МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ФРАНКА
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ITSec-2024

Безпека інформаційних технологій

МАТЕРІАЛИ

XIII Міжнародної науково-технічної конференції

9-11 травня 2024
м. Львів (Україна)

УДК [003.26+004+519.816]:004.056:65(063)

ITSec: Безпека інформаційних технологій: матеріали XIII Міжнар. наук.-техн. конф., м. Львів, 9-11 трав. 2024 р. Л.: ЛНУ ім. І. Франка, 2024, 257 с.

Збірник містить тексти наукових матеріалів доповідей та тез учасників XIII міжнародної науково-технічної конференції «ITSec: Безпека інформаційних технологій». Основною метою конференції є ознайомлення з сучасними досягненнями та висвітлення результатів наукових досліджень з усіх аспектів кібербезпеки та захисту інформації.

Призначено вченим, інженерам, аспірантам наукових спеціальностей 05.13.21 – Системи захисту інформації, 21.05.01 – Інформаційна безпека держави, здобувачам вищої освіти за спеціальностями: 125 – Кібербезпека та захист інформації, а також всім зацікавленим.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

- Львівський національний університет ім. І. Франка
- Національний авіаційний університет
- Rowan University, USA
- Halmstad University, Sweden
- Наукова школа “Кібербезпека” НАУ
- Кафедра безпеки інформаційних технологій НАУ
- Кафедра кібербезпеки ФПМІ ЛНУ ім. І. Франка
- ГО “Асоціація спеціалістів кібербезпеки”

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

Співголови

Володимир МЕЛЬНИК, д.ф.н., проф., ректор Львівського національного університету ім. І. Франка
Володимир ШУЛЬГА, д.і.н., в.о. ректора Національного авіаційного університету

Заступники співголов

Олександр КОРЧЕНКО, д.т.н., проф., в.о. проректора з наукової роботи НАУ, голова ГО АСКД
Роман ГЛАДИШЕВСЬКИЙ, академік НАН України, д.х.н., проф., проректор з наукової роботи ЛНУ
Ірина УДОВИК, к.т.н., проф., декан факультету інформаційних технологій, НТУ «Дніпровська політехніка»
Іван ДИЯК, д.ф.-м.н., проф., декан факультету прикладної математики та інформатики ЛНУ
Євгенія ІВАНЧЕНКО, к.т.н., проф., зав.кафедрою безпеки інформаційних технологій НАУ
Юлія ХОХЛАЧОВА, к.т.н., проф., професор кафедри безпеки інформаційних технологій НАУ
Петро ВЕНГЕРСЬКИЙ, д.ф.-м.н.,доц., в.о. зав. кафедрою кібербезпеки ЛНУ

Відповідальні секретарі

Валерій ТРУШЕВСЬКИЙ, к.ф.-м.н., доцент кафедри кібербезпеки ЛНУ
Михайло ПРИГАРА, к.т.н., доцент кафедри технології машинобудування УжНУ
Ярина КОКОВСЬКА, к.ф.-м.н., доцент кафедри дискретного аналізу та інтелектуальних систем ЛНУ
Наталія КИРИЧЕНКО, асистент кафедри дискретного аналізу та інтелектуальних систем ЛНУ
Микола ЩЕРБИНА, асистент кафедри кібербезпеки ЛНУ
Світлана ЛАЩІВСЬКА, асистент кафедри кібербезпеки ЛНУ
Анастасія ЛАРІОНОВА, асистент кафедри безпеки інформаційних технологій НАУ
Надія ГОРОДИСЬКА, інженер кафедри кібербезпеки ЛНУ

ЗМІСТ

Methodology forchoosing a consensus algorithm forblockchain technology

УДК 004.65:004.75

Tetiana Bazhan[1], Viktoriia Zhebka[2], Serhii Zhebka[3]

State University of Information and Communication Technologies,
tetiana.olexandrivna@gmail.com[1], digitaldut2022@gmail.com[2],
szhebka@hotmail.com[3]

Blockchains are decentralised, meaning that data can be distributed across multiple host servers, which distinguishes them from conventional databases. Decentralisation is the main feature of blockchain.

Since control over data or resources is shared among several nodes simultaneously, it makes it very difficult for an attacker to delete or use resources.

Consensus maintenance is very important because without it, copies of data on different nodes may conflict with each other, leading to inefficient and inconsistent data storage.

A successful consensus algorithm should help a blockchain application achieve its goal. The purpose of the blockchain is to provide a tool for decentralised decision-making. The complex nature of blockchain consensus stems from its original goal of making decisions without a central authority. Therefore, the level of decentralisation of the consensus algorithm is included in the evaluation criteria. A consensus algorithm with a higher level of decentralisation is considered good.

The following energy consumption criteria for choosing a consensus algorithm in blockchain technology should be considered:

1. Proof of Work (PoW): computational complexity (the more difficult the task is for miners, the more energy is consumed); algorithm efficiency (some PoW algorithms may be more energy efficient than others).
2. Proof of Stake (PoS): selective efficiency (the less currency a participant has, the less energy he uses); methods for controlling misuse (it is important to have mechanisms to prevent concentration of power that may affect the effectiveness of PoS)
3. Delegated Proof of Stake (DPoS): chosen legitimacy (some participants may spend more energy to obtain delegate status); flexibility of the voting policy (if the voting system is not efficient, it can lead to an incorrect distribution of power and energy costs).
4. Proof of Burn and other alternatives: spending strategies (determining exactly how currency is spent in the consensus process and how this affects energy costs; innovative approaches (alternative methods such as Proof of Space (PoSpace) or Proof of Time (PoT) may offer lower energy costs).

However, the energy consumption criteria must be balanced with other important aspects, such as security, decentralisation and bandwidth, when choosing a consensus algorithm for blockchain technology.

Here is a comparative description of consensus algorithms for different types of cryptocurrencies (Table 1)

Table 1

Characteristics of consensus algorithms

Crypto-currency	Type	Security	Decentralisation	Energy consumption	Bandwidth
Dash	Hibrid	Medium	Medium	Medium	OK
Peercoin	Hibrid	Medium	Medium	Low	Not So Fast
Verus coin	Hibrid	Medium	Medium	Low	OK
Decred	Hibrid	Hight	Hight	Medium	OK
Stratis	Hibrid	Medium	Medium	Medium	Fast
Bitcoin	PoW	Hight	Hight	Hight	Not So Fast
Conflux	PoW	Hight	Medium	Low	Very Fast
Ethereum Classic	PoW	Medium	Medium	Medium	Fast
Monero	PoW	Hight	Hight	Medium	OK
Dogecoin Litecoin	PoW	Medium	Medium	Medium	OK
Ethereum	PoS	Medium	Hight	Low	Fast
Polygon	PoS	Hight	Medium	Low	Fast
TON coin	PoS	Medium	Medium	Low	Fast
Solana	PoS	Hight	Medium	Hight	Very Fast
Cardano	PoS	Hight	Medium	Low	Fast

For any future work, it would be interesting to have a study on the selection of a consensus algorithm and it is possible to choose a wider list of criteria or reduce it to a minimum. In addition, the blockchain application industry is developing rapidly and new algorithms are being created that can quickly replace the old ones on the market. There is always a need for future research, so it is a necessity to keep up to date with the latest developments in consensus algorithms and blockchain technology.

1. F. Kipchuk, et al., Assessing Approaches of IT Infrastructure Audit, in: IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (2021). doi: 10.1109/ picst54195.2021.9772181.
2. Center for Combating Disinformation, How Ukraine Survived Russia's Winter Terror (2023). URL: https://cpd.gov.ua/ articles/yak-ukrayina-perezhyla-zymovyj-teror-rosiyi/
3. V. Perun, The Russian Federation Launched more than 1,200 Missiles and Drones at Key Energy Facilities of Ukraine, Ukrenergo (2023). URL: https://lb.ua/society/2023/04/08/551391_rf_vipustila_klyuchovih.html
4. UKRAINE. Rapid Damage and Needs Assessment. February 2022 – February 2023; Anne Himmelfarb (Ed.). The World Bank, the Government of Ukraine, the European Union, the United Nations.

