific business problem is some small and medium-sized enterprise owners may lack effective cyber security strategies to protect their businesses from cyber attacks.

Abstract. Modern technologies developed in the digital age expose individuals, businesses, and government entities to potential cyber security vulnerabilities. Therefore development and implementation special strategies is a key point to prevent annual commercial loss that is increasing from year to year. Modern security strategies are mostly of cyber security approach, which includes integration of special software and general policy on data management for any-sized enterprises and are aimed to prevent cyber attacks against themselves. Therefore cyber security awareness and active actions can potentially limit cyber crimes and survivability.

References:

1. Askitas, N., & Zimmermann, K. F. The Internet as a data source for advancement in social sciences, 2015

2. Weber, R. M., & Horn, B. D. Breaking bad security vulnerabilities. Journal of Financial Service Professionals, 2017

3. Arief, B., Bin Adzmi, M. A., & Gross, T. Understanding cybercrime from its stakeholders' perspectives: Part 1 - attackers. IEEE Security & Privacy, 2015

4. Harris, M. A., & Patten, K. P. Mobile device security considerations for smalland medium-sized enterprise business mobility. Information Management & Computer Security, 2019

5. Njenga, K., & Jordaan, P. We want to do it our way: The neutralization approach to managing information systems security by small businesses. The African Journal of Information Systems, 2016

6. Maughan, D., Balenson, D., Lindqvist, U., & Tudor, Z. Government-funded R&D to drive cybersecurity technologies, 2015

7. Malecki, E. J., (2016): Real people, virtual places, and the spaces in between Socio-Economic Planning Sciences. Volume 58, s. 3-12.

8. Bandar, B. M., & Christian, B. (2013). Perceived risk of information security and privacy in electronic commerce. International Journal of Advanced Research in Computer Science, 8. Retrieved from http://www.ijarcce.com/

9. Borrajo, M. L., Baruque, B., Corchado, E., Bajo, J., & Corchado, J. M. (2011). Hybrid neural intelligent system to predict business failure in small-to-medium size enterprises. International Journal of Neural Systems, 21, 277-296. 81 http://dx.doi.org/10.1142/S0129065711002833

10. Borrett, M., Carter, R., & Wespi, A. (2013). How is cyber threat evolving and what do organisations need to consider. Journal of Business Continuity & Emergency Planning, 7(2), 163-171. Retrieved from http://www.henrystewartpublications.com/jbcep

11. Shackelford, S., Fort, T. L., & Prenkert, J. D. How businesses can promote cyber peace. University of Pennsylvania Journal of International Law, 2015

UDC 004.056.5

Kryvoruchko Olena
Kyiv National University of Trade and Economics,
Professor of Department of Software Engineering and Cybersecurity,
Doctor of Engineering sciences
ORCID: 0000-0002-2675-6514
e-mail: ev_ryvoruchko@ukr.net

Khorolska Karyna
Kyiv National University of Trade and Economics,
Assistant of Department of Software Engineering and Cybersecurity
ORCID: 0000-0003-3270-4494
e-mail: k.khorolska@knute.edu.ua

Bebeshko Bohdan
Softorino Inc.
Senior Software Engineer
ORCID: 0000-0001-6599-0808
e-mail: thismushroom@gmail.com

USE OF AI IN DATA PROTECTION

Main area in which AI technologies might be and are used by the organizations is during data processing scopes and more specifically in the process of potential or actual breaches identification and assessment. One can define "personal data breach" as a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed." It is a wide-ranging definition than even the equivalent in law systems around the world. Mostly companies do not consider data breach to be active until the moment when data was exposed in public or during the course of criminal activity.

Therefore, there is a requirement for all of the organizations that involve data processing to identify data breaches that have not been publicly exposed yet, it is the organization's responsibility to define when a breach of security has occurred. It means that the monitoring of data security is a key concept in the area of data processing.

Whenever breach occurs, data controllers must notify supervisory authority without any delay. However, notice is not required if "the personal data breach is unlikely to result in a risk for the rights and

freedoms of natural persons". So, organizations may need to perform an assessment of whether notification is required with significant financial risks if their assessment produces an incorrect answer either way.

Monitoring and assessment are those tasks that can be both handled by AI technology. There are examples of rule-based systems and machine learning systems that support monitoring [1][2] and assessment [3]. In these cases, inputs to the monitoring approach consist of all data and information being collected by the organization's security system; so, an organization with a sophisticated network monitoring system might consider a machine learning approach, while an organization that relies on managers to monitor employees' compliance with policies and procedures would suffer from a checklist approach.

Assessment of security breach, that results in a potential personal data loss, must be reported to the supervisory authority, and so the arguments for an underlying AI system. The 72-hour time limit (that is a time limit for reaction on breach) provides a strong push for organizations to invest in an AI system which will be always at their side, rather than having to engage legal or consultancy advice in a hurry. AI system will need minimal customization to a company's particular circumstances; so, it is likely that an AI software firm might develop a package that multiple organizations can purchase and use.

But the main controversial moment is a question of legal liability of AI system; if system makes an incorrect recommendation, who will be legally at fault? Kingston [4] discusses various models under which an AI system might be considered legally liable in any case scenario. Since GDPR appears to be largely based on strict liability, and there seems no reason to consider an AI risk assessor as an 'innocent agent' that has been incited to illegal activity unknowingly (i.e. used in a way that it was not designed for), then there is a significant likelihood that an AI system that makes an incorrect recommendation would indeed be found liable for the breach. Because of this, any software developing company that is selling an AI system that makes assessment whether a security breach needs to be reported would be strongly advised to follow strict model recommendations, and to make it clear to clients that the system is a decision support system (DSS), developed to save legal experts time in risk assessments rather than to automate every part of the

decision-making process. This should provide the software developing company a legally valid reason to assign the final responsibility for the assessment decision to the human expert rather than to the AI product.

Informational technology integration raises significant business risks for organizations that carry out data processing. AI technology can help to mitigate those risks by supporting risk assessments, monitoring and compliance checking with best practice knowledge. With time savings in availability of advice and in asking all and only the relevant questions [5].

To conclude all above-mentioned compliance-based systems require well-documented strict rules and having explicit reasons for doing so, or for choosing not to do so. Also, the world regularly requires explanations of reasoning, or data processing organizations may require explanations of an AI system's reasoning to convince them that the legal arguments it is making should stand up to secure. For these reason, rule-based technology is more appropriate than machine learning technology in most [6].

Some of the decisions that the idea of data protection requires are one-time decisions for a data processing organization, which means that the only organizations likely to make a business case for an AI system to support those decisions are consultancies who advise multiple organizations on any compliance. In any cases, all organizations are required to monitor continually for security breaches and, if a potential or actual breach occurs, to assess swiftly whether they need to notify the relevant supervisory authority. Monitoring tasks may be better carried out by machine learning than by rule based technology, especially if there is a need to detect unforeseen events or unknown patterns of symptoms.

Abstract. This thesis considers possible use of AI technologies in main areas of data protection field such as support risk assessments and recognition and reporting security breaches. It concludes that AI technologies can satisfy each of these areas. Nevertheless, there are many controversial questions that rises around the idea of AI use in data protection area. Most of these questions are related to the laws on data protection and responsibilities for breaches and failures.

References:

1. Thompson ED, Frolich E, Bellows JC, Bassford BE, Skiko EJ, Fox MS. Proceedings of the Twenty Seventh Conference on Innovative Applications in Artificial Intelligence (IAAI-15) 2015.

2. Vyas N, Farringdon J, Andre D, Stivoric J. Machine Learning and Sensor Fusion for Estimating Continuous Energy Expenditure, 2012

3. Dhurandhar A, Ravi R, Graves B, Maniachari G, Ettl M (2015). Proceedings of the Twenty Seventh Conference on Innovative Applications in Artificial Intelligence (IAAI-15), 2015.

4. Kingston J., Artificial Intelligence and Legal Liability, 2016

5. Cate, F., "Big Data, Consent, and the Future of Data Protection," in Sugimoto, C., Hamid R. Ekbia & Michael Mattioli, eds., Big Data is Not a Monolith 2 (MIT 2016).

6. Oltsik, J., Artificial intelligence and cybersecurity: The real deal, csoonline.com (25 Jan. 2018), available at https://www.csoonline.com/article/3250850/security/artificial-intelligence-andcybersecurity-the-real-deal.html.

UDC 004.415.3: 004.7(043)

Sokorynska Nataliia,
graduate student
sokor-nata@ukr.net

Zaitsev Sergei,
doctor of Technical Sciences, professor
serza1979@gmail.com

Posternak Yuriy,
graduate student
posternak21051976@meta.ua
National University "Chernihiv Polytechnic"

Kurbet Pavel,
graduate student
protokol77777@gmail.com
Science and Research Institute ofInformatics and Law
of the National Academy of Legal Sciences fUkraine

Gorlinsky Boris,
Department of Information Security
gbvksv@gmail.com

METHOD FOR OPTIMIZING ENCODER AND DECODER OPERATION OF A TURBO CODE THROUGH THE USE OF ADAPTIVE SELECTION OF THE STATE DIAGRAMS SIZE

In modern wireless telecommunication data transmission systems, error-correcting codes are used to increase the reliability of information transmission: Hamming codes, Bowes-Chowdhury-Hockingham codes (BCH codes), Reed-Solomon codes, cascade codes, convolutional codes, LDPC codes, turbo codes (TC) and others. The most effective of them are LDPC codes and TCs. The latter in energy efficiency are inferior to the theoretical Shannon boundary of 0.5 dB for a channel with additive white Gaussian noise at a coding rate $R = 1/3$ [1,2].

In wireless data transmission systems of the third 3G and fourth generation 4G (LTE-Advanced), technologies for adaptive power control, modulation and coding parameters are used to increase the reliability of information transmission [3,4]. In this case, one-level schemes are used for adaptation, for example, only the coding rate is changed for the turbo code adaptation.

There is a need to develop methods for multilevel parametric adaptation of turbo codes, and adaptation of the following TC parameters can be envisaged: interleaver (de-interleaver), data block size (size of state diagrams of a turbo code decoder), polynomials of recursive systematic convolutional codes (RSCC), number of component encoders of a turbo code, decoding algorithms.

The method described in the research work [5] is based on the use of two alternation algorithms simultaneously: the first algorithm determines the data frame for shifting by a certain number of positions, and the second algorithm permutes data bits depending on the value of the parameter S. This method is effective for short and medium lengths of S-random interleaver data blocks. The disadvantages of this method are the fixed value of the data bit spacing parameter S, restrictions on the interleaver length, and the estimated complexity of the interleaving algorithm. This method cannot be effectively used, for example, for LTE wireless data transmission systems, where the information block has a length of 6144 bits.

The method described in the research work [6] a two-step S-random interleaver is used. The main goal of this method is to increase the minimum code distance of the TC and reduce the correlation properties of the encoded sequences at the decoder output. The disadvantage of this method is the fixed value of the data bit spacing parameter S, the estimated complexity of the interleaving algorithm and the redundancy in storing information, namely, 2 interleaving tables that are used to deinterleave the input sequence.

As part of the work, the use of S-random interleaver, which is the most effective among other types of interleavers (regular, pseudo-random), is considered for parametric adaptation [7].

The two-level scheme of parametric adaptation of turbocode parameters is proposed in the research work [8]: depending on the state of the transmission channel, the coding rate and the number of iterations of decoding of the turbocode are changed.

In another research work [9], the method is based on the adaptive change of polynomials of recursive systematic convolutional codes that are part of turbocodes in order to increase their correcting properties by increasing the length of the code constraint for each retransmission of a data block for a given encoding rate. At the same time, the turbocode decoding algorithm is modified in terms of the

use of the introduced additional a priori information when calculating the LRLF of each component decoder received on previous requests for retransmission. The results of simulation showed that the application of the method allows to obtain the energy gain of coding and increase the reliability of information transfer in comparison with the known results, for example, the fourth-generation 4G LTE-Advanced mobile communication system.

Method [10] is based on the adaptive selection of parameters of *S*-random interleaver depending on values of the normalized quantity of sign reversals of a posteriori-a priori log-likelihood function ratios regarding the transmitted data bits of turbo-code decoder. The results of simulation modeling show that the rational parameters of *S* separation of data bit interleaving for *S*-random interleaver are obtained depending on the values of signal-to-noise ratio in channel and the normalized number of sign reversals of a posteriori-a priori LLFR of interactive turbo-code decoder.

The results of increasing the efficiency of mobile communication systems through the use of neural networks in conjunction with codes are presented in [11] research works.

The aim of the article is to develop a method for optimizing the operation of the encoder and decoder of a turbo code through the use of adaptive selection of the state diagrams size using the proposed decoding uncertainty indicator in wireless data transmission systems.

There are three decisions about decoding by decoder d, $d \in \overline{1,2}$ iteration of decoding j, $j \in \overline{1,I}$ information bit:

1) Event A_1. Sign changes in the values $L_a^{d,j}(x_t^{\mathrm{C}})$ and $L_e^{d,j}(x_t^{\mathrm{C}})$ iteration j do not occur ($\operatorname{sign}\left(L_a^{d,j}(x_t^{\mathrm{C}})\right) = \operatorname{sign}\left(L_e^{d,j}(x_t^{\mathrm{C}})\right)$), $L(x_t^{\mathrm{C}}) \geq 0$. Make a «firm» decision that a bit has been transmitted $x_t^{\mathrm{C}} = 1$.

2) Event A_2. Sign changes in the values $L_a^{d,j}(x_t^{\mathrm{C}})$ and $L_e^{d,j}(x_t^{\mathrm{C}})$ iteration j do not occur ($\operatorname{sign}\left(L_a^{d,j}(x_t^{\mathrm{C}})\right) = \operatorname{sign}\left(L_e^{d,j}(x_t^{\mathrm{C}})\right)$), $L(x_t^{\mathrm{C}}) < 0$. Make a «firm» decision that a bit has been transmitted $x_t^{\mathrm{C}} = -1$.

3) Event A_3. The sign of the value of a priori $L_a^{d,j}(x_t^{\mathrm{C}})$ and the sign of the value of posterior information $L_e^{d,j}(x_t^{\mathrm{C}})$ of iterations *j* is not equal to zero ($\operatorname{sign}\left(L_a^{d,j}(x_t^{\mathrm{C}})\right) \neq \operatorname{sign}\left(L_e^{d,j}(x_t^{\mathrm{C}})\right)$. Decoding errors may occur.

The uncertainty index for decoder *d*, $d \in \overline{1,2}$ iteration of decoding *j*, $j \in \overline{1,I}$ is calculated using the following procedure:

$$\sum_{d=1}^{2} R^{d,j}(t+1) = R^{d,j}(t) + 1, \quad \text{если } \operatorname{sign}\left(L_a^{d,j}(x_t^{\mathrm{C}})\right) \neq \operatorname{sign}\left(L_e^{d,j}(x_t^{\mathrm{C}})\right),\ t \in \overline{1,N}. \tag{1}$$

The more often the values of the uncertainty indicator *R* increase, the more often incorrectly decoded bits appear, which leads to a deterioration in the reliability of information reception.

The total uncertainty indicator R_Σ is determined by the sum of the uncertainty indicators for all decoding iterations:

$$R_\Sigma = \sum_{j=1}^{I} R^{d,j}. \tag{2}$$

For the convenience of calculations and adaptation, we will normalize the uncertainty indicator:

$$\tilde{R}_\Sigma = \frac{R_\Sigma}{B \cdot \tilde{N} \cdot I} = \frac{\sum_{j=1}^{I} R^{d,j}}{B \cdot \tilde{N} \cdot I}, \tag{3}$$

where *B* – is the number of data blocks of a certain observation window, $\tilde{N}$ – is a variable data block size, *I* – is the number of iterations of decoding a turbo code.

With parametric adaptation based on the calculation of the uncertainty index for the decoder *d*, $d \in \overline{1,2}$, iteration of decoding *j*, $j \in \overline{1,I}$, depending on the accumulated decoding uncertainty values of *B* data blocks, an adaptive selection of the data bit interleaving spacing parameter for an *S*-random interleaver is performed.

Based on the values $\tilde{R}$ the optimal values of the size parameter $\tilde{N}$ of the state diagrams of the encoder and decoder of the turbo code are selected. Information on the value of the parameter $\tilde{N}$ is transmitted to the encoder and decoder of the TC to change the size of the input block and, accordingly, the number of state diagrams of the decoder of the turbo code.

The algorithm for implementing the method for optimizing the coding / decoding of turbo codes is as follows.

Step 1. Formation of the initial state diagram of the encoder and decoder TC.

Step 2. Formation of the set of values of information and verification symbols received by the TC encoder: $\overline{X} = (\overline{X}^{\mathrm{C}}, \overline{X}^{\Pi})$, $\overline{X}^{\Pi} = (\overline{X}^{\Pi 1}, \overline{X}^{\Pi 2})$.

Step 3. The formation of the set of values of information and verification symbols received from the channel for the decoder TC: $\overline{Y}^{1} = (L_c \overline{Y}^{\mathrm{C}1}, L_c \overline{Y}^{\Pi 1})$, $\overline{Y}^{2} = (L_c \overline{Y}^{\mathrm{C}2}, L_c \overline{Y}^{\Pi 2})$.

Step 4. Formation of the set of a priori LRLF values about the transmitted data bits at the 1st and 2nd decoders of the *j*-th iteration

$$\begin{aligned} LA &= \left[L_a^{1,j}(x_1^{\mathrm{C}}) \quad L_a^{1,j}(x_2^{\mathrm{C}}) \quad \ldots \quad L_a^{1,j}(x_{\tilde{N}}^{\mathrm{C}})\right], \\ LA &= \left[L_a^{2,j}(x_1^{\mathrm{C}}) \quad L_a^{2,j}(x_2^{\mathrm{C}}) \quad \ldots \quad L_a^{2,j}(x_{\tilde{N}}^{\mathrm{C}})\right]. \end{aligned} \tag{4}$$

Step 5. The formation of the set of a posteriori LRLF values about the transmitted bits on the 1st and 2nd TC decoders:

$$\begin{aligned} LE &= \left[L_e^{1,j}(x_1^{\mathrm{C}}) \quad L_e^{1,j}(x_2^{\mathrm{C}}) \quad \ldots \quad L_e^{1,j}(x_{\tilde{N}}^{\mathrm{C}})\right], \\ LE &= \left[L_e^{2,j}(x_1^{\mathrm{C}}) \quad L_e^{2,j}(x_2^{\mathrm{C}}) \quad \ldots \quad L_e^{2,j}(x_{\tilde{N}}^{\mathrm{C}})\right] \end{aligned} \tag{5}$$

Step 6. Cycle execution: if $\operatorname{sign}\left(L_a^{d,j}(x_t^{\mathrm{C}})\right) \neq \operatorname{sign}\left(L_e^{d,j}(x_t^{\mathrm{C}})\right)$, то $R^{d,j}(i+1) = R^{d,j}(i) + 1$, $R_{\Sigma} = \sum_{j=1}^{I} \sum_{d=1}^{2} R^{d,j}$, $t \in \overline{1,N}$ for all bits of a block of length *N*, decoders *d*, $d \in \overline{1,2}$, decoding iterations *j*, $j \in \overline{1,I}$. If the condition is not carried out, then $R^{d,j}(i+1) = R^{d,j}(i)$.

1. The article proposes a method for optimizing the operation of the encoder and decoder of the turbo code through the use of adaptive selection of the size of state diagrams using the proposed decoding uncertainty indicator.

2. In contrast to the known results, depending on the signal-to-noise ratio in the channel and the values of the normalized number of sign changes of the posterior-a priori logarithmic relations of the likelihood functions of the transmitted data bits of the turbo code decoder, adaptive selection of the size of the state diagram of the TC encoder / decoder is carried out.

3. The results of simulation showed that depending on the signal-to-noise ratio in the channel and the normalized number of sign changes of the posterior-a priori LRLF of the iterative turbo code decoder, rational parameters are obtained that select the size of the state diagram of the TC encoder / decoder. This allows increasing the reliability of information transfer in comparison with known results, for example, a fourth-generation 4G LTE-Advanced mobile communication system.

4. The method can be used in conjunction with other adaptation methods, for example, adaptation according to the coding rate, polynomials of component codes of the TC, in systems with multi-parameter adaptation, operating under conditions of a priori uncertainty.

Abstract. The article considers the issues of increasing the efficiency of the fifth generation 5G mobile communication systems through the use of adaptive noise-resistant coding. A method is proposed for optimizing the operation of the encoder and decoder of the turbo code through the use of adaptive selection of the state diagrams size using the proposed decoding uncertainty indicator. Simulation results showed that depending on the signal-to-noise ratio in the channel and the normalized number of sign changes of a posteriori-a priori logarithmic relations of the likelihood functions (LRLF) of the iterative decoder of the turbo code, rational sizes of state diagrams for data blocks of the encoder and decoder of the turbo code are obtained. This allows getting the energy gain of coding, reduce the complexity of its hardware and software implementation and increase the reliability of information transfer in comparison with the known results, for example, the fourth generation 4G LTE-Advanced mobile communication system.

Literature

1. Berrou C. Near Shannon limit error-correcting coding and decoding: turbo-codes / C. Berrou, A. Glavieux, P. Thitimajshima // Proc. Int. Conf. On Commun., ICC-93. – Geneva, 1993. – May. – P. 1064 – 1070. DOI: 10.1109/ICC.1993.397441.

2. Berrou C. Near optimum error correcting coding and decoding: turbo-codes / C. Berrou, A. Glavieux // IEEE Trans. on Commun. – 1996. – Vol. 44 (10). – P. 1261 – 1271. DOI: 10.1109/26.539767.

3. Dahlman E. 4GLTE/LTE-Advanced for Mobile Broadband / Dahlman E., Parkvall S., Skold J. – Oxford: Academic Pressis an imprint of Elsevier, 2011. – 431 p.

4. Sesia S. LTE – The UMTS Long Term Evoluton. From Theory to Practice / Sesia S., Toufik I., Baker M. – West Sussex : John Wiley & Sons, 2009. – 626 p.

5. Koutsouvelis K. V. Generating Turbo code s-random interleavers with application of the bubble search sorting method / Koutsouvelis K. V., Dimakis C. E // Wireless Personal Communications. – 2008. – Vol. 46. – P. 365–370.

6. Sadjadpour H. R. Interleaver Design for Turbo Codes / Sadjadpour H. R., Sloane N. J. A., Salehi M., Nebe G. // IEEE Journal on Selected Areas in Communications. – 2006. – Vol. 19. – P. 831 – 837.

7. Dolinar S. Weight distribution for turbo codes using random and nonrandom permutations / Dolinar S., Divsalar D. // The Telecommunications and Data Acquisition Progress (TDA) Progress Report 42–122, Jet Propulsion Lab. (JPL). – 1995. – P. 56 – 65.

8. Zaitsev S. V. Method of Adaptive Decoding in Case of Information Transmission in Condition of Influence of Deliberate Noise / S. V. Zaitsev, V. V. Kazymyr // Radioelectronics and Communications Systems. – Allerton Press, Inc. – New York, 2015. – Vol. 58. – P. 30–40. DOI: 10.3103/S0735272715050039.

9. Zaitsev S. V. Structural adaptation of the turbo code coder and decoder for generating the transmission repeat request under conditions of uncertainty // Radioelectronics and Communications Systems. – Springer, 2017. – Vol. 60. – P. 18–27. DOI: 10.3103/S0735272717010034.

10. Zaitsev S. V. Adaptive selection of parameters of s-random interleaver in wireless data transmission systems with turbo coding / S. V. Zaitsev, V. V. Kazymyr, V.M. Vasilenko, A.V. Yarilovets // Radioelectronics and Communications Systems. – Allerton Press, Inc. – New York, 2018. – Vol. 61. – P. 13–21. DOI: 10.3103/S0735272715050039.

11. Kujima S. Adaptive Modulation and Coding Using Neural Network Based SNR Estimation / S. Kujima, K. Maruta, C.Ahn // IEEE Access. – 2019. – Vol. 7. – P. 183545 – 183553. (DOI: 10.1109/ACCESS.2019.2946973)

УДК 004.4:056.57

Агиевич Сергей Валерьевич
заведующий НИЛ проблем безопасности информационных технологий
НИИ прикладных проблем математики и информатики
Белорусский государственный университет,
agievich@bsu.by

СТАНДАРТЫ РЕСПУБЛИКИ БЕЛАРУСЬ В ОБЛАСТИ ПРИКЛАДНОЙ КРИПТОГРАФИИ

В октябре 2019 году в Республике Беларусь введены в действие шесть государственных стандартов в области прикладной криптографии. Стандарты приняты в серии СТБ 34.101 “Информационные технологии и безопасность” под номерами 50 (правила регистрации объектов информационных технологий), 78 (профиль инфраструктуры открытых ключей), 79 (криптографические токены), 80 (расширенные электронные цифровые подписи), 81 (протоколы службы заверения данных), 82 (протокол постановки штампа времени). Стандарты разработаны в НИИ прикладных проблем математики и информатики Белорусского государственного университета (стандарты с номерами 50, 80, 81, 82 – совместно с компанией «АВЕСТ»).

Базовые криптографические стандарты, принадлежащие той же серии СТБ 34.101, определяют алгоритмы и протоколы для защиты данных обмена между сторонами информационных систем. Речь идет об алгоритмах шифрования, имитозащиты, аутентифицированного шифрования, хэширования, электронной цифровой подписи, транспорта ключа, генерации псевдослучайных чисел и одноразовых паролей, протоколах аутентификации и формирования общего ключа (см. рисунок 1). Набор стандартизированных криптографических инструментов достаточно широк и разнообразен. Однако для полноценного взаимодействия сторон одних алгоритмов и протоколов недостаточно. Необходимо определить форматы сообщений, договориться о стандартных параметрах алгоритмов, наладить управление криптографическими ключами, унифицировать работу с криптографическими токенами (устройствами, которые реализуют криптографическую логику). И это далеко не полный перечень задач, которые необходимо

решить, чтобы информационные системы стали унифицированными, прозрачными, чтобы порог вхождения в систему новых поставщиков криптографических решений стал разумно мал. Именно эти задачи решают принимаемые стандарты. Кратко охарактеризуем их (в удобном порядке).

СТБ 34.101.50 определяет правила регистрации идентификаторов объектов информационных технологий, в том числе объектов, связанных с криптографией – алгоритмов, протоколов, форматов, долговременных параметров алгоритмов. Идентификаторы определяются иерархически, образуя дерево с общим корнем, назначенном Беларуси. Правила регистрации обеспечивают уникальность идентификаторов. Параллельно в СТБ 34.101.50 регистрируется ряд идентификаторов, стандартизируются долговременные параметры, определяются технологии XML-DSig и XML-Enc, предназначенные для защиты документов формата XML.

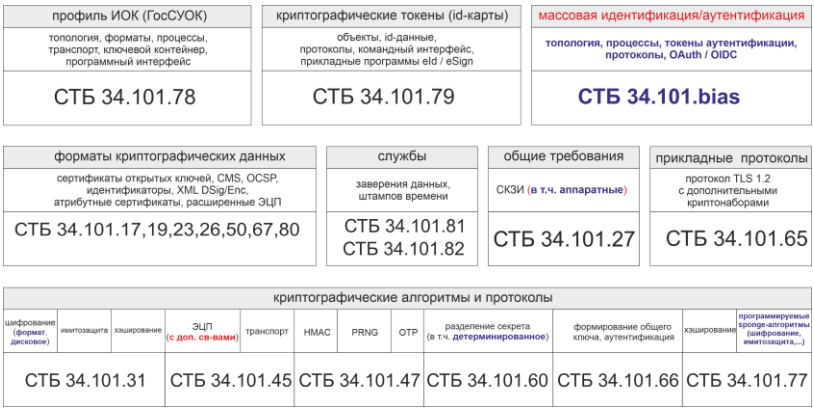


Рисунок 1 – Криптографическая инфраструктура Республики Беларусь (синий цвет – в работе, красный – в планах)

СТБ 34.101.80 определяет форматы расширенной электронной цифровой подписи (ЭЦП). Расширенная подпись, дополнительно к базовой, включает атрибуты подписанного документа и подписавшей его стороны. Атрибуты либо подписываются вместе с документом (за них ручается подписант), либо просто сопровождают документ, помогая проверять подпись и повышая

гарантии проверки. В СТБ 34.101.80 вводятся несколько профилей расширенных ЭЦП: базовый, с контролем времени подписи, долгосрочный, долгосрочный архивный и др. Профили отличаются правилами формирования подписанных и неподписанных атрибутов. Определены 3 формата расширенных подписей: CAdES (на языке АСН.1), XAdES (для встраивания в XML-документы, уточнение формата XML-DSig), PAdES (для PDF-документов). При разработке СТБ 34.101.80 были консолидированы несколько серий международных стандартов. Несмотря на сравнительно небольшой объем (68 страниц), СТБ 34.101.80 содержит необходимые сведения из 2 стандартов серии CAdES, 2 стандартов XAdES, 5 стандартов PAdES и еще одного стандарта по процессам проверки расширенных подписей.

СТБ 34.101.82 определяет протокол постановки штампа времени. Штамп представляет собой криптографическое доказательство существования определенного документа к определенному моменту времени, являясь одним из основных атрибутов расширенных ЭЦП. Доказательство создает служба штампов времени, подписывая хэш-значение искомого документа. СТБ 34.101.82 определяет формат запроса к службе, формат ответа, формат штампа. Основан на двух стандартах Интернет – RFC 3161 и RFC 5816.

СТБ 34.101.81 также основан на стандарте Интернет – RFC 3029. Этот стандарт не получил широкого распространения в силу излишней универсальности и дублирования функций других стандартов. Эксклюзивным механизмом RFC 3029, из-за которого собственно он и был выбран в качестве основы СТБ 34.101.81, является сервис проверки действительности электронных документов с выдачей соответствующих аттестатов. Проверка может быть выполнена в одной криптографической инфраструктуре, а аттестат быть выпушен в другой. Таким образом может быть организован трансграничный (межстрановой) обмен электронными документами, не предполагающий дорогостоящую унификацию и недопустимую централизацию инфраструктур.

СТБ 34.101.78 определяет профиль инфраструктуры открытых ключей (ИОК), рекомендуемый для использования в Беларуси. Фактически речь идет о новой криптографической архитектуре Государственной системы управления открытыми

ключами (ГосСУОК) Республики Беларусь – глобальной республиканской системы распределения открытых ключей физических лиц, юридических представителей, серверов, служб, автономных аппаратных устройств и др. Абонентская база ГосСУОК демонстрирует стабильный рост, но есть и сдерживающие факторы. Основные – отсутствие интерактивных сервисов, недостаточная определенность форматов, отсутствие унификации криптографических средств (программных и аппаратных). Стандарт нацелен на преодоление этих недостатков. В СТБ 34.101.78 конкретизируются стороны ИОК, определяются процессы их взаимодействия, протоколы взаимодействия, уточняются форматы объектов инфраструктуры. Стандарт унифицирует формат ключевых контейнеров программных средств защиты и унифицирует интерфейс взаимодействия с аппаратными средствами.

Полная унификация специализированных аппаратных средств – персональных криптографических токенов – выполнена в СТБ 34.101.79. С помощью токена его владелец может аутентифицироваться перед удаленными прикладными системами, вырабатывать ЭЦП, расшифровывать ключи защиты данных. На токене хранятся идентификационные данные владельца, фактически токен представляется собой id-карту гражданина. За управление объектами токена и взаимодействие с внешними устройствами отвечают прикладные программы. Две обязательные программы: eID – аутентификация и управление идентификационными данными и eSign – выработка ЭЦП и расшифрование ключей. В СТБ 34.101.79 использованы современные криптотехнологии. В частности, PIN может вводиться по радиоканалу, ввод организован так, что даже перехват всех данных канала не позволяет противнику выполнить перебор вариантов PIN (их сравнительно немного). У противника есть только одна разумная стратегия обхода защиты – попытаться самому ввести пароль. Но и здесь его возможности ограничены, поскольку количество попыток ввода контролируется. Перед последней попыткой требуется предъявить специальный пароль CAN, написанный на карте. Проверка знания CAN защищает от атак типа “отказ в обслуживании”.

Следует отметить, что обсуждение двух последних стандартов было организовано на Интернет-платформе Github. Сюда были перенесены существенные замечания из официальных отзывов,

здесь были обработаны дополнительные замечания и предложения. Дискуссия оказалась чрезвычайно полезной и эффективной. Дискуссионные площадки не закрыты, на них принимаются предложения по совершенствованию стандартов.

Аннотация. Рассмотрено шесть государственных стандартов Республики Беларусь в области прикладной криптографии (а именно СТБ 34.101.50, СТБ 34.101.79, СТБ 34.101.80, СТБ 34.101.82, СТБ 34.101.81, СТБ 34.101.78). Базовые криптографические стандарты, принадлежащие серии СТБ 34.101, определяют алгоритмы и протоколы для защиты данных обмена между сторонами информационных систем. Набор стандартизированных криптографических инструментов достаточно широк и разнообразен. Однако для полноценного взаимодействия сторон одних алгоритмов и протоколов недостаточно. Предложенные стандарты решают задачи определения форматы сообщений, помогают договориться о стандартных параметрах алгоритмов, наладить управление криптографическими ключами, унифицировать работу с криптографическими токенами (устройствами, которые реализуют криптографическую логику) и т.п.

Література:

1. BPKI: профиль инфраструктуры открытых ключей / [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/bcrypto/bpki.

2. BTOK: криптографические токены / [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/bcrypto/btok.

УДК 004.891

Азаренко Олена Василівна, професор, *д.ф.-м.н.*
Національний авіаційний університет
azarenko_ev@ukr.net

Хорошко Володимир Олексійович, професор, *д.т.н.*
Національний авіаційний університет
professor_va@ukr.net

Хохлачова Юлія Євгеніївна, доцент, *к.т.н.*
Національний авіаційний університет
hohlachova@gmail.com

ОЦІНКА ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

Технічний захист інформації в інформаційних системах забезпечується застосуванням захищених технічних засобів забезпечення інформаційної діяльності, технічних засобів захисту інформації та засобів контролю, що мають сертифікати відповідності вимогам нормативних документів з технічного захисту інформації (ТЗІ), а також застосуванням спеціальних технічних споруджень, засобів і систем. При цьому засоби ТЗІ можуть функціонувати автономно або разом з технічними засобами забезпечення інформаційної діяльності у вигляді самостійних пристроїв або вбудованих у них складених елементів [1].

Оперативне вирішення завдань ТЗІ в інформаційних системах (ІС) досягається організацією керування системою захисту інформації, для чого необхідно [2]: вивчати й аналізувати технологію проходження інформації в процесі інформаційної діяльності; оцінювати схильність інформації до впливу загроз у конкретний момент часу; оцінювати очікувану ефективність застосування засобів забезпечення ТЗІ; визначати додаткову потребу в засобах забезпечення ТЗІ; здійснювати збір, обробку та реєстрацію даних, що стосуються захисту інформації; розробляти і реалізовувати пропозиції щодо коректності систем ТЗІ в цілому або окремих її елементів.

Основи стратегії захисту інформації в ІС при загальному підході – це вибір основних і найбільш важливих базових системно-концептуальних положень і орієнтирів при плануванні, розробці і реалізації цієї стратегії. При цьому центральним питанням управ-

лінського рішення стратегічного характеру є оцінка обсягу необхідних ресурсів захисту і їхній оптимальний або найбільш доцільний розподіл не тільки необхідного, але й безперервного адаптивно-керованого рівня гарантованого захисту. Гарантованість захисту є важливою вимогою, про яку можна говорити тільки з імовірністю та у контексті обов'язкового виконання вимог і рекомендацій використовуваних при цьому стандартів безпеки.

Основи стратегії захисту інформації містять у собі необхідність використання двох термінологічних понять: стратегія технічного захисту інформації та стратегія безпеки інформації, що захищається, з урахуванням останніх вимог нормативних документів з питань її технічного захисту.

Основною метою реалізації стратегії ТЗІ в ІС є виключення або ускладнення реалізації загроз інформації, зниження збитку від реалізації загроз і забезпечення безпеки інформації.

Універсальних систем захисту на всі випадки не існує, оскільки кожен захист створюється для конкретного об'єкта, його оточення й зовнішнього середовища, під конкретні загрози, функціональні вимоги і необхідний рівень захищеності. При їхній зміні захист має бути здатним адаптуватися до необхідних змін.

Виходячи з вищенаведеного, система захисту складається з декількох ланок і рубежів [2]. Відомо, що при спробі подолати захист, порушник спробує використовувати найбільш слабкий напрямок або рубіж у цій системі. Через це підсумкова міцність СЗІ буде визначатися міцністю найбільш слабкого напрямку або рубежу в цій системі.

Якщо міцність слабкого рубежу не задовольняє заданим вимогам, то цей рубіж зміцнюється або заміняється на більш міцний.

Отже, імовірність ефективного захисту інформації при багаторубіжній системі визначається залежністю:

$$P_{\Sigma} = P_{СЗІ1} \cdot P_{СЗІ2} \cdot K \cdot P_{СЗІN}, \qquad (1)$$

де $P_{СЗІN}$ – імовірність ефективного захисту *N*-го рубежу СЗІ, *N* – порядковий номер рубежу.

Ефективність механізму захисту в значній мірі залежить від реалізації ряду принципів. По-перше, механізми захисту слід проектувати з урахуванням розподілу ресурсів між рубежами й можливістю їхнього перерозподілу. По-друге, питання захисту слід розглядати комплексно в рамках єдиної системи захисту.

Системний підхід забезпечує адекватну багаторівневу багаторубіжну систему захисту, яка розглядається як комплекс організаційно-правових і технічних заходів. Крім того, при реалізації механізмів захисту мають використовуватися передові, науково обґрунтовані технології захисту, що забезпечують необхідний рівень безпеки, прийнятність для користувачів і можливість нарощування й модифікації СЗІ надалі.

Сформулюємо і запропонуємо модель вирішення завдання нападу і захисту в ІС. Нехай комплексна СЗІ характеризується множиною рубежів *P*, які забезпечують протидію множині несанкціонованих дій *Д*. Нехай *P* складається з *n* рубежів, а *Д* містить *m* дій.

Кожний рубіж $p_i \in P$ характеризується доступною потужністю a_n, відповідно до множини *P*. Маємо вектор $a = (a_1,..,a_n)$ ресурсів рубежів.

Кожна несанкціонована дія $d_i \in Д$ відповідає набору дій зловмисника та має необхідний ресурс для виконання поставленого завдання (можливо навіть кількаразового) протягом доби Z_i (опер./доб.). За всіма діями множини *Д* маємо вектор $Z = (z_1,..,z_m)$ необхідних ресурсів.

За кожною дією дано два вектори V_i та W_i, де $V_i = (v_{i1},..,v_{im})$ множини *P*, вектор $W_i = (w_{i1},..,w_{im})$ визначає інтенсивність нападів при нападі d_i із завданнями інших протиправних дій множини *Д*. Тут $w_{ij} = 0$. За всією сукупністю нападів маємо прямокутну матрицю *V* розміру $m \times n$ і квадратну матрицю *W* розміру $m \times m$, складені з векторів V_i та $W_i, 1 \le i \le m$ відповідно. Будемо вважати, що ресурси несанкціонованої дії $d_i \in Д$ можуть бути реалізовані тільки проти одного будь-якого рубежу множини *P*, тобто дія проводиться проти конкретного рубежу.

Оскільки в СЗІ значення $m+n$ достатньо велике, доцільно використовувати для розв'язку цієї задачі евристичні алгоритми оптимізації. В основному, відомі евристичні алгоритми [1] можна віднести або до алгоритмів послідовної протидії підсистеми захисту, або до ітераційних алгоритмів послідовного поліпшення наближень за допомогою парних перестановок завдань між рубежами.

На практиці часто мають місце ситуації, коли кожна неправомірна дія $d_i \in Д$ представлена набором завдань, яким можуть протистояти різні рубежі множини *P*, і коли нападу d_i протистоїть тільки один рубіж. У цьому випадку розглянуте завдання трохи спрощується й може бути зведено до класичного транспортного завдання.

Нехай задано множини *P* і *Д*, де *P* має раніше зазначений зміст і представляється кортежем $< P, a, R >$.

Множина *Д* складається з *m* нападів $\{d_1, .., d_m\}$. Кожний напад $d_i \in Д$ представлений набором завдань і характеризується необхідним ресурсом Z_i для їхньої реалізації. По всіх протиправних діях *Д* маємо вектор необхідних ресурсів $Z = (z_1, .., z_m)$. Необхідний ресурс Z_i нападу d_i може бути припинено одним або декількома рубежами множини *P* за будь-якої розбивки Z_i між собою.

По кожному нападу $d_i \in Д$ даний вектор $V_i = \{v_{i1}, .., v_m\}$, що визначає інтенсивність нападів d_i на рубежі множини *P*. Припускається, що всі завдання, пов'язані з нападом $d_i \in Д$, мають однакову питому (щодо одиниці необхідного ресурсу) інтенсивність f_{ij} протиправних дій проти рубежів $p_i \in P$ тобто:

$$\forall d_i \in Д, p_i \in P \left| f_{ij} = \frac{V_{ij}}{r_j} \right. \qquad (2)$$

Отже, маємо в якості інтенсивностей нападів множини *Д* на рубіж множини *P* і *Д*, представлені відповідно кортежами $< P, a, Д >$ й $< Д, Z, V >$, де *V* – матриця інтенсивностей нападів множини *Д* на рубіж множини *P*.

Потрібно визначити розподіл ресурсів нападів *Д* по рубежах множини *P*. У результаті розподілу ресурсів нападу формується матриця *Q*, у якій кожній протиправній дії має бути зіставлений вектор $q_i = (q_{i1}, .., q_n)$ розмірності *n*, який представляє розподіл ресурсів протиправних дій d_i по рубежах множини *P*, тобто *k*-й компонент q_{ik} вектора q_i є набором завдань нападу d_i на *k*-й рубіж захисту. Сукупність розподілів протиправних дій множини *Д* визначимо як відображення $\gamma : Д \to N^n$, тут N^n – векторний простір *n*-мірних векторів, компоненти яких є цілими числами. Якість розподілу γ буде оцінена значенням середньозваженої довжини $L(\gamma)$ маршруту нападу.

Основою визначення $L(\gamma)$ є штраф для одиниці ресурсу нападу $d_i, i = 1, 2, .., m$, закріпленої за p_j-м рубежем. Якщо одиниця ресурсу нападу діє на p_j-й рубіж, то їй відповідає штраф:

$$c_{ij} = \sum_{k=1}^{n} f_{ik} r_{jk} = \sum_{k=1}^{n} r_{ik} \frac{V_{ik}}{Z_i} \qquad (3)$$

Отже, для кожного нападу $d_i \in Д$ маємо вектор $c_i = (c_{i1}, .., c_m)$, *k*-й компонент c_{ik} якого визначає збиток за одиницю ресурсу нападу d_j, що закріплюється за рубежем p_k.

Таким чином, завдання розподілу необхідних ресурсів нападу між рубежами в наведених вище поняттях і позначеннях може бути сформульовано в такий спосіб.

Нехай задано систему несанкціонованих дій $< Д, Z, V >$ і систему захисту $< P, a, R >$. Потрібно визначити такий позитивний, обмежений та реалізований розподіл γ, щоб $L(\gamma)$ набуло мінімального значення.

Представлена таким чином задача приводиться до класичної транспортної задачі.

Для цього поставимо у відповідність кожному p_i рубежу джерело ресурсу $p_j, 1 \le j \le n$ з наявним ресурсом a_j, а кожному нападу $d_i \in Д$ поставимо у відповідність зловмисника $d_i, 1 \le i \le m$ з необхідним ресурсом z_i. Вартість застосування одиниці ресурсу нападу d_i від зловмисника p_j є компонент c_{ij} вектора c_i. Обсяг ресурсу, який споживається нападом d_i від p_i, є q_{ij}.

Щоб задача мала припустимий розв'язок, потрібно, щоб загальні ресурси зловмисників були, принаймні, не менше загальної можливості захисника [3].

Ця модель транспортної задачі має $n+m+1$ змінних. Для її розв'язку використано симплекс-метод – метод потенціалів [1].

Встановлено, що в припустимому розв'язку сумарна потужність імітованого нападу не може перевищувати сумарного неправильного спрацьовування виходячи з наявних ресурсів захисту та попиту.

Анотація. Сформульовано і запропоновано модель вирішення завдання нападу і захисту в інформаційній системі.

Також сформульовано можливий спосіб завдання розподілу необхідних ресурсів нападу між рубежами в наведених поняттях і позначеннях.

Встановлено, що в припустимому розв'язку сумарна потужність імітованого нападу не може перевищувати сумарного неправильного спрацьовування виходячи з наявних ресурсів захисту та попиту.

Література:

1. Бармен С. Разработка правил информационной безопасности / С. Бармен. – М: ИД «Вильямс», 2002. – 208 с.

2. Довгань О.Д. Методологія захисту інформації / Довгань О.Д., Гулак Г.М., Гринь А.К., Мельник С.В. – К.: Вид. НА СБУ, 2012. – 184 с.

3. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.

УДК 004.056.53

Архипов Александр Евгеньевич,
Киевский политехнический институт имени Игоря Сикорского,
профессор кафедры информационной безопасности
профессор, доктор технических наук,
sonet0515@gmail.com
Архипова София Анатольевна,
Киевский политехнический институт имени Игоря Сикорского,
доцент кафедры информационной безопасности
доцент, кандидат технических наук,
arsofi@ukr.net

АДАПТИВНЫЕ АСПЕКТЫ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Суть проблемы. Практически любая идеология построения системы защиты информации (СЗИ) содержит в себе элементы адаптивного подхода, суть которого – организация защитных сервисов (функций) СЗИ в соответствии с перечнем существующих угроз информации. Успешная СЗИ гарантирует полноту и своевременность адаптации своего функционала защиты к возможным внешним и внутренним угрозам.

В своем развитии проблема адаптации СЗИ прошла несколько стадий. Самую первую можно назвать *стадией естественной адаптации*. Суть ее в том, что для задач, связанных с транспортировкой и обработкой информации, характерен достаточно высокий уровень типизации и стандартизации предлагаемых решений, реализуемых на базе унифицированного программного и технического обеспечения, входящего в состав информационно-коммуникационных систем (ИКС). Анализ инцидентов, фиксируемых в ходе эксплуатации этих ИКС, дает возможность выявить характерные уязвимости в их компонентах, позволяющие организовывать и успешно проводить атаки, наносящие ущерб циркулирующей в ИКС информации. Исследование и обобщение способов предотвращения этих атак привело к построению устойчивых шаблонов типовых защитных мероприятий (профилей защиты). В СЗИ, построенной в соответствии с найденным профилем, реализуется принцип полного перекрытия угроз. Успешность его применения основывается на результатах ретро-

спективного анализа произошедших ранее инцидентов, предполагая неизменность используемых технологий, задействованных в них программно-технических средств, условий функционирования ИКС. Однако для современного темпа развития информационных технологий построение СЗИ с использованием результатов только ретроспективного учета известных типовых угроз является явно недостаточным. Необходимы обнаружение и анализ появляющихся новых угроз неизвестного происхождения, например, путем мониторинга поведенческих аномалий сред функционирования ИКС, использования песочниц, ловушек, других возможных средств и способов выявления атак. В целом составление максимально полного перечня уязвимостей ИКС требует проведение очень детального, кропотливого, длительного и трудоемкого анализа. При этом совершенно не очевидна практическая возможность своевременного реагирования на весь полученный объем сведений в формате построения реальной системы защиты по схеме с полным перекрытием (назовем попытку реализации подобной ситуации *стадией асимптотической адаптации*). Ясно лишь, что любая попытка создания такой СЗИ влечет непомерно большие инвестиции в ее разработку и построение.

