Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

Перша Міжнародна науково-практична конференція
First International scientific and practical conference

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

КИЇВ - 2023

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

І МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

First International scientific and practical conference

“Кіберборотьба: розвідка, захист та протидія”

“Cyberwarfare: intelligence, defense and offensive security”

20.04.2023 – 21.04.2023

ТЕЗИ ДОПОВІДЕЙ

Київ – 2023

Рецензенти:

Радзівілов Григорій Данилович	кандидат технічних наук, професор, заступник начальника інституту з наукової роботи
Чевардін Владислав Євгенійович	доктор технічних наук, старший науковий співробітник, начальник кафедри кібербезпеки
Залужний Олексій Вікторович	кандидат технічних наук, доцент кафедри кібербезпеки
Хусаінов Павло Валентинович	кандидат технічних наук, доцент, професор кафедри кібербезпеки
Юрченко Олег Васильович	кандидат технічних наук, провідний науковий співробітник науково-дослідного відділу наукового центру зв'язку та інформатизаціїї інституту
Ковальчук Людмила Василівна	доктор технічних наук, професор, доцент кафедри кібербезпеки

Кіберборотьба: розвідка, захист та протидія: тези доповідей І Міжнародної науково-практичної конференціїї. – Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2023. – 56 с.

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

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

Робочі мови конференції – українська, англійська.

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

Відповідальний за випуск О. Є. Головко

Підписано до друку 08.05.2023 р. Зам. 74.
Друк. арк. 7,00. Ум.-друк. арк. 6,51. Обл.-вид. арк. 6,05.
Формат паперу 60×84/8. Тираж 5 прим.

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

ЗМІСТ

PhD, Chykriy K. (MITIT)
PhD, Silko O. (MITIT)

USE OF REVERSE ENGINEERING TOOLS FOR ENEMY EQUIPMENT ANALYSIS

A full-scale invasion of the Russian army on February 24, 2022, started a new kind of war — the war of technologies. A number of UAV (unmanned aerial vehicle) models, digital radio, and electronic warfare systems are in use by the enemy and play an important role on the battlefield.

Problem statement. In order to develop effective countermeasures, a deep understanding of enemy technologies is critically important. Traditional methods of visual spectrum analysis, technical analysis of radio signals, and radio jamming of known frequency ranges are still important, but not enough to win this high-tech war.

Potential subjects of such research are captured enemy equipment, both hardware and software. Since providing countermeasures is time-critical and we have no time to lose, reverse-engineering of hardware can be done briefly; only the most important information must be identified: models and characteristics of RF transceivers (frequency ranges, modulation types), models of microcontroller(s) in use, type of external flash memory, if any are present. The most important part is to reverse-engineer the algorithms and data inside such equipment. To start with algorithm analysis, one should extract firmware (binary code) from the MCU (Microcontroller Unit).This is not a simple task as in most cases these chips have readback protection. Methods to bypass such protection depend on the MCU model and may be as simple as using debugging interfaces (JTAG, SWD), but one should be prepared to perform advanced attack techniques and even physical methods (chemical decapsulation).

A number of tools can be used to reverse-engineer the extracted firmware. For firmware native code, Ghidra by the National Security Agency of the United States is one of the best choices as a highly efficient disassembler and decompiler. It is open source, supports many processor architectures, and lets us develop custom analysis components. The goal of this process is to understand both the radio exchange parameters (Frequency-Hopping Spread Spectrum algorithm, modulation type, baud rate) and its content (forward error correction method, exchange protocol logic and format, encryption algorithms, scrambling methods, etc.). This allows finding security vulnerabilities and develop effective passive (for example, detection) and active (for example, interception of control) countermeasures.

Sometimes laptops with important software get captured. If that is the case, both Linux and Windows software is analyzed the same way as if it were compiled with C/C++ or any other native-code compiler. For managed code, there are tools intended for the appropriate type of code: JetBrains dotPeek, JavaDecompiler, and VB Decompiler are some of them.

Binary reverse engineering is performed with data from memory carriers when algorithm analysis is not possible or too difficult to perform (for example, in an FPGA implementation). Knowing the nature of the information contained in this binary data, it is possible to apply both statistical and heuristic methods to identify the structure and format of the information that should be extracted.

Conclusion. Reverse engineering lets one understand the capabilities, algorithms, and usage tactics of captured enemy equipment in order to develop effective countermeasures and provide recommendations to Ukrainian UAV military vendors for building more effective and secure equipment.

PhD, Khmelevsky S. (KNAFU)
Tupitsya I. (KNAFU)
PhD, Parkhomenko M. (KNAFU)
Tupitsya O. (KNAFU)

THE METHOD OF FORMING A STEGANO-CHANNEL FOR THE DELIVERY OF SERVICE DATA IN SPECIAL-PURPOSE INFORMATION AND TELECOMMUNICATION NETWORKS

Introduction

The conduct of hostilities on the territory of Ukraine is accompanied by a dynamic increase in confrontation in the information space. This is due to the fact that recently the enemy's active actions in cyberspace are aimed at the following tasks: destructive impact on the critical infrastructure system (DDoS attacks on critical infrastructure system objects); conducting informational and psychological operations in the information space (throwing disinformation in social networks); cyber attacks aimed at hacking and theft of personal data; theft, modification of data transmitted in special purpose information and telecommunication networks (ITM SP), etc. In connection with this, the requirements for information security of data transmitted by ITM SP are increased from the standpoint of ensuring their integrity.

In connection with this, the issue of finding new approaches to increasing the level of information security of information resource data, from the standpoint of ensuring their integrity, becomes urgent.

The aim of the work is the organization of service data delivery using steganochannel. This will make it possible to create conditions for ensuring the integrity of the information resource due to the secrecy of the process of delivering service information to the final addressee.

Presentation of the main material of research

It is proposed to organize a steganochannel for the transmission of official data under the conditions of using videoconference communication by commanders, headquarters (military management bodies) with subordinate units (subdivisions) to demarcate access to official information while maintaining its integrity. As a steganocontainer, it is suggested to use video images (video frame, document scan, demo image, etc.). This will make it possible to organize the embedding of service information into the original container without making significant distortions to the video information resource.

The developed method of hiding service data in a graphic container involves two stages:

1. Video image cluster analysis. A feature of the specified stage is the performance of data clustering according to the structural indicator - the number of series in the binary structure of image pixels.

It should be noted that a number of scientific studies related to the use of the specified structural feature made it possible to obtain quite effective technologies for coding information resource data for special purpose information communication systems.

Thus, in works [1–3], the restructuring of the alphabet of video image elements ensured the improvement of compression characteristics due to the additional reduction of code redundancy of non-uniform code structures. In turn, in works [4, 5] the formation of arrays of markers for clusters that were formed by a common feature made it possible to increase the level of reliability of coded video data.

2. Steganography transformation of a video image - the process of hiding service data in the original container. This stage includes the following components:

- choosing a cluster for hiding service data, taking into account the requirements for the bandwidth of the stegano channel;
- embedding service data into the elements of the corresponding cluster. For this purpose, the use of the least significant bit method is proposed, due to the low algorithmic complexity and low level of distortion of the original container.

The mathematical description of the implementation of the specified stage is given by the following expression:

$$A(s_j) \xrightarrow{f_{steg}} A'(s_j), \quad (1)$$

where $f_{steg}(a_\psi(s_j), c_\tau)$ is functionality of embedding elements c_τ service message $C(m)$ into a cluster $A(s_j)$;

$A'(s_j)$ is the container-result, which is formed as a result of embedding the SP.

Thus, the result of the steganography transformation of the original container $A(k)$, given by expression (1) is the formation of the elements of the filled container $A'(s_j)$:

$$a'_\psi(s_j) = f(a_\psi(s_j), c_\tau),$$

where $a'_\psi(s_j)$ is an element of a filled container $A'(s_j)$.

Conclusions

The developed method of hiding a service message in a graphic container allows:

- increase the confidentiality of the transmitted data by delimiting access to it (the need to have a key containing information about the cluster, which acts as a container for accessing service data);
- create conditions for preserving the integrity of service data. This is achieved due to the low distortion of the original container (both quantitatively (indicator of peak signal/noise ratio) and qualitatively (properties of the human visual system));
- to organize a steganography channel for the transmission of service data in the conditions of using videoconference communication, the distinguishing feature of which is the simplicity of algorithmic implementation.

Further scientific research will be aimed at the development of practical implementation of the proposed method of delivery of service information - a mobile application for organizing a steganography channel in tactical level units.

REFERENCES

1. Musienko O., Tupitsya I., Borovensky Ya., Novichkov V. The Concept of Restructuring the Information Space on the Basis of a Quantitative Sign to Increase the Efficiency of Video Data Coding in Info Communication Systems. *Systems of Arms and Military Equipment*. 2022. № 1 (69). pp. 71–77. https://doi.org/10.30748/soivt.2022.69.08.

2. Khmelevskiy S., Tupitsya I., Bykov V., Ratskevich S., Pershin O. The Organization Model of the Hidden Channel of Data Transmission in Special Purpose Information and Telecommunication Networks. *Scientific Works of Kharkiv National Air Force University*. 2022. № 3 (73). pp. 52–58. https://doi.org/10.30748/zhups.2022.73.08.

3. Khmelevskiy, S., Tupitsya, I., Mahdi, Q. A., Musienko, O., Parkhomenko, M., Borovensky, Y. (2021). Development of the external restructuring method to increase the efficiency of information resource data encoding. Information Processing Systems, 3 (166), pp. 52–61. https://doi.org/10.30748/soi.2021.166.06.

4. Khmelevskyi S., Tupitsya I., Kibitkin S., Korolyuk N., Romanyuk A., Dziuba I. Creation of a Video Data Reliability Assessment Model for Compression Coding Technology in the Conditions of Errors in the Data Transmission Channel. *Information Processing Systems*. 2022. № 2 (169). pp. 72–86. https://doi.org/10.30748/soi.2022.169.09.

5. Karlov, D., Tupitsya, I., Parkhomenko, M., Musienko, O. and Lekakh, A. (2022) "Compression Coding Method Using Internal Restructuring of Information Space", International Journal of Computing, 21 (3), pp. 360–368. https://doi.org/10.47839/ijc.21.3.2692.

S.Dc in Technical Science, professor, Kovalchuk L. (IPME named by H. Puhov)
Lysenko N. (SSSCIP of Ukraine)
Skorobagat'ko M. (NTUU "Igor Sikorsky Polytechnic Institute")

SECURITY OF DSTU 9041:2020 AGAINST CHOSEN CIPHERTEXT ATTACK

National Standard of Ukraine "Information Technology. Cryptographic Information Security. Algorithm for short message encryption" (DSTU 9041:2020) was adopted almost 3 years ago. There were a lot of publications about its security, such as impossibility to reveal encrypted message or encryption key, under some standard assumption about hardness of Discrete Logarithm Problem (DLP). But one question was still omitted – security of this algorithm against so-called distinguishing attacks.

For a long time such attacks were considered "unserious", because the success of such attack doesn't cause leakage of information about encrypted message or encryption key. But during the last few years a lot of works discuss such attacks, and Standards of different countries, and also International Standards are created taking into account the possibility of such attacks.

The most important distinguishing attacks are Chosen Ciphertext Attack (CCA) and Chosen Plaintext Attack (CPA). CCA is considered successful, if, given some message and two vectors, one of which is ciphertext of the message, and other is random, to define (with probability essentially large than $1/2$), which of them is ciphertext.

CPA is considered successful, if, ciphertext and given two vectors, one of which is plaintext corresponding to given ciphertext, and other is random, to define (with probability essentially large than $1/2$), which of them is corresponding plaintext.

In what follows, we will show that Algorithm of short message encryption, proposed in DSTU 9041:2020, is secure against CCA.

Now we introduce main designations used in the Algorithm.

Let $\overline{E}$ be groups of points of some Edwards curve, and E be its subgroup of large prime order q. Next, let P be its base point, $\operatorname{ord} P = q$. Also for some participant, named Alice, define her secret key as h, $2 \le h \le q-2$, and corresponding public key $H = hP$.

If some other participant, Bob, wants to send message m to Alice, using her public key H, he runs the next Algorithm.

Encryption.

1. Choose random ε, $2 \le \varepsilon \le q-2$, and calculate EC point $R = \varepsilon P = (x_R, y_R)$.

2. Set $r = x_R$.

3. Calculate EC point $T = \varepsilon H = (x_T, y_T)$.

4. Set $t = x_T$.

5. Using symmetric block encryption algorithm E (for example, DSTU Kalyna), calculate $u = E_t(m)$.

The corresponding ciphertext is $C = (r, u)$.

Alica decrypts ciphertext using decryption algorithm.

Decryption.

1. Using her secret key, calculate $T = hP = (x_T, y_T)$.

2. Set $t = x_T$.

3. Using symmetric block encryption algorithm E (for example, DSTU Kalyna), calculate $m = D_t(u)$.

Note that for some reason algorithm Kalyna is used in the Key Wrapped Mode, which essentially reduce performance of the resulting Algorithm.

According to given designations, CCA attack on the encryption algorithm is successful, if having as input:

plaintext m, Alice's public key H, and two vectors, $C_0, C_1 \in \{(r,u);(r,v)\}$, for some random v;

adversary can guess such $i \in \{0,1\}$ that $C_i = (r,u)$.

Proposition:

under decisional Diffie-Hellman assumption, the Algorithm is secure against CCA.

Proof scretch.

Assume the opposite: adversary can distinguish between $C_i = (r,u)$ and $C_{i\oplus 1} = (r,v)$, where $u = E_t(m)$ and v is random. In our definitions, it means that there exists such Oracle O that:

$$\mathrm{O}(m, H, C_o, C_1) = i$$

such that $C_i = (r,u)$ with probability $p >> 0.5$.

Then, using this Oracle, we can solve decisional Diffie-Hellman (DDH) problem, using the algorithm given below.

Let we have two points $P_0 = h_0 P$ and $P_1 = h_1 P$ for some unknown h_0, h_1. Also we have two points, G_0 and G_1, where one of them is random point, and other is $h_0 h_1 P$.

To solve DDH problem means to create such algorithm that having $P_0 = h_0 P$ and $P_1 = h_1 P$ can choose (with probability essentially large than $1/2$) the right $i \in \{0,1\}$ that $G_i = h_0 h_1 P$.

The algorithm is the next.

Input: P_0, P_1, G_0, G_1.

1. Choose random m of the appropriate value.
2. Set $r = x_{P_0}$.
3. Set $u_0 = E_{x_{G_0}}(m)$ and $u_1 = E_{x_{G_1}}(m)$.
4. Set $C_0 = (r, u_0)$ and $C_1 = (r, u_1)$.
5. Run Oracle with input (m, P_1, C_0, C_1).
6. Get Oracle's response $\mathrm{O}(m, H, r, C_o, C_1) = i$.

Output: G_i.

For this algorithm, the probability of success is also p.

The proposition is proved.

Conclusion.

In this work we proved that, under Distinguishing Diffie-Hellman Assumption, the encryption Algorithm, proposed in DSTU 9041:2020, is secure against Chosen Ciphertext Attack. But the question about its security against Chosen Plaintext Attack is still opened. We are going to prove its security against this attack in our next researches.

The other important question is: can we use some other, more simple algorithm with higher performance, instead of Kalyna in Key Wrapped Mode, such that this new algorithm is still secure?

Kripaka Illia (NTUU "Igor Sikorsky Kyiv Polytechnic Institute")
Yakovliev Serhii (MITIT)

TRUNCATED DSTU 4145-2002 DIGITAL SIGNATURES

The problem of digital signatures shortening arises in lightweight cryptography for low-resource devices in context where signatures are stored for a long time, but are relatively rarely verified. In paper [1] Thomas Pornin proposed a method of truncating digital signatures for algorithms ECDSA/EdDSA in paradigm, when the verifier undertakes signature verification at the expense of additional calculations on his side. As a result, author obtained such truncation algorithms for EdDSA and ECDSA in different, but similar way, using a truncation of one part of digital signature. Signature verification procedure in this case is replaced from checking the verification equality to (un)successful restoring the missing part of signature. It is worth noting that EdDSA is based on elliptic curves in Edwards form and ECDSA is based on elliptic curves in Weierstrass form, both over prime field F_p [3].

The Ukrainian national standard DSTU 4145-2002 [2] describes digital signature algorithm based on elliptic curves in Weierstrass form over the fields F_{2^m} of characteristic 2, what makes it different from ECDSA and EdDSA. These elliptic curves have the following form $y^2 + xy = x^3 + ax^2 + b$, where a, b are certain parameters. The nuances and technical details of the arithmetic of elliptic curves in different forms over prime fields and fields of characteristic 2 can be found in [4].

To present the results of the research, it is important to recall the main facts from [2]:

1. The primary formula for checking the correctness of a signature is $R = sP + rQ$, where Q – public key, P – base point, s, r – extracted from signature scalars, T – input message, H – used hash function.

2. Signature D has the following form: $D = (r \parallel s)$;

3. The signature verification algorithm can be described as follows.

a) Extract r and s from the signature D.

b) Calculate a point $R := sP + rQ, \quad R = (x_R, y_R)$.

c) Calculate a field element $y = hx_R$, where h is a field element transformed from hash value $H(T)$.

d) Transform y into integer number r'.

e) Verify the equality $r \stackrel{?}{=} r'$.

A truncated signature is created by dropping a certain number of bits from the left side of the s part (its higher bits). We assume that s has the form of $s = s_0 + s_1 \cdot 2^n$, where s_1 is the unknown t-bit part and s_0 is known part included to signature; therefore, the truncated signature has a form of $D = (r \parallel s_0)$.

Signature verification in this algorithm is based on a search for the authentic part among a huge number of possible values. One can describe this process as follows.

1) Recover a point R from a known number r.

2) Apply the BSGS algorithm [5], modified for this particular case.

3) Check the found point for correctness using two verification equalities. We will assume that the signature is correct if and only if at least one equality is true.

For recovering point R, we define the following algorithm:

Inputs: – r: the part of DSTU digital signature;

– a, b: parameters of used elliptic curve (as defined in the standard [2]);

– h: hash value of the input text ($h = H(T)$).

Outputs: elliptic curve points $R, -R$.

1) Calculate $x_R = r \cdot h^{-1}$ with field operations (inversion and multiplication).

2) Solve the curve equation $y^2 + xy = x^3 + ax^2 + b$ with $x = x_R$ to obtain two values of y_R. Two pairs (x_R, y_R) form both of points $R, -R$.

Then to find the dropped part of the signature a modified BSGS algorithm is used as follows.

Inputs: – r, s_0: the truncated DSTU digital signature;
– P, Q, R: the base point, the public key and the recovered point R;
– t: the length of dropped part of signature.

Outputs: restored value of s_1.

1) Let I, J be two positive integers such that $IJ \geq 2^{t-1}$: $J = 2^{(t-2)/2}$ and $I = 2J$.

2) For $j = 0$ to $J - 1$, define $U_j = s_0 P + jI(2^n P) + rQ$. We compute and accumulate the x-coordinates of points U_j.

3) For $i = 0$ to $I - 1$, define $V_i = R - i(2^n P)$. We compute and check if any of x-coordinates of V_i matches the one from previous x-coordinates of U_j. For any match we have a candidate for the solution $s_1 = i + Ij$. If no match is found, one can conclude that signature is incorrect.

Note that $U_{j+1} = U_j + (I \cdot 2^n)P$ and $V_{i+1} = V_i - 2^n P$, so every point in U and V sets can be calculated with simple addition with precalculated points.

Proposed algorithm for verification of truncated signature can potentially find two candidates, if accidentally $-R$ point was taken as R. This is possible since the verifier doesn't know, which point was used during signature generation. On the other hand, only x-coordinate, equal for both R and $-R$, has the meaning for verification. Nevertheless, if one has some security concerns, he can check both full equalities

$$R = s_0 P + s_1(2^n)P + rQ, \qquad -R = s_0 P + s_1(2^n)P + rQ,$$

and only if one of them is true, he shall conclude that the signature is correct.

We present numerical estimates of the performance of our algorithm. Let's compare them with the ordinary search that would have to be performed in the absence of a more efficient search. For practical purposes we bound t, the length of dropped part of signature, as $8 \leq t \leq 32$.

t-bit truncation of s	Complexity of ordinary search (brute force)	Complexity of proposed algorithm
8	$2^8 = 256$	$I + J = 24$
16	$2^{16} = 65536$	$I + J = 384$
24	$2^{24} = 16777216$	$I + J = 6144$
32	$2^{32} = 4294967296$	$I + J = 98304$

In summary, the proposed DSTU digital signature truncation algorithm has an efficient implementation. It allows appropriate reducing the size of digital signatures and can be applied in protocols used in low-resource devices.

REFERENCES

1. Pornin, Thomas. Truncated EdDSA/ECDSA Signatures. – Cryptology ePrint Archive, Paper 2022/938. – 2022. – Available at: https://eprint.iacr.org/2022/938.

2. ДСТУ 4145-2002. Національний стандарт України. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка.

3. FIPS PUB 186-5:2019. Standards Federal Information Processing. Digital Signature Standard (DSS) – Available at: https://doi.org/10.6028/NIST.FIPS.186-5.

4. Chen, Lily *et al*. Recommendations for discrete logarithm-based cryptography: Elliptic curve domain parameters. – 2023. – Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-186.pdf.

5. Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A. Handbook of applied cryptography. – CRC press, 1996. – 816 pp.

Kuznetsov Oleksandr (University of Macerata)
Frontoni Emanuele (Marche Polytechnic University)
Chernov Kyrylo (V. N. Karazin Kharkiv National University)

WHISPERS IN THE NOISE: DIRECT SPREAD SPECTRUM TECHNIQUES FOR ROBUST IMAGE STEGANOGRAPHY

Abstract: Direct Spread Spectrum (DSS) technology has traditionally been utilized in broadband communication systems, particularly for military communication and environmentally friendly radio channels, where high levels of noise and signal-to-noise ratios below unity are common. In this study, we explore a novel application of DSS technology in the field of image steganography, known as Spread Spectrum Image Steganography (SSIS). SSIS leverages the advancements of noise-resistant broadband communication to conceal information within images, interpreting the cover image as noise in the communication channel. Our research focuses on the development of new classes of spreading sequences that exhibit ensemble and correlation properties, which significantly influence the effectiveness of SSIS. We propose a novel data hiding method based on the direct addressing of spreading sequences, minimizing cover image distortion and achieving high resistance to message detection. Additionally, we explore adaptive spreading sequences that take into account the statistical properties of the cover image, significantly reducing error intensity in recovered messages and enhancing the overall performance of the steganography system. The article presents the results of our experiments, demonstrating the advantages of our steganographic system and validating the theoretical arguments. The findings showcase the potential of SSIS in creating robust and secure communication systems that can effectively function in high-noise environments while preserving the integrity of the cover image.

Keywords: Direct Spread Spectrum; Spreading Sequences; Direct Addressing; Steganography System; Spread Spectrum Image Steganography

The rise of digital communication has brought with it an increasing demand for secure and reliable data transmission methods [1]. As a result, steganography has emerged as an essential tool for concealing information within various media types, including images [2]. Traditional steganographic techniques, however, often struggle with cover image distortion and susceptibility to detection [3]. In response, this article investigates the application of Direct Spread Spectrum (DSSS) technology to image steganography, creating a new approach known as Spread Spectrum Image Steganography (SSIS) [4]–[6].