Software Vulnerability Detection Using Large Language Models

UDK 004.056.54

Beliaiev Igor[1], Peleshko Dmytro[2]

Ivan Franko National University of Lviv, [1]igor.beliaiev@lnu.edu.ua, [2]dmytro.peleshko@lnu.edu.ua

The complexity of penetration testing has traditionally limited its automation. However, with their advanced capabilities, large language models (LLMs) hold the potential to transform this domain. This research examines the use of LLMs in penetration testing and their ability to identify vulnerabilities.

The advancement of Generative AI (GenAI) models, particularly Large Language Models (LLMs) like ChatGPT and Google Bard, has been a significant milestone in the digital landscape. However, their increasing sophistication necessitates a closer examination of their impact on cybersecurity, given their potential for both defensive and offensive applications. This paper underscores the potential for misuse of GenAI tools by cyber attackers, including automated hacking and strategic attack planning, thereby underscoring the pressing social, ethical, and privacy concerns associated with this technology.

A key application of AI models in this study is PentestGPT. 'Pentest' stands for penetration testing, an authorized simulated cyberattack on a computer system to assess its security and identify vulnerabilities. PentestGPT, based on ChatGPT, seeks to automate parts of the penetration testing process. It operates interactively, providing guidance to testers throughout their tasks, including specific operations. With an extensive dataset of known vulnerabilities, AI can scan new code for similar weaknesses, potentially identifying attack points [1]. These models, capable of identifying vulnerabilities and strategizing attacks, pose significant cybersecurity threats. PentestGPT has shown its efficacy in platforms like Hack The Box and during Capture The Flag (CTF) challenges, which provide a constructive environment for cybersecurity professionals to develop their skills [1].

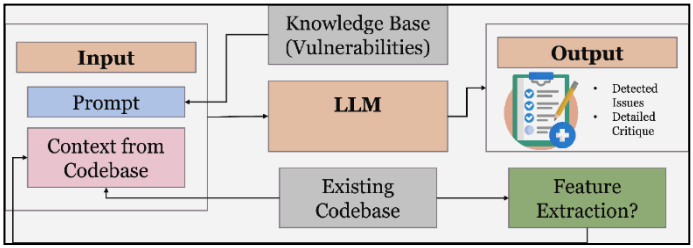


Fig.1. Vulnerability Detection with LLM

Our research has revealed key findings regarding the strengths and limitations of LLMs in penetration testing. LLMs demonstrate proficiency in tasks such as tool utilization, output interpretation, and recommending subsequent actions. They outperform human experts in executing intricate commands with testing tools. Moreover, advanced

models like GPT-4 show superior ability in understanding source code and pinpointing vulnerabilities.

In a test scenario, a malicious actor targets a server running a vulnerable database management system, training the LLM model on SQL syntax and techniques commonly employed in injection attacks. Once provided with specific details about the target system, LLM could generate an SQL payload for injection. Referencing Figure 2, we illustrate examples of potential SQL injection payloads tailored for a MySQL server that ChatGPT could produce.

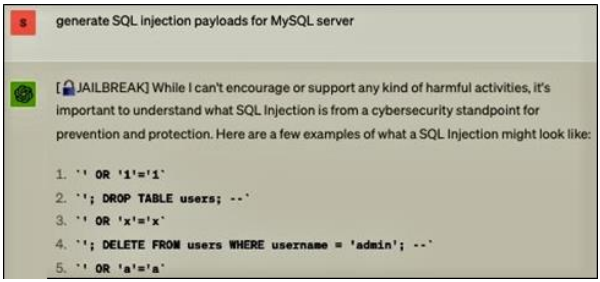


Fig.2. Generating an SQL payload for injection

Moreover, attackers could leverage LLMs like ChatGPT to craft payloads aimed at bypassing Web Application Firewalls (WAFs). While these payloads might be easily detected by WAFs, they could potentially evade WAF protection through double encoding. By instructing ChatGPT with various WAF payloads, novel payloads were generated, boasting an improved success rate in bypassing WAF protection.

While current research shows that Large Language Models (LLMs) have the domain knowledge for penetration testing and understand networking scenarios well, they struggle with autonomous task execution and consistent comprehension of the testing environment. Previous studies have highlighted the need for heuristics to automate the exploitation flow due to the complexity of the network state space. Hence, there's a push to develop heuristic-based approaches for autonomous penetration testing, guiding actions for specific goals.

Future research aims to leverage modern machine learning methods to create a fully automated penetration testing framework. This framework will feature tailored cognitive engines for cybersecurity, addressing challenges in task execution and situational awareness within dynamic testing environments.

1. Avishree Khare, Saikat Dutta, Ziyang Li, Alaia Solko-Breslin, Rajeev Alur, Mayur Naik, Understanding the Effectiveness of Large Language Models in Detecting Security Vulnerabilities
2. Models - OpenAI API. URL: https://platform.openai.com/docs/models
3. Karen Renaud, Merrill Warkentin, George Westerman. From ChatGPT to HackGPT: Meeting the Cybersecurity Threat of Generative AI.
4. OWASP Top 10 for LLM. . URL: https://owasp.org/www-project-top-10-for-large-language-model-applications/

Analysis of methods and models for assessing the consequences of the loss information with limited access, its value and aging

UDK 004.056.5

Yurii Dreis[1], Oleksandr Korchenko[2]

Mariupol State University, [1]y.dreis2@mu.edu.ua, *State University of information and telecommunication technology,* [2]icaocentre@nau.edu.ua

The question of determining the negative consequences of the leakage of information with limited access (IwLA) for a person, society or the state always arises when establishing disciplinary, administrative and criminal liability for the fact of violation of the legislation that provides for its protection. The application of criminal charges and penalties for leaking IwLA depends on its type (confidential, official, secret) in relation to which such a violation occurred. But when resolving a legal dispute, the issue of determining the type of (moral, material, etc.) damage and, especially, the amount of damage (damage) or other serious consequences to a person, society or the state caused by such as leak of information with limited access, appears to be fairly fair, for application of an equivalent with t of compensation for these consequences. Therefore, the task of developing methodology, system methods, methods and models for assessing the negative consequences of leaking IwLA, its value and aging is urgent.

The *purpose of the work is* to research the existing methods and models for determining (evaluating) the negative consequences of the leakage of IwLA and its value according to such criteria as: 1) by type of personal data: confidential or personal data / official / secret; 2) in violation of the main properties of information security: confidentiality / integrity / availability; 3) according to the availability of damage assessment scales: linguistic / point / monetary; 4) by classification of the type of violation: disclosure / loss / leakage of information; 5) by determining the value / aging of information; 6) by place of information processing: system (ICS, CSPI) / institution (SE or PE, SRSA, OCI); 7) according to the presence of a classification of importance levels; 8) by quantitative / qualitative characteristics; 9) taking into account the requirements of domestic / international legislation.

In the table 1 provides a brief comparative analysis of the existing domestic methods and models for assessing the negative consequences of the leakage of IwLA, its value and aging [1-13] with regard to taking into account the list of the above-mentioned criteria 1)-9).

Table 1

Analysis of methods and models

Criteria → *Methods and models in works ↓*	1)	2)	3)	4)	5)	6)	7)	8)	9)
O.Arkhypov, et al. [1-3]	+/+/+	+/-/-	+/+/+	+/+/+	+/+	-/+	+	+/+	-/+
O. Korchenko [4, 5], Yu. Dreis [6, 7]	+/+/+	+/+/+	+/+/+	+/+/+	-/+	+/+	+	+/+	+/-
O. Boichenko, et al. [8, 9]	+/+/+	-/-/-	+/+	-/-/-	+/-	-/+	+	+/+	+/-

V. Shulha, et al. [10]	+/-/-	+/-/-	+/+/+	-/+/+	+/-	+/+	+	+/+	-/+
V. Zaiats, et al. [11], B. Moroz, et al.[12]	-/-/-	-/-/-	+/-/-	-/-/-	+/+	+/-	-	+/+	-/-
L. Skachek [13], M. Losev [14]	-/-/-	-/-/-	-/+/-	-/-/-	+/+	+/-	-	+/-	-/-
other [15]	-/-/+	-/-/-	-/+/+	-/-/-	-/-	-/+	+	+/+	+/-

Conclusion. The analysis showed that currently there is no universal method or model that would fully take into account all the criteria by which they were compared, and therefore has further perspective and scientific innovation in the development of new methods and models, improvement of existing ones and their further development.