Следующим шагом в применении адаптивного подхода к построению СЗИ является *рискориентированная адаптация* процедуры формирования структуры и состава СЗИ, состоящая в сокращении множества «перекрываемых» угроз за счет выявление группы так называемых актуальных угроз. Выделение последних осуществляется путем анализа частных рисков, каждый из которых является результатом успешной реализации той или иной угрозы. Но на практике фактически используется способ усечения списка возможных уязвимостей путем исключения из него неэффективных атак. Критерием недостаточной эффективности атаки является пренебрежимо малый уровень порождаемого ею значения частного риска, возникающего при нарушении нормального режима работы организации, функционирование которой обеспечивается рассматриваемой ИКС. В итоге происходит ограничение перечня эффективных атак, а в списке актуальных угроз остаются лишь те, для которых суммарные риски не исключенных атак оказались выше некоторого минимального порогового

значения. Однако эта достаточно привлекательная на первый взгляд идея требует для своего практического применения наличия первоначального максимально полного перечня уязвимостей ИКС. При этом субъективный характер селекции эффективных атак, и в первую очередь, доминирующее стремление не пропустить опасную атаку, ведет к формированию их расширенного перечня, в итоге – опять к необоснованному росту объема инвестиций в СЗИ [1, 2].

По-видимому практика подобного экстенсивного роста инвестиций может быть прервана возможным введением некоторого предельного уровня их объема. Особо **актуальной** в сложившейся ситуации представляется необходимость объективного (доказательного?) задания этого предельного объема инвестиций. Попытка решения подобной задачи была предпринята в [3], однако полученный результат, базирующийся на введении ряда формальных условий, практически исключает свою привязку к какой-либо конкретной ситуации «атака/защита», к особенностям и свойствам реальной организации, к параметрам и функциям создаваемой СЗИ.

Цель исследования: построение СЗИ, с *целевой адаптацией* к потенциалам атакующей и защищающейся стороны.

Содержательная часть. Под *атакующей стороной* понимается любая сущность (хакер, вредоносный код, внутренний злоумышленник и т.п.), действия которой ведут к причинению вреда информации, циркулирующей в ИКС, что в конечном итоге сказывается на состоянии и стоимости активов организации-владельца ИКС.

Под *потенциалом атакующей стороны* обычно [4]. понимается комплекс следующих факторов: компетентность и уровень мотивации атакующего (при антропогенном характере атаки), ресурсное обеспечение, способствующее успешному осуществлению атаки. Возможность учета названых факторов рассмотрена в [5], где, в зависимости от наличия и выраженности этих факторов, вербально описаны модели типовых сценариев поведения атакующей стороны для следующего набора ролей:

1. С*крипт кидди* - неопытный одиночка, не имеющий существенной подготовки и знаний, использующий для атаки скрипты или программы, разработанные другими, не понимающий меха-

низма их действия, неспособный к креативу, самостоятельным эффективным атакующим решениям, с достаточно скромными ресурсными возможностями; обычно его не волнуют финансовые или политические соображения, он действует из спортивного интереса, стремясь породить хаос, отказ либо нарушение сервисов. По оценке А.В.Лукацкого [6], скрипт кидди составляют до 95% от общего числа злоумышленников, атакующих информационные и компьютерные системы, т.е. это наиболее распространенный тип нарушителя, необходимость защиты от которого является первоочередной задачей, решаемой при построении СЗИ.

Следует отметить, что «под крышу» скрипт кидди можно подвести различные вредоносные коды (вирусы, черви, пр.), за исключением вредоносов нулевого дня.

2. *Самозанятый профессионал*, для которого экономически мотивированный хакинг – основной вид самостоятельной деятельности.

3. *Профессионал-исполнитель* - хакер, выполняющий работы в рамках определенных договорных обязательств (например, в интересах силовых структур или спецслужб).

4. *Хактивист* - идейный хакер («кибер-активист»), стремящийся перенести в киберпространство продвижение политических либо социальный идей (нередко достаточно сомнительного характера), организующий акции гражданского «электронного» неповиновения в киберпространстве, старающийся привлечь внимание власти и общественности (иногда в довольно жесткой форме) к тем или иным вопросам и проблемам современного общества путем синтеза социальной активности и хакерства.

В статье [1] этим типовым вербальным моделям-сценариям в соответствие поставлены математические модели рисков, которым защищающаяся сторона подвергается при возможной реализации выбранного сценария. Эти модели отражают основные особенности и свойства каждого из введенных выше типовых сценариев атаки, в связи с чем они получили название моделей рефлексивных рисков (от лат. reflexus – отображение, отражение).

Успех действий атакующей стороны зависит и от *потенциала защиты*, определяемого в первую очередь объемом инвестиций c в СЗИ, уровнем s информационной зрелости защищающейся

стороны, а также интегральной характеристикой важности защищаемых информационных ресурсов организации, часто также называемой стоимостью или ценностью информационных ресурсов. В качестве этой интегральной характеристики примем q – полные (максимальные) потери защищающейся стороны в случае успешного завершения направленных против нее атакующих действий.

Анализ рефлексивных рисков, их сопоставление с величинами инвестиций в СЗИ позволяет в ряде случаев для выбранного типового сценария атаки оценить значение наибольшего эффективного объема $c_{eff\,\max}$ инвестиций – объема инвестированных в СЗИ средств c, при котором достигается наибольшая интенсивность уменьшения риска возможных потерь на единицу инвестированных средств. В частности, в случае атаки скрипт кидди эта величина составит $0{,}25\,q$, а если предполагается, что атакующие действия, осуществляются профессионалом-исполнителем – $0{,}5\,q$. Полученные результаты представляют собой оценочные значения инвестиций в СЗИ, достаточно близкие к известным из практики эмпирическими оценками объема инвестиций, приведенным в ряде публикаций [7, 8].

Преимущества применения варианта построения СЗИ с целевой адаптацией наиболее ощутимы при использовании дополнительных сведений о потенциале защиты. Здесь один из наиболее важных параметров – оценка уровня s информационной зрелости защищающейся стороны, $0 \le s \le 85$ [1, 5]. Например, в случае атаки скрипт кидди знание значения s для конкретной организации позволяет уточнить величину эффективного объема инвестиций $c_{eff} = q(\sqrt{s} - 1)/s$ для создания СЗИ в этой организации, оценить для данного случая величину остаточного интегрального (обобщенного) риска $R_{in}(c_{eff}) = q/\sqrt{s}$ и соответствующую этому риску вероятность $P_{in}(c_{eff}) = 1/\sqrt{s}$ реализации совокупности угроз, обуславливающих появление интегрального риска $R_{in}(c_{eff})$ [1, 5]. Все это в конечном итоге позволяет в каждой конкретной ситуации оценить величину приемлемого для данной

организации объема инвестиций в СЗИ (по терминологии [5] – «разумного» объема) путем сопоставления количественных оценок показателей c_{eff}, q, $c_{eff\,\max}$, $R_{in}(c_{eff})$, $R(s,c)$, для различных значений параметра c, сбалансировав финансово-экономические возможности организации с ее требованиями и возможностями в сфере информационной безопасности. Например, при эффективном обеспечении выполнения политики информационной безопасности ($s=60$) объем инвестиций c_{eff} может оказаться на уровне $0{,}11q$ - $0{,}13q$, т.е. вдвое ниже $c_{eff\,\max}$. Рассматривая полученный для конкретной ситуации оценочный результат c_{eff} как некоторое ресурсное ограничение, решаем задачу оптимального распределения выделенных инвестиций на ограниченном множестве возможных функций и механизмов защиты, формируя из них структуру СЗИ из условия минимизации остаточного риска организации.

Выводы. Предложен подход к адаптивному управлению информационной безопасностью организации, базирующийся на:

- введении набора вербальных ролевых моделей типовых сценариев поведения атакующей стороны;
- формировании рефлексивных моделей рисков, представляющих собой математические модели введенных выше типовых сценариев поведения атакующей стороны, в которых учитываются параметры участников информационного конфликта;
- использовании рефлексивных моделей рисков для расчета базовых показателей СЗИ и оптимизации ее структуры;
- согласование финансово-экономические возможностей организации с ее требованиями и возможностями в сфере защиты информации, обеспечение эффективного и рационального инвестирования в СЗИ организации.

Аннотация. Рассмотрено применение адаптивного подхода к построению СЗИ организации, суть которого в использовании для управления информационной безопасностью организации сведений об особенностях и характере поведения сторон-участников конфликтной ситуации «атака / защита», возникающий при реализа-

ции атакующей стороной угроз относительно организации-владельца информационного ресурса. Обобщение и «упаковка» указанных сведений реализуется в форме математических моделей – рефлексивных рисков, структура и количество которых определяются выделенными типовыми сценариями» развития ситуации «атака / защита». Анализ и исследование моделей дает оценочную информацию, позволяющую сбалансировав финансово-экономические возможности организации с ее требованиями и возможностями в сфере защиты информации, обеспечивая эффективное и рациональное инвестирование в СЗИ организации.

Литература:

1. Архипов А.Е. Применение рефлексивных моделей рисков для защиты информации в киберпространстве / А.Е.Архипов // Захист інформації. – 2017. – Т. 19, №3. – С. 204-213.

2. Архипов А.Е. Экономико-стоимостной аспект обеспечения безопасности информации. Адаптивный поход. // Економіка, фінанси, облік, менеджмент і право в Україні та світі: збірник тез доповідей міжнародної науково-практичної конференції (Полтава, 1 грудня 2018 р.): у 6 ч. – Полтава: ЦФЕНД, 2018. – Ч. 6. – 63 с., С. 44 - 46.

3. Gordon L.A., Loeb M.P. (2002), "The Economics of Information Security Investment", ACM Transaction on Information and System Security, Vol.5, No4, pp.438-457.

4. ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

5. Архипов А.Е. Риск-ориентированный подход к оцениванию «разумного» объема инвестиций в системы защиты информации / А.Е.Архипов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2018. – № 1(35). – С. 18-29.

6. Лукацкий А.В. Обнаружение атак. – СПб.: БХВ – Петербург, 2003. – 608 с.

7. Андрощук Г.А., Крайнев П.П. Экономическая безопасность предприятия: защита коммерческой тайны. – К.: Изд. Дом «Ин Юре», 2000. – 400с.

8. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. М.: Компания Ай Ти; ДМК Пресс, 2004. - 348с.

УДК 621.39:004.05

***Ахметов Берик Бахытжанович**, к.т.н.*
YESSENOV University, Казахстан
berik.akhmetov@yu.edu.kz

***Адранова Асельхан Багдатовна,** докторант*
Казахский национальный педагогический университет имени Абая, Казахстан assel.adranova@gmail.com

***Кыдыралина Лазат Муктаровна ,** докторант*
Казахский национальный педагогический университет имени Абая, Казахстан lazat_75@mail.ru

***Касымбергибаев Бауржан,** докторант*
YESSENOV University, Казахстан

ПРОБЛЕМАТИКА РАЗВИТИЯ ТЕОРЕТИКО-МЕТОДИЧЕСКИХ ОСНОВ ПРОЕКТИРОВАНИЯ КИБЕРБЕЗОПАСНОЙ ОБЛАЧНО ОРИЕНТИРОВАННОЙ УЧЕБНОЙ СРЕДЫ УНИВЕРСИТЕТА

Введение ООУС в систему высшего образования позволит создавать такие управленческие и учебные структуры университетов, которые обеспечат не только неограниченный доступ к электронным образовательным ресурсам, но и новейшие условия коммуникации и сотрудничества для тех высших учебных заведений (ВУЗ), где отсутствуют мощные ИТ-подразделения и материально-технические ресурсы.

Инновационные изменения в ВНЗ способствуют всестороннему развитию личности студента при реализации парадигмы непрерывного образовании научно-педагогических работников (НПР), формированию ценностей демократического общества.

В современном обществе, открытом для всех и направленном на развитие образования, ключевая роль принадлежит НПР, которому доверено всестороннее развитие учащихся, раскрытие их потенциала и формирование успешного человека и специалиста. Наряду с этим необходимо, чтобы в ВУЗ работали профессиональные и компетентные НПР с высоким уровнем мотивации, всегда готовые помочь студентам. Профессиональная деятельность НПР университета становится сложнее: внедряют-

ся новые педагогические технологии, меняется содержание образования, появляются новые виды деятельности, которые, в свою очередь, требует системного развития информационных компетентностей (ИК) всех субъектов обучения.

В последние годы интерес к образованию значительно повысился, и НПР все чаще обращаются к услугам сети Интернет с целью использования ИКТ для коммуникации, сотрудничества и организации корпоративной работы, а стремительное развитие облачных сервисов стало ведущей тенденцией в решении проблем образовательной мобильности всех участников учебного процесса.

Решение этих проблем являются социально значимыми задачами педагогической науки.

Заметим, что основой исследования ООУС является ряд научных результатов, отражающих внедрения ИКТ в ВУЗах [1-3].

Теоретический анализ научных трудов ведущих ученых в области образования, изучение опыта применения ИКТ в учебном процессе, управленческой деятельности университетов, свидетельствует о наличии противоречий между:

- ростом влияния ИКТ на развитие высшего образования и отставанием теоретических и методических исследований в вопросах системного использования их в учебном процессе;
- значительным дидактическим потенциалом ООУС и отсутствием теоретически обоснованных моделей и эффективных методик его использования в университетах;
- возрастающими требованиями общества к организации учебного процесса в университетах и низким уровнем использованием средств ИКТ и ООУС;
- наличием значительного количества программного, учебно-методического и дидактического обеспечения учебного процесса и отсутствием повсеместного доступа к нему;
- значительным технологическим потенциалом ООУС и низкой учебной мобильностью участников образовательного процесса;
- интенсивным развитием ИКТ и скоростью обновления содержания учебных программ, в частности по техническим и информационным дисциплинам, обеспечивающих формирование ИК студентов.

Таким образом, проблема научно-теоретического обоснования и разработки ООУС, учитывающих практические потребности преподавателей и требования общества к организации учебного процесса, является до конца не решенной. Последнее в свою очередь, негативно отражается на уровне развития ИК субъектов учебного процесса и обеспечении их образовательной мобильности.

Таким образом, актуальность исследования по развитию теоретико-методических основы проектирования кибербезопасной облачно ориентированной учебной среды университета определяется потребностью в формировании нового направления научно-прикладных исследований общенационального уровня по теории и методике разработки и использования ООУС, направленных на развитие ИК НПР и студентов высших учебных заведений.

Аннотация. Актуальность исследования по тематике тезисов доклада обусловлена тем, что сегодня непрерывно возрастают требования к организации и качеству учебного процесса со стороны общества. Сегодня появляются новые возможности для всестороннего развития студентов XXI века, быстрыми темпами развиваются новые, более эффективные информационно-коммуникационные технологии (ИКТ), в частности облачно-ориентированные учебные среды (ООУС).

Литература:

1. Dennis Altman. Power and Community. Organiztaionnal and Cultural Responses to AIDS / Dennis Altman. – London : Taylor & Francis, 1994. – 190 p.

2. Denton D.W. Enhancing instruction through constructivism, cooperative learning, and cloud computing. / D.W. Denton // TechTrends. – 2012. – Vol. 56. – No. 4. – P. 34-41.

3. Dictionary.com [Electronic resource]. – Text. data. – Access mode: http://dictionary.reference.com/browse/modeling (date of access 16.09.15). – The title screen.

УДК 004.4:056.57

Бакрі Медон*, *drbakri@ucts.edu.my*

Гері Лох Чі Віяй* , *gary@ucts.edu.my*
** University College of Technology Sarawak (Малайзія)*

Юрченко Андрій Вадимович, *incyberinfo@gmail.com*
Incyber Technology Sdn Bhd (Малайзія)

Ткач Юлія Миколаївна**, *д.пед.н., доцент*
tkachym79@gmail.com

Шелест Михайло Євгенович**, *д.т.н., професор*
mishel3141@gmail.com
*** Національний університет "Чернігівська політехніка"*

РЕАЛІЗАЦІЯ СТАНДАРТУ ШИФРУВАННЯ SES ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЦИФРОВОЇ ІНФРАСТРУКТУРИ

Інтернет-технології повністю змінили сучасне життя. В рамках концепції Internet-of-Things (IoT) повсюдно формуються елементи електронного світу: електронний уряд, електронні послуги, електронний документообіг, електронні гроші, електронний підпис тощо. Основою успішного існування сучасної цифрової інфраструктури є забезпечення безпеки та конфіденційності інформації, що обертається в ній.

У даний час більшість технологій та продуктів захисту інформації розробляються по більшості фірмами інтернет-індустрії з США, Великобританії, ЄС, Китая, Росії, Ізраїлю тощо. Це, наприклад, виробники телекомунікаційної техніки (Cisco, Huaway), шифраторів (Crypto AG, Omnisec, Mils Electronic), програмного забезпечення (Microsoft), соціальних мереж (Facebook, Вконтакте, Одноклассники), антивірусних систем (Касперский, McAfee), постачальники послуг електронної пошти, мережеві та Інтернет гіганти (Google, Yahoo, AT&T, CenturyLink, Verizon), які за вимогою своїх урядів, як правило, вбудовують бекдори та троянські коні (від рівня чіпа до рівня додатків) з метою збору інформації щодо користувачів [1], що напряму загрожує безпеці національній цифровій інфраструктурі інших країн.

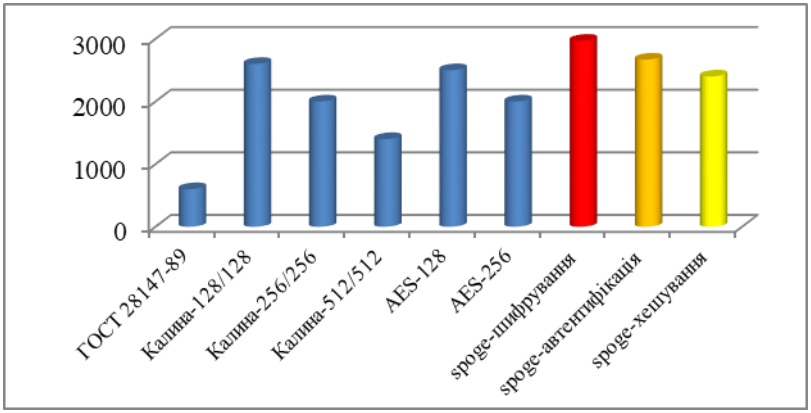
Для реалізації концепції "захищеного кіберпростору", на замовлення уряду штату Саравак (Малайзія), міжнародною групою фахівців розробляються та агрегатуються в єдину систему безпеки необхідні базові елементи: захищена операційна система, інтелектуальна система антивірусної підтримки, захищені сховища зберігання інформації, аналітична підсистема підтримки безпеки тощо.

В рамках цього проекту розроблено також новий стандарт шифрування SES (Sarawak Encryption Standard). Криптоалгоритм даного стандарту використовує в якості криптографічного примітиву так звану sponge-функцію [2]. Sponge-функції можуть ефективно реалізуватися на ПЛІС, тому що в них задіяні тільки логічні операції, циклічні зрушення та XOR. Це дає їм переваги при створенні різноманітних криптоалгоритмів (поточного шифрування, генерації псевдовипадкових чисел, хешування, імітозахисту тощо) та високопродуктивних засобів криптографічного захисту інформації.

Алгоритм SES є алгоритмом автентифікованного шифрування, що може одночасно виконувати функції шифрування та імітозахисту [3], що забезпечує певну гнучкість у функціональності: ключі можуть оновлюватися в процесі обробки даних; можливо шифрувати тільки окремі частини повідомлення; можливо чергувати шифровані та відкриті повідомлення; імітовставки можуть бути відсутні або, навпаки, зустрічатися кілька разів.

Для оцінки швидкодії алгоритму було розроблено програмну модель SES, на якій моделювалось процесу шифрування неперервного потоку даних блоками в 1 Кбайт. На мал.1 наведено відомості з оцінки продуктивності алгоритмів SES на функціях шифрування, імітозахисту та хешування. Для порівняння у таблиці також наведено дані щодо продуктивності алгоритмів шифрування ГОСТ 28147-89, AES та "Каліна" (ГСТУ 7624:2014) з різними розмірами блока.

Експерименти довели, що алгоритми SES випереджають по швидкості існуючі. Ще більшу продуктивність вони досягають при реалізації на програмованих логічних інтегральних схемах. Це дозволило створити лінійку апаратних засобів IP-шифрування Cryptomatics, які можуть підтримувати швидкість шифрування даних від 1 Гбіт/с та вище.



Мал. 1. Оцінка швидкодії алгоритмів (в Мбіт/сек, 64-разрядна платформа Intel Core i5-4670 CPU@3.4 GHz)

На даний час проводиться оцінка стандарту SES національним органом з сертифікації кібербезпеки Малайзії перед його широким використанням. У подальшому планується робота з побудови Blockchain технологій з використанням розробленого алгоритму.

Анотація. Обґрунтовано необхідність та доцільність розробки високошвидкісного алгоритму шифрування SES на базі sponge-функції, який відноситься до алгоритмів автентичного шифрування. Це дає певні переваги щодо створення різноманітних криптоалгоритмів (поточного шифрування, генерації псевдовипадкових чисел, хешування, імітозахисту, тощо) та високопродуктивних засобів криптографічного захисту інформації. Експериментальна реалізація SES на ПЛІС фірми Xilinx продемонструвала швидкісні показники, що значно вищі за відомих алгоритмів шифрування.

Література:

1. Интернет как оружие. Что скрывает Google, Tor и ЦРУ / Левин Яша; Пер.с англ. - М.: Индивидуум, 2019. - 360 с.

2. Agievich S., Marchuk V., Maslau A., Semenov V (2016). Bash-f: another LRX sponge function. Proceedings of the 5th Workshop on Current Trends in Cryptology, Russia (pp. 184–205).

3. Bellare M., Namprempre Ch. (2000). Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm. ASIACRYPT, LNCS (pp. 531–545).

4. Bertoni G., Daemen J., Peeters M., Van Assche G. (2011). Cryptographic sponge functions, Retrieved from http://sponge.noekeon.org/CSF-0.1.pdf.

УДК 004.4:056.57

Балюнов Олексій Олександрович, *к.ф.м.н., доцент*
Національний університет «Чернігівська політехніка»,
abalyunov@gmail.com

ЗАСТОСУВАННЯ СИСТЕМИ WOLFRAM MATHEMATICA У КРИПТОГРАФІЇ

Необхідність комплексного захисту всіх процесів обробки, передачі і зберігання інформації в сучасних комп'ютерних системах зумовило появу численних криптографічних засобів, основною функцією яких є закриття наявної та передаваємої інформації. Сьогодні безпечну роботу інформаційної системи неможливо уявити без електронного цифрового підпису, протоколів ідентифікації та автентифікації абонентів, автентифікації повідомлень і т. д. В основі всіх таких засобів лежать алгоритми шифрування [1,2]. Незалежно від складності алгоритму при практичному використанні він підлягає програмній реалізації. З розвитком інформаційних технологій взагалі та програмної інженерії зокрема, з'являються нові програмні середовища із новими підходами, наприклад, система комп'ютерної алгебри Mathematica від компанії Wolfram Research. Можливості щодо впровадження відомих алгоритмів криптографії в ту чи іншу інформаційну систему і є темою даної доповіді.

Mathematica – система на основі гнучкої символьної мови, яка підтримує багато концепцій програмування, потужні інструменти налагодження, що покликана на спрощення всього процесу створення програмного продукту: від розробки до впровадження. Основними рисами системи є: багатоплатформність; JIT-компіляція; автоматичне конфігурування паралельних обчислень; виконання обчислень з «нескінченною» точністю; підтримка кількох сотень форматів даних для експорту/імпорту; інтегрована в середовище можливість програмування GPU (існує підтримка OpenCL та CUDA); повна функціональність графічного відображення структурованих і неструктурованих даних у 2d і 3d; підключення додатків до будь-якої стандартної СУБД SQL; виклик елементів керування із програм на C, Java, .NET, та інших мовах; автоматична генерація коду на C для використання при компіляції у бібліоте-

ки, в окремих проектах або exe-файлів; можливість підключення динамічних бібліотек; підтримка створення звітів у різних форматах, в тому числі PDF, HTML и RTF, електронні таблиці [3].

Стан і перспективи розвитку систем комп'ютерної алгебри, до яких належить і Mathematica, докладно представлено в роботі [5], визначено їх універсальність, інтелектуальність та потужність у чисельно-аналітичному розв'язку різноманітних задач на основі локальних та розподілених обчислень.

Mathematica знайшла своє місце і в задачах практичної криптографії. Зокрема, в роботі [6] подано реалізацію алгоритму блочного шифрування, доведено, що за допомогою Mathematica процес можна суттєво спростити.

Розглянемо застосування системи комп'ютерної алгебри Mathematica до реалізації найбільш відомого криптографічного алгоритму RSA [4]. Як відомо, в даному алгоритмі процедура цифрового підпису ґрунтується на складності факторизації великих цілих чисел [4].

На першому етапі виконується процес генерації ключів. Його можна реалізувати процедурою:

$$:= Module[\{p,q,\phi,e,d\},\{p,q\} = RandomPrime[\{10^{\lfloor \frac{ndigits}{2} \rfloor - 1}, 10^{\lfloor \frac{ndigits}{2} \rfloor}\},2]; \phi = (p-1)(q-1);\ e = RandomInteger[\{99{,}999\}];\ While[gcd(\phi,e) \neq 1, e = RandomInteger[\{99{,}999\}]]; d = e^{-1} mod \phi; \{pq,e,d\}].$$

Тут, пара чисел $\{p,q\}$ - два великі прості числа, ϕ- функція Ейлера, $\{pq,e,d\}$- відповідно модуль ключа, відкрита й секретна експоненти; стандартна функція $RandomPrime[range,2]$ генерує 2 випадкові прості числа $\{p,q\}$ із вказаного проміжку; функція $RandomInteger[\{a,b\}]$ повертає випадкове ціле число із інтервалу; функція $PowerMod[e,-1,\phi]$ використовується для обчислення d- експоненти, необхідної для процедури дешифрування.

На другому кроці виконується процедура шифрування. Для текстового повідомлення модуль має, наприклад, вигляд:

$$:= Proc\_code[\{ot,num,str\}, ot = ToCharacterCode[openText];\ num = Fold[\#1\ 2\text{^}16 + \#2\&, 0, tcc];\ str = IntegerDigits[num,n];\ PowerMod[str,e,n]],$$

де функція $ToCharacterCode[]$ переводить текст у Unicode – послідовність, кожний елемент якої – ціле число із проміжку $[0;2^{16}]$; функція $Fold[]$ перетворює останню у велике число, роз-

ряди якого утворюють послідовність блоків відкритого тексту; функція $PowerMod[str, e, n]$ за допомогою відкритої експоненти e повертає список із шифрованих блоків.

На останньому етапі в зворотньому порядку виконується процедура дешифрації із використанням функції $FromCharacterCode[]$:

$$:= Proc\_decode[\{pm,num,str\},pm = PowerMod[codeText,d,n]; f = Fold[\#1\,n + \#2\&, 0, pm];$$
$$id = IntegerDigits[num, 216]; FromCharacterCode[str]]$$

Таким чином, на платформі Wolfram Mathematica завдяки невеликій кількості вбудованих функцій вдалося достатньо швидко реалізувати алгоритм шифрування RSA. Зважаючи на означені вище переваги даної системи комп'ютерної алгебри, її можна рекомендувати для використання як в практичній області, так і в освітній сфері.

Анотація. У тезах подано аналіз сучасного стану використання систем комп'ютерної алгебри в задачах криптографічного захисту інформації. На прикладі пакету Wolfram Mathematica показано можливості і переваги подібних платформ програмування, простота реалізації, стійкість і швидкість роботи найбільш відомих алгоритмів шифрування засобами вбудованих інтелектуальних функцій. Результати свідчать про широкі можливості застосування системи Mathematica як у практичній криптографії, так і в освітньому процесі.

Література.

1. Фергюсон Н. Практическая криптография / Н. Фергюсон, Б. Шнайдер. – Москва: Вильямс, 2005. – 424 с.

2. Мухачев В. А. Методы практической криптографии / В. А. Мухачев, В. А. Хорошко. – Киев: ООО «Полиграф-Консалтинг», 2005. – 215 с.

3. Wolfram Mathematica / [Електронний ресурс] – Режим доступу до ресурсу: https://www.wolfram.com/mathematica/index.html.ru?footer=lang

4. Коутинхо С. Введение в теорию чисел. Алгоритм RSA / С. Коутинхо. – Москва: Постмаркет, 2001. – 328 с.

5. Клименко В. П. Современные особенности развития систем компьютерной алгебры / В. П. Клименко, А. Л. Ляхов, Д. Н. Гвоздик. // Математичні машини і системи. – 2011. – №2. – С. 3–18.

6. Казимиров О. Реализация AES на Wolfram Mathematica [Електронний ресурс] / О. Казимиров. – 2011. – Режим доступу до ресурсу: https://habr.com/ru/post/123760/.

УДК 004.621.37

***Бриль Василь Михайлович**, к.т.н., професор*
Національний авіаційний університет
vamibr@ukr.net

ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНІЙ СИСТЕМІ СУЧАСНОГО ПІДПРИЄМСТВА

Сучасний етап розвитку економіки характеризується переходом підприємств на нові умови господарювання, необхідністю розвитку перспективних сфер науки і техніки. Зважаючи на це будь-яке підприємство для ефективного функціонування в умовах ринкової економіки упроваджує інформаційну систему (ІС), яка забезпечує збір і обробку інформації, формування варіантів реагування на ситуації, які постійно виникають в процесі ділової активності. На етапі проектування, розробки і експлуатації ІС необхідно вирішувати завдання ефективної підтримки тих процесів бізнесу, які забезпечують досягнення мети діяльності підприємства. Етап аналізу ІС і її підсистем, принципів їх побудови, аналіз і оцінка оптимальних показників якості і ефективності ІС для виконання процесів бізнесу найбільш критичні і недооцінка даного підходу приводить до негативних результатів впровадження і супроводу ІС об'єктів інформаційної діяльності (ОІД) підприємства [1, 2].

Постановка проблеми в загальному вигляді. Оцінка ефективності функціонування системи захисту інформації (СЗІ) на ОІД підприємства є складним науково-технічним завданням і такі системи оцінюються як в процесі розробки ІС, в період експлуатації, і при створенні (модернізації) СЗІ вже існуючих ІС. При розробці таких систем поширеним методом дослідження є синтез з їх подальшим аналізом [1,2,4]. Система ЗІ синтезується шляхом узгодженого об'єднання пристроїв, блоків, підсистем і аналізується (оцінюється) ефективність отриманого рішення.

Актуальність дослідження. Сьогодні досвід використання ІС (як зарубіжних, так і вітчизняних) на українських підприємствах вказує на те, що не завжди впровадження ІС було успішним і принесло підприємству відчутну фінансову вигоду. Для забез-

печення ефективності ІС в процесі її впровадження є актуальним питання аналізу можливих загроз та ризиків, вибору рішень надійного захисту інформації за мінімум затрат.Ефективність ІС – це характеристика, яка відображає ступінь відповідності системи своєму призначенню, її технічній досконалості і економічній доцільності. Об'єм і складність сучасних ІС невпинно ростуть, тому їх успішний вибір залежить від того, наскільки ефективно вони розроблені на базі сучасних розподілених систем, архітектури і технологій, конфігурації технічних і програмних засобів, рентабельності, сумісності і показників ефективності ІС.На етапі проектування, розробки і експлуатації ІС необхідно в першу чергу вирішувати завдання ефективної підтримки тих процесів бізнесу, які забезпечують досягнення мети діяльності підприємства (системи бізнесу) [6].

Основний матеріал. Оскільки на процеси захисту інформації в ІС основний вплив здійснюють випадкові чинники, то моделі систем захисту є стохастичними. При цьому

моделювання систем ЗІ є складним завданням, тому що такі системи відносяться до класу складних організаційно-технічних систем, яким властиві наступні особливості:

- складність формального представлення процесів функціонування таких систем, головним чином, із-за складності формалізації дій людини;

- різноманіття архітектури складної системи, яке обумовлюється різноманіттям структур її підсистем і множинністю шляхів об'єднання підсистем в єдину систему;

- велике число взаємозв'язаних між собою елементів і підсистем;

- складність функцій, що виконуються системою;

- функціонування систем в умовах неповної визначеності і випадковості процесів, що надають дію на систему;

- наявність управління, що часто має складну ієрархічну структуру;

- розгалуженість і висока інтенсивність інформаційних потоків.

Різноманіття варіантів побудови ІС ОІД підприємств породжує необхідність створення різних СЗІ, що враховують індивідуальні особливості ОІД. У той же час, великий обсях наявних публікацій навряд чи може сформувати чітке уявлення про те як же приступити до створення СЗІ для конкретної ІС ОІД з урахуванням властивих їй особливостей та умов функціонування.

В процесі проектування систем ЗІ необхідно отримати їх характеристики. Деякі характеристики можуть бути отримані шляхом вимірювання. Інші виходять з використанням аналітичних співвідношень, а також в процесі обробки статистичних даних. Проте існують характеристики складних систем, які не можуть бути отримані приведеними методами. До таких характеристик СЗІ відноситься вірогідність реалізації деяких загроз, окремі характеристики ефективності систем захисту та інші.

Вказані характеристики можуть бути отримані єдино доступними методами – методами неформального оцінювання [4,5]. Суть методів полягає в залученні для отримання деяких характеристик фахівців-експертів у відповідних галузях знань. Найбільшого поширення з неформальних методів оцінювання набули методи експертних оцінок. Методом експертних оцінок є алгоритм підбору фахівців-експертів, завдання правил отримання незалежних оцінок кожним експертом і подальшої статистичної обробки отриманих результатів [6].

Складність функцій, значна частка нечітко визначених певних початкових даних, велика кількість механізмів захисту, складність їх взаємних зв’язків і багато інших чинників роблять практично нерозв’язною проблему оцінки ефективності системи в цілому за допомогою одного якого-небудь методу моделювання.

Для вирішення цієї проблеми застосовується метод декомпозиції (розділення або представлення) загального завдання оцінки ефективності на ряд окремих завдань [7].

Головна складність методу декомпозиції при оцінці систем полягає в обліку взаємозв’язку і взаємного впливу окремих завдань оцінювання і оптимізації. Цей вплив враховується як при рішенні задачі декомпозиції, так і в процесі отримання інтегральних оцінок.

Для того, щоб оцінити ефективність системи захисту інформації або порівняти системи по їх ефективності, необхідно задати деяке правило переваги. Таке правило або співвідношення, засноване на використанні показників ефективності, називають критерієм ефективності. Для отримання критерію ефективності при використанні деякої множини до показників використовують ряд підходів. Вибір кращої із двох систем.Дві системи порівнюються спочатку по найбільш важливому показнику. За оптимальну вважається така система, у якої краще цей показник. При рівності

найважливіших показників порівнюються показники, які займають по рангу другу позицію. При рівності і цих показників порівняння триває до отримання переваги в *i*-му показнику.

Підходи до оцінки ефективності СЗІ. Ефективність СЗІ оцінюється як на етапі розробки, так і в процесі експлуатації ІС підприємства. У оцінці ефективності СЗІ, залежно від показників, що використовуються і способів їх отримання, виділяють наступні підходи:

– класичний; офіційний (експериментальний).

Класичний підхід

Під класичним підходом до оцінки ефективності розуміється використання критеріїв ефективності, отриманих за допомогою показників ефективності. Значення показників ефективності виходять шляхом моделювання або обчислюються по характеристиках реальної ІС. Такий підхід використовується при розробці і модернізації СЗІ. Проте можливості класичних методів комплексного оцінювання ефективності стосовно СЗІ обмежені через низку обставин. Високий ступінь невизначеності початкових даних, складність формалізації процесів функціонування, відсутність загальновизнаних методик розрахунку показників ефективності і вибору критеріїв оптимальності створюють значні труднощі для застосування класичних методів оцінки ефективності.

Офіційний підхід

Велику практичну значущість має підхід до визначення ефективності СЗІ, який умовно можна назвати офіційним. Політика безпеки інформаційних технологій проводиться державою і повинна спиратися на нормативні акти. У цих документах необхідно визначити вимоги до захищеності інформації різних категорій конфіденційності і важливості [6]. Вимоги можуть задаватися переліком механізмів захисту інформації, які необхідно мати в ІС, щоб вона відповідала певному класу захисту. Використовуючи такі документи, можна оцінити ефективність СЗІ. В цьому випадку критерієм ефективності СЗІ є її клас захищеності.

Безперечною перевагою таких підходів є простота використання. Основним недоліком офіційного підходу до визначення ефективності систем захисту є те, що не визначається ефективність конкретного механізму захисту, а констатується лише факт його наявності або відсутності. Цей недолік в якійсь мірі компенсується завданням в спеціальних вимогах до цих механізмів захисту.

Одним із найпоширеніших підходів до оцінки якості захисту інформації є визначений поділ реалізованих функцій і завдань, експлуатаційних характеристик і вимог у відповідність технічним завданням на створення системи захисту. Інший спосіб, який використовується у вітчизняній та закордонній практиці – це аналіз функціональної надійності системи, яка також характеризує якісний рівень системи інформаційної безпеки [8].

Оцінка ефективності СЗІ повинна обов'язково враховувати як об'єктивні обставини, так і ймовірні фактори. Питання оцінки ефективності СЗІ від несанкціонованого доступу (НСД):

1. Оцінка коректності реалізації механізмів захисту СЗІ від НСД. На практиці провести таку оцінку є досить важким завданням. Оскільки можливий варіант, коли встановлена у інформаційній системі СЗІ від НСД не перехоплює і не аналізує лише один подібний спосіб звернення до файлового об'єкту, і, за великим рахунком, вона стає цілком даремною (рано чи пізно, зловмисник виявить даний недолік засобів захисту і скористається ним). Звідси отримуємо вимогу до коректності реалізації СЗІ від НСД – вона повинна контролювати доступ до ресурсу за будь-якого способу звернення до ресурсу (ідентифікація ресурсу).

2. Оцінка достатності (повноти) набору механізмів захисту у складі СЗІ від НСД. Тут ситуація багато в чому схожа із ситуацією, описаною вище. Наприклад, вимога до достатності механізмів у СЗІ від НСД для захисту конфіденційних даних у нормативних документах виглядає наступним чином: «Чи повинен здійснюватися контроль доступу суб'єктів до ресурсів, що захищаються відповідно до матриці доступу». Природно виникає неоднозначність визначення того, що віднести до ресурсів, які захищаються? Крім того, необхідно розуміти, що безліч комп'ютерних ресурсів (особливо, коли мова йде про універсальну ОС) для корпоративних додатків зайві, в першу чергу, це стосується всіляких зовнішніх пристроїв.

Висновки. Для забезпечення встановлених рівнів захищеності ІС ОІД підприємства, засоби захисту повинні мати певну гнучкість. Особливо важливим ця властивість є в тих випадках, коли встановлення засобів захисту здійснюється на працюючу ІС і не порушують її заданого функціонування з врахуванням зміни зовнішніх умов з часом. Механізми захисту повинні бути зрозумілими і простими у практичному використанні.

Анотація. Розглядаються питання оцінювання ефективності системи захисту інформації в автоматизованій системі сучасного підприємства, основні підходи такого оцінювання, їх переваги та недоліки.Різноманяття варіантів побудови ІС породжує необхідність створення різних СЗІ, що враховують індивідуальні особливості ОІД. Великий обсяг наявних публікацій не формує чіткого уявлення про створення СЗІ для конкретної ІС, з урахуванням властивих їй особливостей та умов функціонування. Оцінка ефективності СЗІ повинна обов'язково враховувати як об'єктивні обставини, так і ймовірні фактори. В цьому випадку критерієм ефективності СЗІ може бути її клас захищеності.

Література:

1. Замула О.А.Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки/Системи обробки інформації: збірник наукових праць ХУПС.- Вип.2(92).- Харків: ХУПС,2011.- С.53-56.

2. Марка Д. Методология структурного анализа и проектирования. Пер.с англ. – М.: Мета Технология, 1993.- 240 с.

3. Закон України «Про захист інформації в автоматизованих системах.

4. Толюпа С.В.,Самохвалов Ю.Я., Цьопа Н.В. Комплексні системи захисту інформації спеціальних об'єктів та методика їх оцінки // Науково-технічний журнал «Сучасний захист інформації». – 2014. - № 1.- С.81-88.

5. Хорев А.А. Оценка эффективности защиты информации от утечки по техническим каналам //Специальная техника. – 2006. - № 6. - С. 53 – 61.

6. Бешелев С.Д.Экспертные оценки/С.Д.Бешелев, Ф.Г.Гурвич.- М.:Наука,1973.-210с.

7. Захист інформації.Технічний захист інформації.Порядок проведення робіт: ДСТУ3396.1-96.-Режим доступу:http://www.dstszi.gov.ua.

8. Королев В.И. Морозова Е.В. Методы оценки качества защиты информации при ее автоматизированной обработке // Безопасность информационных технологий. – 1995. - № 2. – 215 с.

9. Саати Т. Принятие решений. Метод анализа иерархий. /Т. Саати.- М.: Радио и связь, 1993. – 278 с.

10. Про захист інформації в інформаційно-телекомунікаційних системах:Закон України//Відом.Верх.Ради України.- 1994.-№31.

УДК 004.04

Брынза Наталья Александровна, *доцент, к.т.н.,*
natalia.brynza@hneu.net

Гаврилова Алла Андреевна, *старший преподаватель*
Харьковский национальный экономический университет имени Семена Кузнеца
alla.gavrylova@hneu.net

ОЦЕНКА ПОКАЗАТЕЛЕЙ ДИНАМИКИ СЕТЕВОЙ АКТИВНОСТИ БЛОКЧЕЙН-КОШЕЛЬКОВ НА РЫНКЕ БИТКОИНА

Начало 2019 г. было ознаменовано резким возрастанием количества активных адресов в сети биткоина (BTC), оставив цену далеко позади. Это противоречит распространенному мнению, что данные показатели находятся в прямой зависимости друг от друга и рост одного обуславливает возрастание другого [1]. Следовательно, необходимо выяснить как влияет количество активных адресов, объем транзакций и их соотношение на цену биткоина.

Поэтому целью данной работы является исследование динамики одной из групп характеристик процессов, происходящих при работе с криптовалютами. Данная группа состоит из показателей сетевой активности при работе с криптовалютой на базе технологии блокчейн. Поскольку активные адреса являются лишь мерой того, сколько учетных записей активно совершают транзакции, то необходимо выяснить какие показатели могут использоваться для получения информации о фактическом объеме средств, которые тратят адреса.

В работе предлагается подход к оценке сетевой активности с учетом всех составляющих группы в отличие от предложенных ранее – представлять сетевую активность, зависящую от ее отдельных показателей [1, 2]. Причем взаимосвязь между показателями одной группы не принимались во внимание. Зависимости строились на соотношении выборочно отдельных показателей из разных групп.

Технология блокчейн при работе с криптовалютой отвечает за постоянный учет всех подтвержденных транзакций. При этом все транзакции представляются в виде линейной цепочки из множес-

тва блоков, которые взаимосвязаны между собой и защищены криптографическими доказательствами. Каждый пользователь может проверить цифровые данные всех транзакций, что делает блокчейн абсолютно прозрачной и доступной технологией. Блокчейн выполняет функции общественного банка, в котором все имеют доступ к документации и принимают участие в обработке каждой денежной операции без каких-либо посредников.

Согласно данным Blockchain.com [3], который является обозревателем биткоин-блоков и сервисов криптовалютных кошельков, наблюдается неуклонный рост количества блокчейн-кошельков [4]. Так, с февраля 2018г. по февраль 2020г. их количество возросло в 1,98 раз, что свидетельствует о росте популярности операций с криптовалютой среди пользователей Интернет с разными балансами блокчейн-кошельков. Это должно отражаться на активности пользователей Интернет [5], но объем пула пользователей не всегда является показателем их активности в нем.

Для определения сетевой активности можно использовать такие характеристики, как [6]: наличие уникальных адресов, количество совершаемых операций, сделок, операций без учета популярных адресов, нерастраченных выходов и операций без учета длинных цепочек, число транзакций, общая стоимость на выходе, расчетное количество операций, предполагаемый объем транзакций. Описание перечисленных показателей и динамика их изменения приведены в табл. 1.

Таблица 1

Обобщенная динамика изменения значений показателей сетевой активности пользователей

№ п/п	Название показателя, единица измерения	Описание	Тенденция с февраля 2019 г. по февраль 2020 г.
1	2	3	4
1	Количество используемых уникальных адресов, шт.	Общее количество уникальных адресов, используемых в цепочке блоков Биткоин	снижение
2	Подтвержденные транзакции за день, биткоины	Число ежедневных подтвержденных сделок биткоин, входящих в основную цепочку транзакций	снижение
3	Общее количество сделок	Подтвержденные и неподтвержденные сделки за день	рост

Окончаниее табл. 1

1	2	3	4
4	Коэффициент транзакций, шт./сек.	Количество подтвержденных и неподтвержденных биткоин-сделок, добавляемых к пулу в секунду	циклично
5	Число транзакций, шт.	Количество транзакций, ожидающих подтверждения – необходимо для предотвращения повторного расходования одних и тех же денежных средств	снижение
6	Размер пула (роста), шт.	Количество транзакций в секунду	циклично
7	Количество блоков в транзакциях, шт.	Совокупный размер транзакций, ожидающих подтверждения	циклично
8	Количество неизрасходованных выходов транзакции, шт.	Количество неизрасходованных биткоинов операций выходов	рост
9	Количество операций без учета популярных адресов, шт.	Общее количество биткоинов-сделок, за исключением 100 наиболее популярных адресов (адреса с суммами в диапазоне от 10 000 до 100 000 BTC) или спящие адреса, ожидающие своего часа	снижение
10	Общая стоимость на выходе, BTC	Общая стоимость всех транзакций, выводимых за день (включает монеты, возвращенные отправителю в качестве изменения) (цена продажи)	стабильно
11	Расчетная стоимость сделки, BTC	Общая оценочная стоимость транзакций в цепочке биткоинов (не включает монеты, возвращенные отправителю в качестве изменения) (цена после торгов)	рост
12	Расчетная стоимость транзакции, доллар США	Расчетная стоимость сделки в долларах США	рост

Оценка динамики изменения значений показателей в течение года формировалась исходя из графиков [4] по четырехбальной шкале: «рост» – отклонения, демонстрирующие постоянное увеличение значений, «снижение» – отклонения, демонстрирующие пос-

тоянное уменьшение значений, «стабильно» – отклонения с очень малой амплитудой, несущественные, которыми можно пренебречь, «циклично» – отклонения, демонстрирующие периоды последовательного увеличения и уменьшения значений. По результатам проведенной оценки можно сделать вывод о том, что показатели ведут себя не одинаково и не представлены одинаковыми единицами измерения. Следовательно, для определения оценки всей группы необходимо провести анализ разнородных показателей.

Задача оценки показателей динамики сетевой активности характеризуется набором разнородных показателей (критериев) $< k_i(x) >$, $i = \overline{1,n}$,

$$x^{\circ} = arg \underset{x \in X}{extr} < k_i(x) > ; \forall i = \overline{1,n},$$

которую можно регуляризировать путем формирования обобщенной скалярной оценки (функции полезности $P(x)$) [7]:

$$P(x) = F[\lambda_i, k_i(x)] ; i = \overline{1,n},$$

где λ_i – коэффициенты изоморфизма, приводящие разнородные частные критерии $k_i(x)$ к изоморфному виду.

Процедура многофакторного оценивания является субъективной интеллектуальной процедурой, поэтому носителями исходной информации, необходимой для структурно-параметрической идентификации ее модели являются специалисты (эксперты) в различных проблемных областях, а основным методом получения первичной информации – метод экспертного оценивания. Субъективизм метода экспертного оценивания и широта круга проблемно-ориентированных задач привели к тому, что в настоящее время на практике используются несколько альтернативных моделей многофакторного оценивания.