The primary objective of this research is to explore how DSSS technology, traditionally used in broadband communication systems [7], [8], can be adapted to enhance the performance of image steganography. By treating the cover image as noise in a communication channel, SSIS aims to mimic the challenges faced by military and eco-friendly radio systems in high-noise environments. To achieve this, we develop new classes of spreading sequences and introduce a novel data hiding method based on direct addressing, resulting in minimal cover image distortion and high resistance to message detection.

In addition to examining the theoretical underpinnings of SSIS, this article presents the results of various experiments that demonstrate the effectiveness of our proposed steganographic system. Through these findings, we showcase the potential of SSIS in creating robust, secure communication systems that can operate in high-noise environments without compromising cover image quality.

In conclusion, our study presents an innovative data hiding technique that incorporates novel families of spreading sequences and an advanced embedding method. The proposed approach outperforms existing solutions by offering increased payload capacity and reduced distortions in the container image while maintaining data recovery accuracy. These enhancements hold significant potential for practical applications, including digital watermarking, authenticity verification, and covert data transmission systems.

The results of our experiments highlight the effectiveness and value of the developed technique, emphasizing its potential for broad application across different industries and domains. Future research could explore strategies for further optimization of the method, reducing the computational complexity associated with data recovery while maintaining its performance advantages. Additionally, investigating the robustness of the proposed technique against common image processing operations and attacks, as well as developing countermeasures against potential threats, will be crucial for ensuring the security and reliability of the data hiding process. Adaptation of the method to various types of media, such as audio and video files, could further expand its applicability and impact.

REFERENCES

[1] B. Sklar and F. J. Harris, *Digital Communications: Fundamentals and Applications*, 3 edition. Hoboken: Prentice Hall, 2020.

[2] A. Yahya, 'Steganography Techniques', in *Steganography Techniques for Digital Images*, A. Yahya, Ed., Cham: Springer International Publishing, 2019, pp. 9–42. doi: 10.1007/978-3-319-78597-4_2.

[3] R. Böhme, *Advanced Statistical Steganalysis*, vol. 0. in Information Security and Cryptography, vol. 0. Berlin, Heidelberg: Springer, 2010. doi: 10.1007/978-3-642-14313-7.

[4] L. M. Marvel, C. G. Boncelet, and C. T. Retter, 'Spread spectrum image steganography', *IEEE Transactions on Image Processing*, vol. 8, no. 8, pp. 1075–1083, Aug. 1999, doi: 10.1109/83.777088.

[5] P. U. Eze, U. Parampalli, R. J. Evans, and D. Liu, 'Spread Spectrum Steganographic Capacity Improvement for Medical Image Security in Teleradiology*', in *2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, Jul. 2018, pp. 1–4. doi: 10.1109/EMBC.2018.8512344.

[6] A. Kuznetsov, A. Onikiychuk, O. Peshkova, T. Gancarczyk, K. Warwas, and R. Ziubina, 'Direct Spread Spectrum Technology for Data Hiding in Audio', *Sensors*, vol. 22, no. 9, Art. no. 9, Jan. 2022, doi: 10.3390/s22093115.

[7] G. L. Stüber, 'Spread Spectrum Techniques', in *Principles of Mobile Communication*, G. L. Stüber, Ed., Cham: Springer International Publishing, 2017, pp. 449–499. doi: 10.1007/978-3-319-55615-4_9.

[8] D. Torrieri, 'Chapter 7 Code-Division Multiple Access', in *Principles of Spread-Spectrum Communication Systems*, D. Torrieri, Ed., Cham: Springer International Publishing, 2015, pp. 405–460. doi: 10.1007/978-3-319-14096-4_7.

PhD, Lund M. (NDCA)

AUTONOMY IN CYBERSPACE OPERATIONS – OUTLOOK AND CHALLENGES

Artificial intelligence and autonomous systems are making an impact in a diversity of domains, and expectations are that autonomous and intelligent systems will transform also the field of cyberspace operations [9, p. v]. In this paper the goal is to investigate autonomy in cyberspace operations: What is an autonomous cyberspace operation? What role does autonomy play in cyberspace operations today, and how may autonomy impact cyberspace operations in near future? The paper will concentrate on defensive cyberspace operations, but a similar analysis can be made for offensive operations.

Automation, autonomy and intelligence

The computer technology that forms the basis of cyberspace and cyberspace operations emerges from the pursuit of automating processes that earlier were performed by human beings. A result of this is that all work processes that involve computer technology will be, to a larger or lesser degree, automated in the sense that they will include actions performed by software without the interference of humans. But when will we say that software operates autonomously?

A possible definition of autonomy is that it is a function of a system which enables it to act in such a way as to pursue defined goals and adjust its behavior based on sensory input. Another way to phrase this is the ability to independently make decisions or choices based on input. However, since the ability to make choices based on data (i.e. conditional branching) is a fundamental property of all computer programming, this is not sufficient to distinguish autonomy from automation in software. The concept of autonomy is usually associated with decisions that are "bigger" or "more important" than the trivial choices that computer programs makes all the time, or with "intelligent" or "smart" systems. A further challenge is that what is perceived as non-trivial decision and intelligence in systems changes over time. Properties of computer systems that today are seen as trivial and ordinary, have at earlier times been taken as signs of autonomy and intelligence (see e.g. [3, p. 5]). For these reasons, autonomy is a context dependent property which cannot be defined without considering both the domain and the technological state-of-the-art. In the following, we will attempt at capturing an understanding of *autonomy in defensive cyberspace operations today*.

Autonomy in cyberspace operations

A general observation is that cyberspace operations are conducted by human operators supported by software and following procedures. These procedures may be more or less formalized and vary between different organizations, but may none the less be generalized to idealized sequences of steps describing typical cyberspace operations [1; 5; 12]. Such a model, or idealized procedure, for defensive cyberspace operations is shown in Fig. 1.

This observation enables a more precise definition of autonomy in cyberspace operations: The ability of the software supporting a cyberspace operation to make decisions and perform the next step in the procedure without involvement or interference by a human operator. Furthermore, it will be possible to consider degrees of autonomy. For each step of the procedure the degree of autonomy is given by the degree to which the human operator can monitor and moderate the actions of the software, for the operation as a whole the degree of autonomy is the sum of the autonomy in the steps of the procedure [6, pp. 220–224].

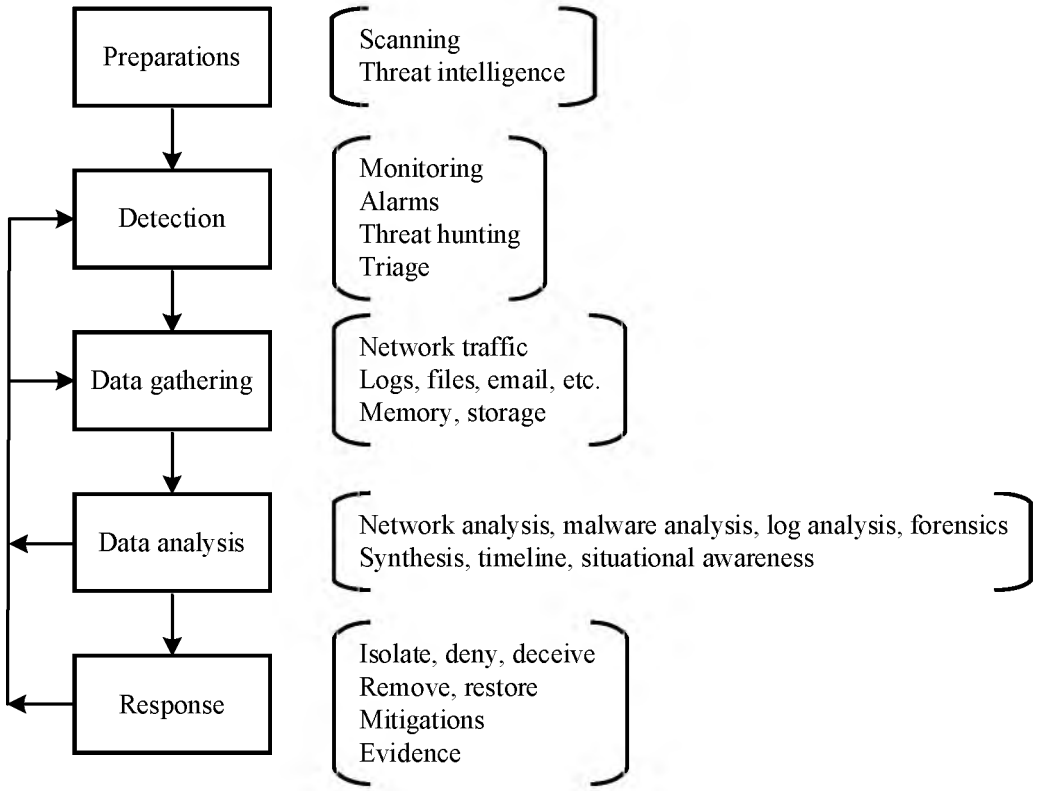

Fig. 1 – Idealized defensive cyberspace operation

It can also be noted that with the understanding of autonomy given above, "intelligence" is orthogonal to autonomy: We can have "unintelligent" software which makes decision based on simple criteria, and "intelligent" software which makes advanced analyses (e.g. based on machine learning) but presents the results to a human operator for decisions.

The model of Fig. 1 is a simplified presentation of the work process of an Incident Response Team (IRT)[1] – a dedicated organization or group of persons responsible for preventing, detecting and responding to cyber security incidents – together with common activities within each or the steps. Each step will involve actions performed by human operators supported by different kinds of software, and decisions regarding the following step. *Detection* is usually based on alarms from network sensors or observations of abnormal behavior by computer systems or users. In both cases, the probability of false positives is relatively high, and *detection* will therefore involve *triage* of alarms and observations to decide whether to escalate the incident to further *data gathering* and *analysis*. *Data analysis* is the basis for decision of what will be the best *response*. In should be noted that, even though the goal of *response* often is to restore normal functions of the defended system, this step may hide tactical decisions. A not uncommon dilemma is whether to contain and remove the attacker as fast as possible, or to continue to monitor to enable further analysis.

Even though the software supporting the process may automate many of the activities involved, we do not consider a defensive cyberspace operation autonomous unless software makes decisions of the kind illustrated above. The *Automated investigation and response* (AIR) functionality of Microsoft's *Defender* products is an example of such autonomy. Detection of, e.g., policy violations or anomalies will automatically start data gathering and analysis related to affected data objects. Based on the analysis, AIR can autonomously perform actions such as blocking programs, files, email, links or network connections, or suspend user accounts. There are obvious advantages of such functionality. Microsoft emphasizes that is frees the operators of the IRT from simpler tasks, that the response is faster, and that attacks may be blocked in an early phase and thus attackers are prevented from establishing a foothold in the defended systems [8; 10].

[1] Computer Emergency Response Team (CERT) and Cyber Security Incident Response Team (CSIRT) are also used.

On the other hand, the cost of false positives must be considered. If an autonomous defense like this is poorly configurated, false alarms that block programs, files or users may potentially harm productivity or the timeliness of critical functions. Furthermore, human intervention will usually be required to decide on further actions, such as what to do with a suspended user account.

Artificial intelligence in defensive cyberspace operations

Machine learning techniques have received much attention in defensive cyberspace operations in recent years, following the general optimism toward application of artificial intelligence in data intensive domains. So far efforts have been concentrated on singular steps in the above model, and especially on monitoring and detection of malware [13,15]. The AIR functionality of Microsoft Defender is an example of such application of artificial intelligence. Microsoft's advantage is the ubiquity of their Windows platform, and the huge amount of technical data this allows them to gather. Furthermore, the problem is reduced to their own platform, for which they have full control [2; 8; 14].

However, beyond the kind of blocking that Microsoft Defender performs, there has been little progression in use of artificial intelligence for directing the processes involved in defensive cyberspace operations. Breniker et al. [4, pp. 46–50] emphasize that little has been done to capture the work processes of IRT operators in a format suitable for machine learning. Further, they argue that the goals of defensive cyberspace operations often are complex and unprecise, and therefore challenging to formalize in a sufficiently precise manner to make them useful for machine learning algorithms. The result is a lack of good training data needed to train artificial intelligences to perform the work processes of defensive cyberspace operations. Sommer and Paxson [11, p. 308] argue that there is a semantic gap between the indicators and anomalies that artificial intelligence and machine learning is good at detecting and the operator's *interpretation* of these as a cyberattack, and that this is a fundamental difficulty.

This is also in line with the conclusions of Zhong et al. [16, pp. 85–86], who experiment with autonomous triage of incidents. They collect sequences of steps of the analysis performed on network traffic by IRT operators in triage, and construct algorithms for autonomous triage from these. The conclusion from these experiments was that even this preliminary step of a defensive cyberspace operation is too complex to make fully autonomous. The fundamental challenge is that the variations in the patters the human operator will search for are large and must be generalized, while at the same time specific knowledge of the defended system is needed. The gap between technical data and abstract attack patterns must still be filled by the human operator. Even though this work was not based on machine learning, the insights are similar to those presented by Breniker et al. and Sommer and Paxson.

Summary

It is not obvious how autonomy in defensive cyberspace operations should be understood, as automation and support from software is a fundamental part of the domain. However, by appealing to models of the work processes of defensive cyberspace operations we can describe autonomy as software making decisions and performing actions in order to get closer to the goals of the operation without direct instructions from a human operator. It is then clear defensive cyberspace operations can exhibit a degree of autonomy.

At the same time there are limits to this autonomy. Defensive cyberspace operations presume detailed knowledge and understanding of the defended systems, and this understanding software cannot currently acquire by itself. Furthermore, autonomous software can make decision on what is good next-steps within a defined tactic when the environment is known, but cannot by itself choose or develop the tactic. Translating the goals an organization sets for an operation into goals that are manageable by software is still a human job. There is great interest in use of artificial intelligence and machine learning in defensive cyberspace operations. This includes ideas that machine learning will "elevate" operations to a "higher form" of autonomy which also handles high-level tactical decision, but so far the application of machine learning methods have been limited to singular steps within a tactic. It makes sense to operate with degrees of autonomy, and it is possible to argue that defensive cyberspace operations in their nature are semi-autonomous with degrees of automation

and human control. We should expect that defensive cyberspace operations gradually will exploit the potential for automating the tasks of the operators and handling of large volumes of data, but in the foreseeable future we should also expect defensive cyberspace operation to rely on human operators for tactical decision. [6, pp. 217–226]. It seems that a research agenda for a higher degree and "higher form" of autonomy should start by investigating and describing the basic building blocks of cyberspace operations tactics and how these correlate to technical indicators, events and actions, i.e., to describe more precisely the "rules of the game".

REFERENCES

1. Adnan, Mohammad, Mike Just, Lynne Beillie, and Hulmi Gunes Kayacik. «Investigating the work practices of network security professionals». *Information & Computer Security* 23, no. 3 (2015): 347–367. https://doi.org/10.1108/ICS-07-2014-0049.

2. Agranonik, Arie, Shay Kels, og Guy Arazi. «Seeing the big picture: Deep learning-based fusion of behavior signals for threat detection». Microsoft Security. Last changed July 23, 2020. https://www.microsoft.com/en-us/security/blog/2020/07/23/seeing-the-big-picture-deep-learning-based-fusion-of-behavior-signals-for-threat-detection/.

3. Berkeley, Edmund C. *Giant brains or machines that think.* New York: John Wiley & Sons, 1949.

4. Bresniker, Kirk, Ada Gavrilovska, James Holt, Dejan Milojicic, and Trung Tran. «Grand Challenge: Applying Artificial Intelligence and Machine Learning to Cybersecurity». *Computer* 52, nr. 12 (2019): 45–52. https://doi.org/10.1109/MC.2019.2942584.

5. Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. *Computer Security Incident Handling Guide.* Special Publication 800-61, Revision 2. Gaithersburg: National Institute of Standards and Technology, 2012. https://doi.org/10.6028/NIST.SP.800-61r2.

6. Conti, Gregory and David Raymond. *On cyber. Towards an operational art for cyber conflict.* Kopidion Press, 2017.

7. Grant, Tim, Ivan Burke, and Renier van Heerden. «Comparing models of offensive cyber operations». In *Leading issues in cyber warfare & security research*, Volume 2, edited by Julie Ryan, 35–55. Reading: Academic Conferences and Publishing International, 2015.

8. Horvitz, Eric. «Applications for artificial intelligence in Department of Defense cyber missions». Microsoft On the Issues. Last changed May 3, 2022. https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial-intelligence-department-of-defense-cyber-missions/.

9. Jajodia, Sushil, George Cybenko, V. S. Subrahmanian, Vipin Swarup, Cliff Wang, and Michael - Wellman, eds. *Adaptive Autonomous Secure Cyber Systems*. Cham: Springer, 2020.

10. Simpson, Daniel, Denise Vangel, Alex Buck, Siddarth Mandalika, Stephanie Savell, Ashok Lobo, and Joe Davies. «Automated investigation and response in Microsoft 365 Defender». Microsoft Learn. Last changed September 27, 2022. https://docs.microsoft.com/en-us/microsoft-365/security/defender/m365d-autoir.

11. Sommer, Robin and Vern Paxson. «Outside the Closed World: On Using Machine Learning for Network Intrusion Detection». In *2010 IEEE Symposium on Security and Privacy*, 305–316. IEEE Computer Society, 2010. https://doi.org/10.1109/SP.2010.25

12. Trent, Stoney, Robert R. Hoffman, David Merritt, and Sarah Smith. «Modelling the cognitive work of cyber protection teams». *The Cyber Defense Review* 4, no. 1 (Spring 2019): 125–135.

13. Truong, Thanh Cong, Ivan Zelinka, Jan Plucar, Marek Čandík, and Vladimír Šulc. «Artificial Intelligence and Cybersecurity: Past, Presence, and Future». In *Artificial Intelligence and Evolutionary Computations in Engineering Systems*. Advances in Intelligent Systems and Computing 1056, edited by Subhransu Sekhar Dash, C. Lakshmi, Swagatam Das, and Bijaya Ketan Panigrahi, 351–363. Singapore: Springer, 2020. https://doi.org/10.1007/978-981-15-0199-9_30.

14. Wang, Ruofan and Kelly Kang. «AI-driven adaptive protection against human-operated ransomware». Microsoft Security. Last changed November 15, 2021. https://www.microsoft.com/en-us/security/blog/2021/11/15/ai-driven-adaptive-protection-against-human-operated-ransomware/.

15. Zhang, Zhimin, Huansheng Ning, Feifei Shi, Fadi Farha, Yang Xu, Jiabo Xu, Fan Zhang, and Kim-Kwang Raymond Choo. «Artificial intelligence in cyber security: research advances, challenges, and opportunities». *Artificial Intelligence Review* 55 (2022): 1029–1053. https://doi.org/10.1007/s10462-021-09976-0.

16. Zhong, Chen, John Yen, and Peng Liu. «Can Cyber Operations Be Made Autonomous? An Answer from the Situational Awareness Viewpoint». In *Adaptive Autonomous Secure Cyber Systems*, edited by Sushil Jajodia, George Cybenko, V. S. Subrahmanian, Vipin Swarup, Cliff Wang, and Michael Wellman, 63–88. Cham: Springer, 2020. https://doi.org/10.1007/978-3-030-33432-1_4.

PhD, Masesov Mykola (MITIT)
Shtonda Roman (MITIT)
Novytskyi Dmytro (MITIT)
Panchenko Sergiy (MITIT)
Ponomarenko Zoya (MITIT)

THE METHODOLOGY FOR CONDUCTING AN INDEPENDENT INFORMATION SECURITY AUDIT OF THE INSTITUTION

A local area network of an institution is a multiservice data transmission network that operates under the unified management and is dedicated to serving the own production needs of the institution, organization or enterprise (hereinafter referred to as the institution). This type network is a closed structure with a sufficiently high degree of protection external access to which is strictly restricted or completely prohibited and access to information within it is filtered with the administrative and technical methods. To provide data protection in local area networks, various organizational and technical methods can be used (assigning responsible scientists, applying access control lists, using VPN, etc.). Creating local area networks, the priority requirements are failure resistance, security and network speed.

The creation of secure computer systems is the purpose of network engineers and programmers, as well as a subject of theoretical research in the field of telecommunications and informatization. Computer system vulnerabilities pose a significant challenge to users because of the complexity and laboriousness of most processes and methods for protecting digital equipment, information and computer systems themselves from unintended or unauthorized access.

Vulnerability (system vulnerability) it is the system incapability to resist the implementation of a particular threat or set of threats. That is, these are certain flaws in a computer system that can intentionally compromise its integrity and cause it to malfunction. Vulnerability can result from programming errors, flaws in system design, insecure passwords, viruses and other malicious programs, scripting and SQL-injections. Thus, a computer system information security can be compromised due to information security (hereinafter - IS) threats realized through vulnerabilities exist in the computer system. To prevent information security breaches an information security audit performed in a timely manner is necessary.

In the process of developing organizational and technical measures to ensure institution information security, the head of the institution grounds the application of compensatory measures or the exclusion of certain requirements from the list of basic ones. To ensure the continuous and effective institution operation in the information field, in view of the current regulatory basis of Ukraine, the authors of the article propose, based on paragraph 3 of Article 6 of the Resolution of the Cabinet of Ministers of Ukraine from June 19, 2019 № 518 to conduct an independent information security audit (hereinafter - IISA) not only at critical infrastructure facilities, but also in institutions by initiative of their managers. An IISA of the institution must assess the sufficiency and relevance of the compensatory measures used to block (neutralize) threats and mitigate risks.

The existent standards are frankly conceptual in nature, allowing information security experts to implement any methods, tools and technologies to assess, develop and manage risks. Different standards admit the use of quantitative and qualitative methods of information security risk assessment, but there is no justification and recommendations on the choice of mathematical and methodological apparatus.Purpose of the research: to describe the main stages of the IISA methodology in the institution based on the determination of information security indicators, to formulate general guidelines for the head of the institution to conduct the IISA.

An independent information security audit of the institution is a systematic, independent and documentary process of obtaining an assessment of the institution`s information security status and its compliance with the requirements, procedures and methodologies defined in the contract between the institution`s management and the auditor, based on the requirements of national standards and the recommendations of international information security standards.

The auditor conducting IISA is a natural or legal entity being independent in its activities and having no conflict of interest with the institution to be audited, as well as having confirmed the qualification for conducting IISA, in accordance with the procedure for attestation (recertification) of information security auditors.

The IISA organization is the responsibility of institution`s head and can be carried out both on a regular and non-regular basis.

The institution head engages an auditor, audit team, information security audit unit (hereinafter referred to as the information security auditor) to conduct the IISA, formed on the basis of the above. The head of the institution may not engage the same information security auditor twice in a row to conduct an IISA. A contract is signed between the head of the institution and the information security auditor to conduct the IISA and an agreement on non-disclosure of confidential information.

The information security auditor conducts the IISA in accordance with the "Independent Information Security Audit Plan" for the institution, which consists of three sections specifying the activities for each component of the IISA: expert, active external and active internal. The Plan shall be approved by the institution`s head where the IISA is conducted. The main result of the institution`s IISA is the report on IISA results.