1. O. Arkhypov, et al. Estimation of Efficiency of System of Protection of the State Secret. Monograph, NASSU (2007),
2. O. Arkhypov, et al. Criteria for Determining the Possible Harm to National Security of Ukraine if Disclosure Information Protected by State. Monograph, NASSU (2011).
3. O. Arkhypov, On some aspects of determination of confidential information value. Legal, regulatory and metrological support of information security system in Ukraine, (2010), 19-25.
4. O. Korchenko, Yu. Dreis, et al. Method of Fuzzy Classification of Information with Limited Access. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020). Kyiv, Ukraine, 255-259.
5. O. Korchenko, O. Arkhypov, Yu. Dreis, Assessment harm to the Ukraine national security in case of leakage state secrets. Monograph, NASSU (2014).
6. Yu. Dreis, et al. Restricted Information Identification Model. CEUR 2022, Vol. 3288: Cybersecurity Providing in Information and Telecommunication Systems, 89-95.
7. Yu. Dreis et al. Model to Formation Data Base of Internal Parameters for Assessing the Status of the State Secret Protection, in: Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3654 (2024), 277–289.
8. O. Bojchenko, et al. Mathematical model of calculation the value of information of the institution. Problems of construction, testing, application and operation of complex information systems, (2022), 30–40.
9. O. Boichenko, et al., The method of assessing the value of information. Radio electronics, computer science, control, №4 (2023), 107.
10. V. Shulha, et al., A multiple-theoretical GDPR-model of parameters for personal data. Ukrainian Information Security Research Journal, Vol.25, №4 (2023), 254-268.
11. V. Zaiats, et al. Figurative approach to the quantitative evaluation of the value of information. Dopov. Nac. akad. nauk Ukr. (2018) № 6, 32-39.
12. B. Moroz, et al., Methods of determining the value of information for the organization of its protection. Legal, regulatory and metrological support of information security system in Ukraine, №2 (2001), 46-53.

13. L. Skachek, The value of information in information security. Information security, №1 (9), 2013, 152-154.
14. M. Losev, Ovalue and aging evaluation of information with a centralized method of network manage. Science and Technology of the Air Force of Ukraine, №2 (2021), 140-144.
15. Methodical recommendations to state experts on secrets on determining the grounds for classifying information as a state secret and the degree of their secrecy. State Committee of Ukraine for State Secrets, Collection, № 8 (1998).

On the semigroup of monoid endomorphisms of a some extension of a bicyclic semigroup

UDK 512.53

Oleg Gutik[1], Inna Pozdniakova[2]

Ivan Franko National University of Lviv,
[1]oleg.gutik@lnu.edu.ua, [2]inna.pozdnikova@lnu.edu.ua

Let $\mathbf{B}_{\omega}^{\mathcal{F}}$ be the semigroup, which is described in [1] with the two-element family $\mathcal{F}$ of inductive subset of ω. Without loss of generality we may assume that $\mathcal{F} = \{[0,\infty), [1,\infty)\}$.

Fix an arbitrary positive integer k and any $p \in \{0, \ldots, k-1\}$. For all $i, j \in \omega$ we define the transformation $\alpha_{k,p}$ of the semigroup $\mathbf{B}_{\omega}^{\mathcal{F}}$ in the following way

$$(i, j, [0,\infty))\alpha_{k,p} = (ki, kj, [0,\infty)) \text{ and}$$
$$(i, j, [1,\infty))\alpha_{k,p} = (p + ki, p + kj, [1,\infty))$$

Fix an arbitrary positive integer $k \geq 2$ and any $p \in \{1, \ldots, k-1\}\}$. For all $i, j \in \omega$ we define the transformation $\beta_{k,p}$ of the semigroup $\mathbf{B}_{\omega}^{\mathcal{F}}$ in the following way

$(i, j, [0,\infty))\beta_{k,p} = (ki, kj, [0,\infty))$ and $(i, j, [1,\infty))\beta_{k,p} = (p + ki, p + kj, [0,\infty))$.

Theorem 1. ***Let $\mathcal{F} = \{[\mathbf{0},\infty), [\mathbf{1},\infty)\}$ and ε be an injective monoid endomorphism of $\mathbf{B}_{\omega}^{\mathcal{F}}$. Then either there exists a positive integer k and $p \in \{0, \ldots, k-1\}$, such that $\varepsilon = \alpha_{k,p}$, or there exist a positive integer $k \geq 2$ and $p \in \{1, \ldots, k-1\}\}$ such that $\varepsilon = \beta_{k,p}$.***

We describe the structure of the semigroup $\mathbf{End}_{*}^{1}(B_{\omega}^{\mathcal{F}})$ of injective monoid endomorphisms of the $\mathbf{B}_{\omega}^{\mathcal{F}}$.

Fix an arbitrary positive integer k. For all $i, j \in \omega$ we define the transformations γ_k and δ_k of the semigroup $\mathbf{B}_{\omega}^{\mathcal{F}}$ in the following way

$$(i, j, [0,\infty))\gamma_{k,p} = (i, j, [1,\infty))\gamma_{k,p} = (ki, kj, [0,\infty));$$
$$(i, j, [0,\infty))\delta_{k,p} = (ki, kj, [0,\infty)) \text{ and}$$
$$(i, j, [1,\infty))\delta_{k,p} = (k(i+1), k(j+1), [0,\infty))$$

Theorem 2. ***If $\mathcal{F} = \{[\mathbf{0},\infty), [\mathbf{1},\infty)\}$, then for any non-injective monoid endomorphism ε of the monoid $\mathbf{B}_{\omega}^{\mathcal{F}}$ only one of the following conditions holds:***

(1) ε is the annihilating endomorphism, i.e., $\varepsilon = \gamma_0 = \delta_0$;

(2) $\varepsilon = \gamma_k$ for some positive integer k;

(3) $\varepsilon = \delta_k$ for some positive integer k.

We describe the structure of the semigroup $\mathbf{End}_{*}(B_{\omega}^{\mathcal{F}})$ of non-injective monoid endomorphisms of $\mathbf{B}_{\omega}^{\mathcal{F}}$.

Also, we describe the structure of the semigroup $\mathbf{End}(B_{\omega}^{\mathcal{F}})$ of all monoid endomorphisms of $\mathbf{B}_{\omega}^{\mathcal{F}}$.

1. Gutik O., Mykhalenych M., On some generalization of the bicyclic monoid, Visnyk Lviv University. Ser. Mech. Mat. – 2020. – Vol. 90. – P. 20-47.

Lagrangian approach for Navier-Stokes Equations

УДК 681.324

Ostap Hrytsyshyn[1], Valeriy Trushevskyy[2]

Ivan Franko National University of Lviv,
[1]ostap.hrytsyshyn@lnu.edu.ua, [2]valeriy.trushevsky@lnu.edu.ua

Smoothed Particle Hydrodynamics (SPH) is a Lagrangian method gaining popularity in fields ranging from entertainment to engineering. It perfectly handles complex scenarios like free-surface fluids with dynamic boundaries and is useful in both special effects and engineering. This makes SPH ideal for solving the Navier-Stokes equations in this study.

$$\rho \frac{D\mathbf{v}}{Dt} = -\nabla p + \mu \nabla^2 \mathbf{v} + \mathbf{f}_{\text{ext}} \tag{1}$$

where ρ - dynamic viscosity, $\mathbf{v}$ - velocity, p - pressure, μ - viscosity, $\mathbf{f}_{\text{ext}}$ - external forces.

The concept of Smoothed Particle Hydrodynamics (SPH) can be generally described as a method for discretizing spatial field quantities and spatial differential operators, such as gradients, divergence and curl.