В качестве обобщенной оценки можно принять аддитивную модель вида [8, 9]:

$$P(x) = \sum_{i=1}^{n} a_i k_i^{н}(x),$$

где $k_i^{н}(x)$ – нормализованные, т.е. приведенные к безразмерному виду, единому интервалу [0, 1] возможных значений и одинаковому направлению доминирования, частные критерии;

a_i – безразмерные коэффициенты относительной важности нормализованных частных критериев. Их нормализация проводится по формуле:

$$k_i^H(x) = \left(\frac{k_i(x) - k_i^{нх}}{k_i^{нл} - k_i^{нх}} \right)^{\alpha_i},$$

где $k_i(x)$ – значение частного критерия;

$k_i^{НЛ}$, $k_i^{НХ}$ – соответственно наилучшее и наихудшее значение частного критерия, которое он принимает на области допустимых решений $x \in X$;

Значения $k_i^{нх}(x)$ и $k_i^{нл}(x)$ определяются по формулам:

$$k_i^{нх}(x) = \begin{cases} \max\limits_{x \in X} k_i(x), \text{ если } k_i(x) \to min; \\ \min\limits_{x \in X} k_i(x), \text{ если } k_i(x) \to max, \end{cases}$$

$$k_i^{нл}(x) = \begin{cases} \max\limits_{x \in X} k_j(x_i), \text{ если } k_j(x_i) \to max, \\ \min\limits_{x \in X} k_j(x_i), \text{ если } k_j(x_i) \to min. \end{cases},$$

где α_i, β_i – коэффициенты нелинейности, которые позволяют реализовать при $\alpha_i, \beta_i = 1$ – линейные, а при $\alpha_i, \beta_i > 1$ и $\alpha_i, \beta_i < 1$ соответственно вогнутые и выпуклые зависимости.

В общем случае модель с учетом введенных обозначений будет иметь вид [10]:

$$P(x) = \sum_{i=1}^{12} a_i k_i^H(x), \; i = 1,12.$$

В ходе проведенного анализа по показателям динамики сетевой активности блокчейн-кошельков на рынке биткоина рассмотрены тенденции изменения каждого показателя группы, разработана модель оценки, включающая каждый показатели группы сетевой активности, а также сформирована обобщенная скалярная оценка всей группы. Согласно разработанной модели в дальнейшем необходимо проверить ее практическую реализацию путем расчета показателей, входящих в модель, и комплексный показатель сетевой активности.

Аннотация. В данной работе было проведено исследование динамики одной из групп характеристик процессов, происходящих при работе с криптовалютами. Данная группа была представлена показателями сетевой активности при работе с криптовалютой на базе технологии блокчейн. Для оценки сетевой активности были использованы 12 показателей. Определены тенденции динамических изменений каждого показателя за год и представлены в виде качественной оценки по четырехбальной шкале. Для оценки группы сетевой активности предложена аддитивная модель, учитывающая как проведение оценки каждого показателя, так и скалярную оценку всей группы.

Литература:

1. Биткоин: сетевая активность опережает рост цены [Электронный ресурс]. – Режим доступа: https://altstake.io/news/bitkoinsetevaya-aktivnostyopereghaet-rost-ceny.

2. Исследование LongHash: цена криптовалюты и активность в сети не всегда связаны [Электронный ресурс]. – Режим доступа: https://bits.media/issledovanie-longhash-tsena-kriptovalyuty-i-aktivnost-v-seti-ne-vsegda-svyazany.

3. Blockchain (компания) Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Blockchain_(%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F).

4. Blockchain [Электронный ресурс]. – Режим доступа: https://www.blockchain. com/ru/charts/my-wallet-n-users?timespan=2years.

5. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World / Don Tapscott //Alex Tapscott – 2016. – 324 с.

6. The Bitcoin Backbone Protocol: Analysis and Applications /Juan A. Garay – 2017. – 44 с.

7. Фишберн П. Теория полезности для принятия решений / П. Фишберн. – М.: Наука, 1978. – 352 с.

8. Штойер Р. Многокритериальная оптимизация. Теория, расчет и приложения / Р. Штойер. – М.: Радио и связь, 1992. – 504 с.

9. Петров К.Э. Компараторная структурно-параметрическая идентификация моделей скалярного многофакторного оценивания / К.Э. Петров, В.В. Крючковский. – Херсон: Олди-плюс, 2009. – 294 с.

10. Петров Э.Г. Методы и модели принятия решений в условиях многокритериальности и неопределенности / Э.Г. Петров, Н.А. Брынза, Л.В.Колесник, О.А. Писклакова. – Херсон: Гринь Д.С., 2014. – 192 с.

УДК 004.051

Бурячок Володимир Леонідович, професор, д.т.н.
Київський університет імені Бориса Грінченка
v.buriachok@kubg.edu.ua

Соколов Володимир Юрійович, аспірант
Київський університет імені Бориса Грінченка
v.sokolov@kubg.edu.ua

Кіпчук Феодосій Валентинович, магістр
Київський університет імені Бориса Грінченка
aimedforce@gmail.com

ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ БЕЗПРОВОДОВИХ ВБУДОВАНИХ СИСТЕМ

Повертаючись до ключових аспектів комп'ютерних систем, потрібно визначити: як працюють вбудовані системи, які завдання вирішають ваші пристрої, архітектура та принцип роботи, чи є необхідність у додаткових модулях, забезпечення безперебійної роботи, налаштування необхідного рівню захисту та запобігання вразливостям, який потенціал розвитку проекту та його масштабованість.

Мета — вирішити проблему «останньої милі». Враховуючи специфіку мережевих пристроїв на основі безпроводових пристроїв, наголошуємо на важливості забезпечення стабільного з'єднання пристроїв, захисту їх роботи від несанкціонованого доступу та запобігання та мінімізація перешкод для нормального функціонування. Використання міні-комп'ютерів дозволяє заощадити багато ресурсів. Такі системи потребують мінімальної потужності, мережевих ресурсів та мають гнучкі налаштування. Вони також мають дуже широке функціональне розширення, завдяки додатковим модулям. Однак вбудовані системи мають також певні обмеження, такі сильно завантажені системи, як серверні частини та сервіси, будуть працювати в невеликому масштабі. Однак при логічній побудові функціональної мережі з таких пристроїв, як клієнти, агенти чи датчики, міні-комп'ютери можуть бути об'єднані у середні та масштабовані мережі [1].

В даний час велика кількість пристроїв здатні взаємодіяти один з одним, що робить їх багатофункціональними. Такі пристрої здатні працювати незалежно, у групах, виступаючи як елемент певної мережі, також відомий як Інтернет речей (IoT).

Безпроводові пристрої можуть бути вразливими до поганого покриття мережі. Цей недолік дозволяє побудувати як мінімум три вектори атаки: з фальшивою точкою доступу, підміною користувача, підробка кінцевого пристрою або точки доступу, засмічення мережі та ін. Ця робота є гарним прикладом заходів безпеки та запобігання подібним атакам [2].

Ця тема також охоплює інші вразливості безпроводових мереж, які мають той самий намір — відмова в обслуговуванні DoS або DDoS [3]. Ця архітектура наразі не нова. В даний час для запобігання DoS-атак потрібне нове рішення та більш міцна архітектура. Незважаючи на поточні випуски оновлених стандартів безпеки безпроводового зв'язку 802.11, на пристроях все ще існує багато вразливостей, тому наразі необхідно проводити аналізи та експерименти з багатьма відомими типами DoS-атак. Для цього створений алгоритм під назвою Альтернативний механізм нумерації (ANM), який запобігає атакам DoS.

Для більш точно налаштованих мереж також потрібно контролювати маршрутизацію потоку даних та керувати на мережевому рівні VLAN [4]. Рішення позиціонується як нова стратегія заходів безпеки. Це забезпечується іншим алгоритмом шифрування для непоширюваного ключа та віртуальної локальної мережі.

Одним із гарних прикладів є використання платформи як точки доступу до мережі з використанням міні-екрану, який може відображати необхідні функції моніторингу [5]. Точка доступу на базі ОС Raspbian вимагає мало ресурсів, представлена у роботі. Використання екранного модуля та програмування дозволяє відображати практично будь-яку інформацію, наприклад: підключені пристрої, стан підключення до шлюзу, спливаючі адреси пристроїв, IP-адреси пристроїв тощо [6].

У функції зовнішньої мережевої карти працювала TP-Link TL-WN722N зі специфікацією мікросхеми AR9271 та зовнішньою антеною [7]. На практиці ця мережева карта була достатньо обмежена для досягнення цілей експерименту. Як результат,

платформа не змогла працювати одночасно з більш ніж 8 пристроями, 1 сервером та 7 клієнтами. Але вбудований контролер CYW43455 підтримує вдвічі більше: 14 клієнтів та 1 сервер.

Алгоритм роботи програмного забезпечення в Business Process Model and Notation (весія 2). Було використане наступне ПЗ у експерименті:

– RPi 3B+ (2.4/5 GHz) з Raspbian Lite OS або OpenWRT;
– MicroSD 16 Gb UHS-I як сховище даних;
– TP-Link TL-WN722N версії 1;
– акумулятора батарея.

Для реалізації точки доступу були визначені наступні програмні засоби:

– hostapd є сервісом для Wi-Fi точки доступу;
– dnsmasq як DHCP-server та DNS;
– ath9k-htc драйвер для TL-WR722N;
– vsftpd як FTP-server.

На початку експерименту OpenWRT було випущено версію 18.0, але вона не спрацювала правильно: при налаштуванні точки доступу конфігурація шлюзу не зберігалася, тому була взята остання стабільна версія 17.0. Але через місяць були виправлені помилки і версія 18.01 була успішно встановлена та працювала правильно (рис. 1).

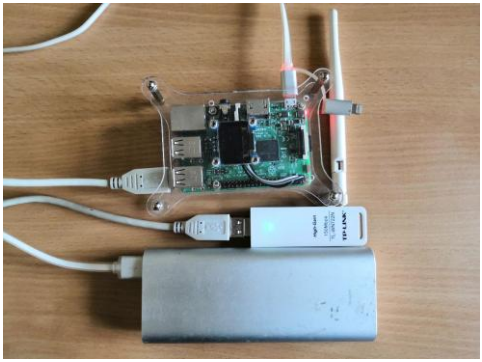


Рис. 1. Експериментальне обладнання

Для імітації стабільного навантаження, близького до умов праці в офісі компанії, було обрано метод генерації трафіку типу з'єднання клієнт-сервер за допомогою FTP: клієнти завантажу-

ють одночасно один великий файл (адже використання файлів різного розміру могло призвести до збоїв у швидкості передачі та помилок).

При виборі FTP-сервера було перевірено кілька програм, і перевага надана vsftpd, який легко налаштувати і який не має обов'язкової бази даних клієнтів та додаткових налаштувань. Крім того, vsftpd використовує мінімальну кількість операційних ресурсів і є досить безпечним, ефективним та не потребує додаткових сервісів на відміну від ProFTPD.

Для повного відстеження завантаження для всіх клієнтів, вибрано файл розміром 30 Мб. Також теоретично цей розмір дозволяє використовувати канал одночасно всіма користувачами, принаймні 90 секунд із 7 підключеними пристроями.

Тестовим середовищем було закрите приміщення, в якому було розміщено 15 персональних комп'ютерів (ПК). Посеред кімнати була розташована точка доступу та один із ПК, який служив сервером. Максимальна відстань від точки доступу до віддаленого ПК досягла 6 м, що є приблизним значенням для роботи в офісних приміщеннях.

На час тестування всі сторонні програми були відключені на усіх станціях, а активність мережі була зведена до мінімуму.

Усіма робочими станціями були Dell OptiPlex 3050 Micro з OS Windows 10 Education, мережевими картами Intel® Dual Band Wireless AC 3165 (802.11ac) 1×1 з зовнішніми антенами, направленими однаково вниз.

Побудувавши поліноміальну лінію тренда (див. рис. 2), легко побачити, що відносне зниження швидкості передачі для обох діапазонів майже однакове і відрізняється приблизно втричі (абсолютний спад швидкості для смуги частот 2,4 ГГц становив 0,04 Мб/с, а для 5 ГГц — 0,18 Мб/с).

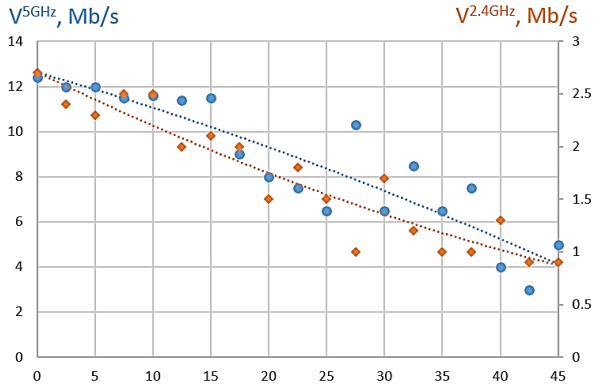


Рис. 2. Передача даних на різних діапазонах

Графік порівняння роботи контролера на різних частотах проводився у закритому приміщенні загальною довжиною до 50 м, непряма видимість без перешкод. У частково зарядженому діапазоні 2,4 ГГц та вільному діапазоні 5 ГГц. Канал 11 обраний для 2,4 ГГц і 5 ГГц для каналу 36 (рис. 3).

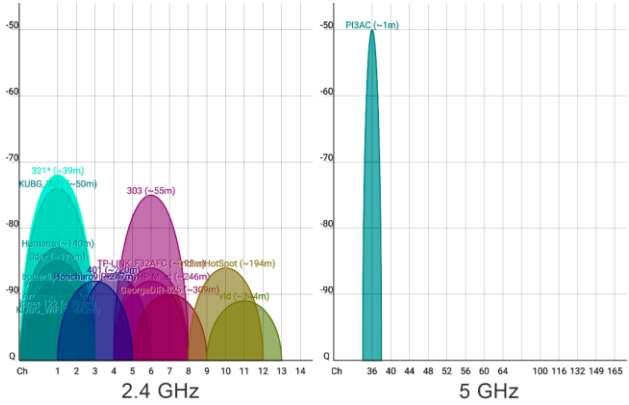


Рис. 3. Сканування частотного діапазону

При вимірюванні та перерахуванні результатів експерименту необхідно обґрунтувати його наукове значення. Для цього отримані результати були оброблені та виведені за допомогою прямої оцінки похибки вимірювання, швидкості завантаження та коефіцієнта Пірсона. Отримано максимальне значення швид-

кості на платформі WRT з максимальною швидкістю 600 кб/с і найнижчою на зовнішній платформі RPi 200 кб/с. Інші вимірювання були неуспішними через нестабільну передачу даних. Також були помилки у вигляді не запущеного завантаження після запуску команди, завантаження закінчувалось не більше ніж на декількох клієнтах і робило неможливим загальний результатів усіх станцій. Ліміт максимальної кількість клієнтів відбувався на адаптері TP-Link. Він був визначений на OpenWRT з внутрішнім адаптером для 7 та 14 клієнтів.

Ця робота окреслює та обґрунтовує поточні проблеми підключення кінцевих пристроїв у безпроводових мережах. Наявні можливості вбудованих систем можуть підтримувати з'єднання від декількох до кількох десятків пристроїв але необхідно ретельно вибирати безпроводові адаптери, які запропоновані виробниками на вбудованих платформах або розробляти рішення з використанням додаткових адаптерів, антен, підтримуваних технологій шифрування та протоколів передачі даних. У цій роботі вбудований мережевий контролер показав себе набагато краще, ніж зовнішній. Відповідно до експерименту, можемо зазначити:

– статистика вказує на можливі помилки в роботі сервісів. Навіть якщо була врахована досить універсальна мова програмування Python, яка імітувала навантаження та нормальне FTP-з'єднання клієнт-сервер;

– обмежена сумісність мережевих контролерів (мікросхем) та роботи мережевих служб ОС, хоча вона досить широка, проте вона не може гарантувати її повну продуктивність. Тож коли потрібно вибрати конкретне обладнання, архітектуру системи та сервіси — потрібно виконати тестування та налаштування прототипу для завершення. Крім того, кожен сервіс та проміжний вузол в системі повинні забезпечуватися достатньою безпекою на всіх рівнях передачі даних через модель OSI.

У наступній роботі планується перевірити службу обміну даними, базу даних або веб-сервер із певним рівнем захисту. А також проведення тесту на проникнення, перевірку стабільності описаних вище заходів безпеки та загальну оцінку вразливості розумних систем.

Анотація. У тезах представлені результати тестування навантаження вбудованих апаратних платформ для рішень Internet of Things. Проаналізовано можливості обладнання. Операційні системи різних виробників були об'єднані в єдину класифікацію і для двох найпопулярніших операційних систем проведено тестування навантаження, яке проводилось на зовнішньому та внутрішньому адаптерах безпроводової мережі. Було розроблено власне програмне рішення на основі мови програмування Python. Кількість пристроїв безпроводового зв'язку становила від 7 до 14. Експериментальні результати будуть корисні при розгортанні безпроводової інфраструктури для невеликих комерційних та наукових безпроводових мереж.

Література:

1. Sokolov V. Yu. Scheme for Dynamic Channel Allocation with Interference Reduction in Wireless Sensor Network / V. Yu. Sokolov, A. Carlsson, I. Kuzminykh // Proceedings of the IV International Scientific and Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T'2017), October 10–13, 2017: abstracts. — Kharkiv : IEEE, 2017. — P. 564–568. — DOI: 10.1109/INFOCOMMST.2017.8246463.

2. Sobh T. S. Wi-Fi Networks Security and Accessing Control / T. S. Sobh // International Journal of Computer Network and Information Security. — 2013. — Vol. 5, no. 7. — P. 9–20, — DOI: 10.5815/ijcnis.2013.07.02.

3. Liu H. A New Secure Strategy for Small-Scale IEEE 802.11 Wireless Local Area Network / H. Liu, H. Zhang, W. Xu, Y. Yang // International Journal of Wireless and Microwave Technologies. — Vol. 2, no. 4. — P. 21–27. — DOI: 10.5815/ijwmt.2012.04.04.

4. Durairaj M. ANM to Perceive and Thwart Denial of Service Attack in WLAN / M. Durairaj, A. Persia // International Journal of Computer Network and Information Security. — Vol. 7, no. 6. — P. 59–66. — DOI: 10.5815/ijcnis.2015.06.07.

5. Buryachok V. L. Using 2.4 GHz Wireless Botnets to Implement Denial-of-Service Attacks / V. L. Buryachok, V. Yu. Sokolov // Web of Scholar. — 2018. — No. 6(24), vol. 1. — P. 14–21. — DOI: 10.31435/rsglobal_wos/12062018/5734.

6. IoT Collection [Електронний ресурс]. — Режим доступу : https://github.com/oestoidea/iot.

7. Raspberry Pi Documentation. Release 0.0 [Електронний ресурс]. — Режим доступу: https://media.readthedocs.org/pdf/raspberry-piintro/latest/raspberry-pi-intro.pdf.

УДК 35.078.3:342.738(091)(02)

Ворожко Валерій Павлович
Національний авіаційний університет,
Галузевий державний архів СБ України, кандидат історичних наук
wp06vv@gmail.com

ПЕРШІ КРОКИ ЗІ СТВОРЕННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ. СЕРПЕНЬ 1991–ТРАВЕНЬ 1993 РР.

Нині Україна протистоїть потужним зусиллям своїх зовнішніх і внутрішніх ворогів, мета яких – ліквідація української незалежної державності, знищення української нації та України як суб'єкта міжнародного права і геополітичної реальності. Сучасні суспільно-політичні виклики зумовлюють необхідність об'єктивного аналізу всіх складових функціонування «державного організму» України та його трансформації в сучасну демократичну країну.

Історіографія досліджень побудови Україною національної системи охорони державної таємниці нараховує низку публікацій. Окремі питання вже висвітлювалися у працях автора цієї публікації, як одноосібних [1, 2], так і в співавторстві [3, 4]. Автором використані документи Центрального державного архіву вищих органів влади і управління України (ЦДАВО України) та Галузевого державного архіву СБ України (ГДА СБУ).

24 серпня 1991 р. Верховна Рада (далі – ВР) УРСР проголосила незалежність України та прийняла основоположні рішення, спрямовані на створення самостійної держави. Проголошення курсу на розбудову незалежної демократичної держави зумовило потребу створення національної системи охорони державної таємниці, яку передбачалося створити з урахуванням змін в економіці, політичній та соціальній сферах, розвитку міжнародного співробітництва та світової практики створення подібних систем. Важливим завданням на той період було подолання негативних наслідків минулого політичного режиму, а саме тотальної засекреченості в усіх сферах життя і діяльності держави та суспільства.

На початковому етапі для охорони державної таємниці застосовувалася система радянського періоду. Серед перших правових актів, прийнятих в державі, була постанова ВР України від 12 ве-

ресня 1991 р «Про порядок тимчасової дії на території України окремих актів законодавства Союзу РСР», яка визначала, що до прийняття відповідних актів законодавства України на території республіки застосовуються акти законодавства СРСР з питань, які не врегульовані законодавством України, за умови, що вони не суперечать Конституції і законам України [5]. У сфері охорони державної таємниці головним нормативним документом залишалася «Інструкція із забезпечення режиму секретності в міністерствах, відомствах, на підприємствах, установах і організаціях СРСР» № 556-126 від 12 травня 1987 р. [6, арк. 283-456].

Поряд з іншими завданнями, що постали перед Україною, не останнє місце займало створення власних органів державної безпеки (контррозвідки), побудова яких проходила з урахуванням досвіду організаційно-правового забезпечення, наявного кадрового потенціалу, матеріально-технічної бази КДБ УРСР. 20 вересня 1991 р. парламент України ухвалив постанову «Про створення Служби національної безпеки України» (далі – СНБУ) [5].

На підставі цього акту до обрання Президента України новостворена служба мала підпорядковуватися Голові ВР України. З 2 січня 1992 р. наказом Голови СНБУ № 01 всі відділи військової контррозвідки по військових, прикордонних округах, внутрішніх військах, флоту, окремих арміях, корпусах, дивізіях та їм рівних, дислокованих на території України, були підпорядковані Управлінню військової контррозвідки СНБУ.

18 лютого 1992 р. Постановою Верховної Ради України було введено в дію Закон України «Про оперативно-розшукову діяльність», який визначив, зокрема, таку підставу для проведення оперативно-розшукової діяльності, як запити повноважних державних органів, установ та організацій про перевірку осіб у зв'язку з їх допуском до державної таємниці [5].

Реорганізаційні процеси, пов'язані з колишнім КДБ, було завершено у першому кварталі 1992 р. Постановою Верховної Ради України від 25 березня вводився в дію Закон України «Про Службу безпеки України», яким було встановлено, що на новостворений орган державної безпеки покладаються, серед інших, завдання оперативного забезпечення, участі у розробці і здійсненні заходів щодо захисту державної таємниці України та досудове слідство про злочини у цій сфері діяльності [5].

Після ліквідації СРСР у нашій державі відбувався розпад організаційної і нормативно-правової основи захисту державних секретів колишнього СРСР, яка поступово вступала в суперечність із законодавством України. В цей час за поданням СБ України, Кабінет Міністрів України (далі – КМУ) прийняв 13 квітня 1992 р. протокольне рішення «Про захист таємної та службової інформації», спрямоване на підвищення відповідальності керівників усіх рівнів за забезпечення режиму секретності, розробку та здійснення ефективних заходів для збереження державної таємниці, виключення несанкціонованих випадків передачі за межі України таємних носіїв інформації [2, с. 30]. Прийняте рішення було важливим кроком у сфері охорони таємної інформації, однак воно кардинально не вирішувало існуючих проблем.

В умовах кризових явищ в економіці, а також відсутності єдиної організаційно-правової системи охорони державної таємниці виникли передумови для витоку таємної інформації. 23–25 тис. режимно-секретних органів (далі − РСО), переважна більшість яких раніше була підпорядкована союзним відомствам, стали певною мірою некерованими, їх штатна чисельність скорочувалася, деякі взагалі було ліквідовано. В країні залишилося від радянських замовлень понад 133 млн. секретних документів, декілька сотень тисяч секретних виробів, понад дві тисячі виконуваних і незавершених науково-дослідних та дослідно-конструкторських робіт [7, арк. 29-52].

Основними продуцентами державних секретів у радянські часи були військові формування та оборонно-промисловий комплекс (далі – ОПК). Особливих проблем з переходом військових таємниць під український прапор не було. Так, 23 грудня 1991 р. наказом Міноборони України № 03 було створено управління шифрованого зв'язку і режиму секретності Збройних сил України. Станом на 1 січня 1992 р. у військах (силах), які дислокувалися (базувалися) в Україні і ввійшли під українську юрисдикцію було 7483 секретних частини і мобілізаційних діловодств. В цілому персонал шифрувальних органів і РСО Міноборони України складав понад 18 тис. осіб. 5 січня 1992 р. міністр оборони України затвердив Положення «Про Управління шифрованого зв'язку і режиму секретності (Восьме управління) Міністерства оборони України» та визначив його статус як центрального шифрувального і центрального РСО Збройних сил України [8, с. 465].

Набагато складніша була ситуація з таємницями ОПК, що залишився в спадщину від колишнього СРСР. Всі підприємства, установи і організації ОПК, які знаходилися на території УРСР, у радянські часи були підпорядковані дев'ятьом міністерствам оборонних галузей промисловості. Крім так званої «дев'ятки», оборонні замовлення розміщувалися на підприємствах та в наукових установах інших відомств. Точна їх чисельність, кількість працюючих та секретних носіїв (паперових носіїв та виробів) була невідома.

На той час наводилися різні дані про наявність в Україні підприємств ОПК чисельністю від 700 до 3594. Найбільш авторитетним джерелом можна вважати Наукову доповідь Національного інституту стратегічних досліджень «Національна безпека України, 1994–1996 рр.», в якій зазначено, що «у 1991 р. близько 700 підприємств [України] виробляли продукцію військового призначення» [9, с. 81-82]. На думку автора і ця цифра завищена. Швидше всього до цих підприємств були зараховані і підприємства, які мали лише мобілізаційне замовлення на вироби подвійного призначення і мали РСО у складі 1-ї штатної особи або сумісника.

29 жовтня 1991 р. Постановою КМУ № 297 був створений Державний комітет України по оборонній промисловості і машинобудуванню. Серед його «питань» забезпечення охорони державної таємниці не згадувалося. 29 квітня 1992 р. Постановою КМУ № 297 комітет ліквідували і на його базі було створено Міністерство машинобудування, ВПК і конверсії до якого увійшли установи і підприємства колишніх 16 союзних міністерств, у т.ч. 9-ті міністерств оборонних галузей промисловості [10, арк. 89]. Про забезпечення охорони державної таємниці також не згадувалося. Разом з тим у постанові був зазначений «спеціальний режим» на підприємствах.

З розпадом СРСР значна частина державних секретів СРСР перетворилася у міждержавні. Враховуючи цей аспект, а також величезний обсяг матеріальних носіїв міждержавних секретів та продовження співробітництва, 22 січня 1993 р. у м. Мінськ між урядами країн Співдружності незалежних держав було підписано «Угоду про взаємне забезпечення збереження міждержавних секретів». До зазначеної Угоди додавалися «Загальні принципи забезпечення режиму секретності при здійсненні політичного,

економічного, науково-технічного і військового співробітництва між державами – учасниками Угоди про взаємне забезпечення збереження міждержавних секретів» [4, с. 135].

Щодо цензури, то в той час ще зберігалися радянські стереотипи. На початку 1992 р. постановою КМУ від 3 січня № 6 було створено Головне управління по охороні державних таємниць у пресі та інших засобах масової інформації при КМУ (ГУОТ України) як правонаступник Укрголовліту – цензорського органу УРСР [4, с. 137].

Першим законодавчим актом, що стверджував інформаційний суверенітет України, став Закон України «Про інформацію», прийнятий Верховною Радою України 2 жовтня 1992 р. [5] Цей Закон визначив режим доступу до інформації, поділивши її на відкриту інформацію та інформацію з обмеженим доступом, закріпив за державою право і обов'язок здійснювати контроль за режимом доступу до інформації. Закон став базовим в інформаційній сфері.

10 листопаду 1992 р. постановою КМУ на базі ГУОТ був створений Державний комітет України з питань охорони державних таємниць у пресі та інших ЗМІ (Держкомтаємниць України) [4, с. 139].

1 грудня 1992 р. Указом Президента України. № 593/92 була створена Державна служба України з питань технічного захисту інформації (ДСТЗІ), на яке покладалися функції щодо реалізації державної політики, організаційного, нормативного, інженерно-технічного забезпечення технічного захисту інформації [4, с. 140] На той час вся діяльність у цій сфері здійснювалася на підставі нормативних документів, затверджених Держтехкомісією СРСР.

Однією з проблем на підготовчому етапі формування власного інституту державної таємниці України було визначення державного органу як спеціально уповноваженого органу державної влади з головним завданням реалізації державної політики у цій сфері діяльності.

В той період існувала думка, що формування системи охорони державної таємниці, аналогічної радянському режиму, могло б створити передумови для зловживань щодо застосування таємної інформації, порушень прав і свобод людини. Демократизація правовідносин у сфері, пов'язаній з державною таємницею,

повинна була передбачати розширення прав і, водночас, підвищення відповідальності керівників усіх рівнів за режим секретності та персоніфікацію питань щодо віднесення відомостей до державної таємниці та їхнє засекречування. Тому було прийнято рішення про створення окремого спеціального уповноваженого органу державної влади з питань охорони державної таємниці.

Верховна Рада України вже на етапі прийняття законів, які регламентували діяльність СБ України, залишила за цим державним органом лише функції спеціальної компетенції як правоохоронного органу. Організаційно-правові функції СБ України щодо охорони державної таємниці були вилучені зі сфери її компетенції.

Визначений ВР України політичний курс щодо формування системи охорони державної таємниці був реалізований відповідними рішеннями уряду держави. Постановою КМУ від 4 травня 1993 р. № 327 було створено Державній комітет України з питань державних секретів (Держкомсекретів України) [4, с. 142].

У 1991–1992 рр. в Україні система охорони державної таємниці формувалася з урахуванням досвіду розвинених країн світу та традиційних засобів і методів, що виправдали себе у вітчизняній практиці, збільшилася відкритість держави перед суспільством, скоротилася чисельність відомостей, що належать до державної таємниці, відкритими стали загальні переліки такої інформації, механізми засекречування та умови розсекречування.

З різних обставин суттєво зменшилась кількість продуцентів секретної інформації та відповідно РСО. Наприкінці першого півріччя 1993 р. було завершено створення державних органів, що забезпечували реалізацію державної політики у сфері охорони державної таємниці. Рішення яких, видані в межах їх повноважень, були обов'язковими для виконання всіма суб'єктами, діяльність яких пов'язана з інформацією, що підлягає охороні з боку держави.

Вказаним державним органам були надані функції у тому обсязі, що дозволяли забезпечити практичну реалізацію державної політики щодо охорони державної таємниці, іншої інформації з обмеженим доступом. Вжиті заходи в складних умовах початкового етапу державного будівництва дозволили створити логічну завершену організаційну структуру державних органів, діяльність яких була спрямована на формування і вдосконалення інституту охорони державної таємниці України.

Анотація. У статті на підставі нормативно-правових актів України, праць українських дослідників та архівних документів розглядаються історичні аспекти створення національної системи охорони державної таємниці в Україні в 1991-1993 рр. Привернута окрема увага до нормативних актів України щодо захисту державної таємниці, а також до процесу формування держаних органів відповідальних за інформаційну безпеку. Метою публікації є вивчення історичних аспектів формування системи охорони державної таємниці в Україні та її захисту від ворожих посягань, що набуває особливого значення під час протистояння російській агресії й необхідності підвищення рівня національної безпеки.

Література:

1. Ворожко В. З історії створення національної системи охорони державної таємниці // Інформаційно-документальні комунікації в глобалізованому суспільстві: Матеріали Міжнар. наук.-прак. конф. 21-22 березня 2013. – К.: НАУ, 2013. – С. 95−96.

2. Ворожко В. Правові основи захисту інформації в Україні // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Зб. доп. – К., 1998. – С. 30−33.

3. Охорона державних секретів незалежної України. Монографія / Мастяниця Й., Шиманський Л., Олійник О., Ворожко В. − К.: Ін-т законодавства ВР України, 2010. – 128 с.

4. Ворожко В. Нарис історії охорони державної таємниці в Україні. Монографія / В. Ворожко, Б. Бернадський, О. Ботвінкін. – К.: Лазурит-Поліграф, 2012. – 188 с.

5. Законодавство України: Офіційний веб-сайт Верховної Ради України. [Електронний ресурс]. – Режим доступу: http://zacon.rada.gov.ua/ cgi-bin/laws. – Назва з екрану.

6. ГДА СБ України, ф.9, спр. 122-сп.

7. ЦДАВО, ф. 5282, оп.1, спр. 7.

8. Лопата А. Записки начальника Генерального штабу Збройних сил України. – К.: Видавничий Дім «Воєнна розвідка», 2015. – 632 с.

9. Національна безпека України, 1994–1996 рр.: наук. доп. НІСД – К.: НІСД, 1997.− 197 с.

10. ЦДАВО, ф. 5282, оп.1, спр. 1.

УДК 004.056.5

***Кобозєва Алла Анатоліївна**, д.т.н., проф.*
Одеський національний політехнічний університет
Alla_kobozeva@ukr.net
***Бобок Іван Ігорович**, к.т.н.*
Одеський національний політехнічний університет
werter666@ukr.net

СТЕГАНОГРАФІЧНИЙ МЕТОД, СТІЙКИЙ ДО АТАК ПРОТИ ВБУДОВАНОГО ПОВІДОМЛЕННЯ

На сьогоднішній день одною з важливих складових комплексного захисту інформації є стеганографічний захист [1-3]. Особливості сучасної комунікації, стрімке зростання обсягів інформації, що передається по каналах зв'язку, приводять до необхідності використання при організації прихованого каналу зв'язку стеганографічних алгоритмів, стійких до атак проти вбудованого повідомлення [3], зокрема до стиску з втратами. Розробці таких стеганоалгоритмів присвячено багато зусиль сучасних фахівців в галузі інформаційної безпеки [4-5], але, враховуючи можливу критичну важливість обсягу правильно відновленої інформації при організації прихованого каналу зв'язку в різних умовах його використання, зокрема, в умовах значних збурних дій (ЗД), питання підвищення ефективності таких алгоритмів (у сенсі обсягу відновленої інформації, забезпечення надійності сприйняття стеганоповідомлення, рівня пропускної спроможності прихованого каналу зв'язку тощо) залишається *актуальним*.

Метою роботи є розробка нового стеганографічного методу, стійкого до атак проти вбудованого повідомлення, в тому числі значних, з одночасним збереженням надійності сприйняття формованого стеганоповідомлення, де в якості контейнера використовується цифрове зображення (ЦЗ).

Як формальне представлення ЦЗ розглядається двовимірна матриця F, яка піддається стандартній розбивці на непересічні $n \times n$-блоки, довільний з яких далі позначається B. Стан (зміна стану) будь-якої інформаційної системи згідно з загальним підходом до аналізу стану й технології функціонування інформаційних систем формально може бути представлений у вигляді

сукупності збурень сингулярних чисел (СНЧ) і лексикографічно додатних ортонормованих сингулярних векторів (СНВ) відповідної матриці (блоків матриці) [6], які визначаються однозначно (шляхом побудови нормального сингулярного розкладання матриці B: $B = U\Sigma V^T$, де U, V – ортогональні $n \times n$-матриці лівих лексикографічно додатних і правих СНВ B відповідно, які представлені стовпцями u_i матриці U і v_i матриці V, $i = 1 \ldots n$, $\Sigma = diag(\sigma_1, ..., \sigma_n)$ - діагональна матриця СНЧ, $\sigma_1 \geq \ldots \sigma_n \geq 0$). СНЧ матриці (блоку матриці) ЦЗ є нечутливими до збурних дій, чого не можна в загальному випадку сказати про СНВ, тому саме СНЧ розглядаються далі як формальні параметри ЦЗ-контейнера, які доцільно використовувати для організації процесу стеганоперетворення шляхом їх збурень [7].

Відповідні СНЧ різних блоків навіть одного ЦЗ можуть значно відрізнятися одне від одного. Це ускладнює процес організації і аналізу їх збурень в процесі стеганоперетворення чи іншої збурної дії на стеганоповідомлення. Для полегшення цих процесів має сенс розглядати не самі СНЧ (в вигляді вектору $\sigma = (\sigma_1, \sigma_2, ..., \sigma_n)^T$), а нормовані СНЧ, отримані шляхом нормування σ, результатом чого є вектор $\overline{\sigma} = \dfrac{\sigma}{\|\sigma\|}$, $\overline{\sigma} = \left(\overline{\sigma}_1, \overline{\sigma}_2, ..., \overline{\sigma}_n\right)^T$, де $\|\sigma\|$ - норма вектора σ.

Основні кроки метода, що пропонується, наступні.

Вбудова ДІ

Крок 1. Матриця F ЦЗ-контейнера розбивається стандартним чином на $2l \times 2l$-блоки малого розміру ($n = 2l$).

Крок 2. Черговий $2l \times 2l$-блок B контейнера, що використовується для вбудови 1 біта p_m ДІ і визначається згідно з секретним ключем, розбивається на чотири $l \times l$-блоки $B^{(i)}$, $i = \overline{1,4}$, що не перетинаються.

Крок 3. Для кожного з 4-х отриманих $l \times l$-блоків $B^{(i)}$, $i = \overline{1,4}$, знайти СНЧ $\sigma_1^{(i)}$ і $\sigma_2^{(i)}$ і відстані між їх k-ими ступенями: $d_k^{(i)} = \left(\sigma_1^{(i)}\right)^k - \left(\sigma_2^{(i)}\right)^k$. Обчислити $d_{\max} = \max\limits_{1 \leq i \leq 4} d_k^{(i)}$.

Крок 4. Згідно з секретним ключем залежно від значення p_m визначається конкретний блок $B^{(j)}$ в межах *B*, в який буде відбуватися безпосередньо вбудова p_m. В цьому блоці в результаті вбудови ДІ потрібно забезпечити

$$\left(\sigma_1^{(j)}\right)^k \geq \left(\sigma_2^{(j)}\right)^k + d_{\max} + \Delta,$$

де $\Delta > 0$. Це робиться шляхом збільшення СНЧ $\sigma_1^{(j)}$, результатом чого є

$$\sigma_{1,new}^{(j)} : \sigma_{1,new}^{(j)} \geq \sqrt[k]{\left(\sigma_2^{(j)}\right)^k + d_{\max} + \Delta}.$$

Крок 5. Відновити $B_{new}^{(j)}$ з урахуванням нового значення першого СНЧ і незмінених інших СНЧ і СНВ.

Крок 6. Побудувати $2l \times 2l$-блок стеганоповідомлення, що відповідає блоку *B* контейнера, враховуючи незмінність всіх $B^{(i)}$, $i = \overline{1,4}, i \neq j$, і $B_{new}^{(j)}$.

Крок 7. Перехід на крок 2 до наступного блоку контейнера, задіяного в стеганоперетворенні, при наявності такого.

Крок 8. Закінчення формування стеганоповідомлення; результат – ЦЗ з матрицею $\overline{F}$.

Декодування ДІ

Крок 1. Матриця $\overline{F}$ ЦЗ-стеганоповідомлення розбивається стандартним чином на $2l \times 2l$-блоки.

Крок 2. Черговий $2l \times 2l$-блок $\overline{B}$ стеганоповідомлення, в якому міститься ДІ, що визначається згідно з секретним ключем, розбивається на чотири $l \times l$-блоки $\overline{B}^{(i)}$, $i = \overline{1,4}$, що не перетинаються.

Крок 3. Для кожного з 4-х отриманих $l \times l$-блоків $\overline{B}^{(i)}$, $i = \overline{1,4}$, знайти:

1.1. СНЧ: $\sigma_{1_S}^{(i)}$, $\sigma_{2_S}^{(i)}$,…, $\sigma_{l_S}^{(i)}$, $i = \overline{1,4}$;

1.2. Кути $\sigma_S^{(i)}$ між векторами $\left(\left(\sigma_{1_S}^{(i)}\right)^k, \left(\sigma_{2_S}^{(i)}\right)^k, ..., \left(\sigma_{l_S}^{(i)}\right)^k\right)^T$ і e_1, $i = \overline{1,4}$.

Крок 4. Визначити:

$$\sigma_S^{(j)} = \min_{1 \le i \le 4} \sigma_S^{(i)}$$

Декодування чергового біту $\overline{p}_m$ ДІ відбувається з $\overline{B}^{(j)}$. Значення $\overline{p}_m$ залежить від того, з якого саме $l \times l$-блоку $\overline{B}^{(j)}$ відбувається декодування (з врахуванням секретного ключа).

Крок 5. Перехід на крок 2 до наступного блоку стеганоповідомлення, задіяного в стеганоперетворенні, при наявності такого.

Крок 6. Закінчення декодування ДІ.

Пропускна спроможність прихованого каналу зв'язку, що будується за допомогою розробленого методу, буде дорівнювати n^2 біт/піксель при будь-якій алгоритмічній реалізації за умови використання всіх блоків матриці ЦЗ-контейнера, отриманих в результаті стандартної розбивки.

При вбудові ДІ на кроці 4 секретний ключ може визначати номер j блоку $B^{(j)}$ залежно від значення p_m, враховуючи, наприклад, його парність/непарність, тобто, якщо $p_m = 0$, то $j = 2 \vee j = 4$, інакше $j = 1 \vee j = 3$. В такому випадку парність/непарність j для $\overline{B}^{(j)}$ на кроці 4 декодування визначить $\overline{p}_m$.

Таким чином, в роботі на основі теорії збурень та матричного аналізу розроблено новий блоковий стеганографічний метод, стійкий до атак проти вбудованого повідомлення, в тому числі значних, з одночасним збереженням надійності сприйняття формованого стеганоповідомлення, що забезпечується використаним математичним базисом.

Вбудова ДІ робиться шляхом використання нечутливих до збурних дій формальних параметрів матриці ЦЗ-контейнера – СНЧ її блоків малого розміру, отриманих шляхом її стандартної розбивки. Збільшення стійкості методу до збурних дій та забезпечення надійності сприйняття формованного стеганоповідом-

лення досягається шляхом збільшення максимального СНЧ блоку, задіяного в стеганоперетворенні, при цьому збурення СНЧ визначається за допомогою піднесення СНЧ блоків у натуральний ступінь *k*.

Анотація**. **В роботі на основі загального підходу до аналізу стану й технології функціонування інформаційних систем, який базується на теорії збурень та матричного аналізу, розроблено новий блоковий поліноміальний ступеня 2 стеганографічний метод, стійкий до атак проти вбудованого повідомлення, в тому числі значних, з одночасним збереженням надійності сприйняття формованого стеганоповідомлення, що забезпечується використаним математичним базисом. В якості контейнера розглядається цифрове зображення. Пропускна спроможність прихованого каналу зв'язку, що будується за допомогою розробленого методу, дорівнює* n^{-2} ***біт/піксель при будь-якій алгоритмічній реалізації за умови використання всіх $n \times n$***-блоків матриці контейнера, отриманих в результаті стандартної розбивки його матриці, при стеганоперетворенні.***

Література:

1. M.E. Saleh, A.A. Aly, F.A. Omara, "Data security using cryptography and steganography techniques," International Journal of Advanced Computer Science and Applications, Vol. 7, Issue 6, pp. 390-397, 2016.

2. S. Malalla, F.R. Shareef, "Novel approach for Arabic text steganography based on the "BloodGroup" text hiding method," Engineering, Technology & Applied Science Research, Vol. 7, Issue 2, pp. 1482-1485, 2017.

3. В.Г. Грибунин, И.Н. Оков, И.В. Туринцев, Цифровая стеганография, М.: СОЛОН-Пресс, 2009. 272 с.

4. Z. Bao, X. Luo, Y. Zhang, C. Yang, F. Liu, "A robust image steganography on resisting JPEG compression with no side information," IETE Technical Review, Vol. 35, Issue 1, pp. 4-13, 2018.

5. J. Tao, S. Li, X. Zhang, Z. Wang, "Towards robust image steganography," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 29, Issue 2, pp. 594-600, 2019.

6. А.А. Кобозева, В.А. Хорошко, Анализ информационной безопасности, К.: ГУИКТ, 2009. 251 с.

7. И.И. Бобок, «Теоретическое развитие общего подхода к проблеме выявления нарушений целостности цифровых контентов, основанного на анализе полного набора формальных параметров», Інформатика та математичні методи в моделюванні, Том 7, № 3, с. 170-177, 2017.

УДК 004.054

Когутенко Марія Євгенівна, *бакалавр*
mari.kogutenko@gmail.com

Ткач Юлія Миколаївна*, д.пед.н., доц.,*
Національний університет «Чернігівська політехніка»
tkachym79@gmail.com

АНАЛІЗ МЕТОДІВ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

На сьогоднішній день, в результаті, швидкого розвитку ІТ-інфраструктури організацій та підприємств, стає більшою і вразливість ресурсів інформаційних систем. Для забезпечення задовільного рівня безпеки цих ресурсів, зазвичай, впроваджують на підприємствах відповідні системи захисту інформації. Окремим кроком побудови таких систем є реалізація процесу аналізу та оцінювання ризиків інформаційної безпеки (ІБ). Метою цього дослідження є аналіз методів оцінювання ризиків ІБ, їх порівняння за певними критеріями та надання рекомендацій, щодо їх вдосконалення на основі проведеного аналізу.

Аналіз ризиків – це аналіз ймовірності того, що можуть відбутися деякі небажані події, а вони в свою чергу негативно вплинуть на роботу підприємства, іншими словами - це процес виявлення факторів ризиків і оцінки їх значимості.

Оцінка ризиків полягає у визначенні величини (ступеню) ризику. Під час оцінювання ризиків беруться до уваги чимало факторів, такі як: цінність ресурсів, оцінка значущості загроз, вразливостей, ефективність існуючих і планованих засобів захисту. Також, є різні підходи: методи, системи, методології для оцінювання ризиків, вибір яких залежить від рівня вимог, що надаються в організації до режиму ІБ.

Для аналізу та порівняння методів оцінки ризиків, було взято три найбільш використовувані на сьогоднішній день методи: CORAS, CRAMM, OCTAVE.

Метод **CORAS** – це метод для оцінки ризиків, він включає в себе комп'ютерний інструментарій, який підтримує документування, створення звітів про результати аналізу, шляхом моделювання ризику. Всі роботи щодо ризиків проводяться за допомогою наступних процедур:

1) підготовчі заходи - збір загальних відомостей про об'єкт аналізу;

2) представлення клієнтом об'єктів, які необхідно проаналізувати;

3) детальний опис завдання аналітиком;

4) перевірка правдивості та повноти документації, представленої для аналізу;

5) заходи з виявлення ризиків (здійснюються, наприклад, у формі семінару) очолювані аналітиками;

6) оцінка ймовірностей і наслідків інцидентів ІБ;

7) виявлення прийнятних ризиків і ризиків, які повинні бути відправлені на подальшу оцінку для можливого усунення;

8) усунення загроз, з метою скорочення ймовірності та/або наслідків інцидентів в області ІБ.

У методі **CRAMM** аналіз ризиків включає в себе ідентифікацію та обчислення рівнів (заходів) ризиків на основі оцінок, присвоєних ресурсів, загроз і вразливостей ресурсів [1]. Контроль ризиків являє собою ідентифікацію, а також вибір контрзаходів, за допомогою яких можна знизити ризики до задовільного рівня.

Метод CRAMM включає в себе три стадії:

1) на першій стадії дослідження, ідентифікуються та визначаються цінності ресурсів, що захищаються. По завершенню стадії, замовник дослідження повинен знати, чи досить для захисту системи впровадження засобів базового рівня, що включають звичні функції безпеки, або ж необхідно проведення більш ретельного аналізу;

2) на другій стадії розглядаються питання, пов'язані з оцінкою рівнів загроз для груп ресурсів та їх вразливостей. По завершенню даної стадії, замовник може отримати оцінені та ідентифковані рівні ризиків для своєї системи;

3) на третій стадії реалізовується пошук необхідних контрзаходів. Загалом, даний пошук дуже добре задовольняє потребам замовника. Наприкінці даної стадії, замовник буде проінформований, як треба модифікувати систему, а також вибирати і опрацьовувати спеціальні заходи протидії, за домогою яких можна знизити або мінімізувати ризики, що лишилися.

OCTAVE - це метод оперативної оцінки критичних загроз, активів і вразливостей [2]. Даний метод включає в себе створення групи аналізу, що займається ІБ. Група аналізу включає співробітників бізнес-підрозділів, які експлуатують систему, і співробітників відділу інформаційних технологій. Метод OCTAVE включає в себе три стадії.