With the purpose of approach systematizing to the analysis of the state of cybersecurity in the institution, which would be based on real indicators obtained during the IISA, the authors proposed a mathematical model for assessing the effectiveness of information security. Methodology is a set of techniques and processes for the expedient conduct of any activity. It is a kind of tactical plan determining the technique and sequence of solving a specific scientific or practical problem.

Efficiency is the balance between the results achieved and the resources used.

For each institution, the effectiveness of information security is calculated by implementing the following steps.

Step 1. Penetration Testing, simulating the actions of an intruder according to the set objectives and definitely by an experienced specialist, is almost always effective.

Step 2. Calculate total efficiency of information security of all technical means of the institution on the basis of the weighting coefficient of each item.

Step 3. Provide an expert assessment of the effectiveness of each organizational measure and an expert assessment of the weighting coefficient of each organizational measure.

Step 4. Calculate the information security effectiveness of organizational measures of the institution.

Step 5. The institution`s management determines the organizational and technical measures to ensure information security in the institution - these are norms and rules that must be obeyed by all staff members.

Step 6. Calculate the employee knowledge efficiency of the institution.

Step 7. Calculate the general information security efficiency of the institution.

Proceeding from the mathematical model in the IISA, the overall information security effectiveness of the institution is a criterion for conducting an assessment of the information security level and depends on the values it adopts.

The peculiarity of the proposed system of information security assessment indicators of the institution is such that it covers economic indicators, technical and software parameters of the information security system and assesses the organizational measures and staff knowledge of the institution information security policy. Also, such information security indicators assessment system can be applied in any institution, regardless of its size, field and direction of activity, making it universal. At the meantime, it is worth noting this article reveals the main stages of the IISA methodology in the institution on the information security effectiveness, and some of the indicators, offered coefficients require additional study and research, which is a promising direction to further research.

PhD, Panchenko I. (MITIT)
Girak P. (MITIT)

ANALYSIS OF VULNERABILITY OF SCADA SYSTEMS OF CRITICAL INFRASTRUCTURE OBJECTS

SCADA (Supervisory Control and Data Acquisition) systems are part of industrial control systems (ICS) and play an important role in managing technological processes at critical infrastructure facilities, such as power plants, power distribution, water supply facilities, and transport systems.

Disruption of the SCADA system can have serious consequences leading to an industrial technological process accident with serious economic losses and threats to public safety.

Vulnerability analysis of SCADA systems is important for assessing the stability of critical infrastructure facilities. The main threats to industrial control systems are malicious or negligent actions of operators, unexpected configuration violations, targeted software attacks at unknown vulnerabilities, and the spreading of malicious programs.

SCADA systems can become the target of cyber attacks. The main vulnerabilities of SCADA systems include:

- insufficient protection against unauthorized access: SCADA systems often lack adequate protection against unauthorized access, which can allow attackers to gain access to the system and perform dangerous actions;
- insufficient protection against viruses and other malware: SCADA systems can be vulnerable to viruses and other malware that can damage the system and reduce its performance;
- insufficient protection against DoS attacks: SCADA systems can be susceptible to DoS (Denial of Service) attacks, which can lead the system to become unresponsive;
- lack of authentication and authorization: SCADA systems can be vulnerable to attacks if they lack proper authentication and authorization;
- lack of cryptographic protection: SCADA systems can be vulnerable to attacks on cryptographic mechanisms used to protect the system from unauthorized access.

Many SCADA systems are in operation for a long time. System updates and maintenance require stopping production processes and significant investments. Therefore, they may not meet modern cybersecurity requirements and are very vulnerable.

Well-known attacks on industrial control systems of critical infrastructure facilities:

- uranium enrichment facility in Iran – Stuxnet (2010);
- power distribution Prykarpattyaoblenergo company, Ukraine – BlackEnergy 3 (2015);
- petrochemical facility in Saudi Arabia – Triton (2017).
- SCADA system vulnerable entry point components include:
- network equipment;
- servers;
- operator stations;
- programmable logic controllers (PLCs), human-machine interfaces (HMI);
- wireless devices;
- programmable sensors and actuators.

Standard industrial protocols such as Modbus TCP/IP, EtherNet/IP, DNP3, IEC 60870-5, Siemens S7, by default, use well-known ports. They can be used to identify SCADA systems and search for vulnerabilities. Also in critical infrastructure uses BACnet IP, KNX IP protocols for building management systems (BMS).

Searching for IP addresses of SCADA system objects based on known protocols and ports can be performed using open search systems, such as Shodan. Nmap and similar software can be used for port scanning and vulnerability detection.

Conclusion. Vulnerability analysis of SCADA systems and other components of industrial systems is important for the reliability of critical infrastructure objects.

PhD, Samoylov I. (MITIT)
PhD, Storchak A. (ISCIP)

ALGORITHM OF USING THE OSINT TECHNOLOGY IN MODERN SERVICES

Relevance: The issue of comprehensive assistance to the military on the battlefield, among other things, is ensured by the search and timely provision of information. Open Source Intelligence (OSINT), i.e., intelligence synthesized using publicly available data, is intended for this purpose. Digital traces left by users on open platforms are analyzed, which can help find the enemy's geo-position, numbers, weapons, etc.

Formulation of the problem: OSINT is a method of gathering information from public or other open sources, which can be used by security experts, national intelligence agencies, or cybercriminals. When used by cyber defenders, the goal is to discover publicly available information related to their organization that could be used by attackers. A major source of intelligence that cannot be overlooked is the vast amount of publicly available information produced by consumers, hackers, newsmakers, and bloggers every single day. Taking into account the large volumes of information in various formats, the task of reducing the time of information collection and increasing the reliability and completeness of the obtained data arises.

Purpose of research: To solve the task, the goal is defined, which consists of analyzing OSINT tools and developing an algorithm for the use of OSINT technology in modern services.

The main provisions: The developed OSINT algorithm is intended primarily for the study of objects that use social networks and modern services (including entertainment ones). The purpose of the algorithm is to collect data about a group of people based on modern services (TikTok, YouTube Shorts) using publicly available OSINT tools for data analysis, collection, and processing.

To implement the proposed algorithm, it is advisable to perform the sequence of actions:

Step 1: Determine the main objective of the OSINT operation. Analyze the tools that will be used for each individual case (Shodan, Google Docker, Metagoofil, Whois, etc.).

Step 2: Choose a workplace to conduct an OSINT operation. Provide a secure Internet connection. Using the tools from Step 1, find the minimum data and the browser anti-detection.

Step 3: Choose a mobile emulator (select the same country as the object under study) while connecting a VPN with the same country as the object under study.

Step 4: Combine the tools used in Step 2 and Step 3 into a virtual machine. Create an account in the required social network (service): use the same data as that of the object under study (to optimize recommendations in the next steps to obtain maximum informativeness).

Step 5: Detail the received information about the object as much as possible and apply it when setting up recommendations: setting tags, activity in comments, likes for videos, subscriptions to other accounts that have at least some relations to our object. If necessary, automate this process using artificial intelligence algorithms or adjust recommendations manually.

Step 6: Collect data obtained as a result of observations after setting recommendations.

Step 7: Determine the geoposition of the object based on the received data array.

Step 8: Detail the personal data obtained in the course of OSINT intelligence, using OSINT tools. Sort the received data by importance and value for further use. Write a final report.

The basis of data collection is the low cyber hygiene of the research objects, careless attitude to the distribution of their own confidential data (inclusion in TikTok, YouTube Shorts, which can reveal the location of the object; posts and comments that can provide data on the circle of communication of the object under study, their friends, relatives, place of work, etc.).

Conclusion: The proposed algorithm allows for a reduction in the time needed to collect information and an in crease in the reliability and completeness of the obtained data. By using OSINT tools effectively and following a systematic approach, it is possible to gather valuable insights from publicly available data. This information can be vital for various purposes, including military intelligence, cybersecurity, and law enforcement. It is essential, however, to maintain a balance between data collection for legitimate purposes and respecting individual privacy rights.

PhD, Shevchenko Andrii (Quipu GmbH)

THE STRUCTURAL MODEL OF AN EXTENDED DETECTION AND RESPONSE SYSTEM

Nowadays, operations in cyberspace have become one of the types of support and maintenance of military operations, which compromise and disable critical infrastructure facilities and elements. In this situation, the issue of timely detection and protection against cyber-attacks and their separate techniques is critical.

The incident response process to cybersecurity incidents using a large stack of technologies is a time-consuming process that is complicated by the gathering, analysis and correlation of information from a variety of monitoring/protection tools and is entirely based on the competence of an analyst who must combine all available indicators into a single attack chain. This leads to an increase in such indicators as the average time to detect an attack and the average time to response to an attack.

One of the main trends in the development of threat response systems is the design and development of extended detection and response (XDR) systems. XDR systems should aggregate endpoint, network, cloud, identity, email, and other security systems into a single ecosystem to detect, investigate, and respond to cybersecurity incidents.

Today, there is no single architecture for an XDR system. A couple of XDR alliances are working in this direction as part of research efforts. But there is no single model of the system. Based on the analysis of existing XDR systems, their main capabilities and requirements for XDR systems, the following version of the XDR structural model is proposed (Fig. 1).

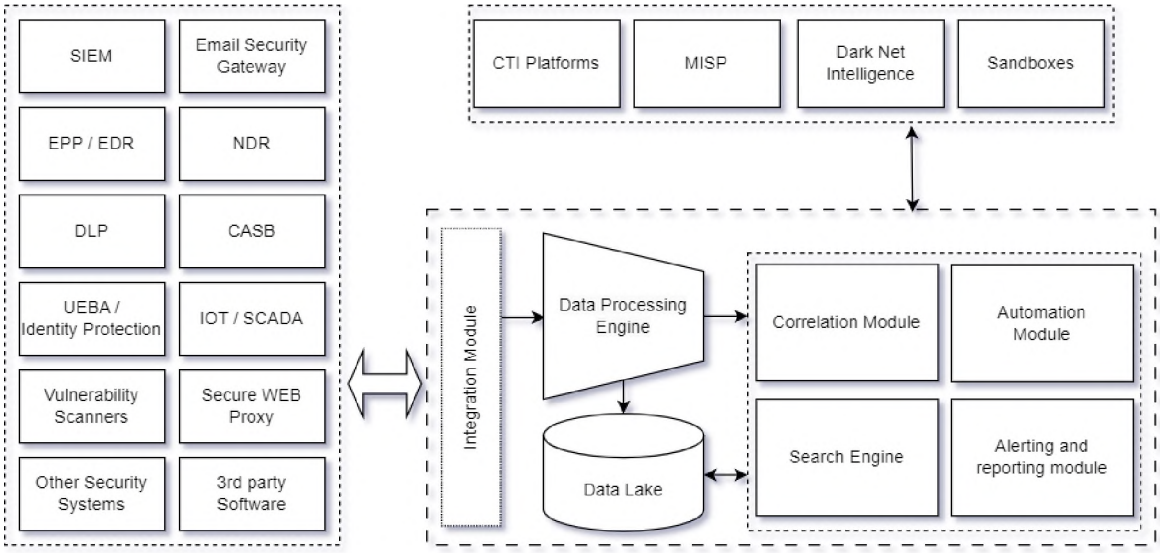

Fig. 1 – XDR structural model

XDR systems should integrate all existing security and detection systems as possible. One of the main problems in creating XDR systems is the processing of data/signals from different information sources because each of the platforms has its own specific "language" for recording and storing events in the system. Therefore, the XDR Data Processing Engine must receive signals from different information sources, read this data and normalize it, and then store it in the data warehouse (data lake). This will allow aggregating signals from different sources with the subsequent construction of detection logic in cross-functional systems.

Given the trend of increasing cyber-attacks, the implementation of XDR provides an opportunity to improve incident response efficiency by implementing a more effective and comprehensive protection and monitoring system without increasing the staff of security operations centers and reducing the cost of maintaining systems.

Yesina Maryna (V.N. Karazin Kharkiv National university, JSC "IIT")
Gorbenko Ivan (V.N. Karazin Kharkiv National university, JSC "IIT")
Ponomar Volodymyr (V.N. Karazin Kharkiv National university, JSC "IIT")

STATE ANALYSIS AND COMPARATIVE ANALYSIS OF POST-QUANTUM STANDARDS OF ASYMMETRIC TRANSFORMATIONS AT INTERNATIONAL AND NATIONAL LEVELS

Given the development and implementation of quantum technologies, including for cryptoanalysis, practical readiness for them mathematical, logical and software, there is now we have the problem of development, evaluation and implementation of post-quantum asymmetric cryptotransformations of electronic signature (ES), asymmetric encryption (AE) and key encapsulation protocol (KEP). This is confirmed by investing in the development of these technologies of unlimited resources [1–7]. The purpose of this report is to analyze the state of development, adoption and implementation of post-quantum standards of cryptographic information protection (CIP) at international and national levels.

The 4th stage of the international competition for development and adoption of post-quantum standards AE, KEP and ES is currently being completed. Recommended as international post-quantum standards AE, KEP and ES is the KEP standard Crystals-Kyber and ES standards Crystals-Dilithium, Falcon and Sphins+ [1–3; 5–7]. At the national level, the post-quantum standard of AE, KEP DSTU 8961-2019 is adopted [4]. The drafts of the ES "Vershyna" and "Sokil" [5; 6] are at the stage of adoption. As the main mathematical apparatus for them is used the mathematical lattices apparatus. National standards are not inferior in terms of characteristics, but exceeding international standards, as they provide protection against classical attacks including 512 bits and quantum attacks 256 bits, and international only 256 bits from classical and 128 bits from quantum attacks [3–7].

To solve the problems of analysis, evaluation and comparison of AE, KEP and ES, a comprehensive technique was developed, which is based on methods – on the basis of unconditional, conditional and pragmatic criteria. These techniques can be applied when evaluating and comparing independently, but the main application is their application in the specified sequence – first using unconditional criteria, then on the basis of conditional criteria and, if necessary, on the basis of pragmatic criteria.

The evaluation first checks the compliance of AE, KEP and ES with system of partial unconditional criteria, then for each cryptographic primitive, which is selected, the unconditional integral criterion is calculated. In the second stage, appropriate estimates are obtained only for standards or projects that have been evaluated by unconditional criteria. For this purpose, the systems of partial conditional criteria are used first, and then the integral conditional criterion is calculated on the basis of them. In the third stage, appropriate estimates are obtained using a pragmatic criteria system.

Fig. 1 shows the histogram of the general relative advantage of AE algorithms. Apparently, the "Skelya" algorithm is the greatest advantage, due to smaller parameters and more performance.

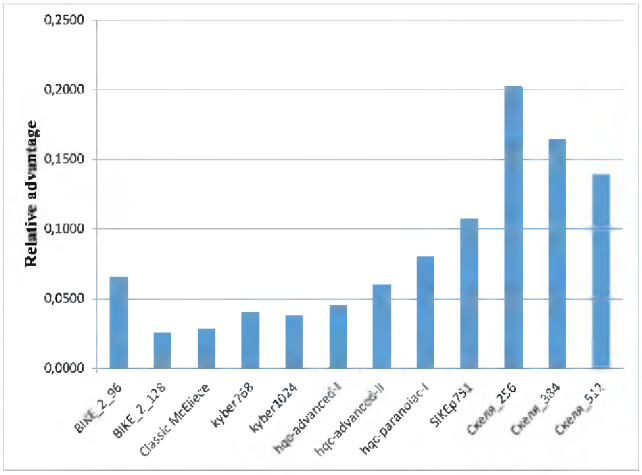

Fig. 1 – Advantages of AE algorithms

Fig. 2 shows histogram of the general relative advantage of ES algorithms. As can be seen from Fig. 2, the draft of the standard ES "Vershyna" with parameters of stability of 128 bits has the greatest advantage, for the more stable parameters, the algorithm "Sokil" has the advantage.

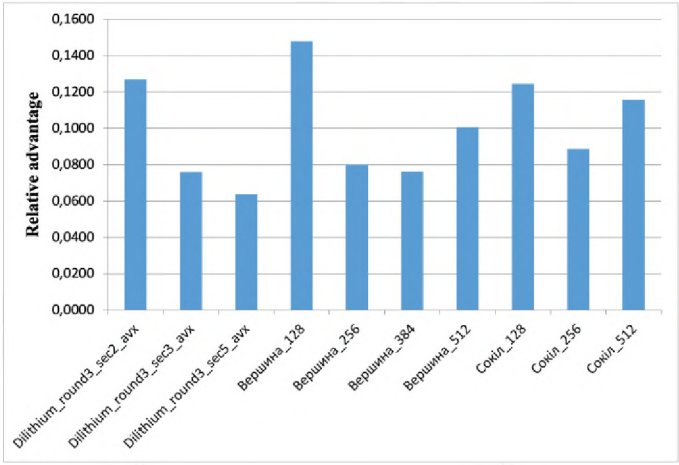

Fig. 2 – Advantages of ES algorithms

Currently, to the post-quantum standards of AE, KEP and ES put forward stringent requirements in relation to information security, technical and economic, and technical and operational characteristics, which are implemented in the adopted international and national post-quantum standards.

REFERENCES

1. Crystals-Kyber. [Electronic resource]. – Access mode: https://pq-crystals.org/kyber/.

2. Crystals-Dilithium. [Electronic resource]. – Access mode: https://pq-crystals.org/dilithium/index.shtml.

3. Falcon. [Electronic resource]. – Access mode: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-2-submissions.

4. DSTU 8961:2019 «Information Technology. Cryptographic protection of information. Asymmetric encryption and encapsulation algorithms».

5. The draft of the national standard of the ES «Information Technology. Cryptographic protection of information. Electronic signature algorithms on algebraic lattice with deviations».

6. The draft of the national standard of the ES «Information Technology. Cryptographic protection of information. Electronic signature algorithms on algebraic NTRU-lattices with a given sample».

7. NIST IR 8413 Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. – Access mode: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf.

PhD, Zaluzhnyi O. (MITIT)
PhD, Yurchenko O. (MITIT)
Andreiev A. (MITIT)

POSSIBILITY OF USING MACHINE LEARNING ALGORITHMS FOR MODULATION RECOGNITION OF RADIO SIGNAL IN MILITARY APPLICATION

Modulation recognition of radio signal with using of machine learning algorithms is the subject of active scientific research. Use of such technologies is very useful for cognitive radio, spectrum surveillance and management, radio electronic reconnaissance. In addition, this is one of the important tasks that must be solved during the organization of effective side-channel attack. Most of the known solutions are based on the use of deep learning, where images of the signal constellation are used as a dataset. At high SNR, techniques which based on signals constellation shape are noise sensitive and efficient. But in the conditions of low SNR the results of that work could be unpredictable. In addition they require significant computing power. The latter is especially important for military applications, when it is necessary to ensure the performance of tasks in a complex noise environment, with minimal expenditure of mobile device energy and time for task performance.

Therefore, the development of the ML model for the classification of the modulation of the incoming radio signal using different learning algorithms is an important task.

The purpose of the research is to analyze the effectiveness of using machine learning algorithms for automatic classification of the modulation of the incoming radio signal in a complex noise environment, time and energy limitations.

In the proposed ML model, the I and Q (In-phase Amplitude, Quadrature Amplitude) coordinates of signal constellation points are used as the dataset. The dataset contains samples of some basic modulation types, generated in MATLAB with a random signal-to-noise-ratio in the range [-5, 20] dB. Developed ML model used datasets for different modulations schemes such as PAM4, PAM16, QPSK, PSK8, APSK32, APSK64, QAM16, QAM32, QAM64. The names of all data sets are related to the used modulations schemes (modulation schemes are classes in the ML model). The first row of all datasets contains the names of the constellation image coordinates (these are features in ML model), modulation schemes, and the SNR. The next lines contain the values of the I and Q coordinates.

Random forest, decision tree, naive Bayes, support vector machine and k-nearest neighbors (KNN) algorithm were used to select the best algorithm for solving the problem. ML models were tested using different algorithms.

Value of precision, recall, and f1-score received and confusion matrix was constructed. The best results were obtained using the KNN algorithm. The results of model testing are illustrated in the Table 1 and the Figure 1.

Table 1 – Value of precision, recall and f1-score received using KNN algorithm

Modulation tips	Encoded labels	Precision	Recall	F1-score
APSK32	0	0.85	0.98	0.91
APSK64	1	0.94	0.64	0.76
PAM16	2	0.86	0.94	0.9
PAM4	3	0.75	0.77	0.76
PSK8	4	0.74	0.8	0.77
QAM16	5	0.62	0.69	0.65
QAM32	6	0.58	0.6	0.59
QAM64	7	0.69	0.58	0.63
QPSK	8	0.74	0.7	0.72

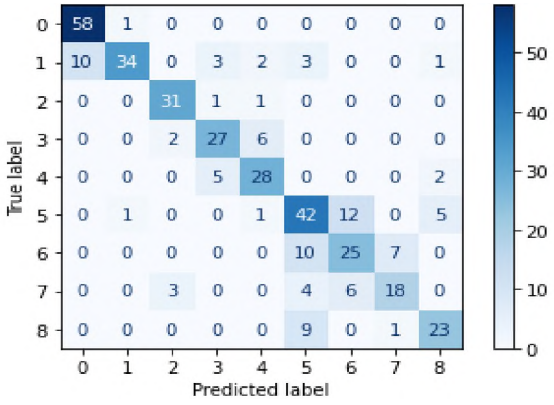

Figure 1. Confusion matrix for KNN algorithm

Thus, to solve the problem of modulation recognition, it is advisable to use the KNN algorithm for the ML model. The proposed model is experimental, and even with a limited dataset, it allows classifying the modulation of the received signal with an accuracy of 0.75 with an SNR in the range of [-5, 20] dB. To obtain better results in further research, it is planned to use separate datasets for each type of modulation and SNR. There will be several thousand such datasets for one type of modulation. One sample for each randomly selected SNR from a range of possible ones.

Базарний С. В. (НУОУ)

УДОСКОНАЛЕННЯ МЕТОДИКИ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ПСИХОЛОГІЧНОГО ВПЛИВУ В ІНФОРМАЦІЙНІЙ ОПЕРАЦІЇ

Останнім часом, коли доступ до інформації став легким та швидким, інформаційні операції стали все більш популярним інструментом забезпечення національних інтересів. В інформаційних операціях використовують різноманітні методи впливу на громадську думку, військово-політичне керівництво та на осіб, що ухвалюють рішення, такі як активне поширення ворогом дезінформації та маніпулювання емоціями визначених цільових аудиторій. Особливо, під час широкомасштабної збройної агресії рф на територію України постало питання у протистоянні ворогу в інформаційному просторі, а саме:

– своєчасного виявлення та реагування на антиукраїнську пропаганду в мережі Інтеренет, яка формується та розповсюджується контрольованими росією ЗМІ;

– протидії поширенню неправдивої інформації за допомогою агентів (ботів) через месенджери та соціальні мережі, яка спрямована на дестабілізацю ситуації, як в Україні так і в країнах, які її підтримують;

– планування та проведення заходів з ідентифікакції та пошку агентів соціальних мереж, які є колаборантами та особами, які підтримують російських військових та війну в Україні;

– збереження та оброблення цифрових матеріалів, що є доказовою базою, які надходять з вилучених технічних засобів, що належали російським військовим;

– розробка та впровадження сучасних інформаційних технологій для оперативного збору інформації з відкритих джерел про військові формування чи інших найманців з незаконних збройних формувань росії.