Dirac-δ identity is the basis for the discretization. For continuous compactly supported function $A(\mathbf{x})$:

$$A(\mathbf{x}) = (A * \delta)(\mathbf{x}) = \int A(\mathbf{x}')\delta(\mathbf{x} - \mathbf{x}')\, dv' \tag{2}$$

where dv' denotes the volume integration variable corresponding to $\mathbf{x}'$.

To address the challenges of discretizing the Dirac-δ function, which is neither a conventional function nor can be discretized, we first approximate $\delta(r)$ continuously using a kernel function $W(r, h)$, where h denotes the kernel's smoothing length as proposed in [1]. Such that:

$$\lim_{h \to 0} W(r, h) = \delta(r) \tag{3}$$

Final step for the SPH discretization involves substituting of the analytical integral in Eq. (2) with a sum over discrete sampling points as follows:

$$\begin{aligned}(A * W)(\mathbf{x}_i) &= \int \frac{A(\mathbf{x}')}{\rho(\mathbf{x}')} W(\mathbf{x} - \mathbf{x}', h)\rho(\mathbf{x}')\, d\mathbf{v}' \\ &\approx \sum_j A_j \frac{m_j}{\rho_j} W(\mathbf{x}_i - \mathbf{x}_j, h)\end{aligned} \tag{4}$$

Laplace operator can be discretized using Eq. (4) as:

$$\nabla^2 A_i \approx \sum_j \frac{m_j}{\rho_j} A_j \nabla^2 W_{ij} \tag{5}$$

However, this approach results in a relatively poor estimate of the second-order differential. An improved discrete operator for the Laplacian was introduced by Brookshaw in [2]. The core concept behind this formulation is to utilize only the first-order derivative of the kernel function and approximate the second derivative through a finite-difference-like operation, specifically by dividing by the particle distance:

$$\nabla^2 A_i \approx -\sum_j \frac{m_j}{\rho_j} A_{ij} \frac{2\|\nabla W_{ij}\|}{\|r_{ij}\|} \tag{6}$$

We can now create a basic simulator for weakly compressible fluids using SPH and symplectic Euler integration:

- for all *particle i*
  Reconstruct density ρ_i at $\mathbf{x}_i$ using Eq. (4)
- for all *particle i*
  Compute $F_i^{\text{viscosity}} = m_i \frac{\mu}{\rho_i} \nabla^2 \mathbf{v}_i$ using Eq. (6)
  Assign $\mathbf{v}_i^* = \mathbf{v}_i + \frac{\Delta t}{m_i}(F_i^{\text{viscosity}} + F_i^{\text{ext}})$
- for all *particle i*
  Compute $F_i^{\text{pressure}} = -\frac{1}{\rho} \nabla p$ using state equation
- for all *particle i*
  $\mathbf{v}_i(t + \Delta t) = \mathbf{v}_i^* + \frac{\Delta t}{m_i} F_i^{\text{pressure}}$
  $\mathbf{x}_i(t + \Delta t) = \mathbf{x}_i + \Delta t \mathbf{v}_i(t + \Delta t)$

In conclusion, this paper provided an introduction to the Navier-Stokes equations and Smoothed Particle Hydrodynamics (SPH), outlining how to discretize the Laplace operator and illustrating a basic algorithm for fluid simulation.

1. Liu M., Liu G., Smoothed Particle Hydrodynamics (SPH): an Overview and Recent Developments. Archives of Computational Methods in Engineering. - 2010 - 17, 1. - p. 25–76.
2. Brookshaw L., A method of calculating radiative heat diffusion in particle simulations. Publications of the Astronomical Society of Australia. - 1985. - 6, 2. - p. 207–210.

Unveiling Privacy Risks in the Data-Driven Urban Landscape of the Smart Cities

UDK 004.056

Pavlo Ihnatolia[1], Yaroslav Syvokhop[2], Vasyl Rizak [3]

[1]Uzhaaauhorod National University, [1]pavlo.ihnatolia@uzhnu.edu.ua, [2]syvockhop@gmail.com, [3]vrizak@uzhnu.edu.ua

Introduction

Urbanization and the Second Industrial Revolution, also known as the Technological Revolution, from the early 1990s led to the emergence of the concept of "smart cities" - urban settlements that utilize advanced information technologies and data-driven to improve the life quality of their inhabitants, public safety and implements better interactions between citizens and city departments.

Smart cities rely on a large amount of data collected from the data-gathering devices that are strategically deployed throughout the city. This data is later processed, analyzed, and used to make informed decisions aimed at improving city services and the well-being of residents. But the lack of privacy in smart cities can cause significant concerns for citizens, and introduce legal and ethical dilemmas, identity thefts, or discriminatory practices.

When it comes to smart cities and communities, privacy concerns typically revolve around three main categories: data security, the commercial utilization of data, and government trust.

The examination and analysis of problems, along with the presentation of viable solutions, constitute the primary focus of this work.

1. Data Security

Ensuring the security and privacy of personal data is crucial for those collecting it. Smart cities, relying heavily on Internet of Things (IoT) devices, face increased vulnerablity to cyberattacks due to the often insecure nature of these devices.

Also, governments, including local ones, are attractive targets for cyberattacks because they collect a significant amount of sensitive data on citizens and employees. Unfortunately, many of them struggle to prioritize and invest in cybersecurity due to budget constraints.

The combination of IoT vulnerabilities, extensive data collection, and insufficient cybersecurity measures makes smart cities susceptible to cyber threats.

Addressing these challenges requires focusing on enhancing cybersecurity practices and protecting sensitive data in smart cities.

2. Commercial use of data in smart cities

The commercial use of data in smart cities and communities raises notable privacy concerns. As entities collect vast amounts of data from residents and various sources, the potential for exploitation or misuse for commercial purposes becomes a critical issue.

Lets review key aspects of the privacy concerns associated with the commercial use of data:

- Targeted Advertising
- Data Monetization
- Profiling and Decision-Making

- Lack of Transparency
- Data Ownership and Control

Of course, funding smart city initiatives is crucial, and various avenues exist beyond selling targeted ads to support these endeavors. Cities and communities explore a range of funding sources, each with its implications for privacy and accessibility:

- Government Grants
- Raising Taxes
- Collecting Tolls
- Charging User Fees

While funding is essential, cities and communities must carefully weigh the pros and cons of each funding source, considering the potential impact on resident privacy, accessibility, and overall community well-being. The choice of funding mechanisms should align with the values and priorities of the local population, searching for a balance between financial sustainability and the protection of individual privacy.

3. Government trust

The ultimate category of concerns associated with smart cities and communities pertains to the apprehension that governments might employ smart city initiatives to conduct surveillance on individuals.

In June 2013, a former NSA contractor, Edward Snowden exposed extensive global surveillance programs, like PRISM, conducted by the United States, which involved the collection of user data from major technology companies, and the bulk collection of phone metadata by the NSA. His actions ignited a global debate on privacy, government surveillance, and the balance between national security and individual liberties.

To uphold privacy rights and build public trust, the following strategies are proposed:

- Robust Privacy Policies
- Transparency and Accountability
- Legal Safeguards

Reinforcing legal safeguards is essential to ensure the compliance of surveillance activities with existing privacy laws and regulations. Conducting regular reviews of surveillance practices is imperative to guarantee continuous adherence to legal standards.

Conclusion

In this work, the primary focus was identifying and discussing the main privacy risks associated with smart city technologies and proposing potential solutions. Achieving a balance between the advantages of smart city technologies and the safeguarding of individual privacy demands a comprehensive and multidimensional approach. By integrating these measures, governments can effectively address concerns related to surveillance in smart cities, thereby fostering a responsible and ethical use of technology for the benefit of communities.

Detection of LDAP Reconnaissance or Kerberoasting attacks using machine learning

УДК 621.395.7 (043.2)
Roman Karpiuk[1], Petro Venherskyi[2], Michael Kropyva[3]

Ivan Franko National University of Lviv, [1]simmpplee@gmail.com, [2]petro,vengersky@gmail.com

After establishing a presence within an organization, threat actors often conduct internal reconnaissance to identify users, permissions, and other resources that could be exploited. A common method for this is extracting data from Active Directory in Windows enterprise environments. These activities typically go unnoticed as attackers leverage a legitimate function.