Перша стадія - здійснення оцінки організаційних аспектів. Під час виконання цієї стадії, група аналізу визначає критерії (показники) оцінки збитку (несприятливих наслідків), які пізніше будуть використовуватися при оцінці ризиків. Також, на даній стадії робиться виокремлення найбільш важливих організаційних ресурсів і оцінюється поточний стан забезпечення безпеки на підприємств. В кінці запроваджуються вимоги до безпеки, а також для кожного критичного ресурсу будується профіль загроз.

Друга стадія, являє собою проведення високорівневого аналізу IT-інфраструктури підприємства, при цьому звертається увага на ступінь, за яким питання безпеки вирішуються підрозділами і працівниками, що відповідають за експлуатацію інфраструктури.

В основі третьої стадії здійснюється розробка плану забезпечення безпеки та захисту інформації. На даній стадії складаються стратегії забезпечення безпеки і плану зниження ризиків. У ході визначення та аналізу ризиків оцінюють збитки від реалізації загроз, встановлюють імовірнісні критерії оцінки загроз, оцінюється ймовірність реалізації загроз.

Для аналізу та порівняння представлених методів управління IT-ризиків був використаний стандарт COBIT [3] - пакет документів, що описують універсальну модель управління інформаційними технологіями. Нижче наведено таблицю 1 [4], яка відображає можливості розглянутих методів з точки зору категорій порівняння. Жирним і курсивним шрифтом в таблиці позначені розділи (групи) категорій. Знак "+" означає, що даний пункт відповідає категорії, а знак "-" не відповідає категорії, представленому в стандарті COBIT.

Таблиця 1

Можливості методів з точки зору категорій порівняння

Категорії порівняння	CRAMM	OCTAVE	CORAS
1	2	3	4
Ризики			
Використання категорій ризиків	+	+	+
Використання поняття макс. допустимого ризику	+	+	+
Підготовка плану заходів по зниженню ризиків	+	+	+
Управління			
Використання поняття «власник ризику»	+	+	+
План робіт по зниженню ризиків	-	+	-
Оцінка бізнес-, операційних-, IT-ризиків	-	+	+
Оцінка ризиків на технічному рівні	+	-	+
Оцінка ризиків на організаційному рівні	+	+	+
Включає проведення тренінгів	-	+	-
Включає проведення зборів, семінарів	-	+	+
Інформування керівника	+	+	+
Способи роботи з ризиками			
Прийняття ризику	-	+	+
Зниження ризику	+	+	+
Виключення (обхід) ризику	-	-	+
Елементи ризиків			
Загрози, вразливості	+	+	+
Активи: матеріальні, нематеріальні; їх цінність	+	+	+
Потенційний збиток, ймовірність реалізації загроз	+	+	+
Типи ризиків			
Бізнес-ризики	-	+	+
Ризики пов’язані з використанням технологій	-	+	+
Ризики пов’язані з порушенням законодавчих актів	-	+	-
Комерційні ризики	+	+	+
Ризики пов'язані з залученням персоналу	+	+	+
Ризики пов'язані з залученням третіх осіб	+	+	+
Повторні оцінки ризиків	-	+	-
Правила з прийняття ризиків	-	+	-

Закінчення табл. 1

1	2	3	4
Способи виміру величини ризику			
Кількісна оцінка, кількісне ранжування ризиків	+	-	+
Якісна оцінка, якісне ранжування ризиків	-	+	-
Процедури роботи з ризиками			
Процедура прийняття остаточних ризиків	-	+	+
Управління залишковими ризиками	-	-	-
Моніторинг ризиків			
Моніторинг з заходів безпеки	-	-	-
Заходи щодо зниження ризиків	-	+	-
Присутність процесу реагування на інциденти ІБ	-	+	-
Документація результатів оцінки ризиків	-	+	+

Аналіз представлених методів показує, що порівняні методи, повністю відповідають вимогам групи «Ризики» та «Елементи ризиків», але недостатньо відповідають категоріям всіх інших груп. Отже, щодо групи «Управління», то тут найкраще відповідає всім вимогам метод OCTAVE, але все ж, доцільно було б впровадити до цього методу оцінку управління ризиками на технічному рівні. CORAS та CRAMM мають необхідність в реалізації плану робіт по зниженню ризиків, до того ж, до методу CRAMM добре було б, ще включити оцінку бізнес-, операційних- та IT-ризиків.

Щодо групи «Способи роботи з ризиками» CORAS має першість, він повністю відповідає вимогам даної групи, в порівнянні з CRAMM, який не включає можливість прийняття ризику, також, даний метод не передбачає виключення (обходу) ризику так само як і OCTAVE.

Розглядаючи групу «Типи ризиків» метод OCTAVE займає першу позицію, він цілком відповідає вимогам цієї групи; метод CORAS має необхідність в забезпеченні розгляду ризиків пов’язаних з порушенням законодавчих актів, а також в повторній оцінці ризиків та визначенні правил прийняття ризиків; метод CRAMM має необхідність в забезпеченні розгляду бізнес-ризиків, ризиків пов’язаних з використанням технологій, ризиків пов’язаних з порушенням законодавчих актів, а також в повторній оцінці ризиків та визначенні правил з прийняття ризиків.

Щодо групи «Способи виміру величини ризику» то методи CRAMM та CORAS не передбачають якісну оцінку ризиків, тобто, якісне ранжування, проте, метод OCTAVE, навпаки, не передбачає кількісну оцінку ризиків.

Розглядаючи групу «Процедури роботи з ризиками», то метод CRAMM не передбачає процедуру прийняття остаточних ризиків та управління залишковими ризиками, на мою думку, доцільно було б додати до даного методу такі процедури; метод OCTAVE та CORAS передбачають процедуру прийняття остаточних ризиків, але відсутня процедура управління залишковими ризиками, яка, на мою думку, добре доповнила б ці методи.

Щодо групи «Моніторинг ризиків» то методи CRAMM та CORAS не передбачають застосування моніторингу заходів безпеки, проведення заходів щодо зниження ризиків, у них відсутній процес реагування на інциденти інформаційної безпеки, а також у методу CRAMM немає документування результатів оцінок ризиків, натомість CORAS передбачає документацію; в свою чергу метод OCTAVE не передбачає лише застосування моніторингу заходів безпеки.

Таким чином, проаналізувавши дані, представлені в таблиці 1, можна зробити висновок, що метод OCTAVE найбільше з порівняних відповідає вимогам стандарту COBIT.

Оцінка CRAMM. До негативної сторони методу CRAMM можна віднести те, що серед способів роботи з ризиками даний метод передбачає тільки зниження ризиків. Прийняття ризику чи його обхід в даному методі не здійснюється. До того ж, ліцензія CRAMM коштує доволі таки дорого. Щодо його переваг, то CRAMM передбачає можливість оцінки ризиків на технічному та організаційному рівнях, а також підготовку плану робіт щодо зниження ризиків.

Оцінка CORAS. Загалом CORAS не передбачає комплексних заходів з управління ризиками. У CORAS не передбачені періодичні проведення оцінки ризиків, а також можливість оновлення їх значень, це говорить про те, що метод придатний для виконання разових оцінок і не передбачається для регулярного використання. Перевагою даного методу є те, що він передбачає прийняття, зниження та виключення ризиків. Також позитивною

стороною CORAS є наявність програмного продукту, що реалізовує цей метод, він поширюється безкоштовно і не потребує багато ресурсів для встановлення і застосування.

Оцінка OCTAVE. Негативною стороною цього методу є те, що він не передбачає виключення (обхід) ризику та управління залишковими ризиками. В цілому цей метод має чимало переваг починаючи від прийняття та зниження ризику і проведенням заходів щодо зниження ризиків, закінчуючи процедурою прийняття остаточних ризиків та структурованим документування результатів оцінок ризиків.

Отже, в результаті проведення аналізу та порівняння методів: CORAS, CRAMM, OCTAVE оцінки ризиків інформаційної безпеки, саме метод OCTAVE найбільше з порівняних відповідає вимогам стандарту COBIT. Направлення подальших досліджень: на основі аналізу порівняних методів, розробити структурно-логічну модель оцінки ризиків інформаційної безпеки, а також метод до даної моделі.

Анотація. У даній роботі, проведено аналіз трьох методів оцінки ризиків інформаційної безпеки: CORAS, CRAMM, OCTAVE. Для аналізу та порівняння представлених методів управління IT-ризиків використовувався стандарт COBIT. Порівнювалися методи за такими основними групами: ризики; управління; способи роботи з ризиками; елементи ризиків; типи ризиків; способи виміру величини ризику; процедури роботи з ризиками. За результатами порівняння проаналізовано дані методи, а також надані рекомендації, щодо їх покращення.

Література:

1. Метод CRAMM [Електронний ресурс]. – Режим доступу до ресурсу: http://wiki.tneu.edu.ua/index.php?title=Метод_аналізу_ризиків_CRAMM

2. Інформаційні ризики сучасних підприємств: моделювання та УПР [Електронний ресурс]. – Режим доступу до ресурсу: https://prezi.com/s8pdildx8vch/presentation/

3. Стандарт COBIT 5: Business Model for IT leadership and management at the enterprise, 2012 ISACA

4. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. – М.: ИНФРА-М_РИОР, 2014.

5. Методологии управления ИТ-рисками [Електронний ресурс]. – Режим доступу до ресурсу: http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/metodologii-upravleniya-it-riskami

УДК 004.056.5

Корченко О.Г., *д.т.н., професор,*

Гребенюк В.М., *д.ю.н.,*
icaocentre@nau.edu.ua

Дрейс Ю.О., *к.т.н., доцент,*
Національна академія Служби безпеки України
dreisyuri@gmail.com

ТЕОРЕТИКО-МНОЖИННА МОДЕЛЬ КРИТЕРІЇВ КРИТИЧНОСТІ ОБ'ЄКТІВ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Існуюче нормативно-правове забезпечення захисту об'єктів критичної інфраструктури (ОКІ) свідчить про наявність низки проблем в енергетичній, інформаційній та інших сферах, що мають малосистемний характер відповідної діяльності, спостерігається нечітка спрямованість формування переліку інформаційно-телекомунікаційних систем (ІТС) ОКІ тощо. Крім, того на концептуальному та нормативному рівнях також не проведено класифікацію ОКІ держави (ОКІД), не сформовано перелік їх ІТС як об'єктів критичної інформаційної інфраструктури (ОКІІ), а також відсутні критеріїв щодо оцінювання негативних наслідків, до яких може призвести кібератака на ІТС ОКІД [1]. Тому, проведення аналізу та формування переліку узагальнених критеріїв віднесення об'єктів до ОКІД з метою чіткого визначення повноти та меж критичної інформаційної інфраструктури держави суб'єктами забезпечення її кіберзахисту є *актуальним* науковим завданням.

Виходячи з викладеного, *метою роботи* є побудова теоретико-множинної моделі критеріїв критичності об'єктів інфраструктури для формування їх переліку та подальшого забезпечення кіберзахисту.

Відповідно до законодавства України критерії та порядок віднесення об'єктів до ОКІ, перелік таких об'єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України (КМУ). В

зазначеному документі також надано і визначення ОКІ та ОКІІ. Але, відповідно до запропонованого проекту Постанови КМУ, до ОКІ можуть бути віднесені підприємства, установи, організації незалежно від форми власності, які: провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах, у сферах життєзабезпечення населення, зокрема, у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, охорони здоров'я; є аварійними та рятувальними службами, службами екстреної допомоги населенню; включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави; є об'єктами, що підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду; є об'єктами потенційно небезпечних технологій і виробництв. Але віднесення таких об'єктів до ОКІ відбувається за сукупністю критеріїв, що визначають їх важливість для реалізації життєво-важливих функцій та надання життєво-важливих послуг, свідчать про існування ризиків і загроз для них, можливість виникнення кризових ситуацій через втручання в їх функціонування, припинення функціонування, людський чинник чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму тощо. Тобто, запропоновано принцип «віднесення таких об'єктів до ОКІ визначається за сукупністю критеріїв», якщо в об'єкті інфраструктури не визначено хоча б одного із вищенаведених критеріїв, то такий об'єкт не може бути віднесений до ОКІ, що є досить дискусійним і суперечливим твердженням, тому й було виключене з кінцевої редакції. Отже, враховуючи наявні нормативні протиріччя та проблеми наведені у [1], одним із завдань для КМУ, є також запровадження критеріїв та методології віднесення об'єктів інфраструктури до рівня критичної, порядок їх паспортизації та категоризації.

Для вирішення цих проблем та протиріч, провівши аналіз наукових праць і узагальнення діючих нормативно-правових документів, пропонується *перелік узагальнених критеріїв віднесення об'єктів до ОКІД* [1]:

1) За сферою діяльності (*СД*) та надання послуг у секторі критичної інфраструктури:

Група	*Критерії*
Підприємства, установи та організації незалежно від форми власності, які провадять діяльність та надають послуги в галузях:	- енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківській та фінансовій сфері; - у сферах життєзабезпечення населення, зокрема, централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я; - є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню; - включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави; - є об'єктами потенційно небезпечних технологій і виробництв; - є об'єктами, що підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду;
Відносяться до сектору критичної інфраструктури держави:	- банківсько-фінансового сектору; - сектору безпеки та оборони; - поштового та транспортного зв'язку (авіаційний, автомобільний, залізничний, морський, річковий, міський електричний транспорт); - паливно-енергетичного сектору; - екологічного сектору; - сектору державного управління та охорони правопорядку; - сектору мережі життєзабезпечення та інші.

2) За категорією об'єктів (*КО*) яким регламентуються особливі умови забезпечення їх захисту та функціонування:

Критерії
«…- підприємства, які мають стратегічне значення для економіки та безпеки держави; - об'єкти, які включені до Державного реєстру потенційно небезпечних об'єктів; - об'єкти підвищеної небезпеки (в т.ч. Перелік особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров'ю громадян, майну, спорудам, навколишньому природному середовищу); - важливі державні об'єкти; - об'єкти, що підлягають обов'язковій охороні підрозділами Державної служби охорони за договорами; - об'єкти, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період; - особливо важливі об'єкти електроенергетики; - особливо важливі об'єкти нафтогазової галузі; - національна система конфіденційного зв'язку; - платіжні системи; - система екстреної допомоги населенню за єдиним номером 112; - аварійно-рятувальні служби; - нерухомі об'єкти культурної спадщини».

3) За критеріями включення до переліку окремих особливо важливих об'єктів (*ОВО*) права державної власності, охорона яких здійснюється виключно державними підприємствами та організаціями на підставі договорів про надання охоронних послуг:

Група	*Критерії*
Зберігаються:	- наркотичні засоби, психотропні речовини і прекурсори; - історичні та культурні цінності загальнодержавного значення;
Виробляються та/або зберігаються:	- озброєння, ракети, боєприпаси, вибухові речовини, вогнепальна спортивно-мисливська зброя, спеціальні засоби, заряджені речовинами сльозоточивої та дратівної дії, засоби активної оборони; - запаси пально-мастильних матеріалів, речового та продовольчого майна;

Здійснюються:	- водопостачання населених пунктів з резервуарами питної води; - захоронення радіоактивних відходів; - провадження діяльності, пов'язаної з державною таємницею; - операції з дорогоцінними металами і дорогоцінним камінням, дорогоцінним камінням органогенного утворення, напівдорогоцінним камінням; - оцінювання якості освіти, проведення та перевірка результатів зовнішнього незалежного оцінювання; - спортивні та/або розважальні заходи; - надання медичної допомоги та медичних послуг;
Розміщується:	- орган державної влади;
Має стратегічне значення:	- відповідно до «Переліку об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держави»;
Належить до:	- об'єкта підвищеної небезпеки відповідно до законодавства.

4) За сукупністю критеріїв, що визначають їх важливість для реалізації життєво-важливих функцій та надання життєво-важливих послуг (*ЖВфп*):

Група	*Критерії*
- існування викликів, ризиків і загроз, що можуть виникати щодо ОКІ;	
Уразливості цих об'єктів, тяжкості настання можливих негативних наслідків, внаслідок чого буде заподіяна значна шкода:	- здоров'ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення); - соціальній сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства); - економіці (вплив на ВВП, розмір економічних втрат, як прямих, так і непрямих); - природним ресурсам загальнодержавного значення; - обороноздатності; - іміджу країни;
Здійснюються:	- водопостачання населених пунктів з резервуарами питної води; - захоронення радіоактивних відходів; - провадження діяльності, пов'язаної з державною таємницею; - операції з дорогоцінними металами і дорогоцінним камінням, дорогоцінним камінням органогенного утворення, напівдорогоцінним камінням; - оцінювання якості освіти, проведення та перевірка результатів зовнішнього незалежного оцінювання; - спортивні та/або розважальні заходи; - надання медичної допомоги та медичних послуг;
Масштабності негативних наслідків для держави, які:	- вплинуть на діяльність стратегічно важливих об'єктів для кількох секторів економіки; - призведуть до втрати унікальних національно значущих активів, систем і ресурсів; - матимуть тривалі наслідки для держави і позначаються на діяльності низки інших секторів;
- тривалості ліквідації таких наслідків та дією подальшого негативного впливу на інші сектори держави;	
- впливу на функціонування суміжних секторів критичної інфраструктури;	
- завдання значної шкоди нормальним умовам життєдіяльності населення.	

5) За наслідками порушення сталого функціонування ОКІ, які можуть спричинити кібератаки (*НК*):

Критерії
«… - виникнення надзвичайної ситуації техногенного характеру та/або негативний вплив на стан екологічної безпеки держави (регіону) (Н1); - негативний вплив на стан енергетичної безпеки держави (регіону) (Н2); - негативний вплив на стан економічної безпеки держави (Н3); - негативний вплив на стан обороноздатності, забезпечення національної безпеки та правопорядку у державі (Н4); - негативний вплив на систему управління державою (Н5); - негативний вплив на суспільно-політичну ситуацію в державі (Н6); - негативний вплив на імідж держави (Н7); - порушення сталого функціонування фінансової системи держави (Н8); - порушення сталого функціонування транспортної інфраструктури держави (регіону) (Н9); - порушення сталого функціонування інформаційної та/або телекомунікаційної інфраструктури держави (регіону), в тому числі її взаємодії з відповідними інфраструктурами інших держав (Н10).»

6) За методикою ідентифікації потенційно небезпечних об’єктів (*ПНО*):

Група	*Критерії*
За видом небезпеки:	- бактеріологічна; - біологічна; - вибухопожежна; - гідродинамічна; - пожежна; - радіаційна; - фізична; - хімічна; - екологічна.
За класифікацією та кодом надзвичайної ситуації (НС):	- техногенні; - природні;- соціально-політичні; - воєнні.
За рівнем можливої НС:	- національний; - державний; - регіональний; - місцевий; - об’єктовий.

7) За категорією критичності (*КК*):

Критерії
- І категорія критичності – критично-важливі об’єкти; - ІІ категорія критичності – життєво-важливі об’єкти; - ІІІ категорія критичності – важливі об’єкти; - ІV категорія критичності – необхідні об’єкти.

8) За наявністю ОКІІ (*ОКІІ*):

Критерії
- комунікаційної або технологічної системи ОКІ; - інформаційні системи; - інформаційно-телекомунікаційні системи та мережі; - автоматизовані системи управління технологічним процесом.

9) За класами наслідків (відповідальності) від категорії складності об'єкта (*КН*):

Критерії
- до класу наслідків СС-1 (незначні наслідки) – I та II категорія складності;
- до класу наслідків СС-2 (середні наслідки) – III та IV категорія складності;
- до класу наслідків СС-3 (значні наслідки) – V категорія складності;

10) За основними критеріями визначення певного критичного інфраструктурного елементу (*ЕКІ*):

Критерії
«…- територіальна досяжність негативних результатів (наприклад, транснаціональний, народний, регіональний, локальний /місцевий); - велика кількість наслідків (наприклад, гуманітарних, матеріальних, економічних, політичних або збитки і втрати по відношенню до навколишнього середовища); - часовий ефект наслідків, особливо коли з'являться негативні наслідки (негайно, за 24 год.); - як довго можуть продовжуватися негативні наслідки (до 24 годин, до 3 днів)».

11) За ознаками ідентифікації об'єктів підвищеної небезпеки (*ОПН*):

Група	*Критерії*
За категорією наявних небезпечних речовин:	- горючі (займисті) гази; - горючі рідини; - горючі рідини, перегріті під тиском; - вибухові речовини; - речовини-окисники; - високотоксичні та токсичні речовини; - речовини, які становлять небезпеку для довкілля (високотоксичні для водних організмів).
За видами та впливом уражальних факторів аварій, що можуть статися виходячи з властивостей небезпечних речовин:	- група 1 (вибух); - група 2 (пожежа); - група 3 (шкідливі для людей і довкілля).

12) За видом інформації, що обробляється (*ВІ*):

Група	*Критерії*
Національні електронні інформаційні ресурси:	- публічна інформацію; - державні інформаційні ресурси; - інша інформація, призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави;
Інформація з обмеженим доступом:	- конфіденційна інформація (в т.ч. персональні дані); - службова інформація; - таємна інформація.

Пропонується наступне теоретико-множинне представлення критеріїв критичності об'єктів інфраструкутури держави як ОКІД у такому загальному виді як:

$$\text{МК} = \{\bigcup_{i=1}^{n} \text{МК}_i\} = \{\text{МК}_1, \text{МК}_2, ..., \text{МК}_n\}, \qquad (1)$$

де $\text{МК}_i \subseteq \text{МК}$ $(i = \overline{1,n})$ – компонент моделі, що відображає *i*-у множину критеріїв, *n* – кількість цих множин критеріїв.

Для *i*-ї множини МК_i визначимо як:

$$\text{МК}_i = \{\bigcup_{j=1}^{n_{i1}} MK_{ij}\} = \{MK_{i1}, MK_{i2}, ..., MK_{in_{i1}}\}, \qquad (2)$$

де $MK_{ij} \subseteq \text{МК}_i$ $(j = \overline{1,n_{i1}})$ – ідентифікатори критеріїв підмножин *i*-ї множини критеріїв, а n_{1i} - кількість цих підмножин.

З урахуванням (2) вираз (1) можна представити у такому вигляді:

$$\begin{aligned} \text{МК} = \{\bigcup_{i=1}^{n} \text{МК}_i\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{n_{i1}} MK_{ij}\}\} = \{ \{MK_{11}, MK_{12}, ..., MK_{1n_{11}}\}, \\ \{MK_{21}, MK_{22}, ..., MK_{2n_{12}}\}, ..., \\ \{MK_{n1}, MK_{n2}, ..., MK_{nn_{i1}}\}\}, (i = \overline{1,n},\ j = \overline{1,n_{i1}}). \end{aligned} \qquad (3)$$

Наприклад, при $\text{n} = 12$, $(\text{i} = \overline{1,12})$ відповідно до [1], модель (1) набуде виду:

$$\begin{aligned} \text{МК} = \{\bigcup_{i=1}^{n_1} \text{МК}_i\} = \{\text{МК}_1, \text{МК}_2, ..., \text{МК}_{12}\} = \\ = \{СД, КО, ОВО, ЖВфп, НК, ПНО, КК, КН, ОКІІ, ЕКІ, ОПН, ВІ\}, \end{aligned} \qquad (4)$$

де МК_1 = *СД*, МК_2 = *КО*, МК_3 = *ОВО*, МК_4 = *ЖВфп*, МК_5 = *НК*, МК_6 = *ПНО*, МК_7 =*КК*, МК_8 = *ОКІІ*, МК_9 = *КН*, МК_{10} = *ЕКІ*, МК_{11} = *ОПН*, МК_{12} = *ВІ*.

Висновок. Запропоновано базову модель переліку узагальнених критеріїв критичності об’єктів інфраструктури, яка за рахунок формульного множинного представлення може доповнюватися іншими та новими критеріями для формування класифікаторів та реєстру ОКІД, їх паспортизації та категоризації, створення переліку їх ОКІІ з метою визначення повноти та меж суб’єктами забезпечення їх кіберзахисту.

Анотація. Проаналізовані критерії критичності об'єктів інфраструктури держави, що визначені законодавством, нормативно-правовими документами та науковими працями у даній сфері. З метою узагальнення переліку цих критеріїв запропоновано сформувати їх у вигляді універсальної множини, яку завжди можливо доповнити новими критеріями не змінюючи її формульного представлення. За рахунок такої теоретико-множинної моделі переліку узагальнених критеріїв критичності можливе подальше створення методології віднесення об'єктів до об'єктів критичної інфраструктури держави, порядку їх паспортизації та категоризації, удосконалення процедури формування переліку інформаційно-телекомунікаційних систем цих об'єктів як об'єктів критичної інформаційної інфраструктури держави з метою подальшого забезпечення їх кіберзахисту.

Література

1. A. Korchenko, V. Hrebenuik, Y. Dreis, A. Hrebenuik, O. Gavrylenko, Criteria for assigning objects to critical infrastructure of Ukraine, Monografia, «Przetwarzanie, transmisja i bezpieczenstwo informacij»: Monografia, Tom 2, Akademia Techniczno-Humanistyczna w Bielsku-Bialej, 2019. – (418 c.). – C.189-196.

УДК 004.056.53

Котенко Наталія Олексіївна
Київський національний торговельно-економічний університет, старший викладач кафедри інженерії програмного забезпечення та кібербезпеки, кандидат педагогічних наук,
kotenkono@ukr.net

Жирова Тетяна Олександрівна
Київський національний торговельно-економічний університет, старший викладач кафедри інженерії програмного забезпечення та кібербезпеки, кандидат педагогічних
zhyrova@knute.edu.ua

Квятковська Анна Олегівна,
Київський коледж зв'язку, циклова комісія інформаційних мереж, викладач вищої категорії
sobolevanna29@gmail.com

АНАЛІЗ ЗАХИЩЕНОСТІ ОСВІТНІХ ХМАРНИХ ВЕБ-СЕРВІСІВ

В освітньому процесі, для якісної його організації, все частіше використовують такі програмні продукти як Teams [6] від Microsoft та Google Classroom [7] від Google. Їх використання є вимогою сьогодення, адже такі сервіси забезпечують мобільність усіх учасників освітнього процесу, дозволяють враховувати індивідуальну траєкторію кожного студента, а також відзначаються особливістю сприймання та засвоєння навчального матеріалу сучасною молоддю. І Teams, і Google Classroom зручно використовувати викладачам у всіх аспектах освітнього процесу: під час лекційних занять, лабораторних та практичних занять, для організації дистанційного навчання тощо.

Google Classroom – безкоштовний веб-сервіс створений Google для навчальних закладів з метою спрощення створення, поширення і класифікації завдань безпаперовим шляхом. Основна мета сервісу – прискорити процес поширення файлів між викладачами і студентами. Може використовуватися вчителями та учнями у школах, або у закладах вищої освіти викладачами та студентами. Даний сервіс характеризується такими особливостями: зручний та оптимізований адаптивний інтерфейс, стабіль-

на робота мобільного додатку, наявність низки необхідних додаткових функціональних можливостей, зручний інструмент адміністрування виконаних усіма користувачами робіт.

«Microsoft Teams» – центр для командної роботи в Office 365 від Microsoft, який інтегрує користувачів, вміст і засоби, необхідні команді для ефективнішої роботи. Застосунок об'єднує все в спільному робочому середовищі, яке містить чат для нарад, файлообмінник та корпоративні програмами. Розроблений для смартфонів, що працюють на платформах Android, iOS, Windows Phone і комп'ютерів з операційною системою Windows 10 S, Windows 7+ або Mac OS X 10.10+ [5]. З 2017 року Microsoft в Office 365 замінила Microsoft Classroom для освітніх установ на Microsoft Teams, тобто на сьогодні Teams забезпечений усім необхідним для використання в навчальних закладах.

Чи безпечними є ці програмні продукти? Яка вірогідність втратити розміщені у них дані? Чи можливе розповсюдження конфіденційних даних через них? Ці та інші питання безпеки часто постають перед користувачами Microsoft Teams та Google Classroom.

Продукт Microsoft Teams заснований на гіпермасштабованій хмарі корпоративного рівня Office 365, яка забезпечує потрібні клієнтам розширені можливості по забезпеченню безпеки і відповідності [1].

Google Classroom доступний безкоштовно для навчальних закладів, некомерційних організацій і приватних осіб. У цьому сервісі немає реклами, а матеріали і дані учнів не використовуються в маркетингових цілях [2]. З метою безпеки в Google Classroom встановлені обмеження на виконання певних дій. Ці обмеження залежать від типу облікового запису. Якщо користувач досягає певного ліміту, то не втрачає можливість виконати відповідну дію.

Google запевняє, що постійно прагне створювати програмні продукти, які у першу чергу захищають конфіденційність користувачів та забезпечити найкращу захищеність даних на просторах Інтернет, не є виключенням і сервіс Google Classroom. Захищеність при використанні Google Classroom досягається за рахунок таких чотирьох складових:

- збереження даних у безпеці;
- в основних програмах G Suite for Education немає оголошень;
- дотримання галузевих норм та найкращих практик;

– чітка інформація про політику конфіденційності та безпеки Google [4].

За захищеністю даних, що зберігаються, обробляються, використовуються у Google Classroom та Microsoft Teams стоять такі флагмани IT-індустрії як Google та Microsoft тому у цілісності та конфіденційності даних можна бути відносно впевненим. Відносно тому, що ніхто і ніколи не дає сто відсотків гарантій, а ще тому, що дуже часто вирішальне значення у цілісності даних відіграє людський фактор. Враховуючи те, що Google Classroom та Microsoft Teams у своїх професійних цілях використовують учителі та викладачі, а також учні та студенти, які не завжди є професіоналами IT-сфери, цілісність даних та їх конфіденційність може бути втрачена за рахунок людського фактору.

Анотація**. **Microsoft Teams та Google Classroom повноцінно використовуються різноманітними освітніми установами. Вони сприяють підвищенню якості надання освітніх послуг, допомагають в організації освітнього процесу. Через них проходит велика кількість різноманітних даних втрата, пошкодження або розголошення яких негативно вплине на освітній процес та його учасників.

Корпорації Microsoft та Google дбають про безпечність своїх продуктів з різних точок зору. Проте це зовсім не означає що можна бездумно використовувати їх продукцію і бути впевненим у захищеності власних даних, завжди і скрізь присутній людський фактор.

Література:

1. Обзор обеспечения безопасности и соответствия в Microsoft Teams. Режим доступу: https://docs.microsoft.com/ru-ru/microsoftteams/security-compliance-overview

2. Сведения о Google Классе. Режим доступу: https://support.google.com/edu/classroom/answer/6020279?hl=ru&ref_topic=7175444

3. Google Classroom. Матеріал з Вікіпедії – вільної енциклопедії. Режим доступу: https://uk.wikipedia.org/wiki/Google_Classroom#cite_note-1

4. Privacy & Security Center. Режим доступу: https://edu.google.com/why-google/privacy-security/?modal_active=none

5. Microsoft Teams. Матеріал з Вікіпедії – вільної енциклопедії. Режим доступу: https://uk.wikipedia.org/wiki/Microsoft_Teams

6. Blokdyk G. Microsoft Teams A Complete Guide – 2019 Edition Paperback – 5STARCooks (December 20, 2018). – 300 p.

7. Zhang M. Teaching with Google Classroom Paperback – Packt Publishing (September 30, 2016). – 256 p.

УДК 004.056.5:519.876.2

Криворучко Олена Володимирівна, *д.т.н, професор*
Київський національний торговельно-економічний університет
kryvoruchko_ev@knute.edu.ua

Гнатченко Т.О., *аспірант*
Київський національний торговельно-економічний університет
t.hnatchenko@knute.edu.ua

Гнатченко Д.Д., *асистент*
Київський національний торговельно-економічний університет
hnatchenko@knute.edu.ua

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМИ МОДЕЛЮВАННЯ БІЗНЕС-ПРОЦЕСІВ

Явищем, що супроводжує неспинний процес інформатизації та вимагає підвищеної уваги з боку підприємців є інформаційна безпека. Зовнішні та внутрішні фактори у вигляді навмисних або ненавмисних дій можуть як задавати шкоду, так і становити реальну загрозу для інформаційного середовища підприємства.

Будь-яке підприємство, що активно провадить бізнес-діяльність, користується відповідною інформаційною системою, і чим більший масштаб діяльності, тим більший обсяг релевантних даних міститься у системі, які є основним об'єктом інформаційних загроз. Однак, проблема інформаційного захисту такого класу програмних рішень як системи моделювання бізнес-процесів є недослідженою та вимагає вивчення, оскільки дані системи все ширше застосовуються на підприємствах з метою аналізу й удосконалення бізнес-моделі.

Моделювання бізнес-процесу – це процес відображення суб'єктивного бачення потоку робіт у вигляді формальної моделі, що складається з взаємопов'язаних операцій. Бізнес-модель – це формалізований опис бізнес-процесів, що відображає реально існуючу або передбачувану діяльність підприємства [1].

Досвід впровадження практики моделювання на вітчизняних підприємствах характеризується наступними позитивними результатами:

- удосконалюється координація дій на нижчому і середньому рівнях управління;

- пришвидшується реагування на зміни у зовнішньому середовищі;

- розроблена система управління надає можливості для реалізації тактичних завдань без додаткових витрат на планування та ін.

На ринку інформаційних технологій існує досить велика кількість програмного забезпечення для моделювання бізнес-процесів. Такі програмні рішення можуть експлуатуватися як окрема інформаційна система або ж існувати інтегровано всередині корпоративних програмних комплексів.

Одним з підходів до класифікації є систем моделювання бізнес-процесів є функціональне призначення програмного продукту [2]:

Група 1 – комп'ютерні інформаційні системи (інформаційні системи класу ERP).

Група 2 – програмні продукти класу СУБД (об'єктно орієнтовані системи управління базами даних: MySQL, mSQL, PostgreSQL, Oracle, Microsoft SQL, Access, Sybase та ін.).

Група 3 - програмні продукти для управління бізнес-процесами (BPM) (наприклад, клієнт-орієнтована стратегія – CRM).

Група 4 - програмне забезпечення класу DocFlow (системи маршрутизації документів) і WorkFlow (системи управління потоками робіт).

Група 5 – моделювання і аналіз бізнес-процесів (на українському ринку використовуються програмні продукти, засновані на інтеграції CASE-технологій і імітаційного моделювання).

Незалежно від форми існування системи моделювання бізнес-процесів (самостійно або інтегровано) необхідно забезпечити належний інформаційний захист такої системи, оскільки відомості, що містяться у ній, мають високий пріоритет для управлінського апарату та характеризуються складною відновлюваністю у разі повної втрати даних.

До найпоширеніших видів загроз інформаційній безпеці підприємства, що підвищують вразливість програмного забезпечення, відносять [3]:

– відсутність регламентованого доступу до файлів даних;

– вільне втручання в програмне забезпечення;

– відсутність протоколювання змін у програмному забезпеченні;

– відсутність регламентації користувачів інформації;

– відсутність дублювання важливих документів на документальних носіях даних;

– часті удосконалення одного і того ж програмного забезпечення різними особами;

– відсутність схем інформаційного забезпечення рівнів управління;

– наявність непідзвітних посадових осіб у системі управління тощо.

Відтак, з метою зниження ступеню впливу потенційних інформаційних загроз, ще на етапі розробки системи моделювання бізнес-процесів має бути реалізований механізм захисту інформації.

Для забезпечення ефективного захисту інформації доцільним є застосування системного підходу, що полягає у поєднанні комплексу заходів, а саме: спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів, морально-етичних заходів протидії тощо.

Реалізація ефективної політики забезпечення інформаційної безпеки корпоративного програмного забезпечення, як правило, спрямована на досягнення таких основних цілей [4]:

1) захищеність інформації (конфіденційність та унеможливлення доступу сторонніх осіб);

2) цілісність (захист від спотворення інформації у будь-якому її вигляді);

3) доступність (забезпечення доступу до інформації зацікавлених осіб).

Таким чином, перелік заходів протидії інформаційним загрозам системі моделювання бізнес-процесів має включати:

- регламентування правил експлуатації відповідної інформаційної системи у вигляді внутрішнього нормативно-правового акту з обов'язковим повним переліком осіб, що допускаються до роботи з програмою та їх правами доступу, а також передбаченими санкціями за порушення правил даного акту;

- своєчасне програмне налаштування доступу користувачів згідно регламентуючого акту;

- регулярне створення копії внесених даних та її запис на довірені зовнішні та/або хмарні носії інформації;

- контроль за дотриманням вимог регламентуючого акту зі сторони служби інформаційної безпеки на підприємстві або іншої призначеної відповідальної особи.

Анотація. Досліджено джерела та основні види інформаційних загроз системі моделювання бізнес-процесів підприємства. У результаті дослідження сформульований перелік ефективних заходів запобігання наведеним загрозам та забезпечення ефективної системи інформаційної безпеки.

Література:

1. Волков О. Стандарти та методології моделювання бізнес-процесів [Електронний ресурс] / Олег Волков – Режим доступу до ресурсу: http://www.connect.ru/article.asp?id=5710.

2. Клепікова О.А. Сучасний стан і місце інформаційних технологій в управлінні підприємством // О.А. Клепікова / Науковий вісник міжнародного гуманітарного університету. Економіка і менеджмент. – Одеса: МГУ, 2013. - № 5. – С. 74-77.

3. Северина С. В. Інформаційна безпека та методи захисту інформації / С. В. Северина // Вісник Запорізького національного університету. Економічні науки. - 2016. - № 1. - С. 155-161.

4. Русіна Ю. О., Острякова В. Ю. Удосконалення системи управління інформаційною безпекою на підприємстві // Міжнародний науковий журнал "Інтернаука". — 2017. — №14. – С. 135-139.

УДК 004.056.53

Лисиця Тетяна Анатоліївна, *levenovskaya98@gmail.com,*

Яковлєв Олександр Олегович, *samehada@i.ua*
Студ. НУЧП, 3 курс, гр. КБ-171

Ткач Юлія Миколаївна, *д.пед.н., доцент, tkachym79@gmail.com*
НУ «Чернігівська політехніка»

SPEAR PHISHING АТАКА: ОСОБЛИВОСТІ ТА СПОСОБИ ЗАХИСТУ

На сьогоднішній день більшість інтернет-користувачів хоча б раз чули про різні випадки здійснення кібератак, а частина з них самі стали жертвами інтернет-шахраїв. Здавалося б: що тут дивного? Більшість користувачів з упевненість стверджують: зловмисники щоразу вигадують нові і нові способи перехоплення чи крадіжки даних, їхні дії стають все більш непередбачуваними, а отже і захистися від таких атак стає принципово складніше. Проте, як не дивно, найбільш популярним інструментом інтернет-шахраїв залишається як раз один з найдавніших із них – фішинг.

Здавалося б: інтернет-користувачі безліч разів бачили повідомлення з попередженнями про те, що не слід повідомляти свої паролі стороннім особам, а працівники різних організацій в обов'язковому порядку були проінформовані про небезпеку відкриття електронних листів з підозрілої адреси, що, в свою чергу, повинно унеможливити загрозу фішингу взагалі або звести її до мінімуму. Але, за статистикою (згідно статистичним даним Trend Micro), станом на кінець 2019 року однією з найбільш популярних загроз в Україні як для окремого користувача, так і для бізнесу, як і раніше залишається фішинг.

Такий результат є наслідком того, що більшість кіберзлочинців замість витрачати час і зусилля на розробку нових технологій злому або проникнення, надають перевагу використанню людської халатності та довіри, а для підвищення ефективності атаки часто зазначають адресу директора організації/самої організації/потенційних клієнтів, тощо. В такому випадку можна говорити про одну із найбільш складних і небезпечних фішинг-атак - Spear Phishing. На відміну від традиційного фішингу, який

передбачає відправку електронних листів мільйонам невідомих користувачів, цей вид атак має сфокусовану дію, а листи точно направлені на конкретного користувача або групу користувачів.

На сьогоднішній день, на жаль, саме даний вид атак демонструє наявність найбільшої уразливості. Для підтвердження даної гіпотези за нашої участі було проведено експеримент у внутрішньому середовищі одного з філіалів українського банку. Його метою була оцінка в реальному часі знань і умінь співробітників банку на випадок отримання шкідливих розсилок від зовнішніх шахраїв, хакерів і т.д..

Співробітникам банку було надіслано підозрілі листи з різним вмістом: резюме від здобувача вакансії, дайджест "Бізнес і Фінанси", рахунок на оплату, "Повернення коштів", "Комерційна пропозиція" і ін.. Файли в листах не містили реальної загрози, проте вони фіксували факти відкриття і запуск макросу. Було відправлено близько 400 тренувальних листів. В розсилку включалися співробітники різних бізнес-напрямків і управлінської вертикалі - від пересічних фахівців відділень до Віце-Президентів деяких напрямків.

Результати експерименту виявилися невтішними:

1. Лише деякі співробітники банку (20 осіб або 5% від загальної кількості) оперативно звернулися безпосередньо в управління інформаційної безпеки (УІБ) з інформацією про отримання підозрілих листів. Ці дії є правильними, адже чим швидше про подібне дізнаються профільні служби, тим швидше загроза буде локалізована і усунена.

2. Багато співробітників, отримавши підозрілі вкладення, відкрили їх і запустили макроси. Фактично, їх комп'ютери стали точками проникнення в мережу банку. Таких співробітників 32, що становить 8% від загальної кількості співробітників, які отримали тестові листи.

3. Решта співробітників, навіть не відкривши отримані файли, переслали одержані листи разом в підозрілим вкладенням колегам, що тим самим сприяло б подальшому поширенню умовного вірусу по мережі банку. Негативні результати були спричинені тим, що далеко не всі співробітники помітили, що поштовий домен відправника маскується під домен іншого банку шляхом заміни лише однієї із букв назви справжнього банку.

Було вирішено вжити заходів і провести декілька тренінгів, спрямованих на підвищення обізнаності в сфері кібербезпеки. У ході продовження експерименту нами було запропоновано такий варіант її забезпечення:

1. Розгляд та розбір разом із працівниками банку найбільш яскравих випадків застосування фішинг-атак та їх наслідків для кращого розуміння ними наявної проблеми.

2. Підбір та аналіз шляхів проникнення для інтернет-шахраїв, обговорення орієнтовних варіантів вмісту електронних листів.

3. В результаті були підсумовані і коротко сформульовані основні правила для працівників банківської установи:

а) не переходити за посиланнями в тілі листа, не відкривати вкладені файли і не виймати архіви, якщо адреса відправника викликає сумніви.

б) перевіряти адресу відправника і URL посилання повідомлень від інтернет-сервісів, замість переходу за посиланням зайти в особистий кабінет в сервісі через пряму адресу.

в) якщо було отримано підозрілий лист від колеги, зв'язатися з ним для уточнення.

г) не відповідати на підозрілі листи.

д) слідкувати, щоб антивірусне ПЗ було ввімкнено, за можливості, перевіряти з його допомогою всі вкладення.

е) не передавати свій пароль від електронної пошти третім особам, особливо при реєстрації, заповненні форм, на прохання для уточнення інформації.

є) у разі виявлення підозрілих елементів в листі, терміново звернутися до УІБ банку.

4. Закріплення знань відбулося у вигляді коротких тестів.

Повторна модифікована незапланована перевірка через місяць показала кращі результати. Відсоток співробітників, які все ж таки відкрили підозрілі файли, зменшився до 7 (29 осіб), пересилка ж таких документів не відбулася взагалі.

Отже, після завершення експерименту ми дійшли висновку, що фішинг-атаки дійсно є значною небезпекою для організацій. Проте проведення різних заходів, що сприяють підвищенню рівня освіченості в сфері кібербезпеки, сприяють відчутному зниженню їх впливу, а отже і зменшенню негативних наслідків для організації.

Анотація: В даній статті було розглянуто актуальність та проблеми небезпечних наслідків застосування кібератак та різноманітних впливів, пов'язаних з використанням соціальної інженерії в межах інтернет-простору. Було виявлено вид атак, застосування яких є найбільш поширеним на сьогоднішній день - фішинг-атаки. Проаналізовано можливість зараження комп'ютерів або розголошення конфіденційної інформації при використанні одного з підвидів фішинг-атак - Spear phishing. На основі проведених досліджень було запропоновано методологію проведення заходів, що сприяють захисту організацій від фішинг-атак типу Spear phishing.

Література:

1. Фішинг [Електронний ресурс] – Режим доступу до ресурсу: https://ru.m.wikipedia.org/ wiki/Фишинг.

2. Статистика по фішинг-атакам [Електронний ресурс] – Режим доступу до ресурсу: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B2_%D0%BC%D0%B8%D1%80%D0%B5.

3. Людські слабкості які використовуються злочинцями при фішинг-атаках [Електронний ресурс] – Режим доступу до ресурсу: http://www.tadviser.ru/ index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3_(phishing).

4. Методика захисту від фішинг-атак [Електронний ресурс] – Режим доступу до ресурсу: https://rmrf.tech/ru_RU/blog/rmrf-1/post/16.

УДК 004.056.5

Лозова Ірина Леонідівна
Національний авіаційний університет
illozovaya@gmail.com

ТЕОРЕТИКО-МНОЖИННЕ ПРЕДСТАВЛЕННЯ ОКРЕМИХ ПАРАМЕТРІВ ДЛЯ КОРТЕЖНОЇ GDPR-МОДЕЛІ

Аналізуючи практику штрафних санкцій за порушення Регламенту GDPR [1], необхідно звернути увагу на те, що контролюючими органами накладаються штрафи різних розмірів в залежності від вчиненого правопорушення. Можна побачити, що штрафи більших розмірів накладаються у випадках, коли порушення стосуються або великих об'ємів персональних даних, або чутливих персональних даних. Головне, на що необхідно звернути увагу – до відповідальності можуть бути притягнуті як організації та підприємства з території ЄС, так і ті, що зареєстровані поза межами ЄС, про що яскраво свідчить справа, яка стосується канадської компанії AggregateIQ.

Отже, адаптуючи свій бізнес під вимоги Регламенту GDPR не можна забувати, що ризик застосування штрафних санкцій залежить виключно від рівня відповідальності, з якою організація підходить до вирішення даного питання. Не можна імітувати відповідність вимогам Регламенту GDPR. Організаціям та підприємствам необхідно проводити організаційні та технічні міри, необхідні для відповідності вимогам GDPR.

Метою даної роботи є представлення двох окремих параметрів «Специфіка, ступінь тяжкості і тривалість порушення, зважаючи на специфіку, обсяг чи ціль відповідного опрацювання, а також кількість суб'єктів даних, які зазнали впливу, і рівень шкоди, заподіяної їм» та «Навмисний або недбалий характер порушення» з використанням теоретико-множинних підходів для побудови кортежної GDPR-моделі, що дозволить формалізувати процес оцінювання збитків від втрати персональних даних.

GDPR-модель побудовано за принципом вибору рівня порушення з коефіцієнтом максимального штрафу та відповідей експерта відповідно до компонентів (параметрів) статті 83(2) Регламенту

GDPR, що реалізує подальше визначення величини нанесених збитків (шкоди) і надає необхідні рекомендацій щодо виявлення та мінімізації недоліків у політиці інформаційної безпеки організації. Відповідно до статті 83(2) Регламенту GDPR, кінцева сума штрафу визначається, враховуючи порушення однієї, декількох або всіх компонент (параметрів) даної статті Регламенту. Тому, GDPR-модель розроблено у вигляді кортежу цих параметрів [2].

Параметр кортежної GDPR-моделі **N** – «Специфіка, ступінь тяжкості і тривалість порушення, зважаючи на специфіку, обсяг чи ціль відповідного опрацювання, а також кількість суб'єктів даних, які зазнали впливу, і рівень шкоди, заподіяної їм» визначаємо виразом:

$$\mathbf{N} = \{\bigcup_{i=1}^{n_2} \mathbf{N_i}\} = \{\mathbf{N_1}, \mathbf{N_2}, ..., \mathbf{N_{n_2}}\}, \quad (1)$$

де **N** – множина критеріїв специфіки, ступеня тяжкості і тривалості порушення, $\mathbf{N_i} \subseteq \mathbf{N}$ $(i = \overline{1,n_2})$ i-та підмножина критеріїв визначення специфіки, ступеня тяжкості та тривалості порушення, а n_2 кількість таких підмножин.