Враховуючи те, що в сучасних умовах Командування кіберсил ЗСУ надає технологічну підтримку Силам Спеціальних операцій а вже Сили Спеціальних операцій відповідають за інформаційні та психологічні операції у кіберпросторі, виникає завдання, щодо моніторингу діяльності агентів впливу у соціальних мережах та електронних ЗМІ, пошуку та аналізу контенту противника.

Тому, саме онлайн-дискусії на форумах, блогах та у соціальних мережах є впливовим елементом, щодо підтримки ухвалення рішень, спрямованих на забезпечення кіберзахисту, зокрема врахування психологічних аспектів впливу на агентів мережі та важливими платформами для поширення спеціальної інформації. Моніторинг онлайн-дискусій є важливою задачею для забезпечення системи інформаційної безпеки, і це являє собою складне завдання через великий обсяг даних та різноманітність джерел інформації. Також існує проблема ідентифікації нових форумів, блогів та агентів соціальних мереж, створених для проведення інформаційних кампаній в рамках проведення інформаційних операцій, кібератак та інших злочинних дій в мережі Інтернет.

Процес моніторингу спрямований на визначення ключових тем та питань, які обговорюються у найбільш активних онлайн-дискусіях, а також чітко визначеного контексту, в якому відбуваються ці дискусії, включаючи джерела інформації, активність та динаміку взаємодії з цільовою аудиторією.

Основна ідея методу тематичного аналізу полягає у тому, що текст стандартизується, видаляються зупинні слова, які не мають суттєвого значення в контексті визначеного тексту і не несуть основного змісту повідомлення, виконується лематизація та видаляються всі елементи, які не стосуються визначеної теми. Наступним кроком є розбиття тексту на частини (ключові слова, речення), і потім ці частини групуються в теми або тематичні кластери на основі відповідності слова та контекстуального значення, в якому вони використовуються.

Існуючі методи оцінки ефективності психологічного впливу в контексті інформаційних операцій мають кілька обмежень. Вони не враховують специфіки онлайн-дискусій, форумів,

блогів та соціальних мереж, і базуються на невеликій кількості ключових показників продуктивності. Запропонрована методика враховує специфіку онлайн-дискусій та дозволяє проводити всебічний аналіз контенту, контексту та динаміки дискусій, а також виявлення нових тенденцій та тем. Дану методику можуть використовувати урядові агентства, дослідницькі організації та інші суб'єкти, що займаються забезпеченням інформаційної безпеки.

Запропонована методика складається з наступних етапів: збір даних та попередній аналіз; тематичний аналіз; аналіз сентименту; визначення впливу; визначення категорій джерел інформації.

Збір даних та попередній аналіз: збирання даних з різних джерел і попередній аналіз даних для визначення найбільш активних дискусій та тем, що обговорюються. У цьому кроці можна використовувати різні методи збору даних, такі як скрапінг веб-сторінок, API для отримання даних з соціальних мереж, тощо. Для попереднього аналізу даних можна використати методи дескриптивної статистики, такі як середнє значення, медіана, дисперсія та інші.

Тематичний аналіз мовленнєвих конструкцій та інших текстових елементів: це процес виявлення тематичних кластерів в текстах. Один з популярних методів для цього - це Latent Dirichlet Allocation (LDA).

Аналіз сентименту: аналізування емоційного забарвлення текстів та визначення сентименту відносно обговорюваних тем. Для математичного опису аналізу сентименту можна використати методи машинного навчання, зокрема класифікацію текстів за наявністю позитивного, негативного або нейтрального сентименту. Це можна виконати за допомогою алгоритмів навчання, наприклад, на основі набору позначених даних (лейблів), де кожен текст має позначку про наявність позитивного, негативного або нейтрального сентименту.

Після визначення тем, які перебувають в центрі уваги та обговорення агентами, а також встановлення емоційного стану даної цільової аудиторії, на основі результатів тематичного аналізу та аналізу сентименту, необхідно проводити оцінювання ефективності психологічного впливу, на агентів тих чи інших джерел інформації. Оскільки інформаційні джерела мають різні характеристики та можуть впливати по-різному на ефективність психологічного впливу, визначення категорій джерел інформації, таких як форуми, блоги, та агентів соціальних мереж, є важливим етапом в процесі застосування даної методики.

Описання удосконалення методики оцінювання ефективності психологічного впливу методом тематичного аналізу моніторингу онлайн-дискусій, форумів, блогів та агентів соціальних мереж в інформаційній операції, а саме покращення оцінки ефективності психологічного впливу за допомогою тематичного аналізу та аналізу сентименту надає можливість визначити окремі теми та певний емоційний стан визначеної цільової аудиторії в онлайн-дискусіях, а також визначити ефективність психологічного впливу на основі результатів тематичного аналізу. Були розглянуті та запропоновані кроки дій такі як, аналіз сентименту, тематичний аналіз та визначення впливу.

Відповідно, враховуючи основну мету, якою є удосконалення методики за рахунок підвищення точності та ефективності оцінки психологічного впливу в онлайн-дискусіях запропоновано новий інструмент для визначення емоційного стану, вплив психологічних факторів на цільову аудиторію. Застосування удосконаленої методики може бути корисним у різних контекстах, а саме у військовій сфері, політиці та соціальних дослідженнях, результати яких можуть допомогти в розумінні впливу психологічних факторів на думки та поведінку цільових аудиторій в онлайн режимі в інформаційному середовищі.

к.т.н. Бовда Е. М. (ВІТІ ім. Героїв Крут)
Бовда В. Е. (ВІТІ ім. Героїв Крут)

МОДЕЛЬ ПРОГНОЗУВАННЯ СТАНУ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ НЕЧІТКИХ НЕЙРОННИХ МЕРЕЖ

В даний час завдання прогнозування стану телекомунікаційної мережі є одним з ключових питань забезпечення їх кібернетичного захисту. Загальновизнано, що в якості засобів для прогнозування можуть використовуватися нейронні мережі, які забезпечують найвищі показники точності передбачувальної аналітики.

Аналіз публікацій показує, що нейронні мережі мають більші можливості для вирішення завдання прогнозування стану телекомунікаційної мережі. Але відомі моделі нейронних мереж не можуть бути безпосередньо використані для цієї мети. Тому виникає питання створення такої моделі, яка дозволила вирішити це завдання.

Процес управління мережею полягає в здійсненні сукупності впливів на керований об'єкт, які вибрані з множини можливих впливів на підставі програми управління та інформації, що надходить про поведінку об'єкта і стан навколишнього середовища для досягнення заданої мети.

Виходячи з того, що завдання прогнозування є окремим випадком завдання регресії, де існує залежність залежної змінної від незалежних за заданих умов, то варіантом вирішення може бути застосування наступних типів штучних нейронних мереж (ШНМ): багатошарового персептрону, радіально-базисної мережі, узагальнено-регресійної мережі, мережі Вольтері та мережі Ельмана, яку можливо модифікувати.

Архітектура модифікованої рекурентної нейронної мережі Ельмана наведена на рис. 1. Використання її передбачає, що процес прогнозування імітується вихідним сигналом деякою нелінійною динамічною системою, яка залежить від множини факторів, у тому числі від минулих станів системи. Ельман запропонував ввести в мережу додатковий шар зворотного зв'язку, що називається контекстним або шаром станів. Цей шар отримує сигнали з виходу прихованого шару і через елементи затримки c подає їх на попередній – вхідний, зберігаючи таким чином оброблювану інформацію з попередніх тактів всередині мережі. На рис. 1 показана мережа з декількома входами мережі Ельмана, де число нейронів у шарі введення m і прихований шар n та q і один вихідний блок.

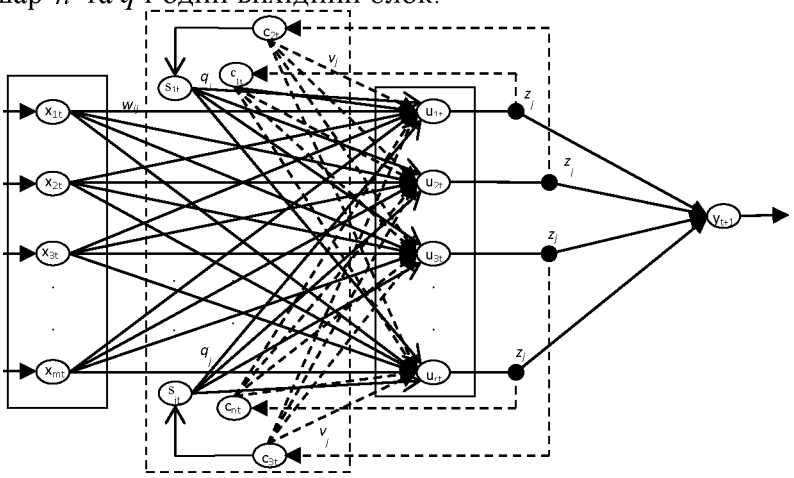

Рис. 1. Мережа Ельмана для прогнозування перевантаження маршрутів

Прихований шар виглядає наступним чином – входи всіх нейронів у прихованому шарі дає мережа:

$$NET_{jt}(k) = \sum_{i-1}^{m} w_{ij} x_{it}(k-1) + \sum_{j-1}^{n} v_{ij} c_{it}(k) + \sum_{g-1}^{l} q_{ij} s_{it}(k), \quad (1)$$

де $c_{jt}(k) = u_{jt}(k-1)$, $i = 1,2,...,n$, $j = 1,2,...,m$; $q_{jt}(k) = c_{jt}(k-1)$, $i = 1,2,...,n$, $j = 1,2,...,m$.

Значення на виході прихованого шару нейронів отримуємо з виразу:

$$u_{ji}(k) = f_H\left(\sum_{i-1}^{m} w_{ij}x_{it}(k) + \sum_{j-1}^{n} v_{ij}c_{it}(k) + \sum_{g-1}^{l} q_{ij}s_{it}(k)\right), \quad (2)$$

де обрана сигмоїдальна функція в прихованому шарі як функція активації: $f_H(x) = 1/(1+e^{-x})$

.

Значення вихідного сигналу прихованого шару визначається наступним чином:

$$y_{t+1}(k) = f_T\left(\sum_{j-1}^{r} z_j u_{jt}(k)\right), \quad (3)$$

де $f_T(x)$ – відображення як функція активації нейрона.

Алгоритмом зворотного поширення є контрольований алгоритм навчання, який мінімізує глобальну помилку E з використанням методу градієнтного спуску. Для моделі стохастичної ефективності часу мережі Ельмана, ми припускаємо, що отримана помилка виходу $\varepsilon_{e_m} = d_{t_n} - y_{t_n}$ та помилка вибірки n визначається як:

$$E(t_n) = 0{,}5\varphi(t_n)\left(d_{t_n} - y_{t_n}\right)^2, \quad (4)$$

де t_n – час відгуку (вибірки) n $(n = 1,2,...,N)$, d_{t_n} – фактичне значення, y_{t_n} – значення виходу в момент часу t_n, а $\varphi(t_n)$ – ефективна функція стохастичного часу. Визначимо $\varphi(t_n)$ таким чином:

$$\varphi(t_n) = \frac{1}{\beta}\exp\left\{\int_{t_0}^{t_n}\mu(t)dt + \int_{t_0}^{t_n}\sigma(t)dB(t)\right\} \quad (5)$$

ефективна функція часу даних розглядається як функція змінної часу. Потім відповідна помилка всіх даних в кожній мережі проходить повторне навчання та визначається як:

$$E = \frac{1}{N}\sum_{n-1}^{N} E(t_n) = \frac{1}{2N}\sum_{n-1}^{N}\varphi(t_n)\cdot\left(d_{t_n} - y_{t_n}\right)^2 \quad (6)$$

Основним завданням алгоритму навчання є мінімізація значення функції стану мережі E до тих пір, поки воно не досягне заданого мінімальне значення ξ шляхом повторного навчання. При кожному повторенні, значення функції стану мережі розраховується і виходить глобальна помилка. Градієнт функції стану мережі визначається $\Delta E = \partial E / \partial W$. Для вузлів у вхідному шарі градієнт з'єднувальної ваги w_{ij} задається формулою:

$$\Delta w_{ij} = -\eta\frac{\partial E(t_n)}{\partial \omega_{ij}} = \eta\varepsilon_{t_n} z_j \varphi(t_n) f'_H(NET_{jt_n}) x_{it_n} \quad (7)$$

для вузлів в рекурентному шарі, градієнт з'єднування ваг задається формулою:

$$\begin{aligned} \Delta v_j &= -\eta\frac{\partial E(t_n)}{\partial v_{ij}} = \eta\varepsilon_{t_n} z_j \varphi(t_n) f'_H(NET_{jt_n}) c_{it_n}, \\ \Delta q_j &= -\eta\frac{\partial E(t_n)}{\partial q_{ij}} = \eta\varepsilon_{t_n} q_j \varphi(t_n) f'_H(NET_{jt_n}) q_{it_n}, \end{aligned} \quad (8)$$

для вузлів ваги в прихованому шарі – градієнт з'єднування ваг v_j задається формулою:

$$\Delta z_j = -\eta\frac{\partial E(t_n)}{\partial z_j} = \eta\varepsilon_{t_n} z_j \varphi(t_n) f'_H(NET_{jt_n}), \quad (9)$$

де η – швидкість навчання $f'_H(NET_{jt_n})$, є похідною функції активації.

Таким чином, запропонований підхід дозволяє ефективно здійснювати прогнозування стану мережі із забезпеченням адаптації до динаміки змін значень досліджуваних параметрів. На відміну від існуючих методів прогнозування в розробленому методі були враховані особливості мережі на основі підрахунку потенціалу нейронів мережі. Даний метод дозволяє підвищити точність та швидкість прогнозування стану мережі за рахунок зменшення обчислювальної складності нейронної мережі.

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

ІДЕНТИФІКАЦІЯ КОРИСТУВАЧА ТА ПРОЦЕСІВ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІКС ТА АС ПРИ ВИНИКНЕННІ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ

Дослідження прихованих можливостей функціональних компонентів операційних систем (ОС), які здійснюють реєстрацію і збереження подій у системі, а також фіксують дії користувачів або процесів із інформаційними об'єктами.

Забезпечення кібербезпеки України, особливо під час збройної агресії російської федерації, є одним із головних завдань перед державою для захисту життєво важливих інтересів людини зокрема та національних інтересів України загалом у кіберпросторі. Основними правилами забезпечення захисту інформаційних ресурсів, які належать до державної таємниці в інформаційно-комунікаційних системах (ІКС) та автоматизованих системах (АС), є обов'язкова ідентифікація користувача та процесів, реєстрація виконання користувачами операцій із оброблення інформаційних об'єктів. Налаштування комплексу засобів захисту дає змогу визначити порушника шляхом встановлення подій аудиту, пов'язаних з інформаційними об'єктами.

Дослідити приховані функціональні компоненти ОС, які здійснюють аудит дій користувачів або процесів по відношенню до інформаційних об'єктів.

Одним з основних правил забезпечення захисту інформаційних ресурсів, які належать до державної таємниці в інформаційно-комунікаційних системах та АС, є обов'язкова ідентифікація дій користувача тобто реєстрація виконання користувачами операцій із оброблення інформаційних об'єктів. Комплекс засобів заходів, який реалізований в ОС та відповідне його налаштування дає змогу, в разі порушення політики безпеки в АС, визначити порушника та встановити хронологію подій, пов'язаних з інформаційними об'єктами.

В ОС *Microsoft Windows* запис та збереження подій здійснюється у відповідних електронних журналах та лог-файлах. На відміну від задокументованих функціональних компонентів ОС *Microsoft Windows*, існують також приховані, які реєструють і зберігають різні типи подій, а також містять важливу інформацію, за допомогою якої можна визначати дії користувачів або процесів. На відміну від задокументованих засобі адміністрування ОС (локальна політика безпеки, планувальник завдань, перегляд подій та інше), система здійснює збір телеметрії за допомогою інших впроваджених функціональних компонентів (час та місце інсталяції різних програмних додатків, вхід/вихід під обліковими записами, робота програмного забезпечення з правами адміністратора, ініціалізація процесів запуску web-компонентів у вбудованому в ПЗ коді тощо).

Функціональний компонент ОС *Microsoft Windows* є часова шкала у файлі *ActivitiesCache.db*. Вона містить інформацію за допомогою якої можливо відновити попередні події. Файл представляє собою базу даних *SQLite* із таблицями *Activity*, *Activity_PackageId*, *ActivityAssetCache*, *ActivityOperation*, *AppSettings*, *ManualSequence*, *Metadata*.

Іншим компонентом є попередня вибірка *prefetch*. Цей компонент зберігає інформацію про запуск програмних додатків користувачем.

Наступним компонентом ОС *Microsoft Windows* є *amcache.hve* – файл реєстру, в якому зберігається інформація про запущені програмні додатки: їх шлях, часові мітки, хеш-значення *SHA1* файлу. Відповідне налаштування комплексу засобів захисту дає змогу, в разі порушення політики безпеки в АС, встановити хронологію подій, пов'язаних з інформаційними об'єктами. Застосування відповідних заходів щодо захисту інформації в ІКС та АС дасть змогу унеможливити виникнення інцидентів кібербезпеки. Зазначена частина прихованих функціональних компонентів ОС для роботи адміністраторів безпеки АС є додатковим джерелом отримання даних аудиту, що дозволяє виявляти факти порушення політики безпеки та встановлення порушника під час проведення розслідувань інцидентів кібербезпеки в АС.

Гнатюк Н. В. (ВА ім. Є. Березняка)

ПРОБЛЕМНІ ПИТАННЯ ФОРМУВАННЯ ДАНИХ З МЕРЕЖЕВОГО ТРАФІКУ ДЛЯ ПОДАЛЬШОГО АНАЛІЗУ

Моніторинг та аналіз мережевого трафіку стали критично важливими для вирішення завдань адміністрування комп'ютерних систем, зокрема під час виявлення та протидії хакерським атакам, розподілення трафіку та планування пропускної здатності каналів. Головним з цих завдань є класифікація потоків даних.

Класифікація мережевого трафіку – це процес аналізу характеру потоків трафіку в мережі, за допомогою якого категоруються дані на рівні протоколів (наприклад, TCP, UDP та IMAP) або за класами додатків (наприклад, HTTP, однорангові (P2P), telnet).

У доповіді розглядаються проблемні питання підготовки наборів даних для класифікації мережевого трафіку та причини відсутності універсальних загальнодоступних наборів для вирішення цього завдання.

Метою проведення досліджень є аналіз методів машинного навчання для класифікації мережевого трафіку, а саме типів, моделей та ознак класифікації, а також наборів даних, на основі яких проводиться навчання та тестування моделей.

Відомо, що для проведення аналізу та класифікації даних мережевого трафіку використовуються методи машинного навчання, так як вони мають суттєві переваги над іншими підходами. Методи, що розглядаються у даному дослідженні, відносяться до класів навчання з вчителем, тобто для навчання моделі необхідно мати розмічений набір даних з прикладами використання в усіх класах. Для найпопулярніших завдань машинного навчання є класичні набори даних, які можна використовувати для навчання моделей та порівняння отриманих результатів з результатами інших досліджень. Але для завдання класифікації Інтернет трафіку неможливо виділити такий набір даних (або набори).

Способи отримання трафіку для класифікації можуть відрізнятися. Найпростішим можна вважати перехоплення реального трафіку у мережі, але виникає проблема розмітки таких даних. Крім того, отримані набори даних незбалансовані за кількістю прикладів кожного класу. Другий підхід – це контрольований збір даних, коли записується тільки трафік, що генерується цільовими програмами, але тут виникають складнощі організації фільтрації фону. Для отримання великої кількості прикладів можуть створюватись генератори штучних даних, що імітують реальний трафік на основі аналізу зразків з мережі. Однак, у цьому випадку необхідно слідкувати, щоб дані не були занадто одноманітними та відповідали реальним. Окремою проблемою постає постійна поява нових протоколів, що вимагають підтримки наборів даних в актуальному стані та вміння визначати раніше невідомі класи.

Оскільки масиви інформації, що отримуються з мережевого трафіку, можуть містити конфіденційні або персональні дані користувачів та збираються без їх дозволу, використовувати такі масиви для інших досліджень майже неможливо. Також не підлягають розповсюдженню набори ознак, так як вони можуть бути недостатніми для інших методів та експериментів або містити помилки обчислення (наприклад, набори даних, отримані за допомогою інструментарію CICFlowmeter: ISCX2012, CICIDS2017, CICIDS2018 тощо).

Зберегти баланс між конфіденційністю та відкритістю можна за допомогою анонімізації цих відомостей, яка приховує персональні та інші дані про користувачів, але зберігає корисні для подальших досліджень ознаки. Було проведено огляд доступних інструментів анонімізації, але не всі вдалося протестувати.

Таким чином, при формуванні набору даних для здійснення класифікації мережевого трафіку необхідно реалізувати виконання наступних завдань: 1. Для кожної досліджуваної групи потрібно знаходити та готувати дані відповідно до мети дослідження. 2. Під час прийняття рішення щодо вибору наборів даних для навчання та тестування класифікатора доцільно врахувати наведені вище твердження та припущення, щоб створена модель відповідала поставленому завданню та могла працювати в реальних умовах.

Громлюк К. А. (ВІТІ ім. Героїв Крут)
Романов Д. О. (ГУЗК ГШ ЗСУ)
Фещенко І. О. (НДІ ВР)

ОСНОВИ ТЕОРІЇ ПЕРКОЛЯЦІЇ ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ ДОСЛІДЖЕННЯ СТІЙКОСТІ МЕРЕЖ

Теорія перколяції є потужним інструментом кібербезпеки для виявлення слабких місць у мережі та підвищення рівня її захисту. Існує три основні типи мережевих збоїв, які використовуються для дослідження: мережеві збої на основі підключення; на основі каскаду та на основі функціональності. Метою доповіді є аналіз застосування теорії перколяції в дослідженнях стійкості безмасштабних мереж, наближених до реальних. У теорії перколяції збій мережі описується твердженням, чи існує гігантський кластер після видалення достатньої кількості вузлів або ребер. Ступінь стійкості мережі можна виміряти розміром гігантського компонента (найбільшим компонентом або кластером).

Для випадкових моделей безмаштабних мереж цільові атаки, засновані на ступені вузла, по суті, еквівалентні звичайному процесу просочування, який регулює випадкову відмову або видалення вузлів. Найбільш вивченим процесом перколяції є випадкове видалення вершин або ребер для мережі, що відповідає випадковим подіям збою або нескоординованим атакам наосліп.

Каскадний збій мережі – це інший тип відмови, до якого можна застосувати теорію перколяції. Каскадний збій означає, що проблема функціонування поширюється від одного вузла мережі до іншого, подібно до епідемії в людських системах. Відповідно, коли сусіди вузла скомпрометовані атакою, вузол вразливий до атаки з відповідним порогом, корелюючим з кількістю скомпрометованих сусідів. У такому разі, на швидкість розповсюдження збою у мережі впливають: область впливу збою, а саме – наскільки корельований збій проник у загальну мережу, що відображається в моделюванні, як максимальна дистанція між першою точкою збою до наступної; ймовірність поширення відмови, яку можливо описати як функцію зв'язку відмов, що представляє ймовірність поширення вихідної помилки функціонування від одного вузла до іншого. Ймовірність поширення відмови можливо змоделювати на основі порогової моделі того, чи досягла кількість несправних (скомпрометованих) вузлів, навколо працюючого, порогового значення. Необхідно врахувати також, що при компрометації критичних вузлів відмови матимуть більший вплив на сусідні вузли.