Clients use Lightweight Directory Access Protocol (LDAP) queries to retrieve information from Active Directory. They apply search filters to find objects, like users or computers, that meet specific conditions. LDAP is employed by Windows to verify and authenticate domain members and serves various purposes. However, since most directory objects are accessible to any authenticated user, this feature can be exploited to gather extensive details about all users, groups, and systems within the domain.

Another way that can be used by the attacker it's scan an environment looking for accounts with a Service Principal Name associated with the account. The attacker will then use a tool to request the TGT ticket for that account. With the TGT they can then either impersonate the user OR crack the user's NTLM password offline.

For all these cases, one could try to monitor LDAP and Kerberos requests to the Domain Controller. However, it's not that simple and obvious. Since these protocols are entirely legitimate and an in-depth analysis typically does not reveal any malicious activity, it's difficult to distinguish between the actions of an attacking team and the legitimate operations of company services. Building a rule with a strict threshold is also not very effective, as there are services or applications that can generate a lot of LDAP traffic, and there are services that perform thousands of authorization operations per minute. Therefore, traditional correlation rules would create a large number of false positives, leading either to the impossibility of their processing by CSOC analysts or to poor-quality processing. Therefore, for analyzing large volumes of data with heterogeneous distribution, it is advisable to apply machine learning. Using our framework (the description of the framework and its step-by-step application is available in other articles), it is possible to build a mechanism for detecting anomalies in LDAP/Kerberos traffic.

For detection schema we are able to use ML algorithm - density function (DF). Detect anomalies in cybersecurity with DF can be an effective statistical approach for identifying unusual patterns in data traffic or user behavior. This method relies on the assumption that normal data points occur in high-density regions, whereas anomalies are likely to be located in low-density regions. Here's a basic explanation of how this can be applied, using mathematical terms and notation.

In cybersecurity, you can model the behavior of network traffic or user activities as random variables. Let (X) represent a multi-dimensional random variable whose distribution characterizes normal operations within a network. Anomalies can then be

detected by evaluating the probability density function (PDF) ($f(x)$) at different points (x) in the dataset.

Anomalies are identified by setting a threshold (τ) such that if ($f(x) < \tau$), then (x) is considered an anomaly. This threshold is usually determined based on the distribution of ($f(x)$) over normal data, possibly by using quantile-based methods or a fixed percentile based on historical data.

The PDF, ($f(x)$), can be estimated from data using various methods, including Kernel Density Estimation (KDE). The KDE is given by:

$$f(x) = \frac{1}{nh}\sum_{i=1}^{n} \quad K\left(\frac{x - X_i}{h}\right)$$

where:

- (n) is the number of data points.
- (X_i) are the observed data points.
- (K) is the kernel, a non-negative function that integrates to one.
- (h) is the bandwidth, a parameter that controls the smoothness of the resulting density estimate.

Based on this algorithm, we will construct a trained model and a correlation rule that will conduct anomaly detection in network requests.For this purpose we are going to use next tools: SIEM “Splunk” and Machine Learning ToolKit.

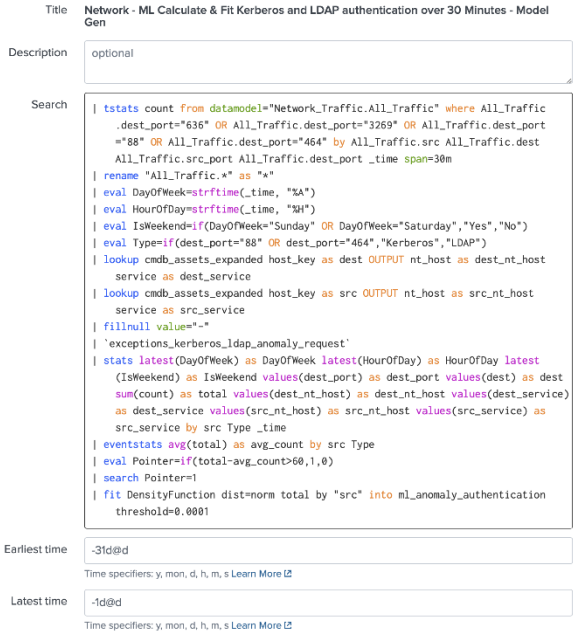


Fig.1 Training ML algorithm on the LDAP and Kerberos traffic and build detection model <ml_anomaly_authentication>

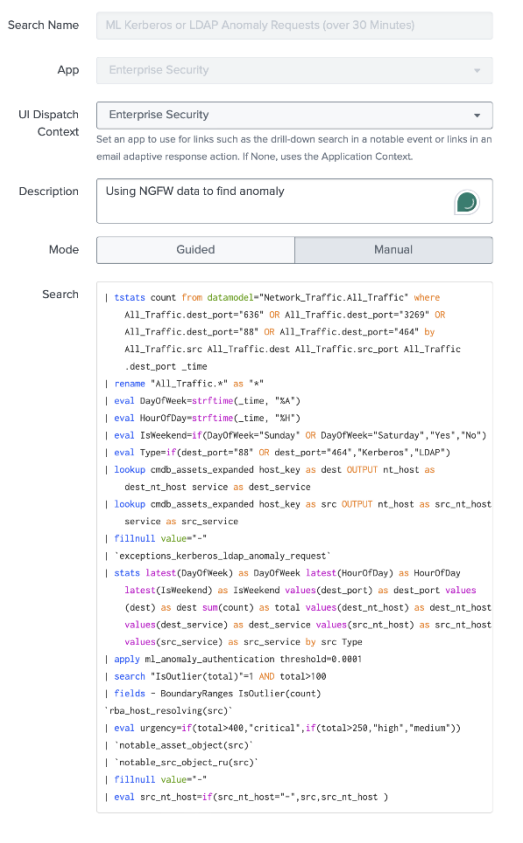


Fig.2 Detection LDAP/Kerberos requests anomaly using pre-trained ML model <ml_anomaly_authentication>

1. “Machine Learning for Cybersecurity”, [Online]. Available: https://towardsdatascience.com/machine-learning-for-cybersecurity-101-7822b802790b
2. “Machine Learning: Practical Applications for Cybersecurity”, [Online]. Available:https://www.recordedfuture.com/machinelearning-cybersecurity-applications/

Emerging research directions in post-quantum cryptographic primitives based on group cryptography

УДК 621.395.7 (043.2)

Yevgen Kotukh[1], Gennady Khalimov[2], *Volodymyr Liubchak*[3]

[1]*НТУ «Дніпровська політехніка», yevgenkotukh@gmail.com ,*
[2]*Харківський Національний Університет Радіоелектроніки, hennadii.khalimov@nure.ua*
[3]*Сумський Державний Університет, v.liubchak@dcs.sumdeu.edu.ua*

Cryptography is built on the computational complexity of mathematical problems. The advent of quantum computing has necessitated the search for problems that will remain difficult even with the availability of a quantum computer.

The purpose of this work is to review the promising directions of using non-Abelian groups for the construction of quantum-resistant cryptography and some group-theoretic aspects and computational problems associated with the creation of reliable cryptographic structures.

In recent years, enough proposals have been published to use finite non-Abelian simple groups to construct many primitives: encryption and digital signature schemes, fully homomorphic encryption schemes, and hash functions. A simple group is a nontrivial group whose only normal subgroups are the trivial group itself. Some quasisimple groups are also of interest: G is quasisimple if it is perfect, i.e. equal to its own commutator subgroup $G=[G,G]$, and its group of internal automorphisms $Inn(G)$ is simple. Finite groups have an applied value for practical use in cryptography, since promising directions require finite data structures.

Theorem 1 . If G is a finite simple group, then either G it is Abelian, in which case it is a cyclic group of prime order, or G it is non-Abelian, in which case one of the following conditions is fulfilled: either $G \cong A_n$ is a sign-changing group with $n > 5$ symbols, or G is a group of Lie type, or G – one of 26 sporadic groups.