Наприклад, при $n_2 = 4$ $(i = \overline{1,4})$ формулу (1) можна представити як:

$$\mathbf{N} = \{\bigcup_{i=1}^{4} \mathbf{N_i}\} = \{\mathbf{N_1}, \mathbf{N_2}, \mathbf{N_3}, \mathbf{N_4}\},$$

де відповідно до [3]: $\mathbf{N_1}$ = «Класифікація втрачених даних»; $\mathbf{N_2}$ = «Протяжність порушення»; $\mathbf{N_3}$ = «Кількість постраждалих суб'єктів персональних даних»; $\mathbf{N_4}$ = «Рівень впливу на суб'єкти персональних даних».

Далі, підмножину $\mathbf{N_i}$ визначимо як:

$$\mathbf{N_i} = \{\bigcup_{j=1}^{n_{2i}} N_{ij}\} = \{N_{i1}, N_{i2}, ..., N_{in_{2i}}\}, \quad (2)$$

де $N_{ij} \subseteq \mathbf{N_i}$ $(j = \overline{1,n_{2i}})$ – *j*-а підмножина груп критерії порушення споріднених за певною темою чи близьких за певними характеристиками у межах *i*-ї підмножини, а n_{2i} кількість груп *i*-ї підмножини.

Відповідно до сформованих підмножин у формулі (2), вираз (1) можна представити як:

$$\mathbf{N} = \{\bigcup_{i=1}^{n_2} \mathbf{N_i}\} = \{\bigcup_{i=1}^{n_2} \{\bigcup_{j=1}^{n_{2i}} N_{ij}\}\} = \{\{N_{11}, N_{12}, ..., N_{1n_{2i}}\}, \{N_{21}, N_{22}, ..., N_{2n_{2i}}\}, ..., \{N_{n_2 1}, N_{n_2 2}, ..., N_{n_2 n_{2i}}\}\}, \quad (3)$$

Наприклад, при $n_2 = 4$ $(i = \overline{1,4})$, $n_{21} = 5$ $(j = \overline{1,5})$, $n_{22} = 5$ $(j = \overline{1,5})$, $n_{23} = 5$ $(j = \overline{1,5})$, $n_{24} = 5$ $(j = \overline{1,5})$, формула (3) матиме вигляд:

$$\mathbf{N} = \{\bigcup_{i=1}^{4} \{\bigcup_{j=1}^{n_{2i}} N_{ij}\}\} = \{\{N_{11}, N_{12}, N_{13}, N_{14}, N_{15}\}, \{N_{21}, N_{22}, N_{23}, N_{24}, N_{25}\}, \{N_{31}, N_{32}, N_{33}, N_{34}, N_{35}\}, \{N_{41}, N_{42}, N_{43}, N_{44}, N_{45}\}\},$$

де: N_{11} = «Публічна»; N_{12} = «Комерційна»; N_{13} = «Конфіденційна»; N_{14} = «Секретна»; N_{15} = «Цілком секретна»; N_{21} = «< 1 Тиждень»; N_{22} = «1 Тиждень – 1 Місяць»; N_{23} = «1 Місяць – 6 Місяців»; N_{24} = «6 Місяців – 1 Рік»; N_{25} = «> 1 Року»; N_{31} = «< 1000»; N_{32} = «1.001 – 50.000»;С N_{33} = «50.001 – 100.000»; N_{34} = «100.001 – 1.000.000»; N_{35} = «> 1.000.000» [4]; N_{41} = «Незначний»; N_{42} = «Низький»; N_{43} = «Середній»; N_{44} = «Високий»; N_{45} = «Катастрофічний».

Ієрархічну структуру параметра **N** можна представити у вигляді схеми на рис. 1.

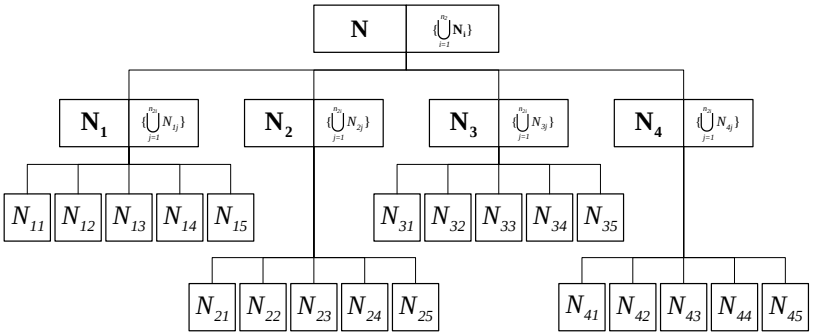


Рис. 1. Ієрархічна структура параметра ***N***

Наступний параметр кортежної GDPR-моделі **CH** – «Навмисний або недбалий характер порушення», визначається виразом:

$$\mathbf{CH} = \{\bigcup_{i=1}^{n_3} \mathbf{CH_i}\} = \{\mathbf{CH_1}, \mathbf{CH_2}, ..., \mathbf{CH_{n_3}}\}, \quad (4)$$

де **CH** – множина критеріїв характеру порушення, $\mathbf{CH_i} \subseteq \mathbf{CH}$ $(i = \overline{1,n_3})$ *i*-та підмножина критеріїв характеру порушення, а n_3 їх кількість.

Наприклад, при $n_3 = 3$ $(i = \overline{1,3})$ формулу (4) можна представити як:

$$\mathbf{CH} = \{\bigcup_{i=1}^{3} \mathbf{CH_i}\} = \{\mathbf{CH_1}, \mathbf{CH_2}, \mathbf{CH_3}\},$$

де: $\mathbf{CH_1}$ = «Рівень галузевої підтримки програмної безпеки організації відповідно до міжнародних стандартів»; $\mathbf{CH_2}$ = «Наявність повідомлення контролерами керівництва про ризики, що були виявлені»; $\mathbf{CH_3}$ = «Дії керівництва на рекомендації з безпеки наглядового органу» [5].

Підмножину $\mathbf{CH_i}$ визначимо як:

$$\mathbf{CH_i} = \{\bigcup_{j=1}^{n_{3i}} CH_{ij}\} = \{CH_{i1}, CH_{i2}, ..., CH_{in_{3i}}\}, \quad (5)$$

де $CH_{ij} \subseteq \mathbf{CH_i}$ $(j = \overline{1,n_{3i}})$ – *j*-а підмножина груп критеріїв порушення, споріднених за певною темою чи близьких за певними характеристиками у межах *i*-ї підмножини, а n_{3i} кількість груп *i*-ї підмножини.

З урахування (5) вираз (4) можна представити як:

$$\mathbf{CH} = \{\bigcup_{i=1}^{n_3} \mathbf{CH_i}\} = \{\bigcup_{i=1}^{n_3} \{\bigcup_{j=1}^{n_{3i}} CH_{ij}\}\} = \{\{CH_{11}, CH_{12}, ..., CH_{1n_{3i}}\}, \quad (6)$$
$$\{CH_{21}, CH_{22}, ..., CH_{2n_{3i}}\}, ..., \{CH_{n_3 1}, CH_{n_3 2}, ..., CH_{n_3 n_{3i}}\}\},$$

Наприклад, при $n_3 = 3$ $(i = \overline{1,3})$, $n_{31} = 5$ $(j = \overline{1,5})$, $n_{32} = 2$ $(j = \overline{1,2})$, $n_{33} = 2$ $(j = \overline{1,2})$, формула (6) матиме вигляд:

$$\mathbf{CH} = \{\bigcup_{i=1}^{3} \{\bigcup_{j=1}^{n_{3i}} CH_{ij}\}\} = \{\{CH_{11}, CH_{12}, CH_{13}, CH_{14}, CH_{15}\},$$
$$\{CH_{21}, CH_{22}\}, \{CH_{31}, CH_{32}\}\},$$

де: CH_{11} = «Максимальний рівень підтримки»; CH_{12} = «Високий»; CH_{13} = «Середній»; CH_{14} = «Низький»; CH_{15} = «Незначний»; CH_{21} = «Так»; CH_{22} = «Ні»; CH_{31} = «Ігнорування»; CH_{32} = «Застосування».

Ієрархічну структуру параметра **CH** можна представити у вигляді схеми на рис. 2.

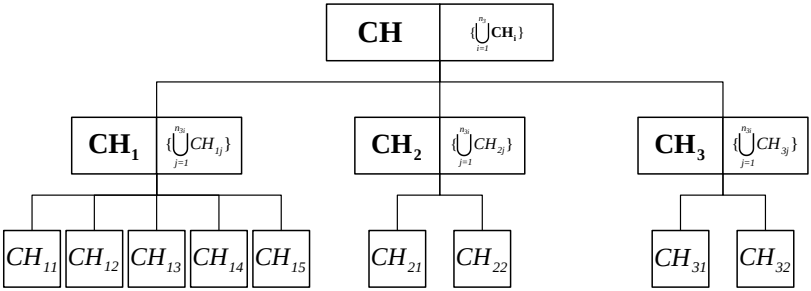


*Рис. 2. Ієрархічна структура параметра **CH***

Отже, розроблено ієрархічну структуру та теоретико-множинне представлення параметрів «Специфіка, ступінь тяжкості і тривалість порушення, зважаючи на специфіку, обсяг чи ціль відповідного опрацювання, а також кількість суб'єктів даних, які зазнали впливу, і рівень шкоди, заподіяної їм» та «Навмисний або недбалий характер порушення», що дозволить побудувати кортежну GDPR-модель, яка формалізує процес оцінювання збитків від втрати персональних даних.

Для фіналізації процесу створення GDPR-моделі в подальшому необхідно здійснити аналогічне представлення інших параметрів, що є складовими зазначеної моделі.

Анотація**. **В роботі представлено параметри «Специфіка, ступінь тяжкості і тривалість порушення, зважаючи на специфіку, обсяг чи ціль відповідного опрацювання, а також кількість суб'єктів даних, які зазнали впливу, і рівень шкоди, заподіяної їм» та «Навмисний або недбалий характер порушення» з використанням теоретико-множинних підходів для побудови кортежної GDPR-моделі, що дозволить формалізувати процес оцінювання збитків від втрати персональних даних.

Література:

1. Штрафи GDPR: кого та за що притягували до відповідальності в 2019 році // bsoprivacygroup.com: [website]. URL: https://bsoprivacygroup.com/node/44 (дата звернення: 10 березня 2020 року)

2. Дрейс Ю.О., Лозова І.Л. Розробка GDPR-моделі параметрів оцінювання наслідків витоку персональних даних // Тези доповідей ІІ Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», – Житомир: Житомирська політехніка, 2019. С. 78-79.

3. РЕГЛАМЕНТ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf (дата звернення: 10 березня 2020 року)

4. Методики и программные продукты для оценки рисков // intuit.ru: [website]. Москва: НОУ «ИНТУИТ», 2009. 7 с. URL: https://www.intuit.ru/studies/courses/531/387/lecture/8996?page=1#keyword37 (дата звернення: 15 березня 2020 року)

5. Y. Dreis, I. Lozova, A. Biskupskyi, Y. Pedchenko, Y. Ivanchenko. GDPR-model of parameters for estimating losses from loss of personal data // Inżynier XXI wieku : X Międzynarodowa Konferencja Studentów oraz Doktorantów, - Bielsko-Biała : Akademia Techniczno-Humanistyczna., 2019. C.127-136.

УДК 351.746:007-047.44

Мехед Дмитро Борисович, *к.п.н., доцент,*
НУ «Чернігівська політехніка»,
d.mekhed@gmail.com

АНАЛІЗ ЗАГРОЗ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ТА ВИЗНАЧЕННЯ МЕТОДІВ ПРОТИДІЇ ЇМ

Прогрес технологій апаратної та програмної складової призводить до появи нових загроз інформаційної безпеки. Аналіз звітної документації українських та європейських компаній, які займаються забезпеченням інформаційної безпеки, дає можливість стверджувати, що кількість унікальних кібератак у 2019 році збільшилась на 20% у порівнянні з 2018 роком. Більше половини всіх кібератак були націлені на державні підприємства, промисловість, медицину, сферу освіти та науки та фінансову галузь. Переважна кількість атак була цілеспрямованими. Зростання частки таких атак зумовлена низкою причин. По-перше, зловмисники воліють не витрачати час на масові кампанії, які не гарантують їм грошового прибутку. По-друге, щорічно з'являються нові групи зловмисників, які спеціалізуються на атаках класу APT (advanced persistent threat).

Серед основних методів атак вже котрий рік поспіль позиції лідерів займають методи соціальної інженерії. Соціальна інженерія - це термін, який використовується для позначення широкого спектру зловмисних дій, що здійснюються за допомогою взаємодії з людиною. Вона використовує психологічні маніпуляції, щоб обманом змусити користувачів робити помилки безпеки або розголошувати конфіденційну інформацію.

Атаки соціальної інженерії не тільки стають все більш поширеними в відношенні підприємств а й все більш витонченими. Атаки соціальної інженерії, як правило, включають в себе деяку форму психологічних маніпуляцій з співробітниками направлених на передачу конфіденційних даних. Зазвичай соціальна інженерія використовує у своїх методах електронну пошту або інше спілкування, яке викликає у жертви терміновість, страх або подібні емоції, змушуючи жертву надати конфіденційну інформацію, перейти за запропонованим посиланням або відкривати уражений файл.

Що робить соціальну інженерію особливо небезпечною, так це те, що вона заснована на людських помилках, а не на слабких місцях в програмному забезпеченні і операційних системах. Помилки, допущені законними користувачами, набагато менш передбачувані, що ускладнює їх виявлення та запобігання, ніж вторгнення на основі шкідливих програм.

Аналіз ідентифікованих кібератак за останні два роки, дав можливість нам класифікувати їх наступним чином:

1. Цькування.

Даний тип атак ґрунтується на завищеному рівні тривожності користувачів через фіктивні загрози. Користувачів вводять в оману, переконуючі, що їх система заражена шкідливим програмним забезпеченням, що спонукає їх встановлювати програмне забезпечення, яке не приносить реальної користі (крім як для зловмисника) або є саме шкідливим.

2. Спокуса.

Як випливає з назви, зловмисники використовують певний вид спокуси, щоб розпалити жадібність чи цікавість жертви. Вони заманюють користувачів в пастку, яка краде їх особисту інформацію або завдає шкоди їх системам.

Найбільш образлива форма спокуси використовує фізичні носії для поширення шкідливих програм. Наприклад, зловмисники залишають приманку - зазвичай заражену шкідливими програмами флешку - в помітних місцях, де їх обов'язково побачать потенційні жертви (наприклад, ліфти, автостоянка цільової компанії). Жертви підбирають її з цікавості і вставляють її в робочий або домашній комп'ютер, що призводить до автоматичної установки шкідливих програм в системі. Шахрайство зі спокусою не обов'язково проводити в фізичному світі. Онлайн форми спокушення складаються з привабливої реклами, яка веде на шкідливі сайти або спонукає користувачів завантажувати заражене шкідливим програмним забезпеченням додаток.

3. Критична ситуація.

Тут зловмисник отримує інформацію за допомогою приводу, що конфіденційна інформація від жертви потрібна для виконання критичного завдання. Зловмисник зазвичай починає з встановлення довіри зі своєю жертвою, видаючи себе за колег, співробіт-

ників поліції, банків і податкових органів або інших осіб, які мають право на отримання подібного роду інформації. Злодій задає питання, які нібито необхідні для підтвердження особи жертви, за допомогою чого вони збирають важливі особисті дані.

За допомогою цієї афери збираються будь-які дані, такі як номери соціального страхування, особисті адреси і номери телефонів, телефонні записи, дати відпустки співробітників, банківські записи і навіть інформація про безпеку, пов'язана з фізичним підприємством.

4. Фішинг.

Цикл кібератаки на основі методів соціальної інженерії можна представити наступним чином:

Рис. 1. Цикл кібератаки на основі методів соціальної інженерії

Найбільш поширені атаки соціальної інженерії походять від фішингу або копій фішингу та можуть змінюватись в залежності від поточних подій, стихійних лих, пандемій або податкового сезону. Фішинг є однією з найбільш експлуатованих форм соціальної інженерії.

Проведений аналіз та класифікація дали нам змогу сформулювати наступні рекомендації для організацій та підприємств стосовно захисту від фішингових атак:

1) Використання ефективних технічних засобів захисту:

– засоби централізованого управління оновленнями для використовуваного ПЗ;

– антивірусні програми (на всіх пристроях), в тому числі спеціалізовані, які, наприклад дозволяють користувачам відправляти підозрілі файли на перевірку перед відкриттям вкладення з листа;

– SIEM-рішення - для своєчасного виявлення атаки, якщо інфраструктура виявилась зараженою;

– автоматизовані засоби аналізу захищеності і виявлення вразливостей в ПЗ;

– мережевий екран рівня додатків (web application firewall) як превентивний захід захисту веб-ресурсів.

2) Захист даних:

– збереження конфіденційної інформації у закритому вигляді з обмеженим доступом;

– регулярне створення резервних копії систем і збереження їх на виділених серверах окремо від мережевих сегментів робочих систем;

– мінімізація привілеїв користувачів і служб;

– використання різних облікових записів і паролів для доступу до різних ресурсів;

– застосування двухфакторної аутентифікації там, де це можливо, наприклад для захисту привілейованих облікових записів.

– парольна політика, що передбачає суворі вимоги до мінімальної довжині і складності паролів;

– обмеження термінів використання паролів (не більше 90 днів).

3) Безпека персоналу:

– підвищення обізнаності працівників в питаннях ІБ;

– регулярне навчання персоналу правилам безпечної роботи в інтернеті,

– пояснення методів атак і способів захисту;

– застереження користувачів від введення облікових даних на підозрілих веб-ресурсах і тим більше від повідомлення такої ін-

формації кому б то не було по електронній пошті або під час телефонної розмови.

– пояснення порядку дій в разі підозр про шахрайство.

Анотація. Діджиталізація продовжує бути однією з основних тенденцій сучасного бізнесу, яка стає причиною використання як апробованих, так і новітніх інформаційних технологій у всіх галузях. У дослідженні зроблено аналіз актуальних загроз інформаційної безпеки та зроблений прогноз основних напрямків проведення кібератак в майбутньому. Серед існуючих загроз інформаційної безпеки вже котрий рік поспіль перші позиції займають методи соціальної інженерії. В ході проведеного аналізу автором було виділено найбільш поширені інструменти і методи, які використовуються для проведення атак соціальної інженерії. У ході дослідження сформульовано низку рекомендацій щодо захисту організацій та підприємств у контексті використання ефективних технічних засобів захисту, безпосереднього захисту даних, а також безпеки персоналу.

Література

1. Концепція технічного захисту інформації в галузі зв'язку України. [Електронний ресурс]. - Режим доступу: http://zakon1.rada.gov.ua.

2. Концепція технічного захисту інформації в галузі зв'язку України. [Електронний ресурс]. - Режим доступу: http://zakon5.rada.gov.ua/laws/show/1126-97-%D0%BF

3. Тотальна війна і комп'ютерний soft, як її головний інструмент. [Електронний ресурс]. - Режим доступу: https://zillya.ua/totalna-viina-i-kompyuternii-soft-yak-golovnii-instrument

4. Фішинг: що це таке і як себе убезпечити? [Електронний ресурс]. - Режим доступу: https://zillya.ua/fishing-shcho-tse-take-i-yak-sebe-ubezpechiti

5. Фішинг: як не стати жертвою шахрайського сайту. [Електронний ресурс]. - Режим доступу: https://gazeta.ua/articles/ema/_fishing-yak-ne-stati-zhertvoyu-shahrajskogo-sajtu/750605

УДК 004.056.5

Пашорін Валерій Іванович, *к.т.н., проф.,*
професор кафедри інженерії програмного забезпечення
та кібербезпеки
Київський національний торговельно-економічний університет
vpashorin@knute.edu.ua

Макоєдова Валентина Олександрівна,
аспірантка кафедри інженерії програмного забезпечення
та кібербезпеки
Київський національний торговельно-економічний університет
v.makoedova@knute.edu.ua

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ВСТУПНИКІВ ПІД ЧАС ПРИЙОМУ НА НАВЧАННЯ ДО ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

В епоху глобальної інформатизації питання захисту персональних даних потребує особливої уваги. Розвиток інформаційних технологій сприяв поступовому витісненню паперового документообігу й переходу на електронну документацію в багатьох сферах життєдіяльності. Освітня сфера в даному питанні не є винятком. З переходом на електронну форму подачі заяв на вступ до закладів вищої освіти (ЗВО), виникла й потреба в захисті персональних даних вступників.

Метою дослідження є аналіз сучасного стану рівня захисту персональних даних вступників у процесі проведення вступної кампанії.

Проблематика безпеки персональних даних є предметом багатьох досліджень, зокрема правовим питанням захисту персональних даних приділили увагу Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М., Єсімов С. С., Гронь О. В. та інші вчені. Проте, питання безпеки персональних даних вступників під час прийому на навчання до закладів вищої освіти є малодослідженим.

Актуальність даного дослідження зумовлена тим, що з розвитком засобів, методів і форм автоматизації процесів обробки інформації, а також масовим застосуванням персональних комп'ютерів інформація стала більш вразливою. З огляду на те,

що нині здебільшого вступники подають заяви до ЗВО в електронній формі, питання захисту персональних даних вступників потребує детального аналізу.

Захист персональних даних та його вдосконалення є предметом державного регулювання. До того ж, забезпечення дієвої системи захисту персональних даних є одним із міжнародних зобов'язань України. Виконання цього зобов'язання має значний вплив на євроінтеграційні прагнення української держави [1].

Останнім часом спостерігається суттєве зростання мережевих атак, спрямованих на доступ до персональних даних, що зберігаються в електронних базах даних організацій та підприємств з метою шахрайських фінансових дій, або «викрадення ідентичності» особистості. Протидія таким атакам, які завдають безпосередньої шкоди фізичним та юридичним особам у сфері забезпечення їх конституційних прав, стає важливим чинником кібербезпеки [2].

Особливістю персональних даних як самостійної категорії інформації, яка потребує захисту, є те, що персональні дані, які окремо можуть здаватися неважливими та не стосуються приватного життя особи, здатні скластися в узагальнюючу картину, що характеризує конкретну особу [3].

Прийом документів для вступу до навчального закладу передбачає процедури, пов'язані зі збиранням, реєстрацією, накопиченням, зберіганням відомостей про фізичних осіб – вступників.

Вступник під час подання заяви надає такі персональні дані: прізвище, ім'я, по батькові, стать, дата й місце народження, місце проживання, громадянство, паспортні дані, реєстраційний номер облікової картки платника податків, адреса електронної пошти, до якої має доступ вступник, номери телефонів, серія та номер документа про освіту, середній бал додатка до документа про освіту, користування спеціальними умовами щодо участі в конкурсному відборі, номер, пін-код та рік отримання сертифіката зовнішнього незалежного оцінювання (для вступників на основі повної загальної середньої освіти) [4].

З 2018 року криптографічний захист інформації електронних кабінетів вступників дозволяє забезпечити надійне збереження персональних даних. Проте, створені захищені канали інформації між пристроєм, з якого входить вступник, та Єдиною електрон-

ною базою з питань освіти (ЄДЕБО) можуть дещо уповільнювати роботу системи під час реєстрації кабінету, або навіть зупинити роботу сервісу реєстрації на деякий час, що підтвердилося під час масової реєстрації вступників у 2018 і в 2019 роках.

Як зауважила директор Державного підприємства «Інфоресурс» Оксана Бєлік, «під час реєстрації електронного кабінету чи першого входу до нього з нового пристрою – комп'ютера, планшета, смартфона – у веб-браузері вступника автоматично встановлюється спеціальне програмне забезпечення. Воно унеможливлює будь-яку модифікацію, видалення третіми особами даних, внесених вступником у кабінет, на шляху від пристрою до безпосередньо кабінету. Процес інсталяції є невидимим для користувача, але може викликати певне уповільнення» [5].

У листі «Щодо дотримання вимог Закону України «Про захист персональних даних» під час вступної кампанії» Міністерство освіти і науки України повідомляє про необхідність обов'язкового ознайомлення всіх вступників, які подають заяви про допуск до участі в конкурсі до закладу вищої освіти, та розміщення на стендах приймальних комісій та на сайтах навчальних закладів інформації зі статті 8 Закону України «Про захист персональних даних». Крім того, форма заяви про допуск до участі в конкурсному відборі на навчання, затверджена наказом МОН, містить інформацію про ознайомлення, що обробка персональних даних, передбачених для вступу на навчання та отримання освітніх послуг, у т. ч. в ЄДЕБО, здійснюється відповідно до законодавства про захист персональних даних.

Джерелом можливих проблем захисту персональних даних залишаються інформаційні системи закладів освіти, що мають ліцензію на інтеграцію з ЄДЕБО, які теж потребують захисту. Створюючи програмні продукти, розробники часто використовують лише стандартні засоби захисту, що надаються системою управління базами даних (СУБД). Однак, тільки провідні фірми-виробники промислових, великих СУБД займаються проблемами захисту інформації на необхідному рівні [6].

Захистити збережену в базі даних інформацію можна через програмне забезпечення, фізичний чи адміністративний контроль. Програмне забезпечення використовується для того, щоб сторонні люди не могли отримати доступ до бази даних через

шкідливе ПЗ, злом або будь-який подібний процес. Прикладом фізичного складника безпеки бази даних, може бути постійний моніторинг бази даних, для виявлення будь-яких потенційних недоліків чи загроз. Адміністративний контроль стосується таких аспектів, як використання паролів, обмеження доступу певних користувачів до деяких частин бази даних або взагалі блокування доступу окремим працівникам.

Важливо узгодити роботу фахівців із безпеки, до компетенції яких безпосередньо віднесено дане питання, з ІТ-фахівцями, які розробляють електронні системи для ЗВО. Необхідно ще на етапі проектування та розробки системи виокремити чинники, які можуть вплинути на безпеку персональних даних та забезпечити неможливість потрапляння персональних даних до сторонніх осіб [7].

Канали передачі інформації між інформаційними системами закладів вищої освіти та ЄДЕБО, та внутрішні канали передачі даних інформаційних систем також мають бути захищеними від несанкціонованого доступу. Загрози, що пов'язані з перехопленням та несанкціонованим доступом до даних у каналах передачі інформації, можуть бути спрямовані на обмеження передачі інформації, її спотворення, копіювання, неправомірне поширення чи незаконне використання [8]. Теж варто проінформувати співробітників, які відповідають за опрацювання даних, які загрози несе використання незахищених каналів передачі інформації.

Отже, у процесі проведення вступної кампанії персональні дані потребують захисту як на етапі їх внесення в систему – реєстрації в ЄДЕБО так і на етапі передачі закладам вищої освіти. Заклади вищої освіти мають належним чином приділяти увагу питанню захисту даних вступників. Тому важливо щоб системи, які застосовують ЗВО для зберігання та обробки даних абітурієнтів містили елементи програмного, фізичного та адміністративного контролю. Необхідно забезпечити дієвий механізм захисту персональних даних вступників, що відповідатиме сучасному стану розвитку інформаційно-комунікаційних технологій.

Анотація. Дана робота присвячена дослідженню проблематики захисту персональних даних вступників під час прийому на навчання до закладів вищої освіти. У роботі було проаналізовано основні методи захисту персональних даних, які мають застосовувати заклади вищої освіти у власних електронних системах інтегрованих із Єдиною електронною базою з питань освіти.

Література:

1. Бем М. В., Городиський І. М. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник / М. В. Бем, І. М. Городиський, Г. Саттон, О. М. Родіоненко ; Європейський Союз, Рада Європи – К.: К.І.С., 2015. – 220 с.

2. Яременко Н. В. Захист персональних даних інформаційно-освітнього простору / Н. В. Яременко // Медична інформатика та інженерія. – 2015. – №2. – С. 59-63.

3. Єсімов С. Персональні дані як предмет захисту права на недоторканність приватного життя / С. Єсімов // Вісник Національного університету "Львівська політехніка". Серія: Юридичні науки. – Львів : Видавництво Львівської політехніки, 2017. – № 884. – С. 120-126.

4. Марусенко Р. І. Режим персональних даних та деякі особливості навчального процесу у вищих навчальних закладах [Електронний ресурс] / Р. І. Марусенко // Право і громадянське суспільство – 2013. - №4. – С. 64-77. – Режим доступу: http://lcslaw.knu.ua/index.php/arkhiv-nomeriv/4-5-2013/item/135-rezhym-personalnykh-danykh-ta-deiaki-osoblyvosti-navchalnoho-protsesu-u-vyshchykh-navchalnykh-zakladakh-marusenko-r-i

5. МОН: електронні кабінети вступників мають найвищий рівень захисту персональних даних, але під час реєстрації це може частково уповільнювати роботу системи [Електронний ресурс] - Режим доступу: https://mon.gov.ua/ua/news/mon-elektronni-kabineti-vstupnikiv-mayut-najvishij-riven-zahistu-personalnih-danih-ale-pid-chas-reyestraciyi-ce-mozhe-chastkovo-upovilnyuvati-robotu-sistemi.

6. Струзік В. А. Аналіз засобів забезпечення додаткового захисту корпоративних баз даних / В. А. Струзік, О. В. Харкянен, С. В. Грибков // Вісник Національного університету «Львівська політехніка». Серія: Автоматика, вимірювання та керування. – Львів : Видавництво Львівської політехніки, 2017. – № 880. – С. 60-67.

7. Гронь О. В. Проблеми захисту персональних даних у контексті сучасної комунікації/ О. В. Гронь, А. К. Погореленко // Науковий вісник Ужгородського національного університету. Серія : Міжнародні економічні відносини та світове господарство. – 2018. – Вип. 19(1). – С. 102-108.

8. Філоненко С. Ф. Захист інформації в системах обробки персональних даних / С. Ф. Філоненко, В. А. Швець, І. М. Мужик // Захист інформації. - 2013. - Т. 15, № 4. - С. 307-315.

УДК 004.056:004.45

Петренко Тарас Анатолійович,
доцент кафедри кібербезпеки та математичного моделювання
Національний університет «Чернігівська політехніка»
mail_taras@ukr.net

ОСОБЛИВОСТІ УПРАВЛІННЯ ДОСТУПОМ В СУЧАСНИХ ОПЕРАЦІЙНИХ СИСТЕМАХ

Ефективність функціонування будь-якої системи захисту інформації сучасного комп'ютера багато в чому залежить від досконалості захисту його операційної системи. Операційна система є найважливішим програмним компонентом будь-якої обчислювальної системи, тому від рівня реалізації політики безпеки в кожній конкретній операційній системі багато в чому залежить і загальна безпека інформаційної системи.

Питаннями захисту інформації за допомогою механізмів операційних систем займаються вітчизняні та зарубіжні науковці: О.К. Юдін, О.М. Весельська, Блавацька Н.М., Зерко А.А., та ін. Проте постійний швидкий розвиток технологій у сфері кібербезпеки та захисту інформації повсякчас дає матеріал для нових наукових досліджень.

У сучасних операційних системах будь-який суб'єкт доступу, перед тим як почати роботу з системою, повинен пройти ідентифікацію, автентифікацію і авторизацію.[1] Саме тому ці процеси є однією з найважливіших складових системи безпеки сучасних операційних систем.

Захист ОС сімейства Unix, Windows, Mac OS у загальному випадку базується на трьох основних механізмах:

– ідентифікація й автентифікація користувача при вході у систему;

– авторизація та розмежування прав доступу до файлової системи, в основі якого лежить реалізація дискреційної моделі доступу;

– аудит, тобто реєстрація подій.[2]

Ідентифікація суб'єкта доступу полягає в тому, що суб'єкт повідомляє операційній системі ідентифікаційну інформацію про себе (логін, ім'я, ідентифікатор, тощо) і таким чином ідентифікує себе.

Автентифікація суб'єкта доступу полягає в тому, що суб'єкт надає операційній системі разом зі своїм ідентифікатором ще й автентифікуючу інформацію (зазвичай пароль), яка підтверджує, що він дійсно є тим суб'єктом доступу, який його визначила операційна система на основі ідентифікатора.

Авторизація суб'єкта відбувається після успішних ідентифікації і автентифікації. При авторизації суб'єкта операційна система виконує дії, необхідні для роботи суб'єкта в системі.

Хоча автентифікація може здійснюватися як для фізичних користувачів, так і для псевдокористувачів (наприклад, фіктивних користувачів, які використовуються операційну систему лише для запуску системних процесів), найбільший інтерес представляє саме автентифікація фізичних користувачів. Якщо в системі задіяна адекватна політика безпеки, фізичний користувач не може просто увійти в систему від імені псевдо користувача. Оскільки псевдокорситувачі мають в операційній системі зазвичай мають розширені права, вхід зловмисника в систему від імені псевдо користувача дає йому широкі можливості для здійснення несанкціонованого доступу.

Автентифікацію та ідентифікацію розмежовують на кілька типів:

1. Ідентифікація і автентифікація за допомогою імені та пароля

Процедура ідентифікації і автентифікації з використанням імені та пароля полягає в тому, що користувач вводить з клавіатури ім'я і пароль, операційна система шукає в списку користувачів запис, що належить цьому користувачу, і порівнює пароль, що зберігається в списку користувачів, з паролем, введеним користувачем. Якщо введена комбінація логіна та пароля присутня в списку користувачів, і пароль збігається з введеним, вважається, що ідентифікація та автентифікація пройшли успішно і починається авторизація користувача.

2. Ідентифікація і аутентифікація за допомогою зовнішніх носіїв ключової інформації.

У цьому випадку інформація ідентифікації і аутентифікації користувача зберігається на флеш-карті, електронному ключі, пластиковій картці тощо. При вході в операційну систему користувача вона зчитує ідентифікатор користувача (ім'я) і відповідний йому ключ (пароль).

Оскільки ключ, що зберігається на зовнішньому носії в електронному вигляді, зазвичай є набагато довшим, ніж пароль, підібрати такий ключ практично неможливо. Ключова інформація на зовнішньому носії інформації зберігається зашифрованою, що не дозволяє випадковому власникові ключа скористатися ним.

На відміну від носіїв ключової інформації на флеш-картах, електронних ключах Touch Memory або пластикових карт Memory Card інтелектуальні пластикові карти крім незалежної пам'яті містять мікропроцесор, здатний виконувати криптографічні перетворення інформації. Тому інтелектуальні карти здатні самостійно перевіряти правильність пароля на доступ до ключової інформації. При автентифікації користувача з використанням інтелектуальної карти перевірку пароля на доступ до карти виробляє не операційна система, а сама карта.

3. Ідентифікація і автентифікація за допомогою біометричних характеристик користувачів

Біометричні системи аутентифікації - системи, що використовують для посвідчення особи людей їх біометричні дані. Біометрична аутентифікація - процес докази і перевірки автентичності заявленого користувачем імені, через пред'явлення користувачем свого біометричного способу і шляхом перетворення цього образу відповідно до заздалегідь певним протоколом аутентифікації. Біометричні системи розпізнають людей на основі їх анатомічних особливостей (відбитків пальців, способу особи, малюнка ліній долоні, райдужної оболонки, голоси) або поведінкових рис (підписи, ходи) [1]. Оскільки ці риси фізично пов'язані з користувачем, біометричний розпізнавання надійно в ролі механізму, що стежить, щоб тільки ті, у кого є необхідні повноваження, могли потрапити в будівлю, отримати доступ до комп'ютерної системи або перетнути кордон держави. Біометричні системи також мають унікальні перевагами - вони не дозволяють відректися від досконалої транзакції і дають можливість визначити, коли індивідуум користується декількома посвідченнями 100 (наприклад, паспортами) на різні імена. Біометрична аутенфікація поділяється на: статичні методи (аутефікація по відбитку пальця, радужній оболонці ока, сітківці ока, геометрії руки, геометрії обличчя та термограмі обличчя) та динамічні (аутенфікація по голосу та клавіатурному почерку).

Кожна людина володіє властивим тільки її набором біометричних характеристик, до яких відносяться відбитки пальців, малюнок сітківки ока, рукописний і клавіатурний почерки тощо. Ці характеристики сьогодні теж використовуються для автентифікації користувача. Підробити біометричні характеристики практично неможливо, тому витрати зловмисника на проникнення в захищену систему можуть перевищити вигоди від проникнення.

Проте, практична реалізація даного біометричних механізмів автентифікації створює наступні проблеми.

- оскільки псевдо користувачі не є людьми і, отже, не мають біометричних характеристик, для їх автентифікації повинен підтримуватися альтернативний механізм. При цьому операційна система повинна гарантувати, що цей механізм не буде використовуватися для автентифікації звичайних користувачів.

- при двох послідовних входах в систему однієї і тієї ж людини її біометричні характеристики ніколи в точності не збігаються. Тому в процесі автентифікації доводиться використовувати математичний апарат теорії розпізнавання образів, і адаптуватися до не неминучості помилок як першого роду (успішний вхід від чужого імені), так і другого роду (відмова в доступі легальному користувачеві).[3]

Підсистема автентифікації сучасних операційних систем складається з кількох програмних модулів, пов'язаних між собою. Так в операційних системах сімейства Windows процес автентифікації WinLogon.exe і так звані бібліотеки-провайдери - замінні бібліотеки, реалізують більшу частину високорівневих функцій процесу автентифікації.

Вхід користувача в операційну систему проводиться таким чином.

1. Провайдер отримує від користувача ідентифікатор і автентифікуючу інформацію. У стандартній конфігурації в якості ідентифікуючої інформації використовується ім'я, а в якості автентифікуючої інформації - пароль.

2. Провайдер здійснює автентифікацію, передаючи ім'я і пароль за допомогою системного виклику LogonUser. При цьому, якщо автентифікація пройшла успішно, створюється маркер доступу користувача.

3. Якщо маркер доступу користувача створено успішно, провайдер здійснює авторизацію користувача, запускаючи процес Userlnit.exe від імені автентифікованого користувача. Для цього використовується системний виклик CreateProcessAsllser, який відрізняється від виклику CreateProcess тим, що процесу який запускається призначається маркер доступу, відмінний від маркера доступу процесу-батька. В даному випадку процесу Userinit призначається тільки що створений маркер доступу авторизованого користувача.

4. Процес Userinit завантажує індивідуальні настройки користувача з його профілю (profile), монтує ключ реєстру, який відповідає цьому користувачу, і завантажує програмне середовище користувача. Після цього Userlnit завершує роботу.

Розуміння процесів що відбуваються під час ідентифікації, автентифікації та авторизації користувача в сучасних операційних системах необхідне для професійної організації захищених інформаційних систем. Проте, слід зазначити що сучасні універсальні операційні системи у повному обсязі не забезпечують всі вимоги до захисту автоматизованих систем для оброблення конфіденційної інформації. Тому, вони не можуть використані без додаткових засобів захисту та застосовуватися для захисту навіть не конфіденційної інформації. Отже, для організації захищених інформаційних систем потрібно застосовувати або захищені спеціалізовані операційні системи, які відповідають державним та міжнародним стандартам у сфері кібербезпеки, або розробляти на основі сучасних універсальних операційних систем більш досконалі механізми захисту інформації.

Анотація: В роботі досліджено особливості проходження процедури ідентифікації, автентифікації та авторизації суб'єктів с сучасних операційних системах як однієї з складових забезпечення захисту інформації і інформаційних системах. Визначено, що для організації захищених інформаційних систем потрібно застосовувати або захищені спеціалізовані операційні системи, які відповідають державним та міжнародним стандартам у сфері кібербезпеки, або розробляти на основі сучасних універсальних операційних систем більш досконалі механізми захисту інформації.

Література:

1. Таненбаум Э., Бос Х. Т18 Современные операционные системы. 4-е изд. - СПб.: Питер, 2015. - 1120 с.

2. Блавацька Н.М. Аналіз відповідності засобів захисту сучасних операційних систем вимогам до оброблення конфіденційної інформації. Інформаційна безпека людини, суспільства, держави. № 2 (12). - Київ, 2013. - с. 109-115.

3. Петренко Т.А. , Лахно В.А. , Григорян Г.С. , "Розробка адаптивної системи розпізнавання кіберзагроз", Безпека українського суспільства в концепції вступу в постіндустріальне суспільство ЄС: Наукові доповіді та тези учасників науково-практичної конференції (м. Київ, 16 грудня 2015 р.), К., 2015. С. 66–76.

УДК 004.056

Полевод Олександр Миколайович, *студент групи КБ-171*
alexsnake97@gmail.com
Національний університет «Чернігівська політехніка»

Трощилов Михайло Олександрович, *студент групи КБ-171*
pchela000000@gmail.com
Національний університет «Чернігівська політехніка»

Ткач Юлія Миколаївна, *д.пед.н., доцент*
Національний університет «Чернігівська політехніка»
tkachym79@gmail.com

OPEN SOURCE INTELLIGENCE ЯК ПРОВІДНИЙ НАПРЯМ КОНКУРЕНТНОЇ РОЗВІДКИ

Вступ

На сьогоднішній день, інформатизація та діджиталізація суспільства стає майже всеохоплюючою. Крім звичних наукових статей, відомостей про життя суспільства та держави, маючи певні навички, в мережі можна знайти повну інформацію про особу або підприємство, при цьому не порушуючи закон. Це стало можливим через те, що люди з різних причин демонструють особисте життя у соціальних мережах, не замислюючись над тим, як і ким ці дані можуть бути використані. Саме тому, на нашу думку, тема пошуку по відкритим джерелам є актуальною і потребує дослідження.

Поняття OSINT

OSINT(Open Source Intelligence) – процес пошуку, збору та аналізу інформації, зібраної із відкритих джерел. Наприклад, отримання інформації про особу чи підприємство із соціальних мереж, особистих сайтів, форумів та пошукових систем.

Виділяють шість основних джерел для *OSINT*

- ЗМІ (друковані газети, журнали, радіо та телебачення з різних країн.)
- Інтернет (онлайн-публікації, блоги, дискусійні групи, медіа громадян (наприклад, відео з мобільних телефонів, вміст, створений користувачами), YouTube та інші відео-хостинги, вікідовідники та інші веб-сайти соціальних медіа (наприклад, Facebook, Twitter, Instagram та ін.). Ці джерела також випереджають безліч інших джерел через своєчасність і легкість доступу.)

- Державні дані (публічні урядові звіти, бюджети, слухання, телефонні довідники, прес-конференції, веб-сайти та виступи. Хоча ці джерела походять з офіційних джерел, вони є публічно доступними і можуть використовуватися відкрито і вільно.)
- Професійні та академічні публікації (інформація, отримана з журналів, конференцій, симпозіумів, наукових праць, дисертацій та дисертацій.)
- Комерційні дані (комерційні зображення, фінансові та промислові оцінки, бази даних.)
- Сіра література (технічні звіти, препринти, патенти, робочі документи, ділові документи, неопубліковані роботи та інформаційні бюлетені.)

Також іноді використовують метод спостереження - радіомоніторинг, використання загальнодоступних даних дистанційного зондування землі та аерофотозйомок (наприклад, Google Earth).

Методи збору інформації

1. Автоматизовані засоби. Розглянемо їх на прикладі ПЗ «Spectrum» від компанії «Інфозахист». Дане ПЗ має такі функціональні можливості:

- Автоматичний збір і аналіз активності об'єкту, що цікавить, у соціальних мережах або мережі інтернет. Аналіз взаємозв'язків, за якими була виявлена найбільша активність (лайки, коментарі тощо)
- Робота з соціальними мережами: Facebook, VK, Одноклассники, Instagram, Twitter та інші
- Робота з месенджерами
- Робота з відкритими базами даних, наприклад, «Миротворець»
- Потужний механізм аналізу даних, включаючи розпізнавання фото та повний цикл аналізу текстової інформації з авторефераванням, що працює на нейронних мережах. Модуль тестового аналізу дозволяє находити та визначити сутності (ПІБ, посади, організації, телефони, географічні назви та інші), визначати тексти, автоматично складати тематичні словники, виявляти тональність тексту. Цей модуль може використовуватись як окреме рішення для роботи з великими масивами текстової інформації.

Аналогами є наступні програми:

- Spiderfoot
- theHarvester
- Recon-ng

2. Сервіси. Вони надають можливість отримати важливі дані про веб-сайт підприємства або персональні сайти. Сервіси можуть надати наступну інформацію:

- Перелік активних мережевих вузлів та портів
- Перелік імен співробітників
- Перелік поштових адрес
- Перелік субдоменів
- Перелік зовнішніх Java-скриптів
- API-ключі
- Акаунти у соціальних мережах
- Пошук за іншими зовнішніми базами

Найбільш популярними та функціональними сервісами такого роду є Shodan, Threatcrowd, DnsDumpster.

3. SOCMINT. Даний підрозділ OSINT спрямований на роботу із соціальними мережами. Вже існує велика кількість онлайн-інструментів для збору інформації у найпопулярніших соцмережах(LinkedIn, Facebook, Twitter, Instagram). Далі наведено перелік найбільш потужних із них:

- Stalkscan - показує всю публічно доступну інформацію про людину.
- Foller - показує інформацію про будь-який відкритий акаунт, включаючи число твітів і підписників, списки, хештеги і згадки.
- Tinfoleak - показує девайси, операційні системи і соціальні мережі, які використовуються користувачем. Також показує локації, співвідносячи твіти користувача з місцями в Google Earth.
- InSpy - Python-програма, яка вміє знаходити працівників тієї чи іншої компанії. Також знаходить технології, що застосовуються в компанії, за заданими ключовими словами.
- www.picodash.com - надає статистику по підписниках конкретного користувача або обраного хештега в форматі CSV. Також відображає лайки і коментарі.

4. Мануальний пошук. Даний метод включає в себе моніторинг популярних веб-ресурсів на наявність інформації про особу/підприємство.

Якщо з усього перерахованого вище потрібно провести тільки декілька перевірок, тоді можна обійтися без встановлення додаткових програм. А якщо проводиться ретельний і тривалий пошук, краще скористатися спеціальним ПЗ, яке допоможе заощадити час.

Далі розглянемо як можна застосувати дану методику на практиці: перш за все, висока обізнаність зловмисника про особу/підприємство значно спрощує застосування одного із найефективніших методів соціальної інженерії:

Таргетований фішинг – можливість розповсюджувати фішингові повідомлення, складені так, що жертва не виявить обману с більшою вірогідністю.

Іншим застосуванням зібраної інформації може бути планування масштабної кібер-атаки на веб-ресурс особи чи підприємства. Така атака нанесе більш серйозних збитків, адже можливі точки входу до системи, були знайдені раніше.

З іншого боку дану методику можна використати і для попередження дій зловмисників. Пошук за відкритими джерелами – ефективний спосіб зрозуміти, як виглядає організація з точки зору зовнішнього потенційного зловмисника. Цей набір заходів дозволяє оперативно оцінити потенційні точки входу до інфраструктури і почати опрацювання заходів для превентивної боротьби із злочинною активністю.

Під час дослідження всіх аспектів даної теми, нами було розроблено концепт програмного модулю для автоматизованого збору інформації про особу у соціальних мережах шляхом розпізнавання обличчя. Далі наведено приблизний алгоритм роботи модулю:

1. Навчена нейромережа аналізує обличчя особи на фото, визначаючи його характерні риси.

2. Шляхом порівняння отриманих даних обличчя із даними обличь акаунтів у соціальних мережах(Facebook та Instagram) програма створює звіт, який містить усі можливі збіги. Для оптимізації даного процесу рекомендується задавати регіон пошуку.

3. Користувач із наведеного переліку обирає найбільш вірогідний збіг за даними. Програма формує досьє по даній особі, використовуючи інформацію із акаунтів.

Перевагою розробленого нами алгоритму є можливість отримати досьє, не порушуючи чинне законодавство України. Подальшим розвитком даного дослідження є програмна реалізація алгоритму у вигляді пошукового модуля.

Провівши дослідження методики пошуку у відкритих джерелах, визначивши основні джерела та способи збору інформації, ми можемо зробити висновок, що OSINT є потужним інструментом для конкурентної розвідки, збирання досьє на осіб, тощо. На основі зібраних даних можна проводити як малі так і масштабні кібер-атаки, застосовувати інформацію для складання таргетованої фішинг-розсилки, яка буде ефективніша від звичайного спаму. Ще одним можливим застосуванням даної методики пошуку є попередження описаних вище загроз особі чи підприємству.