Відмови критичних вузлів розглядаються як мережеві збої на основі функціональності. Моделювання цілеспрямованого видалення вузлів на основі ступеня вузла здійснюється з припущенням, що зловмисник має знання про базову топологію мережі і відображає цільові атаки, де для обчислення значення критичності вузла використовуються різні показники центральності. Наступним зі збоїв на основі функціональності є відмова через перенавантаження, де збій певного вузла може вплинути на функціональність його сусідніх вузлів. Збільшення потоків трафіку, робочого навантаження або перерозподіл навантаження між вузлами може призвести до більшого виснаження ресурсу мережі, що може бути критичним фактором для живучості мережі, якщо мережа сильно обмежена ресурсами. Третім є збій підкомпонента, де несправність одного або декількох вузлів може суттєво кількісно вплинути на загальне надання послуг кластером (модулем) мережі і, відповідно, може розглядатися як збій усіх вузлів у кластері (модулі), що призводить до більшої вразливості мережі згідно з теорією перколяції.

Отже, авторами було розглянуто можливість оцінювання стійкості мереж на основі теорії перколяції. Особливо актуальним для військових потреб є аналіз здійснення цільових атак на критичні вузли мережі. Напрямком подальших досліджень вважається проведення з використанням теорії перколяції вивчення залежності стійкості малих мереж від умов їх функціонування. Зазначене можливо використати для розробки стратегії захисту мережі на основі адаптивного управління її показниками.

Ільїн Д. В. (НУОУ)

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ КІБЕРЗАХИЩЕННОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Ми живемо в епоху цифрових технологій, і мережа інтернет стала необхідною складовою для роботи інформаційних систем військового призначення. Однак, разом з поширенням мережі інтернет, з'явилися і нові загрози для безпеки, зокрема, DDoS-атаки, які можуть перешкоджати виконанню бойових (повсякденних) завдань для яких можуть бути використані інформаційні системи військового призначення.

Сучасні системи боротьби з DDoS атаками стали необхідними складовими елементами кібербезпеки інформаційних систем військового призначення в умовах постійної загрози з боку російської федерації. Однак, не зважаючи на поширеність цих систем, вони мають ряд недоліків у своїй роботі, що зменшує ефективність їх роботи та можливість забезпечення повноцінного захисту мереж від DDoS-атак.

Першим недоліком є те, що більшість систем боротьби з DDoS-атаками засновані на здатності виявлення аномального трафіку та відсіювання його до моменту, коли він досягне сервера. Однак, у кіберпросторі постійно з'являються нові загрози від державних та недержавних акторів, які використовують різноманітні технології та сили для здійснення кібератак. російська федерація є однією з держав, яка активно використовує кіберзброю та кібершпигунство для досягнення своїх політичних та військових цілей. У зв'язку з цим, необхідно постійно вдосконалювати системи захисту від кібератак, зокрема, розробляти нові методики виявлення та запобігання атакам, що дозволить ефективно опікуватися безпекою в кіберпросторі. В результаті, деякі DDoS-атаки все ще можуть досягати мережевої інфраструктури та завдавати значної шкоди.

Ще однією проблемою, що перешкоджає ефективній роботі систем боротьби з DDoS-атаками, є значна кількість хибно-позитивних сигналів, що генеруються такими системами. Це може привести до блокування законних запитів користувачів, та негативно вплинути на виконання бойових (повсякденних) завдань з для яких можуть бути застосовані інформаційні системи військового призначення. Для вирішення цієї проблеми можна застосувати різноманітні методи та алгоритми фільтрації, які дозволяють відсіювати хибні сигнали та забезпечують високу точність виявлення атак. Однак, важливо розробляти такі алгоритми з урахуванням специфіки конкретної інформаційної системи військового призначення та типів трафіку, що забезпечує максимальну ефективність та надійність захисту.

Третім недоліком є складність налаштування та обслуговування систем боротьби з DDoS-атаками. Це може бути особливо складно для підрозділів тактичної ланки, які можуть не мати достатньо кваліфікованого персоналу для розгортання та налагодження цих систем.

Отже, для забезпечення повноцінного захисту від DDoS-атак, необхідно вдосконалювати та покращувати сучасні системи боротьби з даним типом атак, а також розробляти нові методи та підходи до боротьби з цією загрозою. Один зі способів удосконалення систем боротьби з DDoS-атаками направлених на інформаційні системи військового призначення полягає у застосуванні машинного навчання та штучного інтелекту. Завдяки цим технологіям можна розробляти більш точні та ефективні алгоритми виявлення та відсіювання аномального трафіку, що дозволить забезпечити більш високу точність виявлення DDoS-атак та знизити кількість хибно-позитивних сигналів.

Ще одним підходом до вдосконалення систем боротьби з DDoS-атаками є розробка розподілених систем захисту інформаційних систем органів державної влади, місцевого самоврядування та інформаційних систем військового призначення, що дозволяють забезпечити більш високу надійність та стійкість до атак. Застосування розподіленої архітектури дозволить розподілити навантаження між кількома серверами, що знизить ризик перевантаження одного сервера та дозволить забезпечити неперервну роботу системи.

Для забезпечення більшої ефективності систем боротьби з DDoS-атаками, необхідно розробляти та застосовувати нові інформаційні технології, які б використовували удосконалені алгоритми виявлення та аналізу атак, що дозволить забезпечити більш оперативну та ефективну реакцію на атаки. Для цього можна використовувати різноманітні методики моніторингу та аналізу мережевого трафіку, що дозволять виявляти аномальний трафік та запобігати DDoS-атакам з наступними наслідками. Отже, вдосконалення та покращення систем боротьби з DDoS-атаками є важливою задачею для забезпечення безпеки мереж та інфраструктури в цілому. Застосування новітніх технологій та підходів до боротьби з DDoS-атаками дозволить забезпечити більш високу ефективність та надійність систем захисту, що знизить ризик виникнення проблем з безпекою та забезпечить стійку роботу інформаційних систем військового призначення.

Колтовсков Д. Г. (ВІТІ ім. Героїв Крут)

АНАЛІЗ ТЕХНОЛОГІЙ ПОБУДОВИ РОЗВІДЗАХИЩЕНИХ КАНАЛІВ КЕРУВАННЯ БпЛА

Сучасний підхід до ведення бойових дій вимагає перегляду важливості застосування безпілотних літальних апаратів (БпЛА) у вирішенні різноманітних завдань з підвищення боєздатності та нарощування бойових спроможностей підрозділів. БпЛА, в залежності від свого класу та призначення, вирішують широкий спектр завдань, що пов'язані з логістикою, розвідкою, коригуванням та бойовим враженням різноманітних цілей. БпЛА спроможні виконувати бойові завдання як на лінії бойового зіткнення так і в тилу противника. Даний підхід перш за все спрямований на збереження життя та здоров'я особового складу.

Успішність виконання бойових завдань за допомогою БпЛА пов'язана зі складністю ураження їх вогневими засобами. БпЛА за рахунок своїх невеликих габаритних розмірів мають незначну ефективну площу розсіювання (ЕПР) для засобів ППО та ЗРК. Висока маневреність БпЛА дозволяє їм бути майже недосяжними для ураження стрілецькою зброєю.

Крім зазначених переваг, існують вразливі місця в частині каналів керування БпЛА та систем навігації. Значна кількість каналів керування БпЛА побудована з використанням Open source рішень, що дозволяє противнику виявляти дані канали за допомогою засобів радіотехнічної розвідки (РТР) та вживати заходів до їх придушення та подальшого впливу за допомогою засобів радіоелектронної боротьби (РЕБ). Відмова в каналі керування БпЛА призводить до зриву виконання завдання та, як правило, до втрати самого БпЛА.

Метою роботи є визначення технологій побудови розвідзахищених каналів керування БпЛА для зменшення ймовірності їх виявлення засобами РТР.

Канал керування БпЛА представляє собою сукупність приймально-передавальних радіозасобів та середовища розповсюдження між бортом БпЛА та наземною станцією керування та контролю. Канал керування БпЛА призначений для передачі телеметричної інформації з борту БпЛА на наземну станцію керування та контролю (географічні координати, поточна швидкість, висота, курс, параметри системи електроживлення, параметри силового устаткування, діагностична інформація, етапи виконання польотного завдання, параметри встановленого цільового спорядження та інша інформація, в залежності від конфігурації наявних бортових сенсорів) та передачі команд керування (команд відповідного впливу на виконавчі механізми) на борт БпЛА.

Аналіз застосування БпЛА показує, що найбільш ефективним в боротьбі з БпЛА є перехоплення керування та придушення (постановка перешкод для приймального тракту радіозасобів на борту БпЛА) саме каналів керування БпЛА за допомогою засобів РЕБ.

Як правило, засоби РТР та РЕБ поєднані у єдиному апаратно-програмному комплексі та умовно поділені за своїми функціональними призначеннями.

Виявлення каналів керування БпЛА засобами РТР та вплив на них засобами РЕБ можливо поділити на декілька етапів, що реалізуються у визначеній послідовності: енергетичне виявлення передавачів радіозасобів, структурне виявлення сигналів, інформаційне виявлення змісту повідомлень, що передаються та подальший вплив на них.

Виходячи із зазначеної послідовності виявлення та протидії каналам керування БпЛА особливу увагу слід приділяти енергетичним показникам сигналів, що передаються, тобто розглядати фізичний рівень мережевої моделі OSI, який визначає метод передачі даних від одного пристрою до іншого, представлених у двійковому вигляді.

Енергетичні показники сигналів, що передаються по каналах керування БпЛА повинні відповідати таким критеріям, що унеможливлюють та/або суттєво зменшують енергетичне виявлення їх засобами РТР та в той же час забезпечують достатній рівень відношення сигнал/шум на вході приймача БпЛА для здійснення передавання команд керування.

Розвідзахищеність (прихованість) каналів керування БпЛА від засобів РТР можливо розглянути як ймовірність успішного детектування каналів керування БпЛА засобами РТР з заданою достовірністю у визначений часовий інтервал.

Відомо, що канали керування БпЛА, побудовані з використанням технологій розширення спектру сигналів володіють найбільшими енергетичними показниками та володіють властивостями передачі інформації на рівні шумів. Зазначені технології спрямовані на збільшення спектральної щільності потужності та енергії передачі одного біту інформації з заданою достовірністю. До зазначених технологій можна віднести наступні:

псевдовипадкове перестроювання робочої частоти (від англ. *FHSS — Frequency Hopping Spread Spectrum*). Суть методу полягає в періодичній стрибкоподібній зміні частоти опорного сигналу за певним алгоритмом, відомим приймачу і передавачу;

розширення спектра методом прямої послідовності (від англ. *DSSS — Direct Sequence Spread Spectrum*). Суть методу полягає в підвищенні тактової частоти модуляції, при цьому кожному символу переданого повідомлення ставиться у відповідність деяка досить довга псевдовипадкова послідовність;

розширення спектра методом лінійної частотної модуляції (ЛЧМ) (від англ. *CSS — Chirp Spread Spectrum*). Суть методу полягає в перебудові частоти-носія за лінійним законом.

Аналіз наукових публікацій та проведених практичних випробувань показує, що розширення спектру методом ЛЧМ, а саме внутрішньоімпульсною ЛЧМ (ВЛЧМ), володіє найвищими енергетичними показниками серед зазначених. Крім цього, ВЛЧМ, за рахунок своїх унікальних особливостей формування інформаційних повідомлень на фізичному рівні, виявляється стійким до негативного впливу доплеровського зсуву частот та багатопроменевого прийому сигналів, що не притаманне іншим методам розширення спектру. Формування інтервально-імпульсних послідовностей, узгоджених з поточним рівнем шумів в каналі, які передаються шумоподібними сигналами із відомими параметрами лише приймачу та передавачу є ефективним способом прихованої передачі інформації від засобів РТР.

Отже, якщо засобам РТР невідомо метод формування ВЛЧМ сигналів та невідома автокореляційна функція даних сигналів, то ймовірність виявляння даних сигналів мінімальна.

Таким чином важливо мати метод, що дозволяє здійснювати скритий від засобів РТР обмін інформацією між наземною станцією керування та БпЛА. В іншому випадку, при детектуванні засобами РТР будь-яких ознак обміну інформацією між наземною станцією керування та БпЛА, противником буде вжито додаткових заходів, щодо пошуку та всебічного впливу на БпЛА.

Той факт, що відношення сигнал/шум на виході узгодженого фільтра приймача визначається лише енергією корисного сигналу та не залежить від його форми, дозволяє приховувати сигнал в шумах. Дійсно, якщо зменшити амплітуду сигналу та збільшити його тривалість з метою збереження енергії незмінною, сигнал перестає як візуально, так і фактично виявлятися на фоні шумів. Виходячи з того, що енергія сигналу залишається незмінною на тих частотах, де зосереджено його спектр, його спектральна щільність потужності по модулю буде перевищувати спектральну щільність потужності шуму та буде забезпечувати обмін інформацією із заданою достовірністю.

Але, серед зазначених переваг ВЛЧМ сигналів, існує суттєвий недолік щодо швидкості обміну інформацією в каналі керування БпЛА. Використання спеціальних комплексних методів та алгоритмів адаптивного формування та обробки сигнально-кодових послідовностей ВЛЧМ сигналів в каналі керування БпЛА на фізичному рівні дозволяє вирішити дану задачу з метою забезпечення безвідмовного керування БпЛА в складній завадовій обстановці та динамічній зміні параметрів середовища розповсюдження сигналів в умовах постійного моніторингу радіочастотної обстановки засобами РТР.

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

АНАЛІЗ ВРАЗЛИВОСТЕЙ БЕЗДРОТОВИХ МЕРЕЖ WI-FI

Завдяки широкому застосуванні технології бездротової передачі інформації та із зростанням використання *Wi-Fi* технологій для побудови корпоративних мереж постає питання забезпечення захищеності та вибору ефективних методів захисту.

Провести аналіз вразливостей та шляхів підвищення захищеності *Wi-Fi* мереж стандарту IEEE 802.11.

На сьогоднішній день існує різноманітність бездротових мереж *Wi-Fi*, недосконалий захист яких може бути використаний хакерами для отримання несанкціонованого доступу до активів та інформаційних ресурсів користувачів та організацій.

Під час аналізу відомих атак на мережі стандарту 802.11 було з'ясовано, що більша частина вдало проведеного «зламу» відбулася через неправильні налаштування програмного забезпечення користувача або підбір ключа / пароля. Це дало можливість систематизувати вразливості та згрупувати можливі вектори атак. Отже характерними вразливостями є:

трансляція *SSID Broadcasting* по замовченню або використання в якості *SSID* назви організації чи типу пристрою, що дозволяє легко ідентифікувати мережу для здійснення подальших атак;

недосконалі протоколи шифрування *WPA, WPA-2 PSK* дозволяють проводити атаки з переустановленням ключа (KRACK) і захопленням «рукостискання», що дозволяє зламати ключ шифрування та отримати облікові дані шляхом добору пароля (*Brute Forcing*);

навіть використання останнього сучасного протоколу шифрування *WPA-3* не дозволяє повністю захистити *Wi-Fi* мережу: потрібна наявність всіх пристроїв з підтримкою цього протоколу, крім того був виявлений недолік, який відкривав мережеві паролі;

нажаль, *Wi-Fi* мережі за своєю природою вразливі до проведення *DoS* атак, що призводить до споживання ресурсів точок доступу та зайнятості каналів передачі. Це використовується для деаутентифікації користувачів та проведення атаки типу «людина всередині» задля перехоплення потрібного трафіку;

архітектура побудови *Wi-Fi* мереж вразлива щодо можливості створення неавторизованих точок доступу (*Evil Twin*) підключення до яких призводить до можливості викрадення конфіденційних даних;

неправильне налаштування або налаштування «за замовченням» обладнання *Wi-Fi* призводить до можливого несанкціонованого доступу до ресурсів мережі;

чисельні помилки в драйверах пристроїв *Wi-Fi* призводять до можливості використання переповнення буфера для виконання довільних команд – іноді на кільці 0 (режим ядра з високим рівнем привілеїв). На зараз опубліковано численні експлойти, щоб скористатися недоліками помилкових драйверів *Wi-Fi*.

Відомі атаки на мережі *Wi-Fi* варто групувати за наступними напрямками:

атаки на сервіс контролю доступу що мають на меті проникнення в мережу ухиляючись від заходів котролю доступу таких як фільтрація *MAC* адрес на точці доступу та контроль доступу до *Wi-Fi* портів (серед відомих є такі: вардрайвінг, використання шахрайської точки доступу, підробка *MAC* адрес, помилкове асоціювання клієнта, неправильна конфігурація точки доступу, несанкціонована асоціація та інші);

атаки спрямовані на порушення цілісності, коли зловмисники надсилають підроблені кадри контролю, керування або даних через бездротову мережу, щоб спрямувати бездротові пристрої для здійснення іншого типу атак (наприклад, *DoS*) (деякі з найпоширених: ін'єкція *WEP*, ін'єкція кадрів даних, створення дублюючих точок доступу, відтворення даних, атаки з перестановкою бітів, застосування вірусів для бездротових мереж та інші);

атаки на конфіденційність намагаються перехопити конфіденційну інформацію, надіслану через бездротові асоціації, незалежно від того, чи була вона надіслана у вигляді відкритого тексту чи зашифрована протоколами шифрування *Wi-Fi* (основними атаками цієї групи можна вважати: підслуховування, аналіз трафіку, викрадення сеансу, маскування, атака «Людина посередині», *Evil Twin* та інші);

атаки на доступність мають на меті перешкодити доставці бездротових послуг законним користувачам, або пошкодивши ці ресурси, або заборонити їм доступ до ресурсів *WLAN* (відмова в обслуговуванні, збій *EAP*, атаки на маршрутизацію, експлойт *TKIP MIC*, отруєння кешу *ARP*, атаки на споживання енергії та інші);

метою атак аутентифікації є крадіжка особистих даних клієнтів *Wi-Fi*, їх особистої інформації, облікових даних для входу тощо для отримання несанкціонованого доступу до мережевих ресурсів (злам *PSK*, *LEAP,* VPN логінів, атака перевстановлення ключа, вгадування спільного ключа, спекуляція з паролями та інші).

З метою зниження ймовірності проведення зазначених атак та підвищення рівня захищеності *Wi-Fi* мереж потрібно дотримуватись наступних рекомендацій:

змініть *SSID* за замовчуванням або вимкніть його трансляцію;

не використовуйте в якості *SSID*, назви організації чи типу пристрою, назву мережі або будь-який рядок, який легко вгадати;

регулярно перевіряйте бездротові пристрої на наявність проблем із налаштуванням, не використовуйте налаштування «за замовченням»;

розмістить фаєрвол або фільтр пакетів між точкою доступу та корпоративною мережею;

реалізуйте більш надійну техніку шифрування трафіку, наприклад *IPSec*, по бездротовій мережі *Wi-Fi;*

використовуйте надійні паролі та регулярно змінюйте парольні фрази;

розмістить бездротові точки доступу в захищеному місці;

увімкніть фільтрацію *MAC*-адрес на вашій точці доступу або маршрутизаторі;

використовуйте технологію віртуальної приватної мережі (*VPN*), таку як *VPN* віддаленого доступу, Екстранет *VPN* та Інтранет *VPN*;

регулярно скануйте мережу *Wi-Fi* на наявність неавторизованих точок доступу;

використовуйте централізований сервер для аутентифікації такий як *RADIUS*;

перевіряйте наявність оновлень драйверів для бездротового мережевого обладнання та інсталюйте їх, якщо вони є, після чого вони можуть включити в себе оновлені протоколи шифрування з виправленими вразливостями;

використовуйте мультифакторну аутентифікацію;

впровадьте бездротову систему виявлення вторгнень (*WIDS*) / бездротову систему запобігання вторгненню (*WIPS*);

вимкніть мережу, якщо вона не потрібна.

Проведений аналіз вразливостей, векторів атак та шляхів підвищення захищеності *Wi-Fi* мереж дозволить в подальшому побудувати ефективну політику безпеки використання бездротових мереж стандарту 802.11 яка є складовою частиною системи управління інформаційної безпеки організації.

Таким чином, бездротові *Wi-Fi* мережі мають свої характерні вразливості, які можуть бути використані зловмисниками для здійснення атак на активи як організацій так і користувачів. Для запобігання цього необхідно проводити комплекс заходів захисту який ґрунтується на розумінні того, що для безпеки бездротового *Wi-Fi* зв'язку не достатньо тільки коректного налаштування мережевих пристроїв, використання механізму приховування мережі та впровадження сучасних протоколів шифрування – таких як *WPA-2*, *WPA-3*. Застосування технологій віртуалізації, централізованої аутентифікації та тунелювання, не дивлячись на можливе сповільнення швидкості передачі мережею, ефективно покращує рівень захищеності бездротового *Wi-Fi* зв'язку. Крім того, важливо пам'ятати про те, що захист від кіберзагроз є постійним ітераційним процесом, тому необхідно проводити регулярний моніторинг захищеності мережі та аналіз виявлених вразливостей.

Могилевич В. Д. (КНУ ім. Тараса Шевченка)

АНАЛІЗ АТАКИ ПОВТОРНОГО ВИКОРИСТАННЯ КОДУ НА ОПЕРАЦІЙНІ СИСТЕМИ

Досвід бойових дій з російською федерацією показав, що інформаційно- комунікаційні системи є надзвичайно цінними мішенями для супротивника. Зловмисники зміщують свою увагу на новітні методи за допомогою низки дедалі складніших атак, які поєднують уразливості програмного та апаратного забезпечення для створення успішних експлойтів. Такі нові атаки мають значний вплив на інформаційну безпеку, оскільки вони повністю обходять існуючі засоби захисту.

Метою дослідження є аналіз сучасних атак на операційні системи заснованих на пошкодженні пам'яті.

Хоча експлойти на основі пошкодження пам'яті вивчалися більше трьох десятиліть, дослідження показали, що атаки цього типу можуть повністю обійти найсучасніші засоби захисту, такі як *Control-Flow Integrity*, що широко застосовуються на практиці.

Переповнення буфера на основі стека є одним з прикладів класу помилок, який допускає пошкодження пам'яті. Вони є частиною набагато більшого сімейства вразливостей, які також включають помилки на основі купи, уразливості рядків форматування, плутанину типів, використання неініціалізованих даних, помилки use-after-free і double-free, некеровані вказівники, помилки синхронізації та переповнення цілочисельних змінних. Атаки з впровадженням коду вдалося швидко запобігти шляхом розгортання апаратних та програмних засобів захисту, таких як *Data Execution Prevention* (*DEP*), що дозволяє системі позначити одну або кілька областей пам'яті як не виконувані. Позначка областей пам'яті таким чином означає, що код не може виконуватися з цієї області пам'яті, це ускладнює використання переповнення буфера. Таким чином, зловмисники більше не можуть виконати код, який вони ввели в пам'ять програми. Однак аналіз показав, що базова парадигма атак була адаптована для обходу *DEP* шляхом узагальнення атак із впровадженням коду до атак із повторним використанням коду. Під час атаки повторного використання коду зловмисник використовує вразливість, пов'язану з пошкодженням пам'яті, для захоплення потоку керування запущеною програмою, зловмисно модифікуючи вказівник коду замість того, щоб вводити будь-який код. Наприклад, адресу повернення, яка зазвичай зберігається в стеку програми можна змінити так, щоб вона вказувала на деяке місце довільного коду, яке вже присутнє в пам'яті. У найпростішому випадку це дозволяє зловмиснику перенаправити виконання на іншу функцію, таку як функція бібліотеки, яка розгалужує іншу програму та надати зловмисний вхід (наприклад, «/bin/sh» для запуску оболонки).