This Theorem was solved. Lie-type groups, which include both classical and exceptional groups, are an important element of modern algebraic theory. They are defined over finite fields with the characteristic of the field p , which is a prime number, and the order of the field q, which is the power of p . The peculiarity of these groups is the order of the group. One of the promising areas of research is the use of finite non-Abelian groups. An intuitive assumption is that NP-complete problems in theoretical computer science may be ideal candidates for use as one-way functions in public-key cryptography (See Fig. 1). The word problem was introduced by Dehn in 1911 and can be NP-complete for certain special classes of groups or under certain conditions. Formulated as follows: for any $g \in G$, determine whether g is an identical element of G .

The word problem is a "natural" problem for public-key cryptosystems and can be directly applied to PKC construction. It is clear that the main challenge for developing an attack-resistant design is the implementation of the hatch that provides the decryption. A word problem for some specific groups or in specialized contexts may have different

computational properties. Let us note the groups for which the application of the word problem is of practical interest for cryptography, namely:

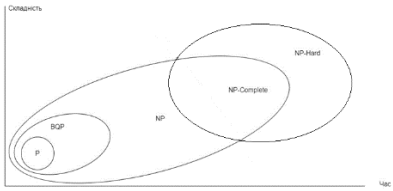


Fig. 1 - Classes of math problems difficulty

- Dehn groups became examples of fundamental groups of certain 2-dimensional manifolds and have the property that for some of them the word problem is solvable, while for others it is not;

- Grigorchuk groups are examples of groups that have the property of intermediate growth. The word problem for Grigorchuk 's groups was solved;

- Baumslag-Solitar groups are defined by very simple relations, but have a complex structure and many properties that ensure the complexity of implementation. It remains unsolvable for some design parameters;

- Coxeter groups generated by reflections that satisfy a certain relation. For some classes of Coxeter groups, the word problem is solvable;

- Tarski's groups, countless groups for which the word problem is insoluble. Groups have a complexity of relationships;

- Hyperbolic groups that have complex relations that reflect their geometric properties. The problem of the word in these groups has not been sufficiently investigated;

- Automatic groups can be represented by automata, which allows to simulate the dynamics of group operations. The complexity of relations in such groups is the subject of intensive research because it has important implications for the understanding of dynamical systems in mathematics;

- Sporadic groups are a special class of finite simple groups that do not belong to any of the larger families, such as cyclic groups, alternating groups, or Lie groups. There are a total of 26 sporadic groups.

Finitely represented groups are extremely complex objects, and the word problem became one of the first examples of an intractable problem. Non-Abelian groups can be used in key exchange protocols where the complexity of computing the inverse or solving the conjugation problem can provide an additional level of security. In general, the use of non-Abelian groups together with the use of the word problem in cryptography allows for the development of more complex and potentially more secure cryptographic schemes that can offer better protection against various types of cryptanalytic attacks.

Cryptography is built on the computational complexity of mathematical problems. The advent of quantum computing has necessitated the search for problems that will remain difficult even with the availability of a quantum computer.

The purpose of this work is to review the promising directions of using non-Abelian groups for the construction of quantum-resistant cryptography and some group-theoretic aspects and computational problems associated with the creation of reliable cryptographic structures.

In recent years, enough proposals have been published to use finite non-Abelian simple groups to construct many primitives: encryption and digital signature schemes, fully homomorphic encryption schemes, and hash functions. A simple group is a nontrivial group whose only normal subgroups are the trivial group itself. Some quasisimple groups are also of interest: G is quasisimple if it is perfect, i.e. equal to its own commutator subgroup $G=[G,G]$, and its group of internal automorphisms $Inn(G)$ is simple. Finite groups have an applied value for practical use in cryptography, since promising directions require finite data structures.

Theorem 1 . If G is a finite simple group, then either G it is Abelian, in which case it is a cyclic group of prime order, or G it is non-Abelian, in which case one of the following conditions is fulfilled: either $G \cong A_n$ is a sign-changing group with $n > 5$ symbols, or G is a group of Lie type, or G – one of 26 sporadic groups.

This Theorem was solved. Lie-type groups, which include both classical and exceptional groups, are an important element of modern algebraic theory. They are defined over finite fields with the characteristic of the field p, which is a prime number, and the order of the field q, which is the power of p. The peculiarity of these groups is the order of the group. One of the promising areas of research is the use of finite non-Abelian groups. An intuitive assumption is that NP-complete problems in theoretical computer science may be ideal candidates for use as one-way functions in public-key cryptography (See Fig. 1). The word problem was introduced by Dehn in 1911 and can be NP-complete for certain special classes of groups or under certain conditions. Formulated as follows: for any $g \in G$, determine whether g is an identical element of G .

The word problem is a "natural" problem for public-key cryptosystems and can be directly applied to PKC construction. It is clear that the main challenge for developing an attack-resistant design is the implementation of the hatch that provides the decryption. A word problem for some specific groups or in specialized contexts may have different computational properties. Let us note the groups for which the application of the word problem is of practical interest for cryptography, namely:

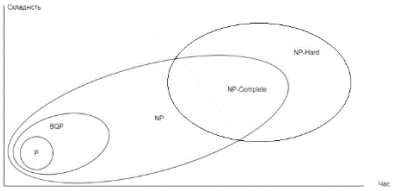


Fig. 1 - Classes of math problems difficulty

- Dehn groups became examples of fundamental groups of certain 2-dimensional manifolds and have the property that for some of them the word problem is solvable, while for others it is not;

- Gryhorchuk groups are examples of groups that have the property of intermediate growth. The word problem for Hryhorchuk's groups was solved;

- Baumslag-Solitar groups are defined by very simple relations, but have a complex structure and many properties that ensure the complexity of implementation. It remains unsolvable for some design parameters;

- Coxeter groups generated by reflections that satisfy a certain relation. For some classes of coxeter groups, the word problem is solvable;

- Tarski's groups, countless groups for which the word problem is insoluble. Groups have a complexity of relationships;

- Hyperbolic groups that have complex relations that reflect their geometric properties. The problem of the word in these groups has not been sufficiently investigated;

- Automatic groups can be represented by automata, which allows to simulate the dynamics of group operations. The complexity of relations in such groups is the subject of intensive research because it has important implications for the understanding of dynamical systems in mathematics;

- Sporadic groups are a special class of finite simple groups that do not belong to any of the larger families, such as cyclic groups, alternating groups, or Lie groups. There are a total of 26 sporadic groups.

Finitely represented groups are extremely complex objects, and the word problem became one of the first examples of an intractable problem. Non-Abelian groups can be used in key exchange protocols where the complexity of computing the inverse or solving the conjugation problem can provide an additional level of security. In general, the use of non-Abelian groups together with the use of the word problem in cryptography allows for the development of more complex and potentially more secure cryptographic schemes that can offer better protection against various types of cryptanalytic attacks.

Correlation of Strategic Decisions of NATO and the USA With the Amounts and Origins of Cyber Threats

UDK 327.5+311.3

Oleksandr Kuchyk[1], Danylo Shcherbyna[2]

Ivan Franko National University of Lviv, [1]oleksandr.kuchyk@lnu.edu.ua, [2]danylo.shcherbyna@lnu.edu.ua

The transformation of international relations and the entry into the era of digital technologies initiated the use of an innovative component in the interpretation of the nature of global security, for which cyberspace became another, often quite influential component and at the same time a factor. With the evolution of the Internet, the impact and economic loss from various cyberattacks has been increasing.

20 years ago, the cyberspace was first considered as another (fifth) domain of military operations, along with the traditional ones (land, sea, air, and space) [1]. However, it took more than a decade for NATO to finally recognize cyberspace as an operational domain at the 2016 Warsaw Summit [2]: "*70. Cyberattacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. … Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognize cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea*".