На нашу думку, більш глибоке вивчення OSINT сприятиме розвитку галузі конкурентної розвідки та підвищить ефективність роботи агентів.

Анотація. У даних тезах проведено дослідження одного із найперспективніших напрямків конкурентної розвідки – OSINT. Було розглянуто основні джерела та методи пошуку. Другим кроком у дослідженні став опис можливих шляхів застосування зібраних даних. Отримані результати показали, що даний напрям є потужним інструментом як і для зловмисників, так і фахівців із інформаційної безпеки.

Література:

1. Сбор информации из открытых источников [Електронний ресурс] – Режим доступу до ресурсу:https://www.antimalware.ru/analytics/ Threats Analysis/Gathering-information-the-way-cybercrooks-see-you

2. Возрастающая роль OSINT [Електронний ресурс] – Режим доступу до ресурсу: https://www.securitylab.ru/blog/personal/ Business without danger/344893.php

3. Целенаправленные атаки: разведка на основе открытых источников (OSINT) [Електронний ресурс] – Режим доступу до ресурсу:https://xakep.ru/2018/05/14/osint/.

4. Розвідка на основі відкритих джерел [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D0%B7%D0%B2%D1%96%D0%B4%D0%BA%D0%B0_%D0%BD%D0%B0_%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D1%96%D0%B2%D1%96%D0%B4%D0%BA%D1%80%D0%B8%D1%82%D0%B8%D1%85_%D0%B4%D0%B6%D0%B5%D1%80%D0%B5%D0%BB

5. Как найти информацию о человеке: Гид по OSINT-инструментам. [Електронний ресурс] – Режим доступу до ресурсу: https://factcheck.kz/metodika-fch/kak-najti-informaciyu-o-cheloveke-gid-po-osint-instrumentam/.

6. Разведка и сбор информации с открытых источников. [Електронний ресурс] – Режим доступу до ресурсу: https://tgraph.io/Razvedka-i-sbor-informacii-s-otkrytyh-istochnikov-12-03.

УДК 004.492.4

Постол Тетяна Геннадіївна, *бакалавр*
tanua.p0st0l@gmail.com

Ткач Юлія Миколаївна*, д.пед.н., доц.,*
завідувач кафедри кібербезпеки та математичного моделювання,
Національний університет «Чернігівська політехніка»
tkachym79@gmail.com

ДОСЛІДЖЕННЯ ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ АНТИВІРУСНИХ ПРОГРАМ

На сьогоднішній день в світі існує більше 1 мільйона комп'ютерних вірусів. Як і раніше єдиним ефективним засобом боротьби з шкідливим програмним забезпеченням (ПЗ) є антивірус.

Антивірусні програми призначені для захисту комп'ютера від загроз (програми-шпигуни, шкідливі програми, віруси, трояни, хробаки), які можуть завдати шкоди вашим файлам, викрасти ваші особисті дані і зробити дуже повільною і проблематичною роботу вашого комп'ютера і веб-з'єднання.

Шкідливі програми стали мати настільки високий рівень складності, що, незважаючи на всі останні інновації, захист вашого комп’ютера може бути під загрозою, якщо у вас не встановлена антивірусна програма.

Принцип роботи антивірусів. Будь-який антивірусний продукт, будь то Avira, Avast, NOD32 і не тільки, працює за тим же принципом, що і вірус:

- стежить за трафіком;
- переглядає порти;
- видаляє і модифікує файли;
- править реєстр;
- збирає статистику і відправляє її розробнику.

Розглянемо дії антивірусного програмного забезпечення та шлях, який проходить ресурс (файл, програма та інформації) при процесі аналізу (рисунок 1):

1. Експертній аналіз виявлених небезпечних файлів, ресурсів, функцій тощо (аналіз здійснюється за допомогою бази даних небезпечних функцій)

2. Верифікація системою штучного інтелекту виявлених небезпечних файлів, ресурсів, функцій тощо (здійснюється за допомогою бази знань верифікації небезпечних функцій).

3. Логічний висновок про властивості виявлених загроз, вірусів і програмних закладок.

4. Автоматичне формування алгоритмів лікування ресурсів, файлів (деактивація небезпечних функцій).

5. Автоматичне лікування файлів, ресурсів і формування звіту.

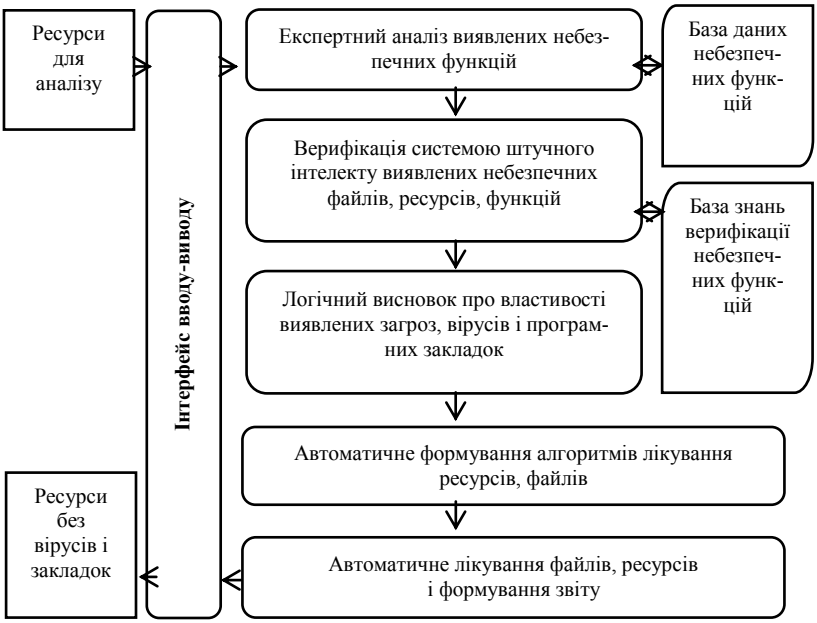


Рисунок 1 – дії антивірусної програми під час аналізу ресурсів

Є багато різних варіантів для користувачів комп'ютерів в області антивірусного програмного забезпечення.

Розглянемо основні функціональні можливості антивірусного ПЗ:

Захист від загроз в реальному часі. Це базова функція всіх антивірусних програм, що представляє собою щосекундний моніторинг активності комп'ютера і своєчасний захист від усіх отриманих загроз.

Антиспам – модуль, що фільтрує поштовий трафік, відправляючи підозрілі листи в окрему папку, де при відкритті листів блокуються мультимедійні дані з метою запобігти проникненню черв'яків. Також здійснюється фільтрація рекламного і агітаційного спаму.

Антифішинг – модулі, спрямовані на своєчасне блокування сторінок-копій, які збирають особисті дані користувачів.

Firewall – захищає комп'ютер від вхідних і вихідних несанкціонованих спроб підключення, як в локальних мережах так і в Інтернеті. Фактично він виконує функції охоронця на вході: відстежує спроби підключення і визначає, які підключення слід дозволити, а які потрібно заблокувати.

Сканування за запитом – це сканування на вимогу всієї файлової системи або окремих файлів і папок. допомогою сканера за запитом користувача

Постійний захист – забезпечує безперервний захист від широкого спектра загроз, скануючи всі доступні файли і повідомлення електронної пошти.

Сканування під час завантаження – це вдосконалена функція, розроблена для перевірки системи на наявність загроз. Сканування почнеться при наступному завантаженні комп'ютера. Ця функція дозволяє перевірити персональний комп’ютер (ПК) на наявність всіх відомих типів шкідливих програм і видалити загрози ще до запуску операційної системи і інших служб.

Евристичний алгоритм – це алгоритм для виявлення шкідливих програм, при якому антивірусна програма контролює всі дії, що виконуються програмою якою перевіряється. В ході евристичного аналізу відслідковуються потенційно небезпечні дії, характерні для вірусів і шкідливих програм інших типів. Тобто, антивірус використовує евристичний аналізатор, який являє собою певний набір правил. Система використовує ці правила, щоб на основі даних, наданих технічним компонентом, винести рішення про те, чи є аналізована програма або аналізована подія шкідливою.

Робота в хмарі – це мережева комп'ютерна система, що надає інформаційні та обчислювальні послуги, ізолюючи користувача від підтримує інфраструктури (серверів, систем зберігання, комп'ютерних мереж, програмного забезпечення) і забезпечую-

чи зручний мережевий доступ до потрібного кількості ресурсів, швидко виділяючи і звільняючи їх у міру необхідності в автоматичному режимі.

Система виявлення вторгнень – призначена для виявлення фактів несанкціонованого доступу до комп'ютерної системи чи мережі або несанкціонованого управління ними в основному через Інтернет.

Система запобігання вторгнень – захищає від шкідливих програм і іншої небажаної активності, які намагаються негативно вплинути на безпеку комп'ютера.

E-mail захист – перевіряє всі листи на наявність шкідливих елементів і спаму.

Веб-захист – це додатковий рівень активного захисту, який в режимі реального часу сканує дані, що передаються під час перегляду веб-сторінок, запобігаючи скачуванню і запуску на вашому ПК шкідливого ПЗ (шкідливих сценаріїв і т. д.).

Автоматичне оновлення - компонент, що забезпечує своєчасне оновлення інших модулів антивіруса і вірусних баз. Виконує оновлення антивірусної бази з сервера фірми-виробника цього антивіруса. У зв'язку з постійною появою нових зразків вірусів даний модуль повинен запускатися як можна частіше, а краще залишити його працювати постійно.

Виконаємо порівняння популярних безкоштовних антивірусних програм: Avast Free Antivirus, AVG AntiVirus Free, 360 Total Security, Avira Free Antivirus та Bitdefender Antivirus Free Edition.

Із таблиці 1 стає зрозуміло, що при тестуванні антивірусних програм, щодо їх взаємодії з системою, найкращий результат показав Avast Free Antivirus.

Можу зазначити, що Bitdefender Antivirus Free Edition Free і 360 Total Security трохи поступаються в швидкості сканування Avast, в той час як AVG AntiVirus Free та Avira Free Antivirus не відстають від нього. Щодо використання пам'яті, то Avira, AVG і 360 Total Security споживають значно більший обсяг пам'яті, ніж Avast і Bitdefender. Також можна помітити, що здійснюється велике використання процесора антивірусами AVG та Bitdefender. Час завантаження системи з антивірусом складає від 1 до 3-х хвилин. Найгірший результат показав антивірусний продукт Avira. Найкращий – Avast, AVG та Bitdefender.

Таблиця 1

Порівняння безкоштовних антивірусних програм

Функціональні можливості	Avast Free Antivirus	AVG AntiVirus Free	360 Total Security	Avira Free Antivirus	Bitdefender Antivirus Free Edition
Наявність російської мови	+	+	+	+	-
Сканування за запитом	+	+	+	+	+
Сканування під час завантаження	+	+	+	+	+
Евристичний алгоритм	+	+	+	+	+
Робота в хмарі	+	-	+	-	+
Вбудований firewall	+	-	-	-	-
Система виявлення вторгнень	+	-	-	-	-
Система запобігання вторгнень	-	-	-	-	-
Постійний захист	+	+	+	+	+
E-mail захист	+	+	-	+	-
Антиспам	+	-	-	+	-
Антифішинг	+	-	+	+	+
Веб-захист	+	+	+	+	+
Автоматичне оновлення	+	+	+	+	+
Хибні спацювання	0,03%	0,17%	0,18%	0,16%	0,12%
Час завантаження системи з антивірусом	1 хв.	1 хв.	2 хв.	3 хв.	1 хв.
Час сканування системних папок	10 хв.	10 хв.	15 хв.	10 хв	20 хв.
Використання процесора	2,5%	16,5%	3,5%	5,5%	15%
Використання пам'яті	40mb	130mb	120mb	175mb	85mb

Таким чином, найоптимальнішим варіантом є антивірусна програма Avast Free Antivirus, що показала хороший результат і при огляді функціоналу, і при тестуванні.

Що стосується недоліків антивірусних програм, то можна відокремити такі недоліки:

- потребують досить великої кількість оперативної пам'яті, що позначається на роботі системи ПК;

- значне використання процесора, що призводить до навантаження на системні ресурси;

- можна помічати хибні спрацювання.

Розглянемо ці недоліки, та надамо можливі рекоментації

Використання процесора та оперативної пам'яті – через особливості роботи евристичного аналізатора та широкого функціоналу який дозволяє антивірусному програмному забезпеченню швидко працювати та надавати належний захист комп'ютеру, антивірус використовує системні ресурси, тобто попросту кажучи, антивірус споживає пам'ять на процесор, що в результаті відображається на роботі комп'ютера.

Майже в усіх антивірусних програмних забезпеченнях споживання системних ресурсів є значною проблемою і часто перед користувачем стоїть вибір між надійним захистом та швидкою роботою комп'ютера.

Нажаль розробники ще працюють над вирішенням цієї проблеми. Тож аби хоч якось знизити навантаження на оперативну пам'ять необхідно перевірити через Диспетчер завдань наявність/відсутність додаткових процесів, які відносяться до антивірусу і можуть використовувати ресурси. Налаштувати графік автоматичного запуску сканування системи, а також необхідно переконатися в коректній роботі самого жорсткого диска (або SSD).

Щодо хибних спрацювань, то можу сказати, що це найбільш вагома проблема всіх антивірусних програм. З метою мінімізації випадків помилкового спрацювання антивірусної програм, компанія-розробник постійно повинна збільшувати потужності тестового центру антивірусної лабораторії, в якій проходять тестування всі вірусні бази, перед тим як потрапити в оновлення антивірусних баз.

Наскільки відомо, то компанії-розробники антивірусних програм активно і динамічно шукають нові шляхи усунення неполадок такого плану, однак повністю виключити помилкові спрацьовування не вдається.

Вся справа в методі евристичного аналізу, технологія якого дозволяє виявляти раніше невідомі віруси. Методи евристичного сканування не забезпечують будь-якого гарантованого захисту

від вірусів, які відсутні в сигнатурному наборі. Це відбувається через використання в якості об'єкта аналізу сигнатур раніше відомих вірусів, а в якості правил евристичної верифікації - знань про механізм формування коду, яка також не повинна бути постійною і видозмінюється при кожному новому зараженні. Цей метод пошуку базується на емпіричних припущеннях, з цієї причини повністю виключити помилкові спрацьовування не можна.

Тож слід зазначити, що будь-який антивірусний продукт має майже аналогічні функціональні можливості та дії під час моніторингу ресурсів, лікуванні. А також в антивірусних програмах присутні деякі недоліки, над якими слід працювати розробникам. Виходячи з попередньо проведеного дослідження, було з'ясовано, що непоганим варіантом для захисту вашого ПК є антивірусна програма Avast Free Antivirus, яка показала непоганий результат.

Анотація. В ході дослідження розглянуто принцип роботи антивірусних програм та їх дії під час аналізу ресурсів і лікуванні. Також визначено функціональні можливості антивірусів та здійснено порівняння чотирьох відомих безкоштовних антивірусних продуктів: Avast Free Antivirus, Panda Antivirus, AVG AntiVirus Free, 360 Total Security, Avira Free Antiviru та Bitdefender Antivirus Free Edition. Досліджено недоліки антивірусів, визначено їх причини та надано рекомендації для їх усунення.

Література:

1. Методика використання антивірусних програм [Електронний ресурс]. – ua-referat – Режим доступу: http://ua-referat.com/Методика_використання_антивірусних_програм

2. Как работает антивирус [Електронний ресурс]. – USERON.RU – Режим доступу: https://useron.ru/bezopasnost/274-kak-rabotaet-antivirus.html

3. Рейтинг антивирусов 2020 - Выбираем лучший антивирус [Електронний ресурс]. – СофтКаталог – Режим доступу: https://softcatalog.info/ru/obzor/reyting-antivirusov

4. Тест проактивной антивирусной защиты [Електронний ресурс]. – ANTI-MALWARE – Режим доступу: https://www.anti-malware.ru/proactive_test_2010

УДК 004.056.5

***Потій Олександр Володимирович**, професор, д.т.н.,*
АТ «Інститут інформаційних технологій»
potav@ua.fm

***Гавриленко Олексій Вадимович**, к.т.н.,*
gavrylav@gmail.com

***Бондаренко Василь Миколайович**,к.т.н.,*
bbazil@ukr.net
Адміністрація Держспецзв'язку

НАПРЯМИ РОЗВИТКУ НАЦІОНАЛЬНОЇ НОРМАТИВНОЇ БАЗИ НИЖНЬОГО РІВНЯ З ПИТАНЬ БЕЗПЕКИ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Національне нормативне забезпечення в сфері безпеки інформації та кібербезпеки є ключовим фактором підтримки державної політики, сприяє впровадженню інновацій та сучасних підходів до захисту інформації, забезпечує охорону інтересів держави, суспільства та окремих громадян в інформаційній сфері та економію всіх видів ресурсів. Тому питання розвитку та підтримки в актуальному стані нормативної бази із забезпечення безпеки інформації в інформаційно-комунікаційних системах з урахуванням сучасних викликів, що постали перед Україною в інформаційній сфері, набувають особливого значення.

Світові тенденції до посилення загроз інформаційної та кібербезпеки, підвищення рівня вразливості інформаційно-комунікаційних систем, промислових систем (SCADA-систем), IoT-систем обумовлюють необхідність розробки та впровадження нових стандартів та нормативних документів з безпеки інформації, що впроваджують нові технології та передовий практичний досвід із захисту інформації.

З урахуванням потреб національної безпеки України та необхідності запровадження системного підходу до розв'язання проблеми забезпечення безпеки інформації критичних інформаційних ресурсів держави на загальнодержавному рівні, удосконалення системи нормативного забезпечення у галузі ін-

формаційної та кібербезпеки є одним із пріоритетів у діяльності Держспецзв'язку та інших органів державної влади, приватного та громадського сектору. Сформована за останні часи система нормативного забезпечення захисту інформації має бути реформована, яка в умовах глобалізації ризиків інформаційної безпеки, ведення гібридної війні проти України, створить умови реального забезпечення безпеки інформації на об'єктах критичної інфраструктури держави.

Існуючі проблеми нормативного забезпечення обумовлені стрімким розвитком нових методологій та підходів до захисту інформації та кібербезпеки на організаційному та системного рівнях, браком ресурсів на розробку та впровадження нових, системних нормативних документів, використанням застарілих нормативних документів та підходів, що не відповідають сучасним реаліям та загрозам безпеки інформації та є стримуючим фактором у досягненні с стратегічних цілей в сфері кібербезпеки.

За окремим напрямками нормативного забезпечення сфері захисту інформації ефективність та значущість національних нормативних документів знижується, оскільки вони в неповній мірі відображають результати науково-технічного прогресу. До того ж рівень їх гармонізації з міжнародними стандартами є недостатнім. Темпи оновлення та актуалізації нормативних документів із захисту інформації та кібербезпеки за останні роки знизились.

Проблеми існуючої нормативної бази в сфері захисту інформації не дозволяють в повній мірі забезпечити необхідний рівень кібербезпеки національних інформаційних ресурсів, вирішувати питання побудови ефективної системи захисту інформації на об'єктах критичної інфраструктури відповідно до існуючих загроз та світових тенденцій в цій сфері.

Тому модернізація системи нормативного забезпечення захисту інформації та кібербезпеки, спрямованої на забезпечення впровадження сучасних підходів на організаційному рівні та рівні інформаційно-комунікаційних систем (далі - ІКС), підвищення рівня захищеності національних інформаційних активів має здійснюватися на основі комплексного вибору пріоритетів розвитку нормативної бази у відповідності до стратегічних цілей, завдань та напрямків розвитку нормативного забезпечення в сфері безпеки інформації та кібербезпеки.

Отже, до основних проблем нормативного забезпечення, що потребують розв'язання, можливо віднести:

- недостатній рівень гармонізації нормативних документів системи технічного захисту інформації (НД ТЗІ) з вимогами міжнародних стандартів, особливо стандартів системи управління інформаційною безпекою (серії ISO/IEC 27k), стандартів з проектування та оцінки безпеки систем інформаційних технологій (серії ISO/IEC 15408) та інших міжнародних стандартів.

- необхідність переходу від існуючої моделі створення КСЗІ та нову модель забезпечення безпеки інформації в ІКС та організаційних системах, що базується на підході управління ризиками;

- недостатність фінансових та людських ресурсів для забезпечення оперативного реагування на нові виклики в галузі безпеки інформації та кібербезпеки шляхом закріплення нових вимог та моделей безпеки у нормативних документах;

- невідповідність існуючої системи розробки та впровадження нормативних документів в сфері захисту інформації та кібербезпеки сучасним вимогам щодо впровадження інновацій та швидкості оновлення нормативних документів;

- нерозвиненість державно-приватного партнерства у сфері розроблення та впровадження нормативних документі в галузі інформаційної та кібербезпеки;

- брак професійних кадрів які володіють компетенціями, що дозволяють швидко засвоювати та впроваджувати вимоги нових нормативних документів в сфері безпеки інформації та кібербезпеки.

Відповідно, головними цілями модернізації нормативної базі з питань безпеки інформації в ІКС повинні бути: запровадження системного підходу до забезпечення безпеки шляхом розробки та впровадження нормативних документів, які забезпечують імплементацію вимог законодавства ЄС, міжнародних стандартів та найкращих світових практик в галузі безпеки інформаційних технологій, передовий практичний досвід інших країн в галузі безпеки інформації, трансформацію вимог нормативних документів системи технічного захисту інформації та впровадження нових моделей та вимог безпеки у практичну діяльність із захисту інформації державних органів, установ, організацій, підприємств та розробників систем та засобів захисту інформації.

До напрямів розвитку системи нормативного забезпечення з питань забезпечення безпеки інформації в ІКС можуть бути віднесені: удосконалення законодавчих основ розробки нормативних документів у сфері забезпечення безпеки інформації в КІС; підвищення ролі нормативного забезпечення у вирішення державних завдань в сфері інформаційної та кібербезпеки; розвиток організаційно-функціональної структури системи нормативного забезпечення системи забезпечення безпеки інформації та кібербезпеки; розвиток економічних основ нормативного забезпечення галузі; розвиток нормативної бази галузі; удосконалення інформаційного забезпечення в області нормативного забезпечення безпеки інформації і кібербезпеки; удосконалення взаємодії з міжнародними та регіональними організаціями зі стандартизації в сфері інформаційної безпеки; підготовка кадрів в сфері безпеки інформації та кібербезпеки.

Першочергові заходи в частині модернізації нормативної бази України з питань забезпечення безпеки інформації в ІКС передбачається реалізувати рамках виконання наступних етапів (завдань):

До основних завдань з адаптації до вимог ЄС та міжнародних стандартів належить (орієнтовний термін виконання - 2020 рік):

1. Розробка Закону України «Про безпеку інформації та інформаційно-комунікаційних систем» (ІКС) закону на заміну Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», а також розробка (удосконалення) відповідних підзаконних нормативно-правових актів (розміщений для громадського обговорення на офіційному веб-сайті Держспецзв'язку).

2. Розробка нормативних документів нижнього (не законодавчого) рівня - системоутворюючого нормативного документу, який встановлюватиме порядок впровадження концепції управління ризиками в державних органах, на підприємствах, в організаціях, в інформаційно-телекомунікаційних системах яких обробляється інформація, вимога щодо захисту якої визначена в законі, та початок розробки першочергових базових нормативних документів на основі підходів ISO 27k та NIST;

На сьогодні в Україні функціонує законодавчо закріплена нормативно-правова база, яка в повному обсязі забезпечує вирішення питання захисту інформації у вітчизняних інформацій-

них системах, від створення до підтвердження відповідності. При цьому нормативна база безпосередньо не застосовує сучасного ризик орієнтованого підходу до захисту інформації (хоча і надає таку можливість) та є нединамічною відносно оперативного реагування на появу нових загроз.

Паралельно в державі здійснюється гармонізація нормативних документів з міжнародними стандартами у сфері інформаційної безпеки. Модель забезпечення безпеки на основі цих стандартів є вільною від основних недоліків існуючої системи і включає ряд гармонізованих на сьогодні стандартів, основні з яких ДСТУ ISO/IEC 27001 [1] та ДСТУ ISO/IEC 15408 [2] (та його інші частини). Модель не забезпечує підтвердження відповідності в Україні в інформаційних системах. Підтвердження може здійснюється відповідно до ISO/IEC 27001, який є стандартом з менеджменту та потребує інтерпретації на конкретному об'єкті.

NIST США впроваджує як методологічну основу забезпечення інформаційної та кібербезпеки концепцію Risk Management Framework (RMF – рамкова модель управління ризиками). Концепція RMF впроваджує структурований, гнучкий підхід до управління ризиками, що пов'язаний із впровадженням інформаційних систем у бізнес-процеси організації. Концепція RMF викладена у NIST SP 800-37 (Rev 2) [3].

Модель забезпечення безпеки інформації на основі стандартів NIST (США) також, як і європейська, є вільною від недоліків вітчизняної нормативної бази та має суттєву перевагу: подібність до української за порядком створення та оцінювання в КІС. Це може спростити сприйняття моделі суб'єктами системи захисту та створює підґрунтя для адаптації на її основі нормативної бази України. Модель містить комплексний підхід з підтвердження відповідності в інформаційних системах, проте, як і попередня, на сьогодні не забезпечує такого підтвердження в Україні.

Основними превагами моделі захисту на основі стандартів NIST (США) є максимальна повнота заходів безпеки порівняно з європейською і міжнародною (середня повнота заходів) та вітчизняною (порівняно низький рівень), а також можливість інтегрування вимог європейських та міжнародних стандартів під час проектування систем захисту інформації. Тому адаптація цієї мо-

делі може бути перспективним напрямком розвитку нормативної бази, в першу чергу, нижнього (не законодавчого) рівня у сфері захисту інформації в ІКС для України.

Розроблений на основі цього підходу в рамках науково-дослідних робіт на замовлення Адміністрації Держспецзв'язку системоутворюючий нормативний документ містить порядок дій з впровадження ефективних, результативних та економічно вигідних процесів управління ризиками для забезпечення безпеки критичних активів і систем, зокрема, процесів:

- підготовки організації до впровадження процесу управління ризиками безпеки на рівнях організації, бізнес-процесів, ІКС;
- категоріювання інформаційної системи та інформації, яка обробляється, зберігається та передається в ІКС;
- вибору і налаштування початкового набору заходів для ІКС з метою зменшення ризиків до допустимого рівня на основі оцінки ризиків;
- реалізації заходів безпеки та опису того, як виконуються заходи безпеки в ІКС та у її робочому середовищі;
- оцінювання заходів безпеки, з метою визначення їх ефективності, тобто, чи задовольняють вони вимогам безпеки;
- акредитації ІКС або застосовуваних заходів безпеки на основі визначення того, що ризик для операцій і активів організацій, фізичних осіб, інших організацій і держави є допустимим;
- моніторингу ІКС та пов'язаних з цим заходів, включаючи оцінку ефективності заходів безпеки, документування змін у системі та робочому середовищі, проведення оцінки ризиків та аналізу впливу втрат, а також звітування про стан безпеки ІКС.

До завдань з розробки та удосконалення нормативних документів з урахуванням адаптованих вимог, можуть бути віднесені:

1. Розробка базових нормативних документів та модифікація існуючих нормативних документів, які підтримують базові документи;
2. Впровадження нових підходів у практику діяльності із забезпечення безпеки інформації державних органів (установ) підприємств, об'єктів критичної інформаційної інфраструктури;
3. Впровадження вимог та рекомендації нових нормативних документів у практику розробників систем та засобів захисту інформації;

4. Удосконалення системи державної експертизи, аудиту та сертифікації в галузі інформаційної безпеки.

До завдань з впровадження та підтримки, які виконуються на постійній основі, можуть бути віднесені

1. Завершення створення та забезпечення ефективного функціонування системи нормативного забезпечення безпеки інформації;

2. Подальше впровадження нових підходів у практику діяльності із забезпечення безпеки інформації державних органів (установ) підприємств, об'єктів критичної інформаційної інфраструктури;

3. Впровадження на постійній основі вимог та рекомендації нових нормативних документів у практику розробників систем та засобів захисту інформації;

4. Актуалізація розроблених нормативних документів на постійній основі;

5. Удосконалення освітніх програм та утворення організаційних основ системи підготовки кадрів з безпеки інформації в ІКС з урахуванням вимог удосконаленої нормативної бази.

Анотація. В роботі розглянуто існуючі проблеми нормативного забезпечення в сфері безпеки інформації та кібербезпеки, сформульовано проблеми чинної нормативної бази з питань захисту інформації в інформаційно-комунікаційних системах, визначено цілі та напрямки та першочергові заходи її модернізації. Зроблено огляд відомих моделей стандартизації з безпеки інформації в ІКС та визначено на його основі перспективний напрямок розвитку нормативного забезпечення, наведено перелік процесів, що міститься у проекті системоутворюючого нормативного документа, який встановлює порядок впровадження концепції управління ризиками в державних органах, на підприємствах, в установах, організаціях.

Література.

1. ДСТУ ISO/IEC 27001: 2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

2. ДСТУ ISO/IEC 15408-2:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2009; IDT).

3. NIST Special Publication 800-37, Revision 2. Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy, Joint Task Force May 2018.

УДК 004.056.4

Рзаєва Світлана Леонідівна, *кандидат технічних наук, доцент*
Київський національний торговельно-економічний університет,
Київ, Україна
rzaevasl@ukr.net

Рзаєв Дмитро Олександрович*, старший викладач*
Київський національний економічний університет
імені Вадима Гетьмана, Київ, Україна
ditomas @ukr.net

ВИКОРИСТАННЯ КОМПЛЕКСНОГО ПІДХОДУ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ AUTOMATIC SALES FUNNEL

Постановка проблеми. Основними напрямами ефективним управління бізнесом є збільшення продажу товарів або послуг із залученням нових потенційних клієнтів через мережу Інтернет. Наразі, в українському бізнес-середовище застосовується нова інформаційна система – automatic sales funnel (автоматизована воронка продажу), яка здатна робити продажі товарів у автоматичному режимі, рушійною силою даного продажу виступає цілеспрямований бот з приєднанням CPM системи, приєднаного до соціальної мережі. Головне завдання проекту – збільшення обсягу продажів продукту компанії, без участі менеджерів з продажу, та захист інформаційних потоків від несанкціонованого втручання і крадіжки інформаційних даних.

Формулювання завдання (мети) дослідження: за посередництвом різних сценаріїв продажів, що входять до складу інформаційної системи automatic sales funnel, збільшити численність потенційних клієнтів, які хоч раз відвідали сторінку, не загубилися і не зникли в нескінченному інформаційному потоці, а були м'яко підведені до покупки. При цьому необхідно забезпечити не тільки збільшення онлайн продажів товарів, а й максимальну ефективність та надійність захисту інформаційних потоків інформаційної системи automatic sales funnel. Однак, на сьогодні ще недостатньо досліджено систему захисту інформаційних потоків інформаційної системи automatic sales funnel від кібератак, тому дана тематика є актуальною.

Новизною виступає розробка програмного забезпечення інформаційної системи automatic sales funnel та системи захисту інформаційних даних від кібератак унікального бізнесу.

Короткий виклад розв'язку поставленої задачі. Automatic sales funnel (автоматичні воронки або автоворонки) – це послідовність дій, які спочатку знайомлять потенційного клієнта з продуктом, а потім ведуть до здійснення нових і нових покупок. Ознайомлення з товаром або послуою та її подальшим придбанням здійснюється на автоматичному рівні. Автоматична воронка продажів означає, що вказані дії виконуються за допомогою автоматичних інструментів, а не вручну. Варіанти реалізації можуть бути різні, але, як правило, існує фіксований комплекс дій – сценарій, який здійснюється за допомогою інструментів автоматизації маркетингу. Уся інформація зберігається у CRM-системі. При користуванні веб-сайтом потенційний покупець отримує вспливаюче вікно-повідомлення що веде до чат-бота реалізованого системою Manychat's що має безпосереднью прив'язку до Facebook через месенджер WhatsApp. визначення проекту автоворонки продажу, розробка веб-дизайну сайту Scandinavian Investment Group, верстка сайту, використання CMS, встановлення CPM системи та її адаптація.

Для впровадження автоворонкі продажів необхідні такі компоненти:

- Сайт. Це ключовий момент. Якщо сайту немає, можна придбати вже готове програмне забезпечення. Теоретично впровадити автоворонку можна і в соцмережах, якщо налаштувати там автосполучення і підготувати лід-магніти та інше.

- Трафік. Автоворонка потрібна для лідогенерації і утримання клієнтів, тобто працює з уже існуючим трафіком. Трафік є необхідною умовою, тому якщо є проблеми із залученням відвідувачів на сайт, які можна вирішити за допомогою SEO, SMM, платної реклами або інших інструментів.

- Автоматичні інструменти комунікації. Як правило, автоворонка здійснюється за допомогою інструментів, які спрацьовують по триггеру.

Для досягнення максимальної ефективності та надійності захисту інформації автоворонки необхідно створити комплексну систему, яка системно забезпечує необхідні складові захисту й

установлює між ними логічний і технологічний зв'язки [1]. Тобто, для забезпечення безпеки інформаційних даних автоворонки продажів необхідно дотримуватись таких правил:

- розробляючи інформаційну систему automatic sales funnel продажів, необхідно користуватись тільки ліцензійним програмним забезпеченням, встановлювати антивіруси, і постійно оновлювати версію. Встановлюючи піратське програмне забезпечення, або купуючи вже створену піратську автоворонку, на комп'ютер може бути встановлено і шпіонські програми, які можуть відслідковувати всю діяльність користувача, а також все що вводиться через клавіатуру. Доречі, встановлюючи зламану операційну систему Windows користувач ризикуєте заразиться вірусом вже на етапі установки. Оскільки деякі «ліві» інсталяційні файли, які у вільному доступі в мережі Інтернет, мають вже ушиті закладки, шпигуни, віруси, приховані радміни тощо.
- на сайті інформаційної системи automatic sales funnel не надавати права доступу до панелі адміністратора неперевіреним працівникам. Для них створити спеціальні облікові записи з обмеженими правами, оскільки несумлінні користувачі можуть несвідомо додати на сайт шкідливий код.
- при розробці інформаційної системи automatic sales funnel продажів програміст повинен дуже уважно писати код, і не допускати помилки, а саме допускати уразливість сайту саме у його вихідних кодах. Якщо авто воронка побудована на готовій CRM-системі керування контентом, то розробники вже подбали про безпеку сайту. Необхідно встановлювати на web-сторінку лише перевірені плагіни, адже в них також може бути заховане шкідливе програмне забезпечення.

Для додаткової інформаційної безпеки сайту інформаційної системи automatic sales funnel можливо застосовувати протокол SSL (Secure Sockets Layer – рівень захищених сокетів) – це криптографічний протокол, який забезпечує захищену передачу інформації в мережі Інтернет. Найчастіше SSL протокол використовують у випадках, коли необхідно забезпечити належний рівень захисту інформації, яку користувач передає на сервер. Це можуть бути дані кредитної карти, паспортні дані, ПІН-коди та інша інформація, яка може бути цікавою для зловмисників.

Безпека сайту інформаційної системи automatic sales funnel – одна з найважливіших складових безперебійної і стабільної роботи Інтернет сторінки. Для забезпечення захисту від витоку, втрати та підробки інформації необхідно використовувати криптографічний захист, або шифрування, що реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Також необхідно створити спеціальну сукупність правил по захисту від кібератак для персоналу, з метою зменшення ризику витоку або втрати інформації через їх можливі помилки.

Анотація: Розглядаються питання, які на сьогодні ще недостатньо досліджені, з актуальної проблеми щодо комплексного підходу забезпечення кіберзахисту інформаційної системи automatic sales funnel. Дана система за посередництвом різних сценаріїв продажів, що входять до складу інформаційної системи automatic sales funnel, спочатку знайомить потенційного клієнта з продуктом, а потім веде до здійснення нових і нових покупок.

Література:

1. Закон України Про основні засади забезпечення кібербезпеки України [Електронний ресурс]. - Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19

2. Nikolay Brailovskyi, Valeri Kozura, Svetlana Kondakova, Volodymyr Khoroshko Analysis of the cybersecurity status of the information space // Scientific & practical cyber security journal (SPCSJ) №4. [Electronic journal]. URL: https://journal.scsa.ge/issue/december-2018/

3. Система захисту інформації приватного підприємства. Організація Служби захисту інформації приватного підприємства. – Режим доступу: http://pnzzi.kpi.ua/14/14_p45.pdf

УДК 004.4; 004.7

Риндич Євген Володимирович, *доцент к.т.н.*
Національний університет «Чернігівська політехніка»,
yevhen.ryndych@stu.cn.ua

Біленкий Георгій Сергійович, *студент*
Національний університет «Чернігівська політехніка»,
gimnasium16@gmail.com

НАВЧАЛЬНИЙ СТЕНД ДЛЯ ВИВЧЕННЯ ДИСЦИПЛІН З ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВОГО ЗАХИСТУ ІНФОРМАЦІЇ

Сучасний етап розвитку комп'ютерних систем та мереж призвів к значному збільшенню та ускладненню складових сучасних систем. Вивчення мережевих систем вимагає як теоретичних, так й практичних навиків. Створення стенду для демонстрації основних етапів побудови мережі, її налаштуванні та обмеженнях, знайомство з мережевим обладнанням та його конфігурацією є одним з кращих способів показати та навчити студентів роботі з апаратним та програмним забезпеченням. Особливим напрямком практичного використання мереж є створення безпечного підключення до зовнішніх мереж та ознайомлення з базовими поняттями маршрутизації та організації безпечної взаємодії головного офісу(HQ) підприємства та його віддалених підрозділів(BO).

При розробці та реалізації циклу лабораторних робіт з мережевих технологій запропоновано використовувати маршрутизатори MikroTik RB2011UiAS-2HnD-IN як основних маршрутизаторах на відокремлених ділянках. Також в стенді використовується MikroTik RB750 який моделює роботу «Глобальну мережі» з зовнішніми IP адресами для емуляції Інтеренту.

Для стенду було обрано мережеве обладнання MikroTik через його відносно невелику вартінсть, різноманітність функцій та зручне налаштування з використанням операційної системи RouterOS.

Дане ПО має великий функціонал. Завдяки ньому можна налаштувати правила маршрутизації, різні інтерфейси та обмеження для доступу, що дозволить студентам отримати практичний досвід для майбутньої роботи в сфері мережевого обладнання та налаш-

тування захищених систем класу АС-2 та АС-3. Слід відмітити, що операційна система розроблена на базі Linux, що дозволяє знизити рівень особливих знань для початку налаштування.

Вбудовані функції безпеки дозволяють за допомогою ознайомити здобувачів з процесами створення тунелів, автентифікації, перевірки цілісності та шифруванню IP-пакетів.

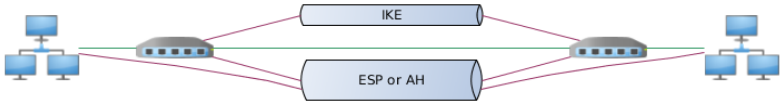


Рис. 1. Схема створення тунелів між віддаленими вузлами

Основні можливості, які можна використати при використанні стенду:

- базові функції комутації;
- базові функції та протоколи маршрутизації, їх безпека;
- створення та дослідження віртуальних мереже(VLAN);
- вивчення технології Network Address Translation (NAT);
- створення та дослідження тунелів з шифруванням та без шифрування (PPTP, PPPoE, SSTP, OpenVPN, L2TP/IPSec);
- дослідження протоколу SNMP;
- дослідження та порівняння алгоритмів шифрування даних;
- дослідження та порівняння базових протоколів автентифікації

В таблиці 1 наведено адресацію мереж, а на рис.2 наведена схема стенду з вказаними IP адресами та обладнанням.

Таблиця 1

IP адреси стенда

№	Призначення	Адреса мережі	Шлюз	Маска мережі
1	Головний офіс	192.168.1.0	192.168.1.254	255.255.255.0
2	Віддалений підрозділ	192.168.100.0	192.168.100.254	255.255.255.0
3	Зовнішня мережа. Провайдер головного офіса	65.65.65.0	65.65.65.254	255.255.255.0
4	Зовнішня мережа. Провайдер віддаленого підрозділа	75.75.75.0	75.75.75.254	255.255.255.0

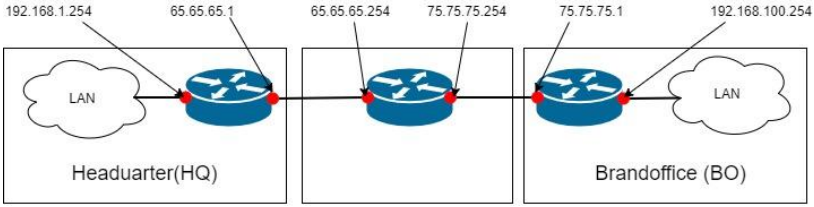


Рис. 2. Схема з'єднання та адресації

В ході розробки та тестування було також виявлено, що для більш поглибленого вивчення деяких дисциплін необхідно додати додаткове обладнання. Так для вивчення захисту зовнішнього периметру доцільно розширити запропоновану схему апаратним брандмауером та зовнішнім аналізатором трафіку та, зважаючи на відтворення критичної інфраструктури додати джерела безперебійного живлення з можливістю відстеження стану та доступу за допомогою мережевих протоколів.

Анотація. У статті досліджується можливість побудови напівнатурні моделі захищеної мережі для досліджень студентами спеціальності Кібербезпека. Вибір основних елементів мережі, які можуть показати студентам основні етапи побудови підключень в локальній та зовнішній мережах. Максимально використати потужності апаратного забезпечення стенду для наочного споглядання процесів маршрутизації, комутації та побудови тунелів для захищеного зв'язку.

Література:

1. Риндич Є. В. та інш. Особливості створення мережевої системи виявлення вторгнень у комп'ютерні системи //Математические машины и системы. – 2018. – №. 3.

2. Глобальні мережі: метод. вказ. до виконання лаб. робіт з дисципліни—Новітні архітектури та засоби побудови глобальних та корпоративних мереж для студ. спец. 8.05010201—Комп'ютерні системи та мережі, 8.05010202—Системне програмування, 8.05010203—Спеціалізовані комп'ютерні системи/уклад.: Є.В. Риндич.–Чернігів: ЧНТУ, 2013.–16 с.

УДК 003.26

Савченко Тетяна Віталіївна, доцент,
кандидат технічних наук
Київський національний
торговельно-економічний університет
sv_t@ukr.net

Сашньова Мар'яна Василівна,
кандидат технічних наук
Київський національний
торговельно-економічний університет
m.sashnova@gmail.com

АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ КВАНТОВОЇ КРИПТОГРАФІЇ

Сучасне суспільство є інформаційним. Тобто практично кожна дія, яку ми здійснюємо в нашому житті, тісно пов'язана з інформаційними технологіями, тому є важливим питання захисту інформації. Проблема кібербезпеки в інформаційному суспільстві набуває особливої актуальності в епоху створення квантових комп'ютерів. Постає задача щодо розробки нових технологій криптографічного захисту для подальшого створення відповідних криптоалгоритмів та ефективних засобів безпеки нового покоління.

Стрімкий розвиток квантових комп'ютерів створює новий виклик перед спеціалістами з кібербезпеки. Особливості квантових обчислень дозволяють реалізувати алгоритми, що створюють можливість порівняно швидкого зламу будь-яких паролів, що засновані на найбільш розповсюджених на сьогоднішній день алгоритмах шифрування. Застосування квантових комп'ютерів дозволяє виконувати логічні операції над квантовими станами частинок, що його утворюють, шляхом унітарних перетворень, не порушуючи багаточастинних квантових суперпозицій в процесі обчислень.

Квантова передача включає шифрування інформації в квантові стани (кубіти), на відміну від класичної передачі, що використовує біти. Для квантових станів використовуються фотони. Квантовий розподіл ключів заснований на певних властивостях квантових станів для організації безпеки.

Фізична реалізація системи квантової криптографії наведена нижче [1].

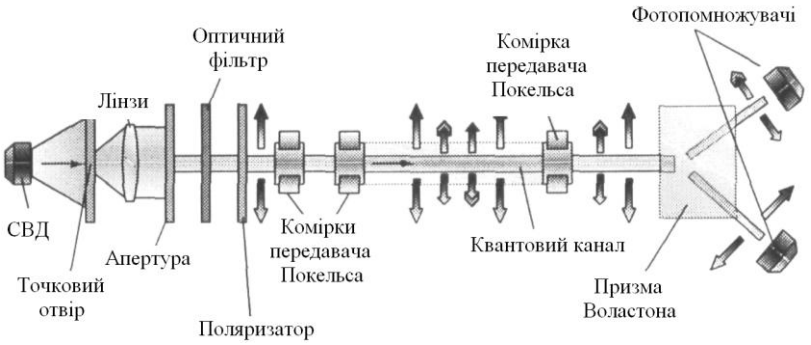


Рис. 1. Схема фізичної реалізації квантової криптографії

Існують різні способи квантового розподілу ключів, проте, вони поділяються на дві основні категорії, в залежності від властивостей, що використовуються.

Перша категорія використовує протокол підготовки та вимірювання. Вимір є невід'ємною частиною квантової фізики. Вимірювання невідомого квантового стану змінює його в деякому роді. Це відомо як квантовий індетермінізм і лежить в основі результатів, таких як принцип невизначеності Гейзенберга і теореми про заборону клонування. Це може бути використано для того, щоб виявити будь-які прослуховування на зв'язку і для розрахунку кількості інформації, яка була перехоплена.

Друга категорія використовує протоколи, що засновані на заплутаності. Квантові стани двох або більше окремих об'єктів можуть бути з'єднані таким чином, що вони будуть описуватися за допомогою комбінованого квантового стану, а не як індивідуальний об'єкт. Це називається заплутаністю і означає, що вимірювання на один об'єкт впливає і на інший. Якщо сплутана пара об'єктів є спільною між двома учасниками, то перехоплення будь-якого об'єкта змінює систему в цілому, розкриваючи присутність третіх осіб і кількість інформації, яку вони отримали.

Узагальнена класифікація квантових методів захисту інформації була запропонована в роботі [2].

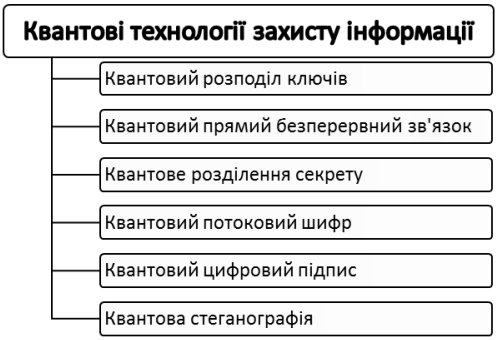


Рис. 2. *Класифікація квантових технологій захисту інформації*

В основі асиметричної криптографії лежить два ключі: один може зашифрувати дані, інший використовується для їх розшифрування. Теоретично квантові комп'ютери будуть здатні вирішувати задачі суттєво швидше порівняно із звичайними комп'ютерами та зможуть розшифрувати закриті ключі. Враховуючи швидкість розвитку квантових обчислень, це може статися вже найближчим часом.

На теперішній час для секретної передачі повідомлення необхідно, щоб секретний ключ був випадковим, довжина ключа була не менша за довжину повідомлення та ключ використовувався лише один раз. Ключова проблема в останньому, тому що жодна третя сторона не повинна отримати доступ до цієї інформації. Завдання безпечного обміну вирішується за допомогою квантового розподілу ключа (Quantum Key Distribution) [2].

Отже, таку систему неможливо зламати тому, що які б обчислювальні ресурси не мав злочинець, у зв'язку з тим, що ключ одноразовий і випадковий, злочинець не може отримати жодної інформації про те, яке повідомлення передане. Тобто такі системи є абсолютно стійкими.

Але для того, щоб шифрувати весь трафік в такому режимі, необхідні дуже високі швидкості генерації ключів, отже, ще багато технічних задач потребують вирішення.

Крім того, є обмеження, пов'язані з відстанню. Справа в тому, що при передачі інформації про ключ за допомогою фотонів, відстань, на яку це можна зробити, суттєво обмежена. Світові рекорди в лабораторіях – це сотні кілометрів.