Важливо зазначити, що атаки повторного використання коду можливі в багатьох системах, деякі з яких навіть не пропонують спеціальної інструкції повернення. Зокрема, можливості динамічного (або непрямого) розгалуження достатньо для створення атак повторного використання коду

Уразливості, що пов'язані з пошкодженням пам'яті, дозволяють зловмисникам взяти під контроль уражену програму та створити серйозні загрози для безпеки операційній системі. З міркувань продуктивності всі основні операційні системи написані на мовах програмування низького рівня, що робить систему вразливою до пошкодження пам'яті у разі помилки. Це означає, що зловмисник, який отримав доступ до системи через вразливу програму у просторі користувача, може націлитися на помилки в коді ядра операційної системи запустивши атаки на вразливості пам'яті в системних викликах або драйверах на низькому рівні коду операційної системи.

Муромець О. С. (ЦНДІ ЗСУ)
к.військ.н., с.н.с. Завацький О. Б. (ЦНДІ ЗСУ)
к.військ.н., с.н.с. Шовкошитний І. І. (ЦНДІ ЗСУ)

ПРОБЛЕМНІ ПИТАННЯ ОРГАНІЗАЦІЇ КІБЕРБОРОТЬБИ У ПЕРІОД ПРОВЕДЕННЯ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

У сучасних умовах збройна боротьба ведеться із застосуванням високотехнологічного озброєння і військової техніки, засобів розвідки, управління й ураження. Інформаційне забезпечення процесів управління та навантаження органів управління постійно зростають. Забезпечення ефективності управління своїми силами і засобами та порушення його у противника надає вагомі переваги над ним в умовах сучасного протиборства. Кібервплив все частіше стає ефективним інструментом несилового контролю та управління як об'єктами критичної інформаційної інфраструктури держави, що може піддатися такому впливу, так і окремо взятими громадянами, їх об'єднаннями. Нині практично всі держави зіткнулись з кіберзагрозами та вимушені формувати системи кібербезпеки та кібероборони. Тенденція перенесення дій у воєнних конфліктах до кіберпростору (як нового бойового середовища) ще більше загострило ці проблеми. Упродовж останніх восьми років росія веде повноцінну кібервійну проти України, нарощуючи свої зусилля, застосовує нові види кіберзброї, змінює тактику та механізми кібернетичного впливу, у тому числі на об'єкти сектору безпеки і оборони держави.

З початком 2022 року повномасштабої агресії росії проти України актуальність зазначених питань суттєво зросла. Зазначене спонукало Україну до запровадження першочергових заходів зі створення спеціальних структур і підрозділів для дій у кіберпросторі. З цією метою у Збройних Силах (ЗС) України було спланповано та проведено ряд організаційних заходів, під час реалізації яких було виявлено низку проблемних питань. У цих умовах виникає завдання щодо висвітлення таких проблемних питань з метою їх подальшого швидкого розв'язання.

Для підвищення ефективності кіберборотьби та кіберзахисту у ЗС України було здійснено низку організаційних заходів, але розмежування функцій з цих питань між різними органами військового управління, на наш погляд, є не завершеним. Зокрема, функції організації, керівництва забезпеченням кібербезпеки у ЗС України були покладені на Головне управління зв'язку та кібербезпеки (J6) Генерального штабу (ГШ) ЗС України. При цьому одним з основних завдань цього управління є "організація та управління забезпечення кібербезпеки ЗС України, захисту інформації в ІКС ЗС України та кіберзахисту ІКС ЗС України, організація, підготовка оборонних кібероперацій ЗС України та участь ЗС України в оборонних кіберопераціях сил оборони". З іншого боку у результаті оргзаходів з кінця 2022 року відбулося виведення Центрального управління радіоелектронної боротьби (РЕБ) зі складу Командування Сил підтримки ЗС України та реформування його у Головне управління радіоелектронної та кіберборотьби ГШ ЗС України. Тобто РЕБ, яка раніше була видом підтримки (оперативного забезпечення) дій військ (сил) фактично була вилучена із системи підтримки ЗС України. Нині перетворена на специфічний вид застосування ЗС України з появою, окрім традиційних завдань (подавлення радіоелектронних об'єктів противника, радіоелектронного захисту своїх систем і засобів управління військами та зброєю, електронної підтримки РЕБ), нових функцій щодо:

організації виконання завдань планування кібероборони України;

планування та ведення РЕБ та кіберборотьби;

управління радіочастотним спектром;

розвитку відповідних спроможностей.

У таких умовах, на наш погляд, виникають деякі проблеми організації кіберборотьби.

Основна проблема пов'язана із незавершеною трансформацією згідно із чинними доктринальними, положеннями "радіоелектронної боротьби" у "електромагнітну та кіберборотьбу", що викликає дві наступні підпроблеми:

1. Проблеми організаційного характеру:

а) цілісність системи підтримки ЗС України та тимчасової невизначеності у порядку її функціонування;

б) незавершеність формування у всіх ланках ЗС України єдиної вертикалі управління радіоелектронною (електромагнітною) та особливо кіберборотьбою, що пов'язано із різною підпорядкованістю органів управління її окремими складовими.

2. Проблеми технічного характеру:

а) така складова, як "кіберборотьба", логічно повинна передбачати наявність певних кіберсил (кіберпідрозділів) та кіберзброї з інтеграцією їх до радіоелектронної (електромагнітної) боротьби, що підтверджується введеними "Концепцією розвитку системи РЕБ у ЗС України на період до 2026 року" поняттями "електромагнітна боротьба", "операції в електромагнітному спектрі", "кібернетична боротьба в електромагнітному спектрі". Проте, нині у структурі ЗС України кіберпідрозділи перебувають у стадії формування, а "кіберзброя", яка відповідно до "Основних напрямів розвитку зброї на нетрадиційних принципах дії та перспектив її застосування ЗС України" належить до "інформаційної зброї" і є різновидом зброї на нетрадиційних принципах дії, поки має занадто абстрактний характер для розуміння обсягів оснащення нею відповідних підрозділів;

б) неготовність існуючих підрозділів РЕБ (без їх суттєвого додаткового оснащення) до ведення операцій в електромагнітному спектрі (проблема протидії оптико-електронним, акустичним засобам розвідки противника, високоточній зброї (ВТЗ) з комбінованими системами наведення) та кіберпросторі.

Найбільш складними та нагальними є проблеми організаційного характеру. Їх розв'язання потребує нормативного врегулювання питань розподілу повноважень у галузі радіоелектронної (електромагнітної) боротьби, кібероборони, кіберборотьби та кіберзахисту.

Для розв'язання проблемних питань технічного характеру (з точки зору критичних спроможностей) необхідно вжити заходів щодо впровадження засобів (технологій) для: розширення спроможностей з протидії дистанційно керованим об'єктам противника – БпЛА, "роям" БпЛА, наземним роботизованим комплексам, засобам ВТЗ з комбінованими системами наведення; набуття у ближчій перспективі спроможностей щодо протидії оптико-електронним засобам (системам) розвідки та управління зброєю, функціонального ураження РЕЗ противника (за рахунок зброї на основі електромагнітного імпульсу та бойових лазерних систем), імітації (створення хибної) радіоелектронної обстановки, здійснення інформаційно-технічного (інтелектуального) впливу на радіоелектронні об'єкти противника.

На підставі наведеного вище можна зробити висновок, що незавершеність організаційних заходів, що тривають у системі управління Збройними Силами України несе загрозу кібербезпеці України та її Збройним Силам. Прийняте рішення щодо трансформації "радіоелектронної боротьби" у "електромагнітну та кіберборотьбу" повинно логічно бути підтримано логічним розмежуванням (розподілом між органами упраління) функцій кіберборотьби (у контексті радіоелектронної або електромагнітної боротьби) та кіберзахисту.

Також одним з головних завдань у сучасних умовах повинно бути завершення формування у всіх ланках ЗС України єдиної вертикалі управління радіоелектронною та кіберборотьбою (електромагнітною та кіберборотьбою), створення на усіх рівнях підрозділів (органів) з відповідними чітко визначеними функціями та завданнями, а також вирішення проблемних питань технічного характеру.

д.т.н. Пількевич І. А. (ЖВІ ім. С. П. Корольова)
к.т.н. Бойченко О. С. (ЖВІ ім. С. П. Корольова)
Лобода В. В. (ЖВІ ім. С. П. Корольова)

МАТЕМАТИЧНА МОДЕЛЬ ОЦІНЮВАННЯ ЦІННОСТІ ІНФОРМАЦІЇ

У суспільстві значно зросла роль інформації та інформаційних ресурсів у всіх сферах життя людини. Перетворення інформації на продукт, що має певну та відповідну цінність, призвело до появи нового об'єкта безпеки – інформації та інформаційних ресурсів. Раніше інформаційна безпека полягала у захисті інформації та інформаційних ресурсів від несанкціонованих дій. В даний час виникає потреба захисту людини, суспільства або держави від загроз, які можуть представляти інформація та інформаційні ресурси. Таким чином, сьогодні загрози, які може нести інформація та інформаційні ресурси, торкаються таких сторін життя людини, як економічна, фінансова, військово-технічна, політична.

Результати аналізу методів оцінювання цінності інформації показали, що сучасні підходи не враховують впливу часу на цінність інформації та не враховується той факт, що згодом інформація втрачає свою цінність та її подальший захист стає недоцільним. Цей факт призводить до вдосконалення концептуальної моделі інформаційної безпеки.

Метою роботи є розробка математичної моделі оцінювання цінності інформації, що враховує такі характеристики, як термін остаточного старіння інформації, рівень обмеження доступу до неї, важливість та форма власності. В цьому випадку оцінювання цінності інформації можна розглядати як завдання обчислення нормованої ваги коефіцієнтів за формулою середнього арифметичного.

Цінність інформації в даному дослідженні слід розуміти як кількісну міру, що визначає ступінь її корисності для власника інформації. Оцінювання цінності інформації на основі методів та прийомів сучасної теорії системного аналізу надає інструменти для визначення відповідних коефіцієнтів на основі характеристик інформації. В роботі вибрано наступні характеристики інформації для оцінювання цінності інформації установи:

1. Рівень обмеження доступу інформації.
2. Період остаточного старіння інформації.
3. Важливість інформації.
4. Форма власності на інформацію.
5. Спосіб зберігання інформації.

Оцінювання вихідної цінності інформації проведено шляхом обчислення середнього значення суми відповідних коефіцієнтів. Кожен із вибраних коефіцієнтів розраховувався методом ранжування. Ранг відповідних інформаційних характеристик визначається з керівних документів щодо організації захисту інформації або спеціально створеної групою експертів.

Результати експерименту показали, що з інформації, що має самі значення, як і початкове значення, з часом значення поточної цінності інформації зменшується. Для відомостей, які у документах першого відділу установи, саме у звітах про діяльність протягом року, початкове значення відомостей дорівнює 0,33. Через рік цінність інформації зменшилася майже у 2,4 рази, а через 2 роки майже у 5 разів. Результати експерименту підтверджують, що цінність інформації має нелінійну функціональну залежність від часу остаточного старіння інформації.

Наукова новизна одержаних результатів у тому, що була запропонована математична модель оцінювання цінності інформації, яка дозволяє отримати кількісну оцінку цінності інформації.

Запропонована математична модель дозволить оцінити цінність інформації та надати інформацію керівнику установи для ухвалення рішення про доцільність подальших витрат на захист відповідної інформації, а це, в свою чергу, дасть можливість автоматизувати процес оцінювання цінності інформації на поточну дату з використанням математичного апарату сучасної теорії системного аналізу.

к.т.н. Погребняк Л. М. (ВІТІ ім. Героїв Крут)
Лукіна К. В. (ВІТІ ім. Героїв Крут)

АНАЛІЗ СУЧАСНИХ МЕТОДІВ МЕРЕЖЕВОЇ СТЕГАНОГРАФІЇ

Досвід війни з російською федерацією показав необхідність підвищення безпеки інформаційних ресурсів в спеціальних електронних комунікаціях. Одним із напрямків підвищення безпеки інформаційних ресурсів є використання стеганографічних методів.

Метою дослідження є аналіз сучасних методів мережевої стеганографії для прихованої передачі даних.

Загальною рисою всіх методів мережевої стеганографії є створення за їх допомогою прихованих каналів передачі в будь-якому відкритому каналі, у якому є надмірність.

Аналіз показав, що методи мережевої стеганографії можна поділити на наступні групи:

методи стеганографії, суть яких у зміні даних у полях заголовків мережевих протоколах та в полях корисного навантаження пакетів. Ідея методів модифікації полів заголовків полягає у використанні деяких полів заголовків для внесення до них інформації, яку необхідно приховати. Це можливо за рахунок деякої надмірності в даних полях, тобто існують певні умови, в яких значення даних полях не будуть використовуватися при передачі пакетів. Найчастіше використовуються поля заголовків *IP* та *TCP* протоколів;

методи стеганографії, в яких змінюється структура передачі пакетів, наприклад, змінюються черговості передачі пакетів або навмисне введення втрат пакетів під час їх передачі. Наприклад, використання характерних особливостей транспортного протоколу із контролем пакетів *SCTP* (*Stream control transport protocol*), таких як мультипоточність та використання множинних інтерфейсів. Методи зміни вмісту *SCTP*-пакетів ґрунтуються на тому, що кожна частина *STCP* пакет може мати змінні параметри. Протокол використовується в сучасних операційних системах *Linux*, *HP-UX*, *SunSolaris,* а також підтримується операційними системами мережних пристроїв *(Cisco IOS*, *RoterOS*);

змішані (гібридні) методи мережевої стеганографії – при їх застосуванні змінюються вміст пакетів, строки доставки пакетів та порядок їх передачі. Ці методи стеганографії використовують два підходи: навмисні затримки аудіо пакетів *LACK* (*Lost Audio Packets Steganography*) та ретрансляція пакетів *RSTEG* (*Retransmission Steganography*). В основі методу *LACK* лежить використання пакетів, які затримуються, або навмисно пошкоджуються та ігноруються приймачем (прикладною програмою), але не стеганографічним додатком. Метод *RSTEG* заснований на механізмі повторної посилки пакетів. Відправник посилає пакет, але одержувач не відповідає пакету з прапором підтвердження. Спрацьовує механізм повторної посилки пакетів, і тепер посилається пакет зі стеганограмою всередині, на який також не приходить підтвердження. При наступному спрацюванні даного механізму надсилається оригінальний пакет без прихованих вкладень, на який приходить пакет із підтвердженням про вдале отримання. Пропускна здатність стенографічного каналу *RSTEG* приблизно дорівнює пропускної здатності методів з модифікацією пакета, і при цьому вище, ніж методи зміни порядку передачі пакетів. Складність виявлення та пропускна здатність *RSTEG* безпосередньо пов'язана з використовуваним механізмом реалізації методу.

Таким чином, у сучасних умовах інформаційної боротьби завдання скритої та надійної передачі конфіденційної інформації є дуже актуальним. Застосування методів мережевої стеганографії, які змінюють властивості одного з мережевих протоколів, а також можуть використовувати взаємозв'язок між двома або більше протоколами дозволяє надійно приховати передачу повідомлення. Дослідження показало, що жоден із існуючих методів мережевої стеганографії не є досконалим. Прихована інформація, незалежно від методу, може бути виявлена: чим більше прихованої інформації внесено до потоку даних, тим більше шансів, що вона буде виявлена методами стегоаналізу. На виявлення прихованого каналу зв'язку впливає кількість пакетів, які використовуються для передачі прихованих даних, так як зростає частота ретрансльованих пакетів. Тому, важливим напрямком подальших досліджень є вдосконалення існуючих методів.

д.т.н. Субач І. Ю. (ВІТІ ім. Героїв Крут)
Власенко О. В. (ВІТІ ім. Героїв Крут)

БАГАТОРІВНЕВИЙ КІБЕРЗАХИСТ БАЗ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

У рамках вторгнення рф в Україну виник перший в світі великий конфлікт, пов'язаний із широкомасштабними кібероперацією. Було здійснено кібератаки, націлені на урядові веб-портали, телекомунікаційні служби, інформаційні системи військового призначення (ІСВП) та критичну інфраструктуру України. Захист цих об'єктів в умовах постійних кібератак є серед головних пріоритетів держави. Аналіз архітектури типової ІСВП показав, що ключовим елементом кожної системи є бази даних (БД). Захист БД, як основного елементу зберігання інформації в ІСВП, повинний бути пріоритетом для відповідних підрозділів кіберзахисту Збройних Сил України.

Типові методи захисту БД, які вбудовані у системи керування БД (СКБД) є недосконалими і не завжди можуть виявляти кібератаки в режимі реального часу. Як показує проведений аналіз, одним з дієвих способів виявлення кібератак в режимі реального часу є розміщення додаткового ступеня їхньої ідентифікації на рівні БД, а саме шляхом включення до периметру захисту системи виявлення вторгнень до баз даних (СВВБД). Механізми роботи СВВБД, в основному, базуються на аналізі мови запитів та побудови поведінкового профілю користувачів БД. Проте, діапазон сучасних кібератак на БД є дуже великим і різнобічним. Кібератаки можуть здійснюватися не безпосередньо на БД, а на середовище в якому вона функціонує. Наприклад, кібератаки на: виснаження ресурсів БД; надмірне споживання пам'яті; блокування потоку вводу-виводу тощо. Слід зауважити, що у даних кібератаках не існує єдиного вектору кібератаки, а є цілий ряд різних способів зловживання функціями БД та еко-системи, в якій вона функціонує. Тому, кіберзахист БД потрібно розглядати виключно з урахування рівнів функціонування БД, а саме: рівня СКБД та БД, рівня операційної системи та рівня мережі. Рівні безпеки повинні будуватися на основі еко-системи в якій функціонує БД. Якщо розглядати багаторівневий захист БД, то система кіберзахисту повинна працювати зі всіма рівнями функціонування БД та відслідковувати дії, які відбуваються в еко-системі БД і збирати дані для аналізу з різних джерел. Якщо дані отримуються з багатьох різнорідних джерел то для кіберзахисту БД, краще використовувати інформаційну технологію, основою якої є SIEM-система, що дозволяє збирати дані від різних джерел, аналізувати їх в реальному часі, виявляючи аномальні дії та вживати відповідні заходи. Консолідація інформації, отриманої з різних рівнів, робить захист БД більш досконалим і ефективнішим.

Аналіз наукових публікацій показав, що вектор досліджень SIEM-систем спрямований на покращення системи у цілому. Так, моніторинг подій в БД, перекладається на відповідні СВВБД і отримання інформації з них. Проте, СВВБД не передбачають роботу з різними різнорідними даними і не розглядають захист БД у комплексі, тому доцільно здійснювати кіберзахист БД на основі SIEM-системи, з вбудованими спеціалізованими модулями, які реалізують функції шкідливої активності саме по відношенню до БД. Подібне рішення, в умовах неповноти та неточності інформації про події, що відбуваються в системі, може бути реалізованим шляхом застосування методів інтелектуального аналізу даних, зокрема, методів теорії нечітких множин та нечіткого логічного виводу. В якості вхідних даних для функціонування запропонованої системи, повинні залучатися не тільки дані безпосередньо про БД, а й операційну систему, комп'ютерну мережу та інші програмні застосунки, які взаємодіють з БД.

Таким чином аналіз існуючих технологій кіберзахисту БД, дозволяє зробити висновок про існуюче у теперішній час протиріччя в науці і практиці, суть якого полягає у невідповідності вимог, які висуваються до методів кіберзахисту БД ІСВП та їхніми можливостями. Усунення протиріччя може бути здійсненим шляхом вирішення наукового завдання з розробки моделей, методів і методик кіберхахисту БД ІСВП в умовах неповноти та неточності інформації на основі теорії нечітких множин та нечіткого логічного виводу.

д.т.н., професор Толюпа С. В. (КНУ ім. Тараса Шевченка)
к.т.н., доцент Пампуха І. В. (КНУ ім. Тараса Шевченка)
Сліпачук Л. О. (КНУ ім. Тараса Шевченка)

ОЦІНКА СИСТЕМИ УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Процес впровадження нових інформаційних технологій в усі сфери життя сучасного суспільства, що вступає в постіндустріальний період свого розвитку, який можна назвати *інформаційним*, неможливий без рішення питань інформаційної безпеки в різних сферах.

Широкомасштабне використання обчислювальної техніки й телекомунікаційних систем, перехід до безпаперової технології, збільшення об'ємів оброблюваної інформації й розширення кола користувачів приводять до якісно нових можливостей несанкціонованого доступу до ресурсів і даних інформаційної системи, до її високої вразливості. В сучасних умовах захист інформації в цілому й захист інформації в автоматизованих інформаційних системах зокрема стає все більш складною проблемою [1].

Оцінювання СУІБ є класичною задачею, в якій оцінюються підсистеми, окремі елементи та вся система взагалі. Це передбачає вибір сукупності показників, яка дозволить оцінити ефективність функціонування її підсистем (елементів) та їх внесок до ефективності функціонування підсистем і системи в цілому.

Такий підхід дозволить врахувати те, що виконання СУІБ – це, в основному, ймовірний процес (значна кількість показників має імовірнісний характер), також поєднати ці показники оцінки з показниками іншого типу та вжити заходів щодо зменшення ступеня невизначеності системи (як стохастичної, так і нестохастичної) [2].

Центральною ланкою розв'язання експертно-аналітичних завдань (ЕАЗ) оцінювання рівня захищеності СУІБ є розробка КМ ПО (концептуальної моделі предметної області), яка формалізує структуру оцінки, що складається з сукупності показників оцінки та зв'язків між ними. Враховуючи зазначене, в основу створення КМ (концептуальної моделі) оцінки рівня захищеності СУІБ було покладено її розподіл на ієрархічні рівні, які описують процес самого забезпечення захисту інформації на ОКІ, процес оцінки способів забезпечення захисту інформації елементів СУІБ та встановлення зв'язків між цими рівнями за допомогою експертно-аналітичних методів [3].

Для реалізації цього підходу як комплексний показник оцінки на кожному ієрархічному рівні приймаємо рівень захищеності інформації:

- системи управління захистом інформації - $R_i^{\text{ЗІ}}$;
- складових системи управління захистом інформації - конфіденційності інформації $\left(R_i^{\text{К}}\right)$, цілісності інформації $\left(R_i^{\text{Ц}}\right)$, доступності інформації $\left(R_i^{\text{Д}}\right)$.

Ці показники для кожного рівня є інтегральними, тобто визначаються послідовною згорткою часткових для нього показників нижнього рівня. Але по відношенню до показників верхнього рівня він сам буде частковим. Так, показники верхнього рівня визначаються послідовною згорткою часткових для нього показників нижнього рівня з використанням математичного апарату нечітких множин. Комплексний показник першого рівня визначається наступним чином:

$$R_i^{\text{ЗІ}} = R_i^{\text{К}} \cap R_i^{\text{Ц}} \cap R_i^{\text{Д}}, \tag{1}$$

де $\cap$ і $\cup$ – знаки логічних операцій "І" та "АБО", відповідно.