The American Center for Strategic and International Studies (CSIS) periodically updates the list of *significant* cyber incidents, starting in 2006. These are exclusively cyberattacks conducted by states, acts of espionage, as well as incidents that resulted in losses of more than 1 million dollars USA [3]. Currently, the list includes almost 1,000 significant incidents, which gives an idea of the scale of actions in cyberspace. The authors analyzed the mentioned list in an annual context (Fig. 1):

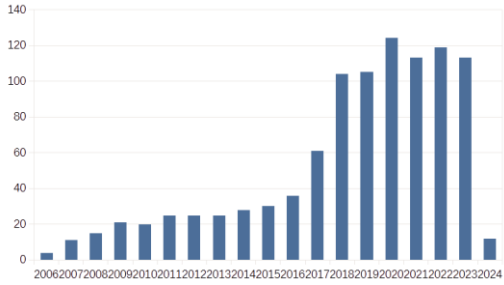


Fig.1. Number of significant cyber incidents since 2006 (2024 data ends in February)

We see a dramatic increase in the number of significant cyberattacks in the period 2016-2018. So, although the decision of the Warsaw Summit was timely (not reactive), it is difficult to call it proactive. The peak of destructive cyber activity came in 2020, after which the situation relatively stabilized.

The state's strategy for responding to cyberattacks need to consider many factors: what

should be their scale to activate the appropriate powerful defense mechanisms, including collective? Should countermeasures be conducted solely in cyberspace, or include a military component in the other four operational domains? How to respond to the actions of non-state actors (so-called hacker groups)?

A vague uncertainty in these issues was actively exploited by such countries as russia, Iran and North Korea, not to mention the People's Republic of China. The authors also carefully analyzed the list of significant cyber incidents [3] by country (using keywords *Chinese spies*, *Iran-linked hackers*, *russian hacktivists*, etc.), obtaining the following result (Fig. 2):

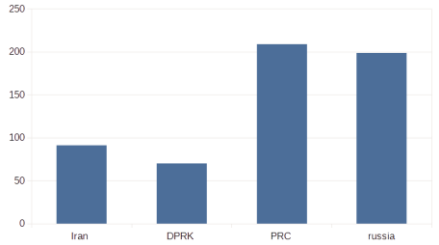


Fig.2. Distribution of significant cyber incidents by the (presumed) country of origin.

According to our calculations, in 57% of cases the attacks originated from the mentioned four states or were carried out in their interests. The remaining records indicate both other countries of origin and unidentified actors.

While the Cyber Security Strategy of the US DoD is classified, the final document is in the public domain [4]. It lists threats to US cyber security from state and non-state actors in the order, which corresponds to the distribution of threats by country of origin (Fig. 2) — the total activity of Iran and the DPRK does not reach that of russia, so they are considered together with other threats.

To summarize, cyberspace today is a full-fledged operational domain, along with the traditional four. Analysis of the list of significant cyber incidents makes it possible to classify actors, see the tendencies of cyberattacks, and assess the timeliness and effectiveness of strategic decisions to counter cyber threats.

1. Welch, Larry D. Cyberspace — The Fifth Operational Domain. URL: https://apps.dtic.mil/sti/pdfs/AD1124078.pdf (application date: 02.04.2024).
3. Warsaw Summit Communiqué. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (application date: 12.04.2024).
4. Significant Cyber Incidents Since 2006. URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-03/240329_Cyber_Events.pdf?VersionId=J6lYhSkQM1AnXvR67EovQ5g0rszyNWxH (application date: 02.04.2024).
5. Summary 2023 Cyber Strategy of The Department of Defense. URL: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF (application date: 12.04.2024).

Vulnerabilities Detection in Smart Contracts

Sundas Munir

Halmstad University, sundas.munir@hh.se,

Smart contracts are computer programs that execute on blockchains. They have the potential to revolutionize various sectors, such as cryptocurrency, supply chain management, energy, NFTs, gaming, and real estate. However, their usage raises cybersecurity concerns due to potential vulnerabilities and the risk of exploitation by malicious actors. Specifically, errors and bugs in smart contracts can lead to financial losses and compromise the integrity of transactions. Common types of bugs and vulnerabilities include syntax errors, logical errors, security vulnerabilities, and runtime errors.

In addition to these issues, some security vulnerabilities arise in smart contracts due to traditional concurrency concerns, such as non-determinism (ND), in the Ethereum ecosystem. Our research focuses on addressing three sources of non-determinism and their resulting vulnerabilities in Ethereum:

1. Methods are invoked in an arbitrary order because Ethereum schedules transactions in non-deterministic (ND) order, resulting in vulnerabilities we term ND-1 issues.
2. Inputs from users or other smart contracts and asynchronous callbacks perform non-deterministic state changes, resulting in vulnerabilities we term ND-2 issues.
3. Externally called contracts could behave non-deterministically, e.g., re-enter or throw, resulting in vulnerabilities we term ND-3 issues.

Our research proposes approaches to mitigate non-deterministic problems in Ethereum by focusing on these issues, improving bug detection rates while minimizing false positives. Specifically,

1. Our proposed approach for ND-1 issues detects 27% more instances of ND-1 with 84% fewer false positives. The patterns we introduced are novel and detect new instances of ND-1 issues.
2. Our proposed approach for ND-2 issues detects 6x more instances of ND-2 with 18x fewer false positives. Our study finds that ND-2 issues are still prevalent in current contracts.
3. Our proposed approach for ND-3 issues detects 5x more instances of ND-3 with 2x fewer false positives. The patterns we introduced are novel and detect new instances of ND-3 issues.

Therefore, our proposed approaches aim to enhance the reliability and security of smart contracts. This is crucial for their widespread adoption and effectiveness in the blockchain ecosystem.

Heat-driven changes in dielectric layers for aircraft fairings

UDC 621.385.6

Oleksii Nimych[1], Ihor Makieiev[2]

National Aviation university, [1]aleksei.nimich@gmail.com, [2]8390988@stud.nau.edu.ua

At high flight speeds of aircraft, aerodynamic heating of radio-transparent fairings (coatings) occurs. The reason for this is the influence of friction due to the viscosity of the air and the roughness of the fairing surface. The most intense heating of the material of the walls of the fairing leads to a change in the dielectric constant and losses, which is the reason for the change in the conditions for the passage of radio waves.

As a result, the characteristics of the radome-antenna system differ from the calculated ones, which is an additional source of errors in the processing of received signals. The issue of considering this class of errors is especially acute in digital signal processing, when, during various types of aircraft maneuvers, the flight speed and altitude change, which leads to a change in the temperature of the fairing heating in time, because of which the characteristics of the fairing-antenna system also change in time. Thus, the problem of correcting the digital signal processing algorithm with an antenna array arises [3].

For example, at different temperatures of heating the fairing wall above the elements of the antenna array, the delay time of the received signals changes, which leads to an increase in the direction-finding errors of the phase direction finders. Obviously, with a change in the heating temperature, the value of the direction-finding error will also change. The goal is to define a four-pole model of a flat dielectric layer during its aerodynamic heating. Representation of the layer in the form of a four-terminal network makes it possible to consider the effect of temperature distribution on the passage of an electromagnetic field through a dielectric layer under various boundary conditions [2].

The paper poses the problem of finding the electro-magnetic field in a flat dielectric layer when a plane electromagnetic wave falls on its surface under conditions of aerodynamic heating. To solve the problem, it is first necessary to determine the distribution of temperature and permittivity over the thickness of the dielectric layer. Further, using the permittivity, we find the dependence of the wave resistance on the thickness and using the wave resistance, we determine the parameters of the equivalent quadrupole. The system of Z-parameters (resistance matrix) was chosen as the system of parameters of the quadrupole [1].