Проблема апаратної реалізації існуючих кубітів – в низькій стабільності, високому «зашумленні» інформації. Це поки що не дозволяє реалізувати весь потенціал існуючих квантових комп'ютерів, але спостерігається значний прогрес.

Вирішенням проблеми ризику квантового зламу існуючих систем криптографії є перехід на інші алгоритми шифрування. Ряд найбільш перспективних алгоритмічних основ для постквантової криптографії наведено нижче:

- Алгоритми решітчатої криптографії: на теперішній час розроблено близько десяти різних алгоритмів. Дослідження активно продовжуються.
- Багатовимірна криптографія: декілька запропонованих рішень виявилися нестійкими до зламу, але очікується, що варіант багатовимірного цифрового підпису, що використовує алгоритм «Райдуга», може стати основою для перспективного квантового цифрового підпису.
- Кеш-криптографія – була винайдена ще в 1970 році. Зацікавленість до цього рішення повернулася після усвідомлення ризиків зламу шифрів з використанням квантових комп'ютерів.
- Інші алгоритми: код з корекцією помилок, ізогенна еліптична крива, системи з симетричним ключем тощо.

Таким чином, технологія квантової криптографії базується на принциповій невизначеності поведінки квантової системи. Принцип невизначеності Гейзенберга полягає в тому, що неможливо одночасно отримати координати та імпульс частинки, неможливо виміряти один параметр фотона, не спотворивши інший. Інакше кажучи, спроба вимірювання взаємопов'язаних параметрів у квантовій системі вносить в ній порушення, руйнуючи вихідні сигнали, - це означає можливість миттєвого виявлення захоплювача в каналі зв'язку.

Незважаючи на безліч невирішених завдань, квантова криптографія залишається найперспективнішим напрямом в області інформаційної безпеки, а квантові лінії зв'язку є найбезпечнішими для передачі секретного ключа. А завдяки безлічі інших переваг можна вважати, що найближчим часом вони замінять всі існуючі алгоритми шифрування інформації.

Анотація. Розглянуто актуальну проблему кібербезпеки в інформаційному сусупільстві та новітні технології криптографічного захисту даних. Проаналізовано сучасні технології квантової криптографії на основі шифрування інформації в квантові стани. Наведено фізичну реалізацію системи квантової криптографії. Проаналізовано різні способи квантового розподілу ключів, що поділяються на дві основні категорії, в залежності від властивостей, що використовуються. Представлено класифікацію квантових технологій захисту інформації. Розглянуто перспективи розвитку квантової криптографії.

Література:

1. Килин С. Я., Хорошко Д. Б., Низовцев А. П. «Квантовая криптография: идеи и практика» – Мн:, 2008. – 392 с.

2. Корченко О.Г. Сучасні квантові технології захисту інформації / О.Г. Корченко, Є.В. Васіліу, С.О. Гнатюк // Захист інформації. — 2010. — № 1. — С. 77–89.

3. A. I. Lvovsky Squeezed light, section in book: Photonics Volume 1: Fundamentals of Photonics and Physics, D. Andrews, eds., Chapter 5: 121–164 Published by Wiley, West Sussex, United Kingdom, 2015.

УДК 004.4:056.57

***Семендяй Сергій Матвійович**, аспірант*
sovnarcom@ukr.net

***Зайцев Сергій Васильович**, д.т.н., професор*
serza1979@gmail.com
Національний університет "Чернігівська політехніка"

МЕТОД ЗАБЕЗПЕЧЕННЯ ДОСТОВІРНОСТІ ІНФОРМАЦІЇ В БЕЗПРОВОДОВИХ ЗАСОБАХ ПЕРЕДАЧІ ДАНИХ ЗА РАХУНОК СТРУКТУРНОЇ АДАПТАЦІЇ ТА ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ

Ефективність функціонування безпроводових засобів передачі даних (далі – БЗПД) залежить від здатності системи забезпечувати задану достовірність прийому інформації в умовах впливу завад різного походження, у тому числі і навмисних, які характеризуються високою спектральною щільністю потужності. У БЗПД стільникового зв'язку канал зв'язку, як фізичне середовище поширення радіохвиль, має свою специфіку, а саме: зони дії стільникового зв'язку – міста і приміські зони, райони з тією або іншою щільністю забудови; мобільна станція, як правило, перебуває поза зоною прямої видимості базової станції і сигнали в точку прийому надходять у ході перевідбиття і дифракції; пересування мобільних абонентів під час сеансу зв'язку вносить у сигнали доплерівські частотні зсуви; наявність великої кількості відбивачів призводить до ефекту розсіювання електромагнітних хвиль і багатопроменевому поширенню (мобільна станція приймає безліч інтерферуючих сигналів).

Внаслідок відзначених явищ у каналі зв'язку мають місце загасання сигналів, повільні та швидкі завмирання сигналів. Канали із завмираннями характеризуються випадковою зміною коефіцієнта передачі, тому параметри сигналів на вході приймача є випадковими і невідомими. Достовірність передачі інформації при цьому погіршується, тому що при прийманні немає можливості використати відомості про дійсні значення параметрів сигналів. Таким чином, випадкові зміни параметрів каналу передачі являють собою мультиплікативну заваду, яка призводить до спотворень переданих сигналів у вигляді випадкової зміни їх

параметрів. Найбільш істотний вплив на властивості переданих сигналів здійснюють швидкі селективні завмирання в каналі, причому ступінь цього впливу визначається співвідношенням параметрів середовища поширення і параметрів сигналу. Ефективним напрямком протидії завадам є застосування в БЗПД технологій розширення спектра сигналу та кодових конструкцій.

На даний час методи забезпечення достовірності інформації в БЗПД досить глибоко й широко досліджені в наукових працях вітчизняних та іноземних вчених. Однак недостатньо досліджені та вимагають додаткового вивчення наступні задачі:

– створення нових та вдосконалення існуючих методів забезпечення достовірності інформації в БЗПД;

– модифікація та спеціалізація існуючих обчислювальних методів з метою підвищення їх ефективності, створення і дослідження нових обчислювальних методів і алгоритмів, що враховують особливості функціонування БЗПД;

– розробка ефективних методів адаптивного завадостійкого кодування для забезпечення заданих характеристик достовірності інформації в каналах з підвищеним рівнем шуму та завадами з врахуванням нечітких правил прийняття рішень.

У роботі вирішується актуальна науково-прикладна задача, що має важливу наукову, практичну й технічну спрямованість – підвищення ефективності перспективних БЗПД через забезпечення достовірності інформації за рахунок розробки методів на основі адаптивного кодування та застосування процесів прийняття рішень штучною нейронною мережею.

Для досягнення поставленої мети необхідно вирішити такі задачі:

проаналізувати існуючі методи забезпечення достовірності інформації в БЗПД;

розробити на основі адаптації кодових конструкцій метод забезпечення достовірності інформації в БЗПД;

розробити та реалізувати у програмному виді обчислювальний метод нечіткого декодування багатокомпонентних турбокодів в БЗПД;

розробити метод підготовки первинної інформації для адаптивних БЗПД.

Об’єктом дослідження мають стати процеси формування і переробки кодованих даних у БЗПД, а предметом дослідження – забезпечення достовірності інформації у БЗПД.

Метод забезпечення достовірності інформації в БЗПД на основі адаптації кодових конструкцій дозволить забезпечити задані показники достовірності інформації та зменшити кількість елементарних операцій цифрових сигнальних процесорів при цифровій обробці кодованих даних. Відмінність даного методу від існуючих, що визначає його новизну, полягає в застосуванні різних за структурою завадостійких кодів, від більш простих до більш складних, в залежності від оцінки відношення сигнал-шум в каналі зв’язку, проведеної в приймачі за допомогою штучної нейронної мережі, що призводить до забезпечення заданих характеристик достовірності інформації та спрощення варіантів синтезу моделей БЗПД. Структура об’єкта управління адаптується до зміни завадової обстановки шляхом варіації масивів даних структури кодів. Після проходження навчання нейронної мережі, визначення оптимальної структури кодів не потребуватиме великої обчислювальної потужності.

Впровадження результатів роботи може дозволити:

моделювати, визначати параметри та виготовляти БЗПД з використанням новітніх цифрових технологій;

кількісно оцінювати методи забезпечення достовірності інформації в БЗПД в умовах різних завад;

підвищувати достовірність інформації та енергетичну ефективність БЗПД;

спростити та знизити вартість робіт при дослідженні, проектуванні і виготовленні БЗПД.

Результати даного дослідження у своїй сукупності мають створити нову інформаційну технологією забезпечення достовірності інформації в БЗПД за рахунок адаптивного кодування з використанням процесів прийняття рішень за допомогою штучних нейронних мереж, що дозволяє оптимізувати та підвищити ефективність застосування методів забезпечення достовірності інформації в БЗПД на етапах їх проектування, виготовлення і експлуатації.

Анотація. Розглянуто метод забезпечення достовірності інформації в безпроводових засобах передачі даних за рахунок структурної адаптації та використання нейронних мереж. Зазначений метод дозволить забезпечити задані показники достовірності інформації та зменшити кількість елементарних операцій цифрових сигнальних процесорів при цифровій обробці кодованих даних. Новизна даного методу полягає в застосуванні різних за структурою завадостійких кодів на основі рішення, прийнятого штучною нейронною мережею за результатами оцінювання відношення сигнал-шум в каналі зв'язку.

Література:

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Скляр. Б. – [2-е изд]. – М. : Вильямс, 2003. – 1104 с.

2. Зайцев С.В. Методи та моделі забезпечення сталої достовірності інформації у безпроводових системах передачі даних : дис. … доктора техн. наук / Зайцев Сергій Васильович. – Чернігів, 2016. – 397 с.

2. Горлинський Б.В. Методи забезпечення достовірності інформації в безпроводових засобах передачі даних за рахунок адаптивного кодування: дис. … кандидата техн. наук / Горлинський Борис Вікторович. – Київ, 2019. – 187 с.

УДК 621.391

Синенко Марина Анатоліївна, *к.ф.м.н., доцент*
Національний університет «Чернігівська політехніка»,
mara.a.snnk@gmail.com

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДИК ТЕСТУВАННЯ ПОСЛІДОВНОСТІ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

На даний час відомий широкий спектр застосування випадкових та псевдовипадкових послідовностей у прикладних задачах, а саме, такі послідовності використовують в імітаційному моделюванні, в області математичної статистики, у чисельному аналізі, для захисту інформації, зокрема, у криптографії. Причому в останньому випадку вимоги до якості псевдовипадкових послідовностей зростають, оскільки від цього у значній мірі залежить секретність інформації, яка передається. Цим пояснюєть необхідність створення ефективних методів генерації та тестування послідовності випадкових та псевдовипадкових чисел.

Не дивлячись на те, що дослідження у цій області тривають уже багато років і існує досить велика кількість алгоритмів тестування послідовностей на випадковість [1-4], задача залишається актуальною і на сьогодні. Так, на даний час не розроблено єдиної методики тестування псевдовипадкових послідовностей.

Мета даної роботи полягає в аналізі існуючих підходів тестування послідовності псевдовипадкових чисел, висвітлення їх переваг та недоліків.

Нагадаємо, що випадковою називають послідовність, яка характеризується рівномірністю, незалежністю та стохастичністю, криптографічною називають послідовність, яка має усі перераховані властивості. Послідовність випадкових чисел називають криптостійкою, якщо не існує поліноміального алгоритму, який на основі перших k бітів послідовності може передбачити $k+1$ біт з ймовірністю більшою 0.5.

Методи оцінки якості генераторів випадкових та псевдовипадкових послідовностей можна поділити на дві групи – теоретичні та емпіричні. Теоретичні методи передбачають теоретико-числовий аналіз алгоритмів генерації псевдовипадкових послідовностей. Емпіричні методи в свою чергу поділяють на графічні та статистичні.

За допомогою графічних тестів стохастичність згенерованої послідовнсті дослідник визначає за видом графічної залежності, наприклад, розподілу на площині. Зрозуміло, що такий спосіб тестування є, до певної міри, суб'єктивним.

На рисунку 1 наведені приклади розподілу на площині послідовностей псевдовипадкових чисел, побудованих за допомогою лінійних конгруентних генераторів $X_{k+1} = (aX_k + b)(mod\ M)$ з параметрами $X_0 = 7; a = 106;\ b = 1283;\ M = 6075$ і $X_0 = 7;\ a = 106;\ b = 1284;\ M = 6075$ відповідно. Як видно, для першої послідовності маємо позитивний результат, для іншої – негативний, тобто перша послідовність виглядає як випадкова (рівномірно розводілена).

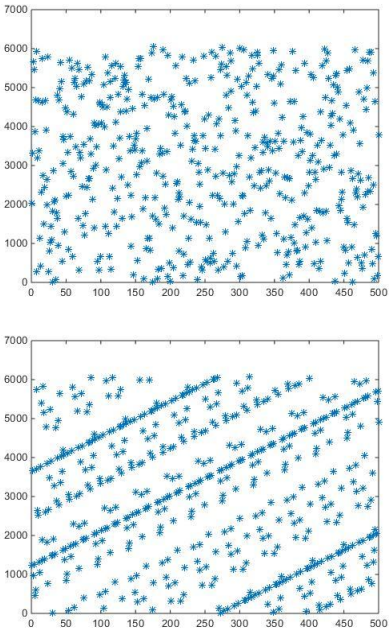


Рис. 1

До другої групи відносять статистичні тести, використовуючи які випадковий характер послідовності можна описати числом (числові характеристики розподілу, стастистика критерію узгодження).

Як приклад можна розглянути критерій Колмогорова-Смирнова (КС-критерій), який використовується для перевірки нулевої гіпотези H_0, що випадкова величина X має закон розподілу $F(x)$.

Нехай $(x_1, x_2, \dots x_n)$ – вибірка значень випадкової величини X, $F^*(x); F(x)$ – емпірична та теоретична функції розподілу з відомими параметрами. Статистика критерію визначається за формулою:

$$D_n = \sup|F^*(x) - F(x)| = \max_{1 \le m < n} \left(\frac{m}{n} - F(x_m)\right).$$

Гіпотеза H_0 відкидається, якщо статистика $\sqrt{n}D_n$ більша за квантиль розподілу K_α при заданому рівні значощості α. Для тестування якості послідовності псевдовипадкових величин за допомогою КС- критерію перевіряємо нулеву гіпотезу, що послідовність підлягає рівномірному закону розподілу. Відповідний код можна створити у системі MatLab.

Відмітимо найбільш відомі статистичні тести.

Тести Diehard, [2] – набір, який містить 12 статистичних тестів для визначення якості випадкових та псевдовипадкових послідовностей, розроблений Дж. Марсалья та опублікований у 1995 р.

Тести Crypt-X розроблені ученими науково-дослідного центру технологічного університету Квінсленда (Австралія) і направлені на тестування псевдовипадкових чисел.

Тести Nist, [3] направлені на розв'язання задач статистичного контролю псевдовипадкових послідвностей, які використовуються у криптографічних модулях.

У роботі [5] проаналізовані недоліки названих тестів, серед яких автори указують неможливість оцінити випадкову числову послідовність окремо по кожному з тестів та надати перевагу одних над іншими та пропонують узанальнену методику перевірки на основі статистичних тестів та теорії нечітких множин.

Багато статистичних методів базується на ідеях теорії інформації (тест Маурера). Один з таких методів, розроблений російськими ученими у 2004 році, дістав назву «Стопка книг», [4]. Експериментально встановлено, що цей метод дозволяє виявляти відхилення від рівномірного розподілу деяких псевдовипадкових послідовностей, які пройшли тести Nist. Ще одна суттєва перевага тесту полягає у тому, що він дозволяє аналізувати ви-

падкові послідовності на вибірках порівняно невеликих об'ємів. Так, для тестування послідовності, згенерованої на основі алфавіту, що містить S символів достатньо вибірки об'єму $\sqrt{S}$.

Висновки. Не дивлячись на наявність значної кількості статистичних алгоритмів для тестування якості генераторів псевдовипадкових числових послідовностей дослідження у цій області продовжуються. Як результат виникають нові та удосконалюються існуючі методи аналізу псевдовипадкових послідовностей. Оскільки для різних класів прикладних задач вимоги до якості таких послідовностей можуть відрізнятись, існують об'єктивні труднощі для створення єдиної методики тестування псевдовипадкових послідовностей.

Анотація. Випадкові та псевдовипадкові числові послідовності використовують при розв'язанні широкого класу прикладних задач математичної статистики, чисельного аналізу, теорії інформації та криптографії. Тому задача генерування та тестування псевдовипадкових послідовностей залишається актуальною на даний час. У роботі розглядаються сучасні підходи аналізу якості генераторів псевдовипадкових числових послідовностей, висвітлюються їх переваги та недоліки.

Література:

1. Random Number Generators: An Evaluation and Comparison of Random.org and Some Commonly Used Generators. Режим доступу: https://www.random.org/analysis2005.pdf

2. Brown R. Dieharder: A Random Number Test Suite. http://www.phy.duke.edu~rgt/General/dieharder.php

3. NIST Sp 800-22. Rev. Ia. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptograhic Applications/ [A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S.Vo] National Institute of Standards and Technology, 2010.

4. Рябко Б.Я., Пестунов А.И.. «Стопка книг» как новый статистический тест для случайных чисел// Пробл. Передачи информ. 2004, т.40, В.1, с.73-78.

5. Ажмухамедов И.И., Колесова Н.А.. Методика оценки качества последовательности случайных чисел// Вестник АГТУ. Сер: Управление, выч. техника, информатика. 2010, №1, с.141-148.

6. Слеповичев И.И. Генераторы псевдослучайных чисел/ Учебное пособие, Саратов: СГУ, 2017. – 118 С.

УДК 004.4:056.57

***Ткач Юлия Николаевна**, д.пед.н., доцент*
tkachym79@gmail.com

***Шелест Михаил Евгеньевич**, д.т.н., профессор*
mishel3141@gmail.com
Черниговский национальный технологический университет

***Карпинский Николай Петрович**, д.т.н., проф.,*
Університет у Бєльсько-Бялій(м. Бєльсько-Бяла, Польща)
mpkarpinski@gmail.com

О РАЗВИТИИ КИБЕРПРОСТРАНСТВА И ЕГО ЗАЩИЩЕННОСТИ

Интернет-технологии и всемирная компьютерная сеть широко пронизали различные сферы человеческой жизни. Обыденными становятся элементы нарождающегося электронного мира: электронного правительства, электронных услуг, электронного документа, электронных денег, электронной подписи и пр. Сформировалась новая сущность *киберпространство* (cyberspace).

Основу киберпространства составляет совокупность распределенных в пространстве взаимосвязанных электронных устройств (компьютеров, серверов, сетевых маршрутизаторов, хранилищ данных, шифраторов и пр.) с соответствующим программным обеспечением, с помощью которых создается и циркулирует (обрабатывается, передается и хранится) информация. С инфраструктурной точки зрения киберпространство можно рассматривать как глобальное адресное пространство, которое состоит из национальных и региональных сегментов интернета.

Киберпространство, помимо прочего, постепенно превращается в пятый театр военных действий (наряду с наземным, морским, воздушным и космическим), где вместе с военными планируется участие спецслужбы страны, хакеров и всех тех, кто может создавать и использовать компьютерные вирусы для нанесения ударов по врагу. Войны будущего будут вестись в режиме онлайн, когда неприятель, кроме применения сил на поле сражения, будет использовать уязвимости компьютерных систем государственных структур и объектов критической инфрастуктуры для их разрушения и уничтожения, а также социальные

сети для создания паники населения в масштабе страны и снижения его способности к сопротивлению агрессии. Таким образом, сегодня кибервойны из фантастических романов перекачивали в реальность.

Ряд стран (в первую очередь, США, Россия, Китай) проводят государственную политику, которая рассматривает киберпространство как поле боя, вследствие чего направляют свои усилия на полный контроль в этой сфере, создавая средства и возможности на осуществление такого контроля. Для решения этой задачи происходит колобарация государственных структур с техноиндустрией интернета - крупными производителями микроэлектроники, вычислительной и телекоммуникационной техники (Cisco, Huaway), шифраторов (Crypto AG, Omnisec, Mils Electronic), программного обеспечения (Microsoft), социальных сетей (Facebook, Вконтакте, Одноклассники), антивирусных систем (Касперский, McAfee), поставщики услуг электронной почты, сетевые и интернет гиганты (Google, Yahoo, AT&T, CenturyLink, Verizon) в целях сбора информации о пользователях. Это происходит с помощью встраивания бэкдоров и передачи спецслужбам секретных уязвимостей в аппаратном и программном обеспечении, в том числе используемых ключей шифрования [1].

Таким образом, мы является свидетелями формирования *военно-сетевого комплекса* (по аналогии создания военно-промышленного комплекса в 60-х годах XX века), когда интересы и возможности спецслужб и военного сектора государства переплетаются с интересами и возможностями частных структур, что в ближайшее время разительно меняет как само киберпространство, так и характер военных действий в нем.

С точки зрения интересов страны, киберпространство нужно рассматривать как часть национальной инфраструктуры, которая имеет очерченные границы и нуждается в системе безопасности, как и остальные элементы государственной инфраструктуры. Основная проблема киберпространства - это обеспечение безопасности информации, которая в нем циркулирует, и устойчивость его национального сегмента к кибератакам.

Тенденция развития безопасности киберпространства показывает, что государственные органы не будут основными игроками в этой сфере, во всяком случае постоянными лидерами. Они бу-

дут вырабатывать стратегию, устанавливать законы и контролировать стандарты безопасности киберпространства, а ключевые объекты инфраструктуры должны будут их соблюдать. Повседневная работа по защите ключевых промышленных объектов станет заботой корпораций, которые справятся с этой задачей не хуже государства. Они создадут новый вид услуг по сканированию, анализу трафика и применению собственных методов обнаружения вредоносных программ и хакерской активности - методов, которые будут основаны на тех данных, которые компании будут собирать в режиме реального времени в своих информационных сетях, а также в сетях своих клиентов. Получается своего рода краудсорсинг. Они будут не просто расследовать уже свершившиеся вторжения, а предлагать свои услуги по защите сетей клиентов от потенциальных угроз, подобно тому, как охранные фирмы предлагают обезопасить наши дома и офисы от грабителей. Эти же организации будут создавать киберармии и обучать их воевать в сетях, что в конце концов приведёт к интеграции с арсеналом военной мощи государства.

Для того, чтобы защититься от повседневных киберугроз будут создаваться безопасные зоны Интернета, т.е. полноценные кибернетические инфраструктуры, в которых безопасности будет поставлена во главу угла, а трафик анализироваться более активно и тщательно, чем в общедоступном интернете. Это будет "экозона безопасности", онлайн аналог особо охраняемой территории.

Повышенная кибербезопасность станет привлекательным потребительским качеством, той особенностью, которой будут привлекать клиентов. Компании, которые возьмутся за создание и обслуживание таких защищенных киберзон (интернет-провайдеры, банки и др., имеющие дело с персональными данными), будут привлекать наиболее опытных и квалифицированных сотрудников, поскольку уровень зарплат у них намного выше, чем в государственном или военном секторе. Как и в любой частной организации, владельцы такой инфраструктуры смогут ограничивать пользование ею, устанавливать правила и требовать их выполнения, а также предлагать особые преимущества, прежде всего безопасность. В пределах этих сетей будет тщательно анализиро-

ваться трафик на предмет вредоносных программ, посылаться предупреждения о потенциальной угрозе личным данным, производится контроль тех, кто пытается войти в сеть, и не допускать в неё любых подозрительных пользователей.

Значительный рост числа угроз, нарушений и правил кибербезопасности, имевших место в последние годы, превратили процесс моделирования угроз (рис.1) из интересной теоретической концепции в необходимые практические действия, которые должны быть реализованы на всех этапах жизненного цикла защищенного киберпространства (проектировании, создании и функционировании его аппаратных и программных составляющих).

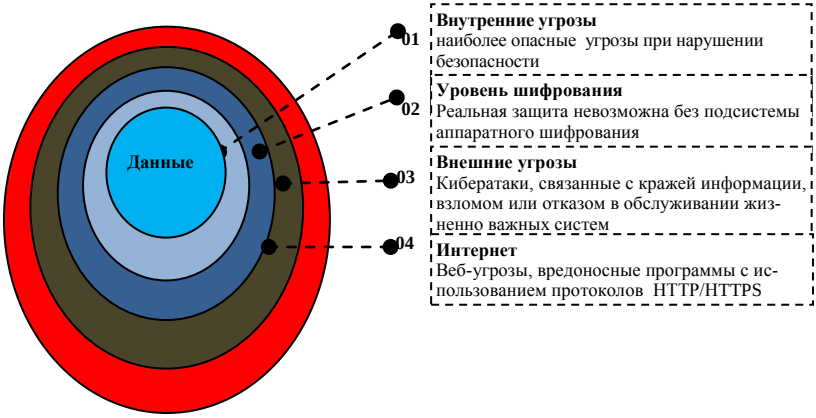


Рис. 1. Модель угроз

Важным элементом защищенного киберпространства является аналитическая поддержка, которая должна обеспечивать отслеживание идентификаторов угроз (IP-адреса компьютеров и серверов, на которых хранятся украденные данные; адреса электронной почты, с которой происходит рассылка писем-ловушек с вирусами) и новейших средств и методов, которые используют хакеры для взлома своих целей и несанкционированного получения информации. В этой области разработанная корпорацией Lockheed стратегия Cyber kill chain стала поворотным моментом в эволюции кибероборонь от внешних угроз [2]. Данная стратегия состоит из семи различных этапов и предлагает концептуа-

льную схему как выстроить уровни защиты на дальних подступах и заблокировать взломщиков до того, как они доберутся слишком близко к цели.

Аннотация. Рассмотрено суть киберпространства, установлено, что его основу составляет совокупность распределенных в пространстве взаимосвязанных электронных устройств с соответствующим программным обеспечением, с помощью которых создается и циркулирует (обрабатывается, передается и хранится) информация. Анализ тенденции развития безопасности киберпространства показал то, что государственные органы не будут основными игроками в сфере кибербезопасности, во всяком случае постоянными лидерами. Они будут вырабатывать стратегию, устанавливать законы и контролировать стандарты безопасности киберпространства, а ключевые объекты инфраструктуры должны будут их соблюдать. Установлен важный элемент защищенного киберпространства - аналитическая поддержка, которая должна обеспечивать отслеживание идентификаторов угроз и новейших средств и методов, которые используют хакеры для взлома и несанкционированного получения информации.

Література:

1. Интернет как оружие. Что скрывает Google, Tor и ЦРУ / Левин Яша; Пер.с англ. - М.: Индивидуум, 2019. - 360 с.

2. Кибервойн@: Пятый театр военных действий / Шейн Харис; Пер.с англ. - М.: Альпина нон-фикшин, 2020. - 390 с.

УДК 32.019.51:323.28(569.4)

***Трегубов Дмитро Миколайович**, полковник*
Воєнно-дипломатична академія імені Євгенія Березняка,
начальник кафедри спеціальних дисциплін
dimman3t@gmail.com

ДОСВІД ІЗРАЇЛЮ ЩОДО ПРОТИДІЇ ТЕРОРИСТИЧНИМ ЗАГРОЗАМ У КІБЕРНЕТИЧНОМУ ПРОСТОРІ

Проаналізовано досвід Ізраїлю щодо захисту національного кібернетичного простору, обґрунтовано доцільність застосування цього досвіду органами державної влади та спеціальними службами України в контексті протистояння гібридній агресії Російської Федерації.

Ключові слова: Ізраїль, кіберпростір, тероризм, інформаційна безпека, боротьба з кібертероризмом, ізраїльські спецслужби.

Постановка проблеми в загальному вигляді. В умовах гібридної агресії Російської Федерації проти України актуальним є питання організації ефективної протидії вітчизняних силових структур сектора безпеки та оборони терористичним загрозам у сфері інформаційного (кібернетичного) простору. Зокрема, на фоні активної антиукраїнської пропаганди, яку відкрито ведуть російські засоби масової інформації, Кремль використовує будь-які можливості щодо незаконного проникнення в кібернетичний простір України з метою маніпулювання інформацією та її сприйняттям на свою користь.

Силові структури сектора безпеки та оборони України мають об'єктивно оцінювати наявні можливості щодо протидії РФ в кібернетичній сфері, прогнозувати напрям можливих загроз, нарощувати відповідний потенціал та пропонувати вищому військово-політичному керівництву України аргументовані варіанти рішень щодо протидії виявленим загрозам національній безпеці України. Для обґрунтування таких пропозицій доцільно використовувати досвід провідних держав світу щодо захисту кібернетичного простору, зокрема Ізраїлю.

Аналіз останніх досліджень та публікацій. В [1] розкрито елементи нормативно-правової бази щодо захисту інформацій-

ного простору; у [3] – державну стратегію Ізраїлю щодо протидії кібертероризму; у [6] – сучасні технології та засоби маніпулювання свідомістю, проблемні питання ведення інформаційних війн і спеціальних інформаційних операцій; у [4] розглянуто методи боротьби з кібертероризмом в умовах швидкого розвитку ІТ-технологій; у [5] – потенційно вразливі для кібератак об'єкти критичної інфраструктури.

Водночас проблемні питання щодо ефективної протидії кібертероризму в умовах гібридної агресії, використання досвіду держави Ізраїль в інтересах органів державної влади України розкрито недостатньо.

Мета доповіді: обґрунтувати доцільність використання досвіду Ізраїлю щодо захисту національного інформаційного (кібернетичного) простору в умовах гібридної агресії Російської Федерації проти України.

Виклад основного матеріалу. Держава Ізраїль є однією з перших країн світу, які визнали важливість захисту своїх критичних інформаційних систем. Воєнно-політичне керівництво країни приділяє особливу увагу питанням забезпечення кібернетичної безпеки в усіх державних структурах.

За оцінками ізраїльських аналітиків, останнім часом хакерські атаки дедалі частіше спрямовано не тільки на сервери спеціальних служб і державних організацій, а й на сервери цивільних об'єктів, що створює громадський безлад та антиурядові настрої у країні. Терористичні акти на таких об'єктах можуть бути надзвичайно результативними оскільки проблеми населення зумовлюють появу руйнівних для держави сил. Так, протягом 2015–2019 років найчастіше об'єктами хакерських атак в Ізраїлі були важливі елементи систем енерго- і водопостачання, фінансові структури та окремі складові транспортної системи.

У своїй діяльності для створення маніпуляційних фейків терористичні організації поєднують відомості, добуті з кібернетичного простору, з тими, що отримують з відкритих загальнодоступних джерел. Такі заході терористичні організації називають електронним джихадом, метою якого є саботаж, створення хаосу в реальному світі, а також досягнення інших руйнівних цілей.

Слід відзначити, що в Ізраїлі діє трирівневий принцип національної оборони, що стосується кібербезпеки:

- зміцнення безпеки та поліпшення якості захисту на рівні окремого органу (підприємства, компанії тощо);

- захист на рівні держави;

- вирішення питань кібербезпеки на рівні міжнародного співробітництва.

Основним нормативно-правовим документом щодо дотримання вищевказаного принципу інформаційної (зокрема кібернетичної) безпеки є постанова Кабінету Міністрів Ізраїлю №84/б від 2002 року. Згідно з нею за дотримання інформаційної безпеки відповідають Міністерство оборони Ізраїлю та служба загальної безпеки (ШАБАК), а головним державним органом у сфері забезпечення інформаційної безпеки Ізраїлю є Рада національної безпеки Ізраїлю. Відповідальність поділено таким чином:

- ШАБАК відповідає за дотримання безпеки на більшості об'єктів інформаційної інфраструктури Ізраїлю, за винятком об'єктів, які перебувають у сфері відповідальності Міністерства оборони Ізраїлю;

- у комерційних установах такі функції покладено на спеціальні структурні підрозділи, що створені за кошти комерційних установ, проте відповідно сертифіковані в ШАБАК та підзвітні йому з питань дотримання вимог нормативно-правової бази.

У відповідній постанові Кабміну Ізраїлю визначено рівні безпеки в комп'ютеризованій інфраструктурі та впроваджено орган забезпечення національної інформаційної безпеки (the National Informational Security Authority), на який покладено регуляторні та дорадчі функції у сфері інформаційної безпеки.

У листопаді 2010 року, зважаючи на розвиток кібернетичного простору та зростання рівня загроз у цій сфері, прем'єр-міністр Ізраїлю доручив Верховному комітету з питань науки та технологій створити робочу групу з розробки Національного плану під назвою «The National Cyber Initiative», спрямованого на введення Ізраїлю до п'ятірки країн-лідерів у світовому кібернетичному просторі. До робочої групи увійшли представники основних структур, що відповідають за профільні напрями (науково-дослідних установ, оборонної та безпекової сфери тощо). За результатами діяльності робочої групи було створено Національне кібернетичне бюро («The National Cyber Bureau» – NCB) як дорадчий орган уряду та прем'єр-міністра.

Основним напрямом діяльності NCB є надання рекомендацій главі уряду та Кабінету Міністрів з питань, пов'язаних із загальнодержавною політикою та діяльністю в кібернетичному просторі широкого спектра (у цивільній, військовій, економічній, безпековій сферах). На NCB покладено завдання щодо координації між різними державними структурами питань захисту кібернетичної інфраструктури від кібератак, пропаганди кібертехнологій, заохочення застосування технологій кібернетичного захисту в індустріальній сфері, формування національної концепції щодо врегулювання надзвичайних ситуацій у кібернетичному просторі.

Ізраїльські фахівці відзначають, що за майже кожну четверту хакерську атаку можна класифікувати як загрозу вищого рівня, тобто ретельно підготовлену і яка несе реальну загрозу для об'єктів критичної інфраструктури).

За своїм характером загрози в Ізраїлі поділяються на такі категорії:

нецілеспрямовані з низьким рівнем небезпеки (наприклад, несистемні хакерські атаки на один або декілька сайтів, несистемна розсилка шкідливого програмного забезпечення тощо);

цілеспрямовані з низьким рівнем небезпеки (наприклад, людські хакерські атаки на конкретні державні інформаційні ресурси);

нецілеспрямовані з високим рівнем небезпеки (наприклад, автоматизовані системні атаки на велику кількість урядових інформаційних порталів);

цілеспрямовані з високим рівнем небезпеки (наприклад, автоматизовані системні атаки на конкретний урядовий інформаційний портал) – ця категорія вважається найбільш небезпечною.

За оцінками експертів, більшість ізраїльських політиків та керівників сектору безпеки високого рангу періодично потерпає від різного роду кібератак на мобільні пристрої зв'язку під час офіційних візитів і неформальних закордонних поїздок. Зокрема, всі мобільні пристрої офіційних делегацій Ізраїлю, що прибували до Росії протягом 2015–2019 років, було атаковано кіберпідрозділами ФСБ РФ, на них знайдено ознаки спроб впровадити «шкідливе» програмне забезпечення. В Ізраїлі з метою протидії таким атакам фахівці компанії «First Point Mobile Guard Ltd» розробили

та реалізували концепцію захисту мобільних пристроїв від зовнішніх атак по каналах зв'язку та Інтернет мобільного оператора. Вони створили захищену дублюючу базову мережу, яку під'єднано до оператора мобільного зв'язку, при цьому всі службові команди оператора проходять через систему безпеки дублюючої базової мережі. Таке рішення дає можливість ідентифікувати спроби різних видів атак на мобільні пристрої. В Ізраїлі таким чином здійснюється захист мобільних пристроїв усіх урядовців високого рангу, офіцерів ЦАХАЛ, співробітників ШАБАК та інших спецслужб.

Ізраїль належить до категорії країн з потужними ІТ-технологіями, що дає змогу не тільки активно захищати власну інфраструктуру, а й використовувати кібернетичний простір для атаки на інформаційні ресурси та мережі потенційного противника. Універсальних міжнародних правових механізмів, що обмежують використання програмно-апаратних засобів для ураження комп'ютерних систем, не розроблено тому Ізраїль застосовує їх без узгодження з міжнародними організаціями та іноземними державами. Зокрема, на початку 2010 року воєнно-політичне керівництво Ізраїлю прийняло концепцію, що допускає кібератаки на сервери та електронні адреси, через які робляться спроби руйнування інформаційного простору, комп'ютерних систем і електронних баз даних Ізраїлю.

В Ізраїлі поруч з державними структурами, що в основному застосовують силові методи протидії проти тероризму і зовнішнього інформаційного впливу, цілеспрямовану роботу в цьому напрямі здійснюють деякі неурядові організації. Серед них Міжнародний інститут з протидії тероризму (International Institute for Counter-Terrorism) – ізраїльська громадська організація, що досліджує історію тероризму, сучасний стан, рівень загроз, методи і способи боротьби, а також прийняті на державному рівні рішення. У популярному методичному посібнику «Все, що потрібно знати про тероризм», підготовленому цим інститутом, не тільки привернуто увагу до проблеми, й систематизоване уявлення населення про особливості прояву тероризму в Ізраїлі. Діяльності ізраїльських громадських контртерористичних організацій притаманний пропагандистський характер, вони прагнуть

донести до аудиторії думку про неприпустимість пособництва терористам, а також про загрозу «громадянської недбалості» – небажання населення турбуватися про свою безпеку та безпеку оточуючих.

Зважаючи на потенційні хакерські загрози ззовні, Ізраїль постійно вдосконалює засоби кіберзахисту. Ізраїльська модель стратегії захисту кіберпростору спирається на накопичений досвід, що дає можливість ізраїльським фахівцям залишатися на передових позиціях у світі. Представники ізраїльського уряду неодноразово наголошували, що Ізраїль прагне до взаємовигідного обміну досвідом з іншими країнами. У цьому контексті для боротьби та нейтралізації діяльності терористів у кібернетичному просторі він активно співпрацює з фахівцями Кібернетичного командування ЗС США.

Висновки: 1. Розмитість конфігурацій інформаційної інфраструктури в Україні дає можливість маніпулювати інформацією та її сприйняттям на користь країні-агресору.

2. За результатами аналізу системного підходу Ізраїлю щодо захисту національного кібернетичного простору обґрунтовано доцільність застосування цього досвіду органами державної влади та спеціальними службами України в контексті протистояння гібридній агресії Російської Федерації проти України. Крім захисних функцій українські фахівці мають нарощувати такий потенціал у кіберпросторі, зокрема, створювати нове програмне забезпечення, що необхідне як для захисту від кібератак, так і для їх проведення.

3. Перспективним напрямом удосконалення системи кібербезпеки в Україні є активізація зусиль уповноважених правоохоронних органів нашої держави стосовно міжнародного співробітництва з Ізраїлем, що надасть можливість впровадити у практичну площину кращі практики зарубіжного досвіду в контексті удосконалення вітчизняної моделі кібербезпеки.

Анотація. Доповідь підготовлена на підставі досвіду практичної діяльності уповноважених структур Ізраїлю, що відповідають за попередження і нейтралізацію терористичних атак у кібернетичному просторі на об'єкти критичної інфраструктури.

Автор обґрунтував доцільність використання зазначеного досвіду Ізраїлю щодо захисту національного інформаційного (кібернетичного) простору в умовах гібридної агресії Російської Федерації проти України.

Запропоновано конкретні рекомендації уповноваженим органом України у сфері кібербезпеки щодо підвищення ефективності їх функціонування.

Література:

1. Про боротьбу з тероризмом : Закон України від 20.03.2003 р. № 638-І. Відомості Верховної Ради України. 2003. № 25. Ст. 180. (Із змінами, внесеними згідно із Законами, № 2581-VIII від 02.10.2018, ВВР, 2018, № 46, ст. 371).

2. Стратегія кібербезпеки України : Указ Президента України від 15.03.16 р. № 96 // Офіційний вісник України. – 2016. – № 23. – Ст. 899.

3. Асиметрична стратегія Ізраїлю в період становлення держави : висновки для України : аналітична доповідь. Київ : Національний інститут стратегічних досліджень, 2018. Розд. 1. С. 7 – 12.

4. Гребенюк М.В., Леонов Б.Д., Досвід Ізраїлю у сфері забезпечення кібербезпеки. №2 від 2018. С. 45 – 50.

5. Tabansky L, Ben I Israel, Cybersecurity in Israel, DOI 10.1007/978-3-319-18986-4_5. (Дата звернення 25.02.2020).

6. Wirkuttis Nadine, Klein Hadas, Cyber, Intelligence, and Security, Volume 1. № 1. URL : inss.org.il/publication/arifitial-intelligence-cybersecurity/. (Дата звернення 15.02.2020).

7. Charles J, Brooks, Christopher Grow, Philip Craig, Donald Short, SYBEX Inc., 2021 Challenger Drive Alamedia, CA, United States/ URL : dl.acm.org/doi/book/10.555/3306803. (Дата звернення 15.02.2020).

8. Alpher N. Yossi. Periphery : Israel`s Search for Middle East Allies. – Rowman & Littlfield, 2015. 196 p.

УДК 004.056

Трубей Антон Иванович,
заведующий НИЛ прикладной информатики
Учреждение Белорусского государственного университета «НИИ прикладных проблем математики и информатики»
trubeia@mail.ru

ТЕОРЕТИКО-ВЕРОЯТНОСТНАЯ МОДЕЛЬ ФИЗИЧЕСКОГО ПРОЦЕССА НА ОСНОВЕ ШУМОВОГО ДИОДА, ИСПОЛЬЗУЕМОГО В ГЕНЕРАТОРЕ СЛУЧАЙНЫХ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Введение

В соответствии с [1] для физических генераторов случайных числовых последовательностей (ФГСЧП), входящих в состав средств криптографической защиты информации (СКЗИ), должна быть разработана теоретико-вероятностная модель (ТВМ) используемого в генераторе случайного физического процесса и проведена экспериментальная проверка соответствия указанной модели реализации соответствующего ФГСЧП.

При изучении любой системы методом математического моделирования необходимо построить ее математическую модель, то есть при помощи математических соотношений описать функционирование системы. Как правило, реальная система находится под воздействием случайных факторов или сам механизм функционирования содержит элементы случайности. Такая система называется стохастической, а для ее описания используется аппарат теории вероятностей и математической статистики. Математическая модель, содержащая элементы случайности (события, величины, векторы, процессы) называется вероятностной моделью [2]. ТВМ – это модель, основанная на применении статистической или теоретико-вероятностной методологии по отношению к повторяющимся феноменам, в которой обеспечивается учет случайных факторов в процессе функционирования системы. Данная модель оперирует количественными критериями при оценке повторяющихся явлений и позволяет учитывать их нелинейность, динамику, случайные возмущения за счет

выдвижения на основе анализа результатов наблюдений гипотез о характере распределения некоторых случайных величин, сказывающихся на поведении системы.

По существу, теоретико-вероятностные и статистические модели отличаются уровнем неопределенности знаний о моделируемой системе, существующей на момент синтеза модели. В случае, когда представления о системе основываются исключительно на гипотезах о характере системы и возмущающих воздействий, не подкрепленных результатами наблюдений, ТВМ является единственно возможной. Если на этапе синтеза модели уже существуют данные, полученные опытным путем, то появляется возможность подкрепления гипотез за счет их статистической обработки.

Экспериментальная проверка ТВМ, положенной в основу ФГСЧП, включает статистическое оценивание параметров ТВМ и статистическую проверку гипотез о функциях распределения ТВМ.

1. Описание гипотез о вероятностных функциях распределения физического источника случайности на основе шумового диода

Наиболее часто в ГСЧП в качестве первичного источника энтропии используется физический источник случайности на основе шумового диода. В частности, в физическом источнике случайности на основе шумового диода аналоговый сигнал, через конденсатор подается на вход компаратора. Выход компаратора подается на вход таймера, работающего в режиме счетчика. Таймер производит подсчет количества импульсов с выхода компаратора на заданном временном интервале. В качестве случайного бита принимается младший бит (0 или 1) счетчика таймера.

Результаты повторных измерений случайной величины ξ (числа отсчетов) могут значительно различаться. Количество отсчетов с выхода компаратора во временном интервале является случайным событием. Необходимо определить вероятность $P_k(t)$, что в интервале времени t счетчик зарегистрирует k импульсов. Если для ξ, представляющей собой число событий за фиксированное время, выполняются условия:

а) ξ может принимать только целые положительные значения, включая 0;

б) вероятность двух (и более) событий на достаточно малом временном интервале бесконечно мала по сравнению с вероятностью одного события;

в) события статистически независимы (во времени или пространстве);

г) время (или пространство) однородно для изучаемых событий,

то ξ имеет распределение Пуассона (распределение дискретного типа).

Таким образом, можно выдвинуть гипотезу, что случайная величина ξ, представляющая собой число импульсов с выхода компаратора шумового диода на заданном временном интервале t, также должна иметь распределение Пуассона:

$$P_k(t) = \frac{(nt)^k}{k!} e^{-nt} = \frac{\lambda^k}{k!} e^{-\lambda}, \qquad (1)$$

где $\lambda = nt$, n – среднее число импульсов за единицу времени, то есть, их интенсивность.

Математическое ожидание (среднее количество отсчетов) и дисперсия соответственно равны: $M(\xi) = nt = \lambda$; $D(\xi) = nt = \lambda$. То есть, распределение Пуассона полностью определяется заданием только одного параметра – среднего количества отсчетов.

Условия формирования распределения Пуассона, указанные в п.п. а) – г), иногда могут нарушаться. Например, парное прохождение импульсов нарушает условия а) – г). Кроме того, любое устройство затрачивает на измерение и регистрацию события конечное время, в течение которого оно не способно «правильно» обработать следующее событие. Это так называемое мертвое время (*dead time*). Влияние мертвого времени нарушает условия в), г). В этом случае ξ будет иметь другое распределение.

Анализ формулы (1) показывает, что с ростом k распределение становится симметричным. При $\sqrt{\lambda} \gg 1$ – становится практически полностью симметричным. Условие $\sqrt{\lambda} \gg 1$ означает, что вероятности близких значений k будут почти одинаковы, и в

этом случае целесообразно рассматривать вероятность не отдельного значения *k*, а вероятность попадания *k* в заданный интервал значений Δk вблизи некоторого значения *k*. Тем самым совершается переход от дискретного распределения к непрерывному. При больших значениях *k* распределение Пуассона переходит в нормальное распределение, для которого дисперсия равна математическому ожиданию.

2. Проверка гипотез о законе распределения с применением критерия согласия хи-квадрат, когда по выборке оцениваются параметры распределения

Предположим, что некоторый алгоритм осуществляет моделирование случайной величины ξ (например, количество отсчетов с выхода компаратора на заданном временном интервале). В результате n-кратного обращения к данному алгоритму моделируется случайная выборка $X = \{x_1, \dots, x_n\}$. Необходимо при помощи *X* проверить гипотезу H_0 о том, что случайная величина ξ имеет функцию распределения $F_\xi(x) = F_0(x)$, где $F_0(x)$ – фиксированная функция распределения при некоторых неизвестных значениях параметров $a_j (j = 1, \dots, s)$.

Предположим, что выборка разбита на *r* групп, соответствующих *r* непересекающимся множествам $S_1, \dots, S_r$. Обозначим наблюдаемую группу частот $v_1, \dots, v_r$, а соответствующие вероятности – $p_i(a_1, \dots, a_s)$, $(i = 1, \dots, r)$. Если бы значения параметров были известны, то можно было бы применить критерий хи-квадрат:

$$\chi^2 = \sum_{i=1}^{r} \frac{[v_i - np_i(a_1, \dots, a_s)]^2}{np_i(a_1, \dots, a_s)}. \qquad (2)$$

Однако в данном случае значения параметров a_j неизвестны и должны быть оценены по выборке. Существует множество различных методов оценки параметров a_j, так что свойства выборочного распределения статистики χ^2 будут в той или иной степени зависеть от избранного метода. В частности при применении ме-

тода оценки по минимуму χ^2 необходимо определить «наилучшие» значения параметров $a_j (j = 1, \dots, s)$ так, чтобы сделать величину χ^2 сколь угодно малой. Доказано, что величина χ^2 при подстановке этих значений a_j в формулу (2), при $n \to \infty$ имеет распределение хи-квадрат с *r*–*s*–1 степенями свободы [3].