Для другого рівня використовуються такі вирази:

$$R_i^{\text{К}} = R_i^{\text{ДК}} \cap R_i^{\text{АК}} \cap R_i^{\text{ПВ}} \cap R_i^{\text{ПК}} R_i^{\text{КО}} \text{ та /або}$$
$$R_i^{\text{ДК(АК,ПВ,ПК,КО)}} = \bigcap_{i=1}^{N} \left(R_i^{\text{ДК(АК,ПВ,ПК,КО)}} \right); \tag{2}$$

де $R_i^{\text{ДК}}$ – показники рівня довірчої конфіденційності інформації; $R_i^{\text{АК}}$ – показник

адміністративної конфіденційності; $R_i^{\text{ПВ}}$ – показник повторного використання; $R_i^{\text{ПК}}$ – показник прихованих каналів; $R_i^{\text{КО}}$ – показник конфіденційності при обміні.

$$R_i^{\text{Ц}} = R_i^{\text{ДЦ}} \bigcap R_i^{\text{АЦ}} \bigcap R_i^{\text{В}} \bigcap R_i^{\text{ЦО}} \text{ та /або}$$
$$R_i^{\text{ДЦ(АЦ,В,ЦО)}} = \bigcap_{i=1}^{N} \left(R_i^{\text{ДЦ(АЦ,В,ЦО)}} \right); \quad (3)$$

де $R_i^{\text{ДЦ}}$ – показник довірчої цілісності; $R_i^{\text{АЦ}}$ – показник адміністративної цілісності; $R_i^{\text{В}}$ – показник відкату; $R_i^{\text{ЦО}}$ – показник цілісності при обміні.

$$R_i^{\text{Д}} = R_i^{\text{ВР}} \bigcap R_i^{\text{СВ}} \bigcap R_i^{\text{ГЗ}} \bigcap R_i^{\text{ВЗ}} \text{ та /або}$$
$$R_i^{\text{ВР(СВ,ІЗ,ВЗ)}} = \bigcap_{i=1}^{N} \left(R_i^{\text{ВР(СВ,ГЗ,ВЗ)}} \right). \quad (4)$$

де $R_i^{\text{ВР}}$ – показник використання ресурсів; $R_i^{\text{СВ}}$ – показник стійкості до відмов; $R_i^{\text{ГЗ}}$ – показник гарячої заміни; $R_i^{\text{ВЗ}}$ – показник відновлення після збоїв.

Знак $\bigcap$ може бути не тільки "І", як і знак $\bigcup$ – не тільки "АБО". Семантичний відтінок операцій може змінюватися від "І" до "АБО" та навпаки, що породжує семантичний спектр відповідних оцінок.

Процедура згортки у кожному випадку здійснюється за різними правилами: від простого арифметичного сумування до використання методів нечіткої логіки за допомогою ТНМ. В останньому випадку визначення інтегральних оцінок виконується на основі відповідних нечітких логічних операцій.

Таким чином, на основі викладеного підходу створена чітка ієрархічна сукупність показників, яка характеризує рівень захищеності інформації СУІБ на ОКІ. Вона складається з ряду окремих показників (простих і узагальнених) різного рівня (елемент, система) та інтегрального загального показника – рівня захищеності інформації СУІБ. Ця сукупність показників спільно з КМ ПО (загальною та частковими) є основою методики оцінки СУІБ. Під методикою оцінки СУІБ розуміється комплекс організаційних заходів і методів, програмних засобів, побудованих на єдиній теоретичній та інструментальній основі, які забезпечують комплексне вирішення питань організації та проведення такої оцінки, адекватної обробки, аналізу та видачі результатів.

Методика оцінки СУІБ, що пропонується, спрямована на вирішення двох взаємопов'язаних завдань. Перше (основне) – оцінки потенційного рівня захищеності інформації СУІБ на ОКІ взагалі та її складових зокрема. Методика та ММ оцінки СУІБ розроблені на основі ієрархічної сукупності показників захищеності, принципах побудови ММ оцінки рівня захищеності СУІБ, визначенні інтегральних показників на основі часткових. У той же час методика, що пропонується, використовує як окремі елементи положення всіх раніше відомих підходів та сумісна з ними.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ю. А. Тарнавський. Технології захисту інформації [Електронний ресурс]: підручник. – КПІ ім. Ігоря Сікорського. 2018. – 162 с.

2. Бараннік В. В. Наукоємні технології в інфокумунікаціях: обробка, захист та передача інформації: монографія / під загальною редакцією В. М. Безрука, В. В. Барапніка. – Х.: ФОП Бровін О. В., 2018. – 328 с.

3. Голев Д. В., Кононович В. Г., Хомич С. В. Методики оцінки інформаційної захищеності телекомунікацій: навч. посіб. – Одеса: ОНАЗ ім. О. С. Попова, 2018. – 236 с.

д.т.н., професор Толюпа С. В. (КНУ ім. Тараса Шевченка)
Шевченко А. М. (КНУ ім. Тараса Шевченка)

УПРАВЛІННЯ АДАПТАЦІЄЮ ДЛЯ ЗМІНИ ПАРАМЕТРІВ І РЕЖИМІВ РОБОТИ ЗАСОБІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ ТЕОРІЇ ІГОР

Традиційні ймовірнісні методи, що використовуються при моделюванні кібернетичного впливу (КВ) на інформаційні системи у чистому вигляді не дозволяють описати сценарії ініціювання КВ, тому до існуючих імовірнісних моделей розвитку КВ має бути включений апарат теорії ігор, що дозволяє враховувати раціональний характер поведінки зловмисників, та проводити оцінки ймовірності здійснення різних сценаріїв кібератак [1].

Процес управління в ігрових системах завжди носить дискретний характер, так як кожна гра представляє собою послідовність окремих ходів. Процес, що управляється ігровою системою, може бути направлений або проти організовано діючого супротивника, або проти випадкового процесу. В першому випадку має місце „боротьба" двох або більшої кількості алгоритмів. В другому випадку має місце „боротьба" алгоритмів з випадковими збурюючими факторами [2].

В обох випадках можна чітко виділити сторони, що приймають участь у грі. Зазвичай в літературі розглядаються ігрові системи з двома діючими сторонами: А та Б. Сторона А – процеси або об'єкти, що управляються даною ігровою системою. Сторона Б – протидіюча система, дії якої підкоряються певному алгоритму, або ж випадкові збурюючі фактори.

Ігрові системи управління по своєму призначенню повинні зберігати працездатність та ефективність для широкого діапазону (множини) можливих дій Б сторони (в загальному випадку – всіх супротивних сторін). За цією ознакою ігрові системи управління відносяться до систем з мінімальною необхідною апріорною інформацією про Б сторону.

Повна апріорна інформація про Б сторону потрібна була б в тому випадку, якщо б ігрова система здатна була функціонувати тільки при суворо визначених діях Б сторони, що, очевидно, повністю знецінює застосування ігрової системи.

Особливістю інформаційного конфлікту підсистеми оперативного управління інформаційною безпекою і системи, яка їй протидіє є те, що протидіючі сторони, які мають декілька способів дій, можуть застосовувати їх багаторазово, вибираючи найкращий спосіб з урахуванням інформації про дії протилежної сторони [3].

Для характеристики поточного стану конфлікту будемо використовувати показник захищеності інформаційної системи $a_{ij} = P_{\text{пом}}$ при реалізації в ній i-ї, $i \in I = \{1, 2, \ldots n\}$, стратегії (способу) захищеності й застосуванні j-ї, $j \in J = \{1, 2, \ldots m\}$, стратегії (способу) створення кібервпливу, m і n – кількість стратегій захищеності і створення кібервпливу, реалізованих у системі інформаційної безпеки (СІБ) і в системі, яка їй протидіє (ПС), відповідно.

Стороною А назвемо підсистему оперативного управління СІБ, стороною В – ПС, а величину a_{ij} – виграшем сторони А (програшем сторони В) у ситуації (i, j). При традиційному ігровому підході до аналізу захищеності СІБ передбачається, що сторонам відома матриця гри і скінченна множина стратегій супротивника, але невідомо, яка стратегія реалізується в конкретній ситуації. У цьому випадку в матричній грі формалізується ситуація вибору стратегій захисту в умовах невизначеності. Однак такий підхід не відображує динаміку конфлікту, а також можливість цілеспрямованого вибору стратегій захисту на кожному кроці залежно від інформації про дії ПС. Тому пропонується для опису розглянутого конфлікту використати модель крокової матричної гри із запізнюванням і помилками в інформованості сторін про дії супротивника (матрично-ігрового процесу).

Сутність ігрового алгоритму управління полягає в порівнянні великої кількості можливих даних в умовах якісно різних рішень, визначенні оптимального або найкращого з урахуванням всіх обмежень рішення та формування відповідної команди.

Постановка завдання. Задано: матриця гри $\mathbf{A} = (a_{ij})_m^n$, множини чистих стратегій сторін А і В, для яких існує рішення в змішаних стратегіях (P^*, Q^*, v), а також ймовірнісно-часові характеристики протидіючої системи. Стратегіями СІБ є параметри і режими роботи засобів засобів захисту інформації, стратегіями протидіючої системи – різні види кібервпливу та способи несанкціонованого зйому інформації.

Необхідно: визначити оптимальну змішану стратегію СІБ і необхідні ймовірнісно-часові параметри сторони А, що гарантують максимальний або заданий рівень її середнього виграшу за час $T >> T_{\text{СІБ}}$.

Обмеження: СІБ і протидіюча система мають в своєму розпорядженні скінчену кількість стратегій; свої стратегії сторони (А і В) використовують незалежно один від одного, тобто кожна зі сторін не має на початку гри інформації про дію, що здійснюється іншою стороною; системі інформаційної безпеки відомий час $\Delta t_{\text{оц}}$, за який протидіюча система зможе оцінити обстановку, прийняти рішення і змінити свої робочі параметри.

Задача параметричної оптимізації алгоритмів функціонування СІБ полягає у визначенні такої оптимальної стратегії $a^* \in A^*$, при якій забезпечується максимальна ефективність функціонування системи інформаційної безпеки протягом необхідного часу функціонування.

Одним з можливих рішень ігор у змішаних стратегіях є збільшення швидкості реакції (зниження часу адаптації) однієї зі сторін, що дозволяє підвищити результативність використання стратегій.

З врахуванням трьох етапів циклу управління (контроль, ідентифікація й регулювання) визначимо критерії оптимізації $k_{\text{а}}$ СІБ, що бере участь у формуванні елементів ігрової матриці, на кожному етапі. Скороченню часу контролю буде сприяти зменшення кількості елементів вектора інформаційних параметрів h, що використовуються в трьохетапній ідентифікації та не впливають на якість контролю, а також зниження частоти сканування параметрів, які змінюються повільно

$$n(h_n) \to \min, \quad m(h_m^I) \to \min.$$

Час ідентифікації, що включає розрахунок елементів і рішення матричної гри, можна скоротити за рахунок реалізації принципу прогнозування і визначення обмеженої кількості найбільш імовірних стратегій протидіючої системи, завдяки чому розмірність ігрової матриці зменшується. Відповідно зменшується і кількість елементарних обчислювальних операцій: від $\left|S_{ij}\right|_{I\times J}$ до скороченого $\left|S_{ij}\right|_{I\times K}$, при K = 1, 2, 3.

Крім того, частина часу ідентифікації може поєднуватися з контролем і регулюванням параметрів. У цьому випадку етап регулювання для заздалегідь спрогнозованої стратегії ПС може починатися при наявності перших даних контролю про зміну стратегії протидіючою системою.

Таким чином, теорія ігор дозволяє запропонувати рекомендації по формуванню стратегії управління режимами. Причому, принаймні, для певних типів конфліктів і матриць виграшів ці рекомендації дозволяють системі інформаційної безпеки отримати виграш і досягнути поліпшення своїх технічних характеристик.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорії диференціальних ігор та диференціальних перетворень / Р. В. Грищук. – Монографія. – Житомир. – 2010. – 280 с.

2. Толюпа С. В. Системи виявлення вторгнень та функціональна стійкість розподілених інформаційних систем до кібернетичних загроз / Н. В. Лукова-Чуйко, С.В. Толюпа, В. С. Наконечний, М. М. Браіловський: монографія. – К.: Формат, 2021. – 407 с.

3. Toliupa S., Babenko T., Trush A. The building of a security strategy based on the model of game management. In 2017 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2017 - Proceedings (pp. 57–60).

Фесьоха Н. О. (ВІТІ ім. Героїв Крут)
доктор філософії Фесьоха В. В. (ВІТІ ім. Героїв Крут)

РЕГУЛЯРИЗАЦІЯ ОЗНАКОВОГО ПРОСТОРУ БІОМЕТРИЧНОЇ МОДЕЛІ КЛАВІАТУРНОГО ПОЧЕРКУ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ ФАКТОРНОГО АНАЛІЗУ

В умовах сьогодення критична інформація є стратегічним національним ресурсом. Однак водночас зростає й потенційна вразливість суспільних процесів від інформаційного впливу, особливо в процесах, які стосуються критичної інфраструктури. Тому ефективне забезпечення конфіденційності, доступності та цілісності інформації в таких інформаційних системах (ІС) потребує особливої уваги, оскільки її розголошення може призвести до небезпечних, дестабілізуючих, деструктивних наслідків, які шкодять інтересам держави.

У руслі сказаного особливе місце посідає питання несанкціонованого доступу до інформаційних ресурсів ІС критичної інфраструктури. У переважній більшості випадків дане питання вирішується шляхом удосконалення процедури автентифікації користувача ІС, оскільки саме на даному етапі встановлюється відповідність пред'явленого ідентифікатора користувачу системи.

Аналіз останніх публікації в даній предметній області показав, що найбільш актуальними методами автентифікації є такі, в основу яких покладено поведінкову біометрію клавіатурного почерку (КП) користувачів ІС. Це пов'язано з тим, що КП користувача має певну (унікальну) стабільність, що дозволяє з прийнятною вірогідністю визначати його легітимність у відповідності до пред'явленого ідентифікатора. Поряд з цим, у процесі удосконалення процедури автентифікації користувачів ІС на відміну від завдання вибору науково-методичного апарату для подальшої побудови класифікатора недостатньо уваги приділяється формалізації індивідуальних (унікальних) характеристик користувачів, що негативно впливає на адекватність їх біометричних моделей (профілів) КП, і як наслідок тягне за собою зниження показників точності і достовірності процедури автентифікації.

Серед існуючих способів синтезу біометричної моделі (профілю) користувачів ІС доцільно виділити спосіб, що ґрунтується на синтезі множини досліджуваних ознак КП користувачів ІС у спільний ознаковий простір, однак його застосування потребує вирішення завдання нелінійної сепарабельності ознакового простору КП у рамках задачі класифікації (розпізнавання) користувачів ІС, яке виникає як наслідок досить близьких значень для різних користувачів.

З метою вирішення даного завдання у доповіді запропоновано підхід до реінжинірингу ознакового простору біометричної моделі КП користувачів ІС шляхом його регуляризації (додавання нових даних до умови з метою вирішення некоректно поставленого завдання). Регуляризацію ознакового простору пропонується здійснювати на основі факторного аналізу (система підходів до вивчення взаємозв'язків між значеннями змінних на багатовимірному просторі ознак), оскільки використання саме такого підходу дозволяє на множині існуючих ознак КП визначити приховані неочевидні корисні на практиці взаємозв'язки, які достатньо повно описують їх відмінність. Як правило, після визначення таких прихованих фактів формується новий зменшений простір ознак, який описує мінливість початкового ознакового простору. Проте, такий підхід не є ефективним для малочисельного простору ознак, до класу яких відноситься множина параметрів КП. Особливістю запропонованого підходу до регуляризації ознакового простору КП, що відрізняє його від існуючих є процес збільшення розмірності початкового ознакового простору біометричної моделі КП користувача ІС на основі визначених прихованих фактів, що дозволяє підвищити ефективність процедури автентифікації користувачів ІС.

Серед множини методів факторного аналізу особливої уваги заслуговує метод головних компонент (principal component analysis, PCA), оскільки він забезпечує можливість виокремлення з усього спектру досліджуваних ознак КП лише ті, які з них є найбільш

інформативними (мінливими у часі). Кожна згенерована нова ознака представляється додатковим виміром на ознаковому просторі біометричної моделі КП користувачів ІС. На рисунку 1 представлено узагальнена схема результату регуляризації 2-х вимірного ознакового простору засобами методу головних компонент.

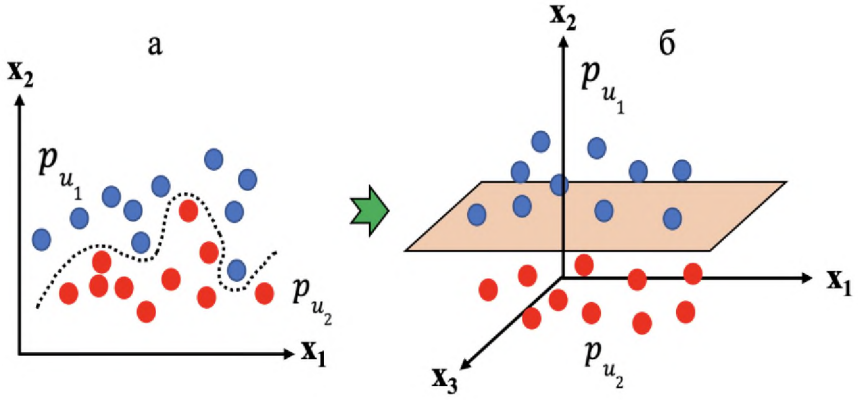

Рис. 1. Узагальнена схема результату регуляризації 2-х вимірного ознакового простору засобами методу PCA

Так, до 2-х вимірного ознакового простору (x_1, x_2) профілів користувачів (p_{u1}, p_{u2}) додається виявлений прихований фактор (и), який описує найбільшу їх мінливість у вигляді нової ознаки (x_3). Внаслідок чого стає можливим знайти таку гіперплощину на 3-х вимірному ознаковому просторі, яка розділить вектори статистичних значень користувачів лінійно, що у свою чергу вирішує зазначене вище завдання нелінійної сепарабельності ознакового простору.

Таким чином, застосування запропонованого у доповіді підходу до регуляризації ознакового простору біометричної моделі КП підвищити показники точності та достовірності процедури автентифікації системами контролю і розмежування доступу. Додатковим результатом застосування даного підходу є забезпечення можливості виявлення факту субституції уже авторизованого користувача ІС за іншим наявним ідентифікатором у системі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про національну безпеку України» (Відомості Верховної Ради (ВВР), 2018, № 31, ст. 241).

2. Фесьоха В. В. Аналіз існуючих рішень автентифікації користувачів інформаційних систем та мереж спеціального призначення / В. В. Фесьоха, Н. О. Фесьоха, О. Д. Доброштан // Збірник наукових праць ВІТІ. – 2020. – № 3. – С. 129–136.

3. Фесьоха В. В., Фесьоха Н. О. Модель нечіткої автентифікації користувачів інформаційних систем органів військового управління на основі поведінкової біометрі. *Захист інформації*. 2021. Т. 23, № 2. С. 116–123.

4. Zero-day polymorphic cyberattacks detection using fuzzy inference system / V. V. Fesokha et al. *Austrian Journal of Technical and Natural Sciences*. 2020.

5. Алексеев В. А., Маслий Д. В., Горелов Д. Ю. Сравнительный анализ перспективных технологий аутентификации пользователей ПК по клавиатурному почерку. *Радиотехника*. 2017. № 189. С. 195–201/

6. Krutohvostov D., Khitsenko V. Password Authentication and Continuous Authentication by Keystroke Dynamics Using Mathematical Statistics. *Voprosy kiberbezopasnosti*. 2017. No. 5(24). P. 91–99.

7. Kaplina A., Loboda O. Principal component analysis for weighted data in the procedure of multidimensional statistical forecasting. *Efektyvna ekonomika*. 2021. № 11.

к.т.н. Хусаінов П. В. (ВІТІ ім. Героїв Крут)

АСПЕКТИ ПРИЙНЯТТЯ РІШЕНЬ ПРИ РЕАЛІЗАЦІЇ ІНЖЕНЕРНО-ТЕХНІЧНИХ ЗАХОДІВ КІБЕРЗАХИСТУ

Інженерно-технічні заходи кіберзахисту спрямовані на забезпечення всіх етапів життєвого циклу програмно-апаратних систем (підсистем) для запобігання кіберінцидентам, виявлення та захисту від кібератак, ліквідації наслідків кіберінцидентів (кібератак), відновлення сталості і надійності функціонування об'єкта кіберзахисту.

Запобігання кіберінцидентам (кібератакам) полягає у мінімізації ризиків інформаційної безпеки внаслідок ймовірного порушення конфіденційності, цілісності, доступності, несанкціонованого доступу до інформаційних ресурсів, у тому числі, штатного режиму функціонування об'єкта кіберзахисту. Нагадаємо основні підходи до запобігання кіберінцидентів (кібератак), які утворюють методичний базис програмно-апаратних систем (підсистем) відповідного цільового призначення:

автентифікація та авторизація користувачів;
розмежування доступу до інформації, логічних об'єктів та апаратних засобів;
автентифікація інформації та обчислювальних процесів;
мережне екранування;
криптографічний захист каналів обміну інформацією;
інвентаризація та реконфігурація налаштувань апаратних засобів;
оновлення та реконфігурація програмних засобів;
антівірусний захист;
виявлення кібератак;
реєстрації подій функціонування операційних систем та мережного трафіку;
контроль цілісності та резервне зберігання інформації;
резервування засобів та розподіл навантаження між ними;
пошук вразливостей.

Виявлення та захист від кібератак, ліквідація наслідків кіберінцидентів (кібератак) уособлює оперативне (кризове) реагування на них (у тому числі, відновлення сталості і надійності функціонування об'єкта кіберзахисту) розглядається у контексті організаційно-технічної моделі кіберзахисту. Програмно-апаратні системи (підсистеми) технологічної інфраструктури організаційно-технічної моделі кіберзахисту призначені для забезпечення основних напрямів діяльність команд реагування на комп'ютерні надзвичайні події:

оцінка та аналіз кіберінцидентів (кібератак);
виявлення кіберінцидентів (кібератак);
управління та координація ліквідацією наслідків кіберінцидентів (кібератак);
інформування про кіберінциденти (кібератаки).

Сукупність практичних задач зі створення та організації експлуатації програмно-апаратної системи (підсистеми) кіберзахисту у широкому сенсі відносяться до таких класів задач прийняття технічних рішень:

аналіз та синтез структури (організаційної, інформаційної, морфологічної і т. ін.);
вибір складу засобів (апаратних, програмних, програмно-апаратних);
регламент та технічне обслуговування засобів;
технічне діагностування, забезпечення надійності та живучості системи (засобів);
інформаційна підтримка оперативного (кризового) реагування.

Виходячи з викладеного, до розгляду пропонується наукова програма (дорожня карта) розвитку методичних аспектів прийняття технічних рішень при створенні та організації програмно-апаратних систем (підсистем) кіберзахисту. Основою постановки задач такого класу є формальний опис множини альтернативних рішень та критеріїв оптимального вибору одного з них. Результат обґрунтування принципу оптимальності може мати форму як строгої максимізації (мінімізації) значення критерію, так і оперування векторним представленням багатьох критеріїв (багатокритеріальна задача).