Исследования проводились на суммарной выборке объемом 10 240 000 отсчетов. Суммарная выборка была разбита на 10 выборок объемом 1 024 000 отсчетов. На основании эмпирического анализа частот встречаемости отсчетов можно сделать вывод, что значения частот, в том числе средние значения, с течением времени постепенно смещаются в сторону увеличения. Это означает, что физический процесс, генерируемый источником случайности на основе шумового диода, является недостаточно стационарным (возможно, за счет постепенного нагревания диода).

Проверка гипотез о функции распределения осуществлялась для выборок объемом соответственно: 10 240 000 отсчетов и 3 072 000 отсчетов (за большей, чем первая). При этом проводилось объединение малочисленных крайних групп отсчетов слева и справа ($\xi \le 33;\ \xi \ge 55$). В таблице 1 приведены оценки параметров – математического ожидания и дисперсии.

Таблица 1

Оценки параметров для выборок различного объема

Объем выборки	10 240 000 отсчетов	3 072 000 отсчетов
$\hat{m} = \frac{1}{n}\sum_{i=1}^{r} v_i \xi_i$	43,63	44,15
$\hat{\sigma}^2 = \frac{1}{n-1}\sum_{i=1}^{r} v_i (\xi_i - \hat{m})^2$	14,25	14,29

Рассмотрим применение критерия хи-квадрат для различных гипотез о предполагаемом распределении случайной величины ξ, представляющей собой количество импульсов с выхода компаратора на заданном временном интервале. В качестве возможных функций распределения рассмотрим распределение Пуассона, отрицательное биномиальное распределение, нормальное распределение.

2.1. Распределение Пуассона. В случае справедливости гипотезы значения математического ожидания и дисперсии должны быть равны. Однако из таблицы 1 видно, что оценки математического ожидания и дисперсии значительно различаются. Следовательно, гипотеза отвергается.

2.2. Отрицательное биномиальное распределение. Если выборки обнаруживают значимое отклонение от распределения Пуассона, то совпадение можно значительно улучшить, выдвинув гипотезу о том, что параметр λ является случайной величиной с плотностью вероятности $\frac{a^x}{\Gamma(x)} x^{x-1} e^{-ax}$, где a, x – положительные параметры. В общем случае выборки описываются отрицательным биномиальным распределением. В случае справедливости гипотезы между оценками математического ожидания и дисперсии должно соблюдаться соотношение $\hat{\sigma}^2 = \frac{\hat{m}}{p}$, где $0 \leq p \leq 1$. То есть дисперсия должна быть не меньше математического ожидания. Однако из таблицы 1 видно, что условия не выполняются. Таким образом, гипотеза отклоняется.

2.3. Нормальное распределение. Сравниваем теоретические и опытные частоты с помощью критерия хи-квадрат согласия по формуле (2), задаем уровень значимости α и определяем число степеней свободы $k = r - 3$, где r – число групп после объединения. С использованием программного комплекса STATISTICA, на основе полученных выборок были построены соответствующие гистограммы. На рисунке 1 приведена гистограмма частот для выборки объемом 3 072 000 отсчетов.

Из гистограммы, приведенной на рисунке 1, видно, что она имеет одну ярко выраженную вершину. Распределение частот отсчетов достаточно симметрично. При этом не удалось подтвердить гипотезу о нормальном распределении на приемлемом уровне значимости, хотя значение критерия χ^2 становится существенно меньше, чем для выборки объемом 10 240 000 отсчетов. Это означает, что данная выборка в большей степени согласуется с гипотезой о нормальном распределении, чем суммарная выборка. Возможно, процесс функционирования генератора с течением времени стабилизировался (дальнейшее нагревание диода существенно замедлилось).

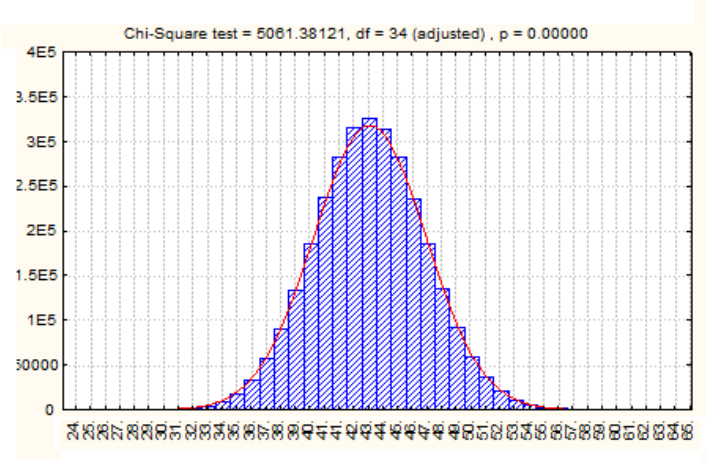


Рисунок 1. Гистограмма частот выборки объемом 3 072 000 отсчетов

2.4. Смесь распределений. Во многих практических задачах выборка может соответствовать не одной, а нескольким моделям. Распределение такой выборки описывается смесью распределений. Конечной смесью L распределений $(2 \le L < \infty)$ с плотностями распределения компонент смеси $[F_l(x)]\,(L = 1, \dots, L)$ называется плотность распределения вида [4]:

$$p_\xi(x) = \sum_{l=1}^{L} \pi_l \, f_l(x), \qquad (3)$$

где π_l – удельные веса (априорные вероятности) компонент смеси: $\pi_1 + \dots + \pi_L = 1$.

3. Оценка стабильности вероятностных характеристик физического процесса, используемого в ГСЧП

Функционирование физического датчика случайных чисел (ФДСЧ) основано на преобразовании некоторого случайного физического процесса по определенному правилу в случайную последовательность с равномерным распределением на интервале [0, 1]. Основным недостатком данного метода является возможная нестабильность вероятностных характеристик случайной величины используемого процесса. Поэтому при исследовании ФДСЧП необходимо оценить стабильность

функционирования параметров ФДСЧП, то есть рассмотреть гипотезу о том, что распределение вероятностей наблюдаемой случайной величины физического процесса зависит от времени $p\{\xi_t = i\} = p_{i,t}$, и определить статистическую значимость отклонений данных параметров с течением времени. Для подтверждения стабильности эмпирического закона распределения необходимо осуществлять проверку устойчивости работы ФДСЧП в течение определенного времени.

Предположим, что имеем комплект, состоящий из $M \geq 2$ двоичных последовательностей, выработанных датчиком в промежутки времени $\Delta t_1, \dots, \Delta t_M$. Из данного комплекта сформируем M независимых выборок, полученных в результате статистического анализа данных последовательностей. Каждая из выборок есть реализация некоторой полиномиальной схемы с исходами $1, \dots, N$. Объемы выборок равны $n_1, \dots, n_M$. Обозначим $n = \sum_{k=1}^{M} n_k$, $n_0 = min\{n_1, \dots, n_M\}$, $\nu_{k,i}$ – частота (число появлений) символа i. В качестве выборок можно рассматривать, например, частоты встречаемости пересекающихся (непересекающихся) -грамм, гистограммы частот F_k попадания вероятностей p_{ij} в каждый из 10 подинтервалов, на которые разбивается интервал [0; 1]. Гипотеза однородности предполагает, что вероятностные свойства наблюдаемой последовательности не изменяются во времени. То есть, во все промежутки времени $\Delta t_1, \dots, \Delta t_M$ вероятности $p_{k,1}, \dots, p_{k,N}$ исходов $1, \dots, N$ не изменились. Это означает, что возможные изменения внешних условий и отклонения параметров физического датчика не являются статистически значимыми.

Полагаем, что выборки статистически однородны и что для них выполняется гипотеза H_0, если $p_{1,i} = \dots = p_{M,i}$; $i = 1, \dots, N$. В противном случае будем говорить, что выполняется альтернатива H_1. При альтернативе вероятности исходов могут быть постоянными или изменяться с ростом объемов выборок.

Для проверки однородности, обычно, используют статистику хи-квадрат:

$$\chi^2 = \sum_{k=1}^{M}\sum_{i=1}^{N}\frac{(\nu_{k,i}-n_k m_i/n)^2}{n_k m_i/n} = n\sum_{k=1}^{M}\sum_{i=1}^{N}\frac{1}{n_k m_i}\left(\nu_{k,i}-m_i\frac{n_k}{n}\right)^2,$$

где $m_i = \sum_{k=1}^{M}\nu_{k,i}$.

При гипотезе H_0 и $n_0 \to \infty$ статистика χ^2 сходится по распределению к распределению хи-квадрат с $(M-1)(N-1)$ степенями свободы. При этом для всех ожидаемых частот должно соблюдаться условие: $n_k p_{k,i} \geq 10$.

В нашем случае для проверки однородности выборок будем использовать модификацию статистики хи-квадрат, предложенную А.М. Зубковым [5]:

$$\zeta^2 = \inf_{\substack{q_1,\dots,q_N>0;\\ q_1+\dots+q_N=1}} n\sum_{k=1}^{M}\sum_{i=1}^{N}\frac{1}{n_k m_i}(\nu_{k,i}-q_i)^2 = \left(\sum_{i=1}^{N}\sqrt{\sum_{k=1}^{M}\frac{\nu_{k,i}^2}{n_k}}\right)^2 \qquad (4)$$

Если и справедлива гипотеза H_0, то при $n_0 \to \infty$ статистика $\zeta^2 - n$ также сходится к распределению хи-квадрат с $(M-1)(N-1)$ степенями свободы.

Для анализа был взят комплект из 10 выборок по 1 024 000 отсчетов каждая. По формуле (4) осуществлялась оценка однородности комплекта в целом. В этом случае $\zeta^2 - n = 153\,953.3$ для 9×30=270 степеней свободы. Это означает, что выборка в целом чрезвычайно неоднородна. Проводилось также попарное сравнение выборок на однородность по формуле (3). Результаты сравнений приведены в таблице 2. На пересечении *i*-й строки и *j*-го столбца представлены значения статистики $\zeta^2 - n$, вычисленные при сравнении *i*-й и *j*-й выборок. Число степеней свободы: 1×30=30.

При попарных сравнениях также отмечается неоднородность выборок. Чем больше разность между номерами выборок (*i, j*), тем больше статистическое различие между ними. Выборки, зарегистрированные в соседние промежутки времени, более однородны, чем выборки, выработанные через более длительные временные отрезки. Таким образом, подтверждаются результаты эмпирического анализа выборок.

Таблица 2

Проверка однородности выборок при попарном сравнении

№ выборки	2	3	4	5	6	7	8	9	10
1	220	3 943	9 843	27 209	32 323	30 654	49 324	50 778	77 230
2		2 992	7 097	24 926	29 589	37 445	35 697	56 683	72 582
3			2 776	6 731	9 852	25 557	31 870	30 682	53 979
4				2 316	3 938	75 20	21 979	28 635	39 314
5					484	3 216	5 057	10 819	29 190
6						869	3 780	7 402	24 503
7							756	3 939	9 139
8								959	5 379
9									2 499

4. Оценка наличия марковской зависимости

Однородная цепь Маркова *s*-го порядка ($s < \infty$) описывает зависимость каждого наблюдения только от *s* предыдущих состояний. С ростом *s* число параметров цепи Маркова порядка *s* растет с экспоненциальной скоростью (порядка N^{s+1}), что ограничивает применение этой модели небольшими значениями *s*.

Для выявления марковской зависимости в анализируемой последовательности строилась статистическая оценка порядка цепи Маркова $\hat{s}$. Значение $\hat{s} > 0$ говорит о наличии марковской зависимости, значение $\hat{s} = 0$ соответствует последовательности независимых испытаний.

Метод максимального правдоподобия, который традиционно используется для построения статистических оценок, не применим для оценивания порядка цепи Маркова. Использование данного метода для решения этой задачи приводит к проблеме, известной как *over-fitting* – чрезмерной «подгонке» модели под имеющиеся данные. В результате выбирается наиболее сложная модель, поскольку за счет увеличения числа параметров становится возможным увеличивать функцию правдоподобия. Поэтому для построения оценок порядка *s* использовался информационный функционал Байеса (BIC), который учитывает число параметров модели [6]. Он имеет вид:

$$\mathrm{BIC}(s) = -2\hat{l}(X,s) + D\log n, \qquad (5)$$

где $\hat{l}(X,s)$ – статистическая оценка логарифмической функции правдоподобия, вычисленная по последовательности $X = (x_1,...,x_n)$ в предположении, что порядок цепи Маркова равен *s*, $D = N^s(N-1)$ – число независимых параметров модели.

Оценка $\hat{s}$ определяется при решении задачи на минимум: $\hat{s} = \arg\min_{0 \le s^* \le S} BIC(s^*)$, где S – максимально допустимое значение порядка s, задаваемое априори исходя из имеющихся данных. В таблице 3 приведены значения BIC для $s = 0, 1, 2, 3$, вычисленные по анализируемой последовательности X.

Таблица 3

Значения BIC для последовательности X объемом 10 240 000 отсчетов

s	0	1	2	3
BIC(s)	28 093 850.4	28 103 693.1	28 580 777.7	48 050 062.4

Таким образом, в результате оценивания порядка для модели однородной цепи Маркова на основе байесовского информационного критерия было получено $\hat{s} = 0$, которому соответствует минимум BIC. Это означает, что по критерию принято решение о несогласии последовательности с моделью однородной бинарной цепи Маркова, т.е. марковская зависимость в последовательности не обнаружена.

5. Оценка статистических свойств выходной бинарной последовательности

Выходная бинарная последовательность получена из первичной последовательности посредством определения значения младшего бита счетчика количества отсчетов (0 – четное число, 1 – нечетное число). Вычислим гипотетические вероятности 0 и 1 в выходной бинарной последовательности. В таблице 4 приведено количество четных и нечетных отсчетов в гистограммах частот выборок, а также оценки их согласия с равновероятным распределением по критерию χ^2.

Таблица 4

Распределение четных и нечетных отсчетов в выборках

Объем выборки	10 240 000 отсчетов	3 072 000 отсчетов
Число нечетных отсчетов	5 121 613	1 536 263
Число четных отсчетов	5 118 387	1 535 637
P-значения статистики χ^2 (с одной степенью свободы)	0.313395	0.720967

Из таблицы видно, что для обеих выборок принимается гипотеза о равновероятном распределении четных и нечетных отсчетов. Следовательно, в бинарных последовательностях распределение 0 и 1 будет близко к равновероятному.

Аннотация.

1. Физический процесс, генерируемый источником случайности на основе шумового диода, является недостаточно стационарным.

2. Частоты встречаемости отсчетов достаточно симметрично распределены относительно математического ожидания и имеют одну моду. При этом не удалось подтвердить гипотезу о нормальном распределении на приемлемом уровне значимости.

3. Наличие марковской зависимости с применением байесовского информационного критерия (BIC) не выявлено.

4. Вероятности отсчетов согласуются с гипотезой о равновероятном распределении четных и нечетных отсчетов. Следовательно, в выходных бинарных последовательностях распределение 0 и 1 также будет близко к равновероятному.

Литература:

1. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации. [Электронный ресурс]. – 2016. – Режим доступа: https://www.tc26.ru. – Дата доступа: 12.04.2018.

2. Харин, Ю.С. Практикум на ЭВМ по математической статистике: Для мат. спец. ун-тов / Ю.С.Харин, М.Д.Степанова. – Мн.: издво «Университетское». – 1987. – 304 с.

3. Крамер, Г. Математические методы статистики / Г. Крамер – М.: Мир, 1976.

4. Харин, Ю.С. Математические и компьютерные основы статистического анализа данных и моделирования: учеб. пособие / Ю.С.Харин, В.И.Малюгин, М.С.Абрамович. – Минск: БГУ, 2008. – 455 с.

5. Зубков, А.М. Об одной статистике для проверки однородности полиномиальных выборок / А.М. Зубков, Б.И. Селиванов // Дискретная математика. – 2014.

6. Csiszar, I. Consistency of the BIC order estimator / I. Csiszar, P. Shields // Electronic research announcments of the American mathematical society. – 1999. – Vol. 5. – P. 123–127.

УДК 004.891

Хохлачова Юлія Євгеніївна, доцент, к.т.н.
Національний авіаційний університет
hohlachova@gmail.com

Аясрах Ахмад Расмі Алі
Національний авіаційний університет
ahmadaesr@gmail.com

МОДЕЛЬ ПОТЕНЦІЙНО НЕБЕЗПЕЧНОГО КОРИСТУВАЧА

Особливістю інформаційних систем (ІС) в першу чергу є їх принадливість для окремих осіб чи певних груп, які з метою використання цих ІС та їх ресурсів прагнуть бути чи є користувачами систем. Ця принадливість найчастіше є обумовленою характером та об'ємом інформації, яка вводиться, обробляється, зберігається та циркулює в системах. Якщо та чи інша особа (користувач ІС) здійснює спробу несанкціонованого доступу до об'єкта захисту, то такий користувач є порушником [1].

Отже при аналізі захищеності ІС, насамперед, необхідно розглянути об'єкт захисту (тобто ІС) та модель порушника.

Для опису об'єктів захисту введемо набір $O=\{o(t)\}$, що описує склад об'єктів, які захищають. З урахуванням потокової схеми опису систем захисту додатково в розгляд введемо набір $C=\{c(r)\}$ (або $C=\{c(i,j)\}$), що описує зв'язки (взаємодії) між елементами об'єкта, де $c(i,j)=1$ – якщо є зв'язок між елементами, $o(i)$ й $o(j)$, і $c(i,j)=0$ – якщо зв'язку немає.

Очевидно, що такий опис об'єкта у виді довільної мережі $<O,C>$ є найбільш загальним, однак для урахування особливостей розглянутої моделі й вирішення завдань, пов'язаних з одержанням оцінок, необхідно, по-перше, для кожного елемента та зв'язку мати відповідні характеристики (відповідно, множини $H(O)$ й $H(C)$) і, по-друге, для моделювання захисту принципово важливо розрізняти якісно різні зв'язки (інформаційні, керуючі тощо). Уточнення типу зв'язків може бути здійснене різними шляхами, наприклад, у характеристиках зв'язку $h(c)$ з

множини $H(C)$. Але, оскільки множини характеристик будуть використовуватися лише при одержанні оцінок, для простоти формулювання моделі введемо список зв'язків $C=[C_1,C_2,...,C_n]$, де $C_1,C_2,...$ відповідають зв'язкам 1-го, 2-го та інших типів.

Також при описі об'єкта захисту необхідно врахувати такий параметр, як цілісність, тобто ступінь пошкоджень і рівень працездатності об'єкта $P(<O,C>)$. Його введення в модель об'єкта є доцільним через використання тестування об'єкта захисту й внутрішньої діагностики СЗІ. Таким чином, кожний суб'єкт $o(t)$ у складі об'єкта захисту O й зв'язок $c(i,j)$ отримують свій коефіцієнт працездатності $P=p(c(i,j))=0..1$ та $P=p(o(t))=0..1$ відповідно, де коефіцієнт p буде змінюватися в інтервалі від 0 (повна не функціональність – руйнування) до 1 (повна працездатність).

Крім того, повний опис об'єкта неможливий без урахування його зовнішніх зв'язків і переліку взаємодіючих з ним зовнішніх об'єктів, які позначаються: EO – для зовнішніх об'єктів і EC – для зв'язків із зовнішніми об'єктами. Оскільки урахування зовнішніх взаємодій є особливо важливим при побудові комплексних оцінок, то істотними є відповідні множини характеристик $H(EO)$ і $H(EC)$ [2].

У термінах вирішуваного завдання оцінки безпеки інформаційних мереж опис зовнішнього середовища має містити не тільки опис зовнішніх об'єктів, але й опис передбачуваного порушника. У найпростішому випадку порушник описується множиною зовнішніх впливів (загроз) $T=\{t_i\}$ з відповідними характеристиками $H(T)=\{h(t)\}$. У загальному випадку необхідно розглядати різні типи зовнішніх впливів: $T_1,T_2,...$. Це відповідає різним цілям порушника: знімання інформації, проникнення, руйнівні дії і т.д. Таким чином, у загальному випадку є список множин: $T=\{t_i\}$ при $i=1,...,N$, який описується відповідним списком характеристик $H(T)$.

Крім того, у моделі також необхідно врахувати так звані внутрішні «напіввзаємодії», що відповідають, з одного боку, можливому впливу на об'єкт (елемент об'єкта), а з іншого – можливості елемента самому виконати дії, не передбачені технологією і які можуть мати небажані наслідки [3].

Нехай можливі різні впливи на елементи й зв'язки об'єкта захисту (вразливості) характеризуються відповідно множинами $U(O)$ та $U(C)$, де $U(O)=\{u(i)\}$ та $U(O)=\{u(i,j)\}$.

Аналогічно, можливість елемента (зв'язку) виявити активність, тобто виявити деякий вплив, непередбачуваний технологією обробки інформації (наприклад, вихід з ладу елемента (зв'язку)), буде позначатися $v(i)$ або $v(i,j)$ з множинами $V(O)$ і $V(C)$ відповідно, а множини $V(O)=\{v(i)\}$ та $V(C)=v\{(i,j)\}$, у свою чергу, можуть поєднуватися в список V.

Як складові описи об'єкта U і V для одержання оцінок мусять мати відповідні набори характеристик $H(U)$ і $H(V)$.

Передбачається, що загрози мають створювати пари з різними «уразливостями» – u з множин $U(O)$ і$U(C)$, тобто «зовнішній вплив» (загроза з боку порушника) має відповідати «можливості такого впливу» (уразливості) для створення пари (t,u) (якщо такий зовнішній вплив не конкретизований, крім того, для певного об'єкта, такого як $t=t(i)$ або $t=t(i,j)$). У результаті такого зовнішнього посилання загроза може «розбудовуватися» як по відповідних технологічних (санкціонованих) зв'язках моделі, так і по нетехнологічних, які в загальному випадку є парами виду (v,u).

Отже, до складу моделі, що описує порушника, крім безпосередніх загроз входять відзначені вище множини вразливостей U і внутрішніх впливів V як фактори, що сприяють нападу і як єдині джерела впливів за відсутності зовнішнього порушника.

Анотація. При аналізі захищеності ІС розглянуто об'єкт захисту (тобто ІС) та модель порушника з урахуванням відповідних характеристик та уточненням типів зв'язків. Описано об'єкт захисту з урахуванням цілісності, тобто ступеня пошкоджень і рівня працездатності об'єкта, а також його зовнішніх зв'язків і переліку взаємодіючих з ним зовнішніх об'єктів.

Показано, що до складу моделі, яка описує порушника, крім безпосередніх загроз входять відзначені множини вразливостей і внутрішніх впливів як фактори, що сприяють нападу і як єдині джерела впливів за відсутності зовнішнього порушника.

Література:

1. Бурячок В.Л. Інформаційна та кібербезпека: соціальний аспект / Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. – К.: ДУТ, 2015. – 288 с.

2. Анин Б.Ю. Защита компьютерной информации / Анин Б.Ю. – СПб: БХВ-Санкт-Петербург, 2000. – 384 с.

3. Козюра В.Д. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах / Козюра В.Д., Ткач Ю.М. та інші. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. – 144 с.

УДК 004.056.5

***Часновський Єгор Анатолійович**, аспірант*
Національний університет біоресурсів
та природокористування
egor.chasnovskii@gmail.com

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПРОЦЕСІ УПРАВЛІННЯ РЕСУРСАМИ КІБЕРЗАХИСТУ

В процесі діяльності будь-яких сучасних інформаційних та інформаційно-телекомунікаційних систем на підприємствах виникає питання щодо належного дотримання базових парадигм інформаційної безпеки – цілісності, безпечності та доступності. Враховуючи, що більшість активів підприємств перебувають у цифровому вигляді, загроза несанкціонованого доступу через цифровий пристрій і його програмне забезпечення безсумнівно має грати ключову роль при побудові системи менеджменту ІБ підприємства та оцінці ризиків ІБ. Своєчасне проведення процедури оцінювання та надалі управління ризиками інформаційної безпеки в режимі реального часу грає ключову роль. В даному випадку мінімізації часу та ресурсів дозволить отримати реальні результати оцінювання ступеню ризику в момент запуску програмного засобу, що значно підвищить ефективність процесу оцінювання та управління ризиками інформаційної безпеки (ІБ).

Метою роботи є дослідження існуючих інформаційних технологій оцінювання ризиків ІБ в процесі управління ресурсами кіберзахисту.

Розглянемо деякі з актуальних для оцінювання та управління ризиками методи, які сьогодні використовуються.

Метод ISRAM. Метод аналізу ризиків інформаційної безпеки (ISRAM) був розроблений у грудні 2003 року в Національному науково-дослідному інституті електроніки та криптології та Технологічному інституті Гебзе. Це кількісний підхід до аналізу ризиків та модель опитування, яка використовується для аналізу ризиків ІБ.

Метод включає дві основних ознаки ризику – ймовірність і наслідки проведення двох окремих і незалежних досліджень. Метод базується на моделюванні ризику як комбінації ймовір-

ності та наслідку порушення безпеки. Фактором ризику в підході ISRAM є числове значення від 1 до 25. Це числове значення відповідає якісному, високому, середньому або малому значенню, і саме ця якісна величина, на якій базуються рішення з управління ризиками. Вона складається з семи кроків, перші чотири етапи є етапом підготовки, де будуються опитування. Під час кроку 5 опитування завершуються, а аналіз ризиків виконується під час етапу 6. Останнім кроком є оцінка результату. Результатом аналізу є числове значення ризику, який розраховується за допомогою формули. Цей метод є масштабованим, оскільки входи не є специфічними для групи / сценаріїв і можуть бути повторно використані з незначною корекцією [1].

Метод NIST. Метод NIST (National Institute of Standards and Technology) являється методом оцінки ризиків Національного інституту стандартів і технологій США. Методика охоплює широке коло завдань, що пов'язані зі стратегією управління ризиками і є основою для розроблення власної системи управління ризиками. Запропонований процес оцінювання ризику ІБ, представляється у вигляді таблиці, що відображає залежність ризику від двох вхідних змінних: потенційного збитку і ймовірності можливого інциденту. При цьому значення кожної змінної, зокрема ризику, оцінюється за трирівневою шкалою. Такий «жорсткий» механізм отримання оцінок ризику суттєво обмежує точність результатів, забезпечуючи їх оперативність та відтворюваність.

Програмне забезпечення RiskWatch. Розроблений американською компанією RiskWatch, є потужним засобом аналізу та управління ризиками. У сімейство RiskWatch входять програмні продукти для проведення різних видів аудиту безпеки. Воно включає в себе наступні засоби аудиту та аналізу ризиків: RiskWatch for Physical Security – для фізичних методів захисту ІС; RiskWatch for Information Systems – для інформаційних ризиків; HIPAA-WATCH for Healthcare Industry – для оцінки відповідності вимогам стандарту HIPAA; RiskWatch RW17799 for ISO17799 – для оцінки вимогам стандарту ISO17799. У методі RiskWatch в якості критеріїв для оцінки і управління ризиками використовуються «пророцтво річних втрат» (Annual Loss Expectancy - ALE) і оцінка «повернення від інвестицій» (Return on Investment - ROI).

Сімейство програмних продуктів RiskWatch, має масу переваг. RiskWatch допомагає провести аналіз ризиків і зробити обґрунтований вибір заходів і засобів захисту [2].

Метод COBRA. Метод COBRA (Consultative Objective and BiFunctional Risk Analysis, developer — C & A Systems Security Ltd, Велика Британія) орієнтований на підтримку вимог стандарту ISO 17799. У комплект програмного забезпечення (ПЗ) входять модулі COBRA ISO 17799 Security Consultant, COBRA Policy Compliance Analyst и COBRA Data Protection Consultant, а також менеджер модуля COBRA, який призначений для налаштування та зміни наявної бази знань. COBRA та її методологія за умовчанням розвивалися інтенсивно для правильного вирішення питань ОР ІБ [3]. COBRA був розроблений у повній співпраці з однією з найбільших світових фінансових інституцій.

Отже, на сьогоднішній день для оцінювання ризиків ІБ використовується низка методів та програмних засобів. За принципом своєї роботи дані методи та програмні засоби можна розділити на якісні, кількісні та якісно-кількісні. Для підтримки прийняття рішень в процесі управління ресурсами кіберзахисту доцільно використовувати якісно-кількісні методи, адже вони дозволяють отримати результат у вигляді числових даних так і в його якісному представленні. В той же час не всі існуючі засоби дозволяють у повній мірі виконати поставлені завдання, оскільки вимагають роботу експертів відповідної предметної області та практично не включають інструментів отримання результатів в режимі реального часу, що на сьогоднішній день є однією з основних вимог.

Анотація. Забезпечення безперервності роботи сучасних інформаційних та інформаційно-телекомунікаційних систем вимагає дотримання базових парадигм інформаційної безпеки – цілісності, безпечності та доступності. Для своєчасного виявлення загроз інформаційної безпеки необхідно здійснювати процедури оцінювання та управління ризиками кібербезпеки. Сучасні засоби оцінювання та управління ризиками інформаційної безпеки дозволяють автоматизувати ці процеси. Тому актуальним є дослідження існуючих інформаційних технологій, що дозволять здійснювати процеси оцінки та управління ризиками інформаційної безпеки автоматизовано.

Література:

1. Risk Management Tools. Program Risk Management Tools [Електронний ресурс] – Режим доступу: World Wide Web. – URL: http://mitre.org/work/systemsengineering/guide/riskmanagementtools.html.

2. RiskWatch [Електронний ресурс] – Режим доступу: World Wide Web. – URL: http://www.riskwatch.com/.

3. Программное обеспечение для проведения оценки рисков. [Электронный ресурс] – Режим достууа: World Wide Web. – URL: http://www.securitylab.ru/blog/personal/secinsight/202.php.

УДК 004.732

Шестак Яніна Володимирівна, к.т.н.[1]

Мирутенко Лариса Вікторівна, к.т.н., доцент[2]

Оксіюк Олександ Глібович, д.т.н., професор[3]

Київський національний університет імені Тараса Шевченка [123]

lucenko.y@ukr.net[1], myrutenko.lara@gmail.com[2], oksiuk@ukr.net[3]

ОПТИМІЗАЦІЯ РОЗПОДІЛУ АПАРАТНИХ РЕСУРСІВ ІНФОРМАЦІЙНИХ СИСТЕМ

Активне впровадження розподілених інформаційних систем (РІС) пов'язано з високою ефективністю алгоритмів паралельної обробки запитів при виконанні запитів, адаптацією яких характеризуються зазначені системи [1, 2]. Тим не менш оптимізація РІС на рівні побудови універсальної математичної моделі є нетривіальною задачею. При цьому типові проблеми, що мають бути вирішені при розробці РІС поділяються на системні та архітектурні. До системних проблем відносять задачі ефективного налаштування системи під конкретний набір завдань та ефективне керування системою у режимі мультизадачності. У свою чергу, до архітектурних проблем відносять задачі визначення продуктивності обчислювальних вузлів системи та мінімізацію затримки при передачі даних, для вирішення чого застосовуються методи балансування навантаження [3, 4].

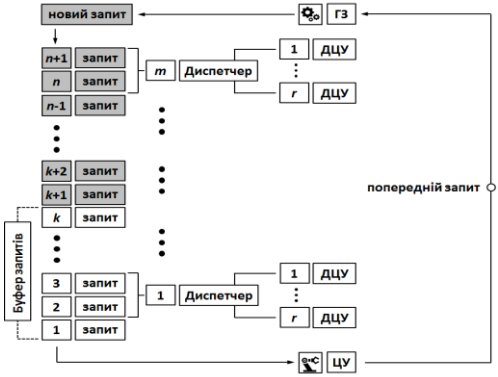


Рис. 1. Базова схема керування РІС з диспетчером балансування навантаження

Загальний підхід, що може бути використано при побудові моделі балансування навантаження РІС (рис. 5) має включати у себе такі функціональні елементи як генератор запитів (ГЗ) та центр управління (ЦУ). ГЗ виконує роль терміналу, тобто створює запити і відправляє їх на обробку, формуючі таким чином потоки запитів. ЦУ при цьому обробляє отримані від ГЗ запити і містить у своїй структурі, обчислювач, буфер запитів, що накопичує необроблені запити та диспетчери, що складаються з додаткових центрів управління (ДЦУ). ДЦУ запускаються диспетчером з метою обробки запитів, що знаходяться у черзі в буфері. При мінімальному трафіку надходження запитів всі обчислення здійснюються на рівні ЦУ згідно з порядком черги їх подання ГЗ. Актуальною для більш детального розгляду ситуацією є той випадок, коли зі збільшенням кількості запитів обчислювальна потужність ЦУ не дозволяє обробити всі запити, внаслідок чого відбувається накопичення запитів в буфері. При досягненні заданої кількості запитів у буфері, ЦУ запускає окремі потоки диспетчерів, що балансують навантаження апаратно-програмного комплексу РІС. Диспетчер обчислює кількість ДЦУ, що необхідна для зменшення кількості запитів у буфері, причому кожен ДЦУ запускається в окремому потоці.

При балансуванні навантаження на апаратні ресурси РІС має визначатися розподіл навантаження між окремими кластерами внутрішньої мережі комплексу та у рамках окремого кластеру. Рівень навантаження визначається через коефіцієнт завантаження центральних процесорів (ЦП) серверів, що є функцією від таких показників як кількість циклів однієї сесії, сумарна кількість запитів, середнє значення тактової частоти процесорів комплексу, коефіцієнт багатоядерності процесорів комплексу, коефіцієнт завантаження операційної системи (ОС) та коефіцієнт завантаження пов'язаний з процесами, які не мають відношення до запитів.

Розроблена модель показала, що при балансуванні навантаження має бути визначена пропорція розподілу запитів між серверами, а також проведене динамічне корегування зазначеної пропорції при зміні умов роботи системи. У рамках даного дослідження було запропоновано ввести поняття відносного рейтингу окремого серверу, що розраховується на основі даних про кількість запитів, які надходять на зазначений сервер, і загальну сумарну кількість запи-

тів системи з серверів. Рівень відносного рейтингу серверу системи дозволяє визначити оптимальну долю запитів для окремої робочої платформи, таким чином, щоб завантаження для всіх серверів було однаковим у межах допустимої похибки.

Анотація. Проведено аналіз сучасних методів розробки алгоритмів паралельної обробки запитів, що можуть бути впроваджені у рамках моделей розподілених інформаційних систем. Побудовано базову схему керування роботою розподіленої інформаційної системи, що включає у себе такі функціональні елементи як генератор запитів, центр управління та додаткові центри управління. Введено поняття рівня навантаження серверу як цільової функції від параметрів організації та функціонування апаратно-програмного комплексу системи. Показано, що зазначений показник дозволяє визначити оптимальну долю запитів для окремого серверу, таким чином, щоб завантаження для всіх серверів було однаковим.

Література:

1. Gupta H. Load Balancing In Cloud Computing / H. Gupta // International Journal of Recent Trends in Engineering and Research. — 2017. — т. 3 № 3. — 260-267.

2. Li K. Performance analysis of power-aware task scheduling algorithms on multiprocessor computers with dynamic voltage and speed / K. Li // IEEE Transactions on Parallel and Distributed Systems. — 2008. — т. 19, № 11, с. 1484–1497.

3. Li K. Energy efficient scheduling of parallel tasks on multiprocessor computers. Journal of Supercomputing. — 2012. — т. 60, № 2. — с. 223–247.

4. Li K. Power allocation and task scheduling on multiprocessor computers with energy and time constraints / K. Li, Zomaya A.Y., Lee Y.C. // Energy-Efficient Distributed Computing Systems. — 2017. — т. 1, с. 1-37.

5. Li K. Algorithms and analysis of energy-efficient scheduling of parallel tasks / K. Li, I. Ahmad, S. Ranka, // Handbook of Energy-Aware and Green Computing. — 2012. — т. 1, № 15, с. 331-360.

УДК 004.932.2

Штефанюк Євгеній Федорович, *аспірант,*
кафедра захисту інформації,
Національний університет "Львівська політехніка"
yevhen.sht@gmail.com

Опірський Іван Романович, *професор, д. т. н.,*
кафедра захисту інформації,
Національний університет "Львівська політехніка"
iopirsky@gmail.com

АНАЛІЗ АЛГОРИТМІВ, ЗАСТОСОВАНИХ У СИСТЕМІ РОЗПІЗНАВАННЯ ФЕЙКОВИХ ЗОБРАЖЕНЬ ASSEMBLER

Вступ

Сьогодні стрімкий розвиток соціальних мереж та засобів масової комунікації в мережі Інтернет призвів до небувалого розквіту громадянської журналістики – діяльності громадян, які беруть активну участь у процесі збирання, аналізу та поширення інформації, не маючи при цьому професійної журналістської підготовки. Зараз майже кожен має можливість публікувати та поширювати майже будь-яку інформацію за допомогою таких платформи як Facebook, YouTube, Twitter, Instagram тощо. Причому, часто ці платформи використовуються і владою для поширення суспільно важливої інформації.

Паралельно, відбувається розвиток алгоритмів на зразок Deepfake, які здатні створювати високоякісну імітацію голосу та зображення для створення неправдивих (фейкових) фото та відеоматеріалів. Такі інструменти вже були успішно застосовані зловмисниками для отримання матеріальної вигоди [1]. Це доводить, що рівень розвитку таких інструментів досяг рівня, який уможливлює їхнє застосування як інструменту для проведення атаки.

Враховуючи вищезазначене, комбінація можливостей створення імітацій на фото- та відео-матеріалах та широкої доступності засобів масової комунікації в мережі Інтернет може становити серйозну загрозу інформаційній безпеці користувачів. Таким чином, особливо актуальним на даний момент є завдання вчасного розпізнавання фейкових новин та фото- відеоматеріа-

лів. Зараз розробляються спеціальні програмні засоби, робота яких базується на останніх досягненнях в галузі нейронних мереж та машинного навчання.

Метою даного дослідження є аналіз однієї з останніх розробок в галузі детектування фейкових зображень – експериментальної системи Assembler, яка була розроблена дочірнім підрозділом Jigsaw конгломерату Alphabet [2]. Ця система є продуктом спільної роботи декількох дослідницьких груп університетів та компаній, які займаються інформаційною безпекою. Вона призначена для ефективного розпіднавання фейкових зображень з мережі Інтернет.

Наукова новизна даного дослідження підтверджуєтсья відсутністю єдиного аналізу алгоритмів, які застосовуються в даній системі.

Аналіз технік та алгоритмів, які використовуються в інструменті Assembler

Assembler використовує декілька спеціалізованих детекторів для розпізнавання специфічних властивостей зображення, які зазвичай модифікуються при створенні фейку. Застосування декількох детекторів в перспективі здатне значно підвищити ефективність розпізнавання. Нижче ми проаналізуємо їхні особливості.

Паттерни кольору та шуму (Color & Noise Patterns)

Ця модель машинного навчання поєднує два різних підходи. Вона використовує значення кольорів зображення для пошуку аномалій, таких як сильні контрастні відмінності або неприродні межі. Система також вивчає шум на зображенні на предмет наявності невідповідностей між його окремими частинами. Всі ці ознаки разом можуть вказувати на факт використання спеціалізованого програмного забезпечення для редагування зображень [3].

Копіювання чи переміщення поля густини (Dense-Field Copy-Move)

Цей алгоритм полягає у знаходженні схожих на вигляд ділянок зображення, і визначенні, чи було один з них скопійовано і вставлено в іншу область. Він базується на використанні алгоритма швидкого пошуку найближчого сусіда, PatchMatch, який особливо підходить для обчислення полів щільності зображення. [4].

JPEG брижі (JPEG Dimples)

Цей алгоритм знаходить ділянки стиснених зображень JPEG, які не відображають очікуваних шаблонів стиснення, що вказує на те, що зображення, можливо, було відредаговане в цих областях.

Метод, який використовує алгоритм полягає у виявленні артефактів JPEG, які можуть виникнути залежно від вибору математичного оператора, що використовувався для перетворення коефіцієнтів DCT з плаваючої точки до цілих значень. Виявилося, що більш часто використовувані оператори округлювання до найменшого (floor operator) або найбільшого (ceiling operator) вводять періодичний артефакт у вигляді одного темного або яскравого пікселя у блоках розміром 8 × 8 пікселів. Беручи до уваги природу цього артефакту, його поширеність у комерційних камерах та можливість його кількісної оцінки, даний алгоритм можна використовувати для виявлення широкого спектру цифрових маніпуляцій з зображеннями. [5].

Сплески консистентності (Self-consistency splice)

Дана техніка являє собою модель машинного навчання, яка вивчає властивості пікселів зображення, щоб визначити, чи могли для їхньої генерації бути використані різні шаблони метаданих EXIF. Якщо такі шаблони виявлено, то це може означати, що для створення даного зображення було використано більше однієї цифрової камери.

Алгоритм в основі моделі використовує автоматично записані фотографічні метадані EXIF як вихідний сигнал для тренування моделі. Це дозволяє визначити, чи є зображення справжнім, тобто чи увесь його вміст міг бути створеним одним конвеєром візуалізації.

Ця модель самоузгодженості застосовується для виявлення та локалізації сплайсів зображення. Метод Self-consistency splice показує хороші результати на множині реальних зображень, незважаючи на те, що жодні видозмінені зображення не були використані на етапі тренування моделі. [6].

Splicebuster

Цей алгоритм призначений для виявлення невідповідностей у моделях шуму при порівнянні різних частин зображення. Наявність таких невідповідностей може свідчити про те, що для створення цього зображення було використано більше однієї цифрової камери (різні виробники та моделі).

Алгоритм базується на функціях для виявлення сплайсингу зображення без будь-якої попередньої інформації. Локальні параметри обчислюються із суміжності залишків зображення та використовуються для отримання синтетичних параметрів функції. Припускається, що сплайс і вихідне зображення характеризуються різними параметрами. Вони аналізуються на самому зображенні за допомогою алгоритму очікування-максимізації разом із сегментацією у справжніх та сплайнованих частинах.

Результати на широкому діапазоні тестових зображень показують, що навіть невеликий навчальний набір обмеженого розміру може бути достатнім для надійної локалізації сплайсингу. [7].

StyleGAN-детектор (StyleGAN Detector)

Ця модель машинного навчання була натренована розрізняти реальні зображення людей від фейкових зображень, які були створені спеціально за допомогою техніки StyleGAN.

StyleGAN була початково створена компанією NVIDIA. Ця техніка дозволяє отримувати реалістичні штучно згенеровані зображення за допомогою нейронних мережє типу GAN (Generative-Adversarial Network). Її суть полягає у використанні двох нейронних мереж – генератора та дискримінатора. Генератор вчиться створювати максимально реалістичні зображення, а дискримінатр тренується відрізняти їх від справжніх. StyleGAN пропонує нову архітектуру мережі «генератор» GAN, яка забезпечує новий метод управління процесом генерації зображень. Генератор в StyleGAN вносить невеликі коригування "стилю" зображення на кожному шарі згортки, щоб маніпулювати функціями зображення для цього шару [8]. Завдяки цьому, модель може розрізняти високорівневі особливості зображення (як-от особа на зображенні) від низькорівневих (наприклад, зачіска). Це дозволяє генератору змінювати одну рису на зображенні не впливаючи на інші.

StyleGAN-детектор – це спеціалізована модель нейронної мережі, створена Jigsaw. Вона дозволяє детектувати зображення, які були створені за допомогою техніки StyleGAN-мереж [3].

Media Forensics Challenge Dataset

Модель Assembler навчається класифікувати зображення як маніпульовані або не маніпульовані, зокрема, на наборі даних Media Forensics Challenge Dataset, який розповсюджується National Institute of Standards and Technology (NIST) в рамках Media Forensics Challenge.

Media Forensics Challenge Dataset – це тестовий масив даних, який підтримується NIST і використовується для тренування моделей машинного навчання у галузі цифрової криміналістики [9]. Зокрема, він використовується у відомому змаганні Media Forensics Challenge. За допомогою цього конкурсу NIST підтримує наукові дослідження та допомагає просувати сучасні технології цифрової криміналістики

Висновки

Враховуючи стрімкий розвиток засобів масової Інтернет-комунікації та ефективних інструментів для створення фейкових зображень, особливої актуальності набуває завдання ефективного розпізнавання фейків для забезпечення інформаційної безпеки користувачів мережі Інтернет. Однією з останніх розробок в цій галузі є інструмент Assembler, розроблений компанією Jigsaw. В ньому одночасно використовуються декілька різних технік та алгоритмів для аналізу зображення. Кожен з них натренований розпізнавати певні особливості зображення, та на основі їхнього аналізу визначати ступінь стороннього впливу на його характеристики. Застосування одразу декількох алгоритмів потенційно здатне підвищити ефективність розпізнавання фальсифікованого зображення.

Наразі інструмент Assembler проходить тестову перевірку в декількох відомих компаніях, які займаються перевіркою достовірності інформації в мережі Інтернет [2], і незабаром будуть опубліковані перші результати його роботи.

Анотація. У роботі наведено огляд інструменту для детектування фейкових зображень Assembler. Проведено короткий аналіз алгоритмів та технік, які в ньому використовуються: показано суть кожного методу, наведено короткий аналіз алгоритму, на якому він базується, а також вказано сферу його застосування. Зроблено висновок щодо можливої ефективності детектування системою Assembler фейкових зображень на основі наявних даних.

Література:

1. Catherine Stupp. Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case // The Wall Street Journal - Aug. 30, 2019. - https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

2. Davey Alba. Tool to Help Journalists Spot Doctored Images Is Unveiled by Jigsaw [Електронний ресурс] // The New York Times – February 4, 2020. -Режим доступу до ресурсу: https://www.forbes.com/sites/jvchamary/2017/09/16/how-face-id-works-apple-iphone-x/#6c01e626624d

3. Assembler. Collaborators [Електронний ресурс] // Jigsaw, Google Research. – Режим доступу до ресурсу: https://jigsaw.google.com/assembler/collaborators/

4. D. Cozzolino, G. Pogg, L. Verdoliva. Efficient Dense-Field Copy–Move Forgery Detection // IEEE Transactions on Information Forensics and Security – листопад, 2017, том 10, випуск 11, 2284-2297 с.

5. S. Agarwal, H. Farid. Photo forensics from JPEG dimples. // IEEE Workshop on Information Forensics and Security (WIFS - 2017), Ренн - 2017, 1-6 с.

6. Minyoung Huh, Andrew Liu, Andrew Owens, Alexei A. Efros. Fighting Fake News: Image Splice Detection via Learned Self-Consistency [Електронний ресурс] // Cornell University – 2018. - Режим доступу до ресурсу: https://arxiv.org/abs/1805.04096

7. Cozzolino, Davide і Poggi, Giovanni і Verdoliva Luisa. Splicebuster: A new blind image splicing detector. // IEEE Workshop on Information Forensics and Security, Рим – 2015.

8. Jamshed Khan. StyleGAN: Use machine learning to generate and customize realistic images. [Електронний ресурс] // Heartbeat – 31 липня 2019. -Режим доступу до ресурсу: https://heartbeat.fritz.ai/stylegans-use-machine-learning-to-generate-and-customize-realistic-images-c943388dc672

9. Haiying Guan, Mark Kozak, Eric Robertson та ін. MFC Datasets: Large-Scale Benchmark Datasets for Media Forensic Challenge Evaluation. [Електронний ресурс] // NIST – 11 січня, 2019. - Режим доступу до ресурсу: https://www.nist.gov/publications/mfc-datasets-large-scale-benchmark-datasets-media-forensic-challenge-evaluation

НАУКОВЕ ВИДАННЯ

І Міжнародна науково-практична конференція
«БЕЗПЕКА РЕСУРСІВ ІНФОРМАЦІЙНИХ СИСТЕМ»

(м. Чернгів, 16-17 квітня 2020 р.)

Збірник тез

I International scientific-practical conference
«SECURITY OF INFORMATION SYSTEMS RESOURCES»

(Chernihiv, April, 16-17, 2020)

The collection of abstracts

Комп'ютерне складання та верстання О. С. Смєлова

Підписано до друку 04.05.2020. Формат 60×84/16.
Ум. друк. арк. – 12,44. Тираж 100 пр. Зам. № 507/20.

Редакційно-видавничий відділ Національного університету
«Чернігівська політехніка»
14035, Україна, м. Чернігів, вул. Шевченка, 95.
Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру
видавців, виготівників і розповсюджувачів видавничої продукції
серія ДК № 4802 від 01.12.2014 р.