д.т.н. Чевардін В. Є. (ВІТІ ім. Героїв Крут)
Марчук О. В. (ВІТІ ім. Героїв Крут)
Лаврик І. В. (ВІТІ ім. Героїв Крут)
Бродовський А. П. (ВІТІ ім. Героїв Крут)

ТЕХНІКИ ТА ПІДХОДИ ДО ПРОВЕДЕННЯ КІБЕРЗМАГАНЬ НА ОСНОВІ СУЧАСНИХ КІБЕРПОЛІГОНІВ

Проведення кібернавчань є потужним інструментом тренування навичок фахівців та команд з кіберзахисту, відпрацювання спільних заходів щодо пом'якшення наслідків, виявлення та реагування на часті кібератаки, які ініціюватимуться проти їхніх об'єктів ІТ-інфраструктури.

Сутність кібернавчань полягає в підготовці та реалізації заходів щодо кіберзахисту від активних дій команди (команд) зловмисників, які мають назву Червоні. Декілька Синіх команд беруть участь у навчанні та змагаються між собою, щодо швидкості, ефективності прийнятих заходів, щодо відбиття атак Червоних. Кожна Синя команда намагається захистити свою ІТ-інфраструктуру від атак, здійснених у реальних умовах Червоними і перевірити свої можливості під тиском безперервного потоку атак які сформовані за реалістичними сценаріями.

Участь у цьому заході надає нагоду для перевірки та розвитку своїх навичок з реагування в умовах реальних кібератак за допомогою Ідентифікації, Захисту, Виявлення, Реагування, Відновлення та Звітності.

Для проведення кіберзмагань (кібернавчань), як правило застосовується одна з трьох форм проведення змагань.

Форма 1. Передбачає проведення змагань у вигляді виконання переліку завдань, які розташовані за зростанням їх складності. Кожен учасник або команда-учасниця виконуючі завдання з пошуку артефактів у відповідних віртуальних середовищах або в інших умовах відповідно до завдання при позитивному розв'язанні завдання, отримує флаг, який має еквівалент в заохочувальних балах. Таким чином, за певний час проведення змагання учасники розташовуються в турнірній таблиці відповідно до отриманої кількості балів, що і визначає переможців змагання.

Форма 2. Завдання сформовані з моделюванням реальних середовищ, які містять в собі певні уразливості. Наявні уразливості за певним розкладом у певний час експлуатуються з застосуванням відповідних сценаріїв їх експлуатації в автоматичному режимі, який здійснюється у відповідності з налаштуваннями та задуму змагання. Учасники або команди-учасники повинні своєчасно реагувати на дії в кіберпросторі та здійснювати фіксацію і відповідне звітування щодо подій, які відбулися. За це учасники отримують в автоматичному режимі заохочувальні бали. За певний час проведення змагання учасники розташовуються в турнірній таблиці відповідно до отриманої кількості балів, що і визначає переможців змагання.

Форма 3. Для проведення цієї форми змагання формуються реальне віртуальне середовище з емулюванням всіх послуг, сервісів, засобів та систем, які містять в собі певні уразливості, дозволяють змінювати параметри середовищ за рішенням користувачів. Користувачі кіберсередовища поділяються умовно на суспільство, команди кіберзахисту та хакерську спільноту. Всі дії в кіберпросторі можуть здійснюватись з автоматичними налаштуваннями та відповідно до задуму змагання, так і можливі будь-які варіації та альтернативні дії хакерської спільноти та команд кіберзахисту. Команди кіберзахисту повинні своєчасно реагувати на дії в кіберпросторі та здійснювати фіксацію і відповідне звітування щодо подій, мати або будувати та впроваджувати стратегію кіберзахисту, налаштовувати та робити все для утримання працездатності відповідних сегментів та елементів кіберпростору, який мають в своєму розпорядженні. За це учасники отримують в автоматичному та ручному режимі заохочувальні бали. За певний час проведення змагання

учасники розташовуються в турнірній таблиці відповідно до отриманої кількості балів, що і визначає переможців змагання. Спираючись на існуючі результати багатьох кіберзмагань, звіти щодо проведення кіберзмагань (навчань) розглянемо ключові можливі методики дій кожної групи учасників кіберзмагання, включаючи як гравців так і організаторів.

Червоні. Ключова роль червоної команди (Red Team) полягає у проведенні багатоетапних атак на інфраструктуру згідно затвердженого плану змагань. Під час проведення навчань команди червоних проводять атаки, які мають місце в реальному житті. Для їх проведення використовуються у тому числі утиліти операційної системи Kali Linux. Команда червоних застосовує техніки та процедури APT-атак відповідно до підручника для червоних команд та виконує завдання відповідно пунктів плану згідно сценарія навчань.

Сині. Ключова роль команд синіх (Blue Team) полягає у виконанні розробленої стратегії захисту IT інфраструктури, а також оперативному реагуванні на інциденти та мінімізації наслідків від них.

Зелені. Ключова роль команди зелених (Green Team) полягає у розгортанні, масштабуванні та підтримці всієї інфраструктури для проведення змагань.

Білі. Ключова роль команди білих (White Team) полягає у високорівневому управлінні проведенням змаганнь, координацією та оцінюванням роботи інших команд.

В ході проведеної роботи були враховані відомі результати щодо порівняння відомих платформ для проведення кіберзмагань та навчань з кібербезпеки, таких як Crossed Swords (CCDCOE, 2019), Locked Shields (CCDCOE, 2019), SteadFast Cobalt (NCI Agency, 2019) та інші. В якості тестового кіберполігону для проведення апробації методик дій відповідних команд під час підготовки та проведення змагань (навчань) було використано кіберполігон Cybexer Technologies, що задовольняє вимогам сьогодення та дозволяє створювати та розробляти різноманітні сценарії проведення кіберзмагань (навчань) на національному та міжнародному рівні.

Але при цьому слід зазначити, що практично для всіх платформ, які були розглянуті під час досліджень, існує істотне обмеження на зміну параметрів середовища, яке було розроблено для проведення кіберзмагання, що не дозволяє синім командам у разі змінювати архітектуру мережі. Гравці не можуть змінювати програмно-апаратні фаєрволи, комутатори та маршрутизатори, які є інфраструктурними, при цьому які використовуються для моніторингу мережі, фільтрації трафіку та інших задач синіми командами. Цей недолік пов'язаний зі складністю реалізації такої можливості, його усунення потребує суттєвого збільшення вартості та складності програмно-апаратної платформи кіберполігону.

В рамках проведеної роботи були отримані відповідні методики, які дозволяють здійснювати моделювання справжньої глобальної мережі, реалізовувати виконання дій командами, що атакують (червоні), що захищають інфраструктуру (сині), що формують задум та розробляють сценарії розвитку подій в кібергрі (білі), що готують: налаштовують, інсталюють та підтримують кіберполігон (зелені), що моделюють штатні дії в кіберпросторі (жовті). Запропоновані методики були опрацьовані під час проведення кіберзмагань з курсантами та офіцерами інституту, а також в рамках підготовки до міжнародних навчань, таких як Defence Cyber Marvel та Locked Shields. В роботі наведені категорії оцінок, що отримують гравці та середовище для кібергри, що дозволяє ефективно контролювати, керувати процесом гри та формувати результати змагань і робити рекомендації для гравців.

В результаті проведених досліджень отримано бачення та підходи до планування, підготовки, моделювання та підтримки платформи для реалізації кіберцидентів, реагування на кіберінциденти на міжрегіональному, національному та міжнародному рівні.

В подальшій роботі планується розробити методику інтегральної оцінки результатів дій синіх команд, що надасть змогу більш ефективно планувати стратегії дій синім командам а також застосувати штучний інтелект для планування та виконання дій командами червоних.

Шиповський В. В. (НУОУ)

ЗАСТОСУВАННЯ МОДЕЛІ OODA LOOP ДЛЯ АНАЛІЗУ КІБЕРЗАГРОЗ ТА ЇХ ВПЛИВУ НА ІНФОРМАЦІЙНІ СИСТЕМИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У сучасному світі інформаційні технології відіграють важливу роль у функціонуванні критичної інфраструктури та повинні мати належний рівень захисту. Одним із підходів до розв'язання проблеми кібербезпеки є використання моделі OODA loop, яка дозволяє протидіяти кіберзагрозам шляхом збору інформації, її аналізу, прийняття рішення та відповідних дій.

Модель OODA loop (рис. 1) – це підхід до прийняття рішень та дій у ситуаціях, коли необхідно швидко реагувати на змінні обставини. Модель складається з чотирьох етапів: спостереження, оцінка, прийняття рішення та дія.

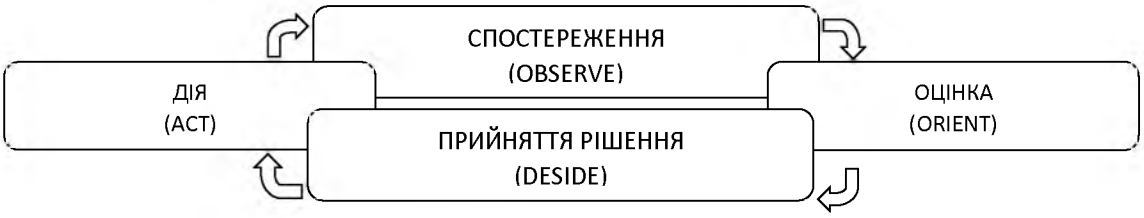

Рис. 1. Модель OODA loop

Перший етап – *спостереження* – передбачає збір інформації про оточуюче середовище та інші важливі параметри.

Другий етап – *оцінка* – передбачає аналіз інформації, отриманої на першому етапі.

Третій етап – *прийняття рішення* – полягає в виборі оптимального варіанту дій на основі оцінки, проведеної на попередньому етапі.

Четвертий етап – *дія* – полягає в реалізації вибраного варіанту дій на практиці.

Для оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури складові моделі можемо застосувати наступним чином наступним чином:

Спостереження: Збір інформації про наявність потенційних кіберзагроз та існуючі кіберзаходи, які застосовуються для захисту інформаційної системи об'єкта критичної інфраструктури.

Оцінка: Аналіз потенційних загроз та існуючих захисних заходів, що дозволяє визначити пріоритетність потенційних загроз та наслідків, які вплинули на роботу системи SCADA (аббр. від англ. Supervisory Control And Data Acquisition – диспетчерське управління і збір даних) об'єкта критичної інфраструктури.

Прийняття рішення: Вибір оптимального варіанту захисних заходів та стратегії захисту, що відповідає виявленим загрозам та можливостям захисту об'єкта критичної інфраструктури.

Дія: Реалізація заходів та стратегій захисту, здійснення моніторингу та аналізу інформації для виявлення нових кіберзагроз, оцінювання ефективності застосовуваних заходів та максимальне відновлення роботи ураженого об'єкта критичної інфраструктури.

Таким чином, застосування моделі OODA loop для оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури дозволяє ефективно реагувати на змінюваність ситуації та вчасно приймати відповідні рішення для захисту інформаційних систем.

Отже, модель OODA loop є корисним інструментом для оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури. Використання цієї моделі дозволяє збирати та аналізувати інформацію про потенційні кіберзагрози, що дозволить вчасно виявляти проблеми та приймати відповідні заходи для їх запобігання.

к.т.н. Штаненко С. С. (ВІТІ ім. Героїв Крут)

ПРОГРАМОВАНА ЛОГІКА ЯК СПОСІБ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ СУЧАСНИХ УПРАВЛЯЮЧИХ СИСТЕМ ВІД АПАРАТНИХ ЗАКЛАДОК

Сучасні управляючі системи різного призначення (автоматизовані системи управління – АСУ, автоматизовані системи управління технологічними процесами – АСУ ТП, автоматизовані системи управління військами – АСУВ тощо) відносяться до об'єктів критичної інформаційної інфраструктури. При цьому данні об'єкти в якості основних елементів містять засоби обчислювальної техніки – процесори, блоки пам'яті, перетворювачі, датчики, вимірювальні та виконавчі пристрої, елементною базою яких є інтегральні схеми.

Відповідно до класифікації [1] інтегральні схеми (ІС) поділяються на цифрові, аналогові та аналогово-цифрові. У свою чергу, цифрові ІС поділяються на стандартні та спеціалізовані. Стандартні ІС мають практично жорстку внутрішню структуру, без впливу на характер їх функціонування. Спеціалізовані ІС мають індивідуальний характер функціонування, при цьому доводиться тією чи іншою мірою їх розробляти під конкретне замовлення. У цьому напрямі найважливішим досягненням стало поява програмованих логічних інтегральних схем (ПЛІС).

Слід зазначити, що у зв'язку з глобалізацією і складністю ІС, а також з урахуванням масового використання в різних галузях людської діяльності на перший план виходить проблема надійного та безпечного їх функціонування. А це в свою чергу пов'язано із забезпеченням не лише кіберстійкості цифрових пристроїв та обчислювальних систем, а також із забезпеченням захищеності життєво важливих інтересів людини і громадянина, суспільства та держави. Саме без вирішення цієї проблеми цифрові пристрої та обчислювальні системи не зможуть повноцінно виконувати покладені на них функції, крім цього можуть виступити провідником кібератак на управляючі системи.

Зазначимо, що в останні роки з'явилися нові потенційні загрози безпеці в даній сфері, які базуються на апаратних засобах, – так звані апаратні закладки або апаратні трояни, які є навмисною зловмисною модифікацією електричної схеми або її конструкцією, що призводить до неправильного функціонування цифрових пристроїв та обчислювальної системи. Подібно до програмної закладки (програмного трояну), апаратна закладка представляє собою свого роду чорний вхід в цифровий пристрій. При цьому апаратний троян має додаткову перевагу – він постійно присутній на найнижчому рівні обробки інформації, що веде до збереження загроз відмови або відхилення від нормального функціонування ІС протягом усього часу використання цифрового пристрою або обчислювальної системи. Апаратна закладка може тривалий час залишатися бездіяльною та активуватися самостійно або за допомогою програмного забезпечення, у яке навмисно закладена така можливість.

Апаратні закладки є відносно новими загрозами для кібербезпеки, при цьому вони суттєво розширюють можливості для атаки на технологічні системи. Раніше атаки обмежувалися лише програмними засобами, зосереджуючись на слабких місцях програмного забезпечення. При цьому засоби захисту конкретного програмного забезпечення розроблялися виходячи з автентичності апаратного забезпечення, тому загальноприйняті підходи до захисту програмними засобами не здатні забезпечити безпеку від апаратних троянів. З цього погляду апаратні закладки є досить складною проблемою забезпечення безпеки сучасних управляючих систем.

Виходячи з сказаного одним із підходів до надійного та безпечного функціонування сучасних управляючих систем, здатних протистояти шкідливим атакам, є застосування в якості елементної бази інтегральних схем з програмованою структурою, тобто ПЛІС.

Програмовані логічні інтегральні схеми є матрицею програмованих логічних елементів з *SPLD* (*Simple Programmable Logic Devices*), *CPLD* (*Complex Programmable Logic Device*), *FPGA* (*Field-Programmable Gate Array*), *FLEX* (*Flexible Logic Element Matrix*) структурами.

За рахунок цих структур створюється новий клас розвитку мікроелектроніки – універсальні системи на кристалі (*System-on-Chip – SoC*).

Система на кристалі або *SoC* представляє собою обчислювальну систему, реалізовану в інтегральному виконанні, до складу якої входить високопродуктивний процесор або декілька процесорів, математичний процесор обробки даних та цифрової обробки сигналів, додаткові модулі пам'яті, набори периферійних пристроїв (контролерів) тощо. Така організація обчислювальної системи набула широкого поширення за допомогою своєї універсальності, малого енергоспоживання і навіть можливості реконфігурації її алгоритмічної структури. Зазначимо, що на сьогодні системи на кристалі витісняють громіздкі обчислювальні структури, реалізовані за допомогою набору інтегральних схем, замінюючи їх сучасними мікроконтролерами (*PIC*, *AVR*, *MSP*430, *STM*-32, *Cortex-M*, *TSP*-32 тощо), програмованими логічними інтегральними схемами (ПЛІС – *CPLD*, *FPGA*, *FLEX*) та одноплатними комп'ютерами типу *Raspberry Pi* [2].

Слід зазначити, що на відміну від стандартних ІС, логіка роботи ПЛІС не визначається при виготовленні, а задається шляхом програмуванням. Для цього використовуються програматор та інтегроване середовище розробки (*IDE – Integrated Development Environment*), що дозволяють задати бажану структуру цифрового пристрою у вигляді принципової електричної схеми або програми спеціальними мовами опису апаратури *Verilog*, *VHDL*, *AHDL*.

Так, згідно з [3; 4] саме застосування ПЛІС у якості елементної бази побудови сучасних управляючих систем відкриває нові можливості щодо підвищенні кіберстійкості цифрових пристроїв та обчислювальних систем до кібератак, як програмного, так і апаратного характеру. В основі даного підходу лежить принцип реалізації активної відмовостійкості, який включає наступні етапи: виявлення відмови (кібератаки) шляхом застосування існуючих методів контролю технічних засобів; локалізація відмови (реагування на кібератаки) шляхом застосування методів тестового та функціонального діагностування; відновлення правильного функціонування системи шляхом реконфігурації її внутрішньої структури на рівні логічних елементів. При цьому зазначимо, що в основу реконфігурації внутрішньої структури цифрових пристроїв та обчислювальних систем покладене положення прескриптивної теорії, яка розглядає питання цілеспрямованого управління об'єктами різної природи, що перебувають у стані «конфлікту» з іншими об'єктами [5].

Таким чином, реалізувавши принцип активної відмовостійкості на сучасній програмованій елементній базі, ми маємо можливість протидіяти не лише кібератакам програмного і апаратного характеру на цифрові пристрої та обчислювальні системи, а й підвищити кіберстійкість управляючих систем загалом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Engr Fahad. Types of Integrated Circuits, Classification of ICs by Structure. URL: https://www.electroniclinic.com/types-of-integrated-circuits-classification-of-ics-by-structure/ (дата звернення 15.03.2023).

2. Saleh, Reyad & Wilton, Steve & Mirabbasi, Shahriar & Hu, Alan & Greenstreet, Mark & Lemieux, Guy & Pande, Partha & Grecu, Cristian & Ivanov, Andre. (2006). System-on-Chip: Reuse and Integration. Proceedings of the IEEE. 94. 1050–1069. 10.1109/JPROC.2006.873611.

3. Штаненко С. С. Самохвалов Ю. Я. Забезпечення кібербезпеки АСУ ТП шляхом застосування ПЛІС технології / С. С. Штаненко, С. В. Толюпа, Ю. Я. Самохвалов. Науковий журнал Київського національного університету імені Тараса Шевченка. Безпека інформаційних систем і технологій № 1, 2021 стр. 44–52. ISSN 2707-1758.

4. Штаненко С. С. Адаптація мікропроцесорних систем управління до несприятливих впливів / С. С. Штаненко, Ю. Я. Самохвалов // Сучасна спеціальна техніка: ДНДІ МВС України. Київ. 2022. № 3 (70). С. 89–100. ISSN: 2411-3816.

5. Обухов В. Е. Синтез избыточных дискретных устройств с реконфигурацией структуры / В. Е. Обухов, В. В. Павлов, Киев: Наукова думка, 1979. 156 с.

Штонда Р. М. (ВІТІ ім. Героїв Крут)
Остапчук В. М. (ВІТІ ім. Героїв Крут)
Радзівілов Г. Д. (ВІТІ ім. Героїв Крут)

ВИКОРИСТАННЯ РІШЕННЯ ENDPOINT DETECTION AND RESPONSE ДЛЯ КІБЕРЗАХИСТУ МОБІЛЬНИХ ПРИСТРОЇВ

У сучасних реаліях, мобільний пристрій (далі – МП), є майже у кожної людини. А отже і кожен МП в тій чи іншій мірі позиціонується в мережі Інтернет. Використання незахищених МП користувачами, призводить до втрати важливої інформації та виникнення кібервпливів на них.

Для вирішення даного питання пропонується розглянути рішення Endpoint Detection and Response (далі –EDR), як запоруку кібербезпеки на МП користувачів. EDR – це рішення, що виявляє, досліджує підозрілу діяльність та забезпечує кібербезпеку, як на хостах, так і на МП, яке в себе включає моніторинг та збір даних про безпеку МП у режимі реального часу за допомогою автоматизованих підходів реагування на кіберзагрози.

За допомогою EDR розгортається місце/пункт для створення сучасних команд кібербезпеки, які відображаються в якості контрольного списку. EDR захищає "цифровий периметр" від кіберзагроз та проблем кібербезпеки кількома ключовими способами.

Комплексний збір даних моніторингу дозволяє EDR скласти повне уявлення про потенційні кібератаки. Постійний моніторинг усіх МП – онлайн та офлайн – полегшує аналіз кібербезпеки та реагування на кібератаки/кіберінциденти. Це дозволяє проводити глибокий аналіз кібербезпеки та надає розуміння, адміністраторам безпеки щодо аномалій та вразливостей, що виникають в мережах для усвідомлення майбутніх кіберзагроз. Виявлення кожної загрози виходить за рамки встановленого антивірусного програмного забезпечення, а отже здатність EDR забезпечувати реакцію в режимі реального часу на широкий спектр кіберзагроз дозволяє адміністраторам безпеки візуалізувати потенційні кібератаки/кіберінциденти, навіть коли вони здійснюють вплив на хости та МП, і все це в режимі реального часу.

Дані можливості дозволяють запобігти втратам інформації, відсікаючи кібератаки на їх початкових стадіях до того, як відбудуться критичні втрати або компроміси. Реагування в режимі реального часу також дозволяє виявити підозрілу або несанкціоновану поведінку в мережі, дізнавшись про першопричину кіберзагрози, перш ніж вона зможе вплинути на роботу.

Також EDR можна інтегруватися з іншими інструментами безпеки, що дозволяє корелювати дані з МП, мережі та SIEM для розвитку більш глибокого розуміння практик та методів, що застосовуються зловмисниками, які намагаються отримати несанкціонований доступ до цифрових активів користувачів.

Рішення EDR можна вважати набором традиційних антивірусних програмних засобів. Антивірусні програмні засоби самостійно обмежені в області застосування в порівнянні з більш новими рішеннями EDR. Таким чином, антивірусні програмні засоби є частиною EDR.

Антивірусні програмні засоби виконують основні функції, такі як сканування, виявлення та видалення вірусів, де EDR виконує безліч інших функцій. Окрім антивірусних програмних засобів, EDR може містити кілька функцій, включаючи моніторинг, білий/чорний список та інші, всі вони призначені для забезпечення більш повного захисту від відомих та нових кіберзагроз.

Оскільки зловмисники вдосконалюють свої атаки та використовують передові технології для отримання доступу до мереж та даних користувачів, простий антивірусний програмний засіб на основі підписів, не в змозі виявити своєчасно загрози "нульового дня" або багатошарового рівня, а от системи EDR можуть виявляти всі типи кіберзагроз в МП, забезпечуючи відповідь у режимі реального часу на ті, які ідентифіковані/виявлені. Тому для забезпечення захисту інформації та кіберзахисту МП рекомендовано використовувати рішення EDR.