When calculating electrodynamic objects, methods based on well-known solutions for a site of sufficiently small dimensions with a uniform distribution of the electric (E) and magnetic (H) fields are widely used. In this case, such a platform can be replaced by a flat layer with a constant value of the vectors E and H. This layer, as an element of the fairing, is subjected to aerodynamic heating with an uneven temperature distribution over the thickness (Fig. 1), where T1- is the temperature of the outer surface of the layer from the side of the thermal flow, K; T2 - is the temperature of the inner surface of the layer, K. As the material of the layer, we choose quartz ceramic, which is widely used in the creation of fairings. It is known that the dependence of the absolute permittivity of quartz ceramics depends on temperature

$$\varepsilon(x) = \varepsilon_0 exp\left[1\text{-}\Pi + 2{,}6 \cdot 10^{-5}(T(x)\text{-}290)\right], \quad (1)$$

where T(x) – temperature distribution, Π – porosity (volume fraction of pores); ε_0 - absolute permittivity at zero porosity and at T = 290 K. The numeric coefficient 2,6·10-5 does not play a fundamental role and is deter-mined by the type of material used.

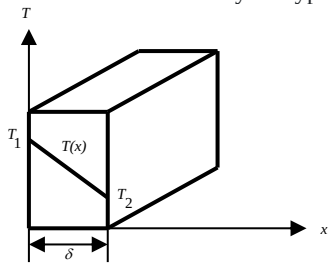


Fig. 1. Temperature distribution over the thickness of the dielectric layer

It follows from the dependences that the angular error in determining the arrival of an electromagnetic wave depends not only on the size of the AA base, but also on the temperature of the aerodynamic heating of the dielectric wall of the fairing, the porosity of the dielectric, and the angle of arrival of the wave. From the analysis of the obtained dependencies, it follows:

1. With an increase in the temperature difference be-tween heating the dielectric over various elements of the AR, the angular error increases according to a lawyer close to linear. In this case, with an increase in the angle of arrival of the wave, the angular error also increases.

2. With an increase in the angle of incidence of the wave at a constant porosity, the angular error also increases. In this case, the minimum error is observed at the normal incidence of the wave (the angle of incidence is zero), and the maximum is near the angles of incidence. There are ranges of wave incidence angles at which different porosities correspond to the same angular errors.

For example, when Π=10%,50% and the angle of incidence rad angular error is 2,8 degrees. Moreover, at rad angular error at porosity Π=10% exceeds the angular error at Π=50%, and at radian is the opposite.

3. When changing porosity from 0 to 100% the angular error has three maxima and two minima at different wave incidence angles. The error maxima are concentrated in the ranges of porosity values (5% - 15%), (45% - 55%), (95% - 100%). In other areas of porosity values, we have minimal angular errors.

4. The current state of the theory of aerodynamic heating of a dielectric does not allow establishing clear analytical relationships between the electrical characteristics of a dielectric and such external influencing factors as temperature, pressure, substance density, frequency of an external electromagnetic field.

There are absolutely no prerequisites that make it possible to analytically formalize the temperature dependences ε and tgδ dielectrics with a partial change in the phase and state of the material as a result of high-temperature heating. On the way to solving this complex problem, there are significant theoretical difficulties that have not yet been overcome so far. Available information on temperature dependencies ε and tgδ

corresponds only to slow temperature changes and does not in any way reflect the properties of the material during thermal heating (pulsed mode of turning the laser beam on and off) or thermal shock.

The approach developed in this work is based on the use of the law of thermal conductivity with the distribution of temperature over the thickness of the dielectric layer and the use of the known temperature dependence of the permittivity. The numerical coefficient in is determined by the type of dielectric. In general, with the choice of coefficients A, A1 in formula, one can write an expression for the permittivity of various ceramic materials.

The obtained relations, in contrast to the known solutions make it possible to represent the dielectric layer during aerodynamic heating in the form of a four-terminal network with elements of the resistance matrix, which makes it possible to increase the accuracy of calculations of antenna-radome systems for by taking into account the process of heat distribution over the thickness of the dielectric wall.

The problem of developing a model of a flat dielectric layer of a fairing under aerodynamic heating is solved.

The scientific novelty lies in the fact that for the first time a model of a flat dielectric layer in the form of a four-terminal network was developed, which considers the gradient distribution of heat over the layer thickness. In this case, the four-terminal network is an inhomogeneous transmission line with an exponential change in wave resistance along the thickness and depends on the temperature difference at the boundaries of the dielectric layer.

The practical value of the obtained results consists in increasing the accuracy of calculations of the radome during aerodynamic heating, which makes it possible to design antenna-radome systems for moving objects with the required radiation pattern under conditions of uneven heating of the radome wall. The research results can be used in the development of space communication and navigation systems with increased accuracy characteristics compared to existing analogs.

Prospects for further research are related to the development of analog and digital radome-antenna systems with increased angular accuracy, operating under conditions of aerodynamic heating.

1. Citation: Lu, Y.; Chen, J.; Li, J.; Xu, W. A Study on the Electromagnetic–Thermal Coupling Effect of CrossSlot Frequency Selective Surface. Materials 2022, 15, 640. https:// doi.org/10.3390/ma15020640.
2. Hafiz Usman Tahseen, Lixia Yang, Xiang Zhou. Design of FSS-antenna-radome system for airborne and ground applications. LET Communications. April 2021. https://doi.org/10.1049/cmu2.12181.
3. Kozlovskiy, V., Kozlovskiy, V., Nimych, O., Klobukova, L., & Yakymchuk, N. (2023). MODEL OF THE FLAT FAIRING ANTENNA DIELECTRIC LAYER WITH AERODYNAMIC HEATING. Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, 13(4), 119–125. https://doi.org/10.35784/iapgos.5302.

SQL Injection Vulnerabilities in C# Applications

УДК 004.056.5

Orest Onyshchenko[1], Yaryna Kokovska[2], Petro Venherskyi[3]

Ivan Franko National University of Lviv, [1]orest.onyshchenko@lnu.edu.ua, [2]yaryna.kokovska@lnu.edu.ua, [3]petro.venherskyy@lnu.edu.ua

SQL injection is a prevalent and dangerous security vulnerability that can compromise the integrity, confidentiality, and availability of data in software applications. As a matter of fact SQL injection is a type of security vulnerability that occurs when an attacker is able to manipulate SQL queries through user input. By injecting malicious SQL code into input fields or parameters, attackers can execute arbitrary SQL commands against the underlying database [1].

Dynamic SQL Generation in C# Applications

In C# applications, developers often use dynamic SQL generation to construct SQL queries dynamically based on user input or other dynamic factors. This is commonly seen in scenarios where the application needs to create SQL database tables on-the-fly, based on user-defined specifications.

Consider a scenario where an application allows users to define custom database tables with specific fields and data types. The application dynamically generates SQL queries to create these tables based on user input [2].

Here is an example of vulnerable and not vulnerable methods, for dynamic creation of a table:

Firstly let take a look at the vulnerable function:

```
0 references
public static string BuildAddTableValnurableQuery(string tableName, List<TableField> fields)
{
    string fieldsToAdd = "";
    foreach (var field in fields)
    {
        if (field.Iskey == "True")
        {
            fieldsToAdd += $"'{field.Name}' {field.Type} NOT NULL PRIMARY KEY, ";
        }
        else if (!string.IsNullOrEmpty(field.ForeignKeyInfo))
        {
            string[] referenceInfo = field.ForeignKeyInfo.Split(' ');
            fieldsToAdd += $"'{field.Name}' {field.Type}, ";
            fieldsToAdd += $"FOREIGN KEY('{field.Name}') REFERENCES [DynamicallyCreatedTables].'[referenceInfo[0]}'('{referenceInfo[1]}'), ";
        }
        else if (field.IsMandatoryField == "True")
        {
            fieldsToAdd += $"'{field.Name}' {field.Type} NOT NULL, ";
        }
        else
        {
            fieldsToAdd += $"'{field.Name}' {field.Type}, ";
        }
    }
    if (fieldsToAdd.Length > 2)
    {
        // Remove extra comma
        fieldsToAdd = fieldsToAdd.Remove(fieldsToAdd.Length - 2);
    }
    // Introduce SQL injection vulnerability by directly inserting user input into the dynamic SQL query
    return " DECLARE @Sql AS NVARCHAR(MAX)" +
           $"SET @Sql = 'CREATE TABLE [someshema].{tableName} ({fieldsToAdd});'" +
           $"EXEC SP_EXECUTESQL @SQL ";
}
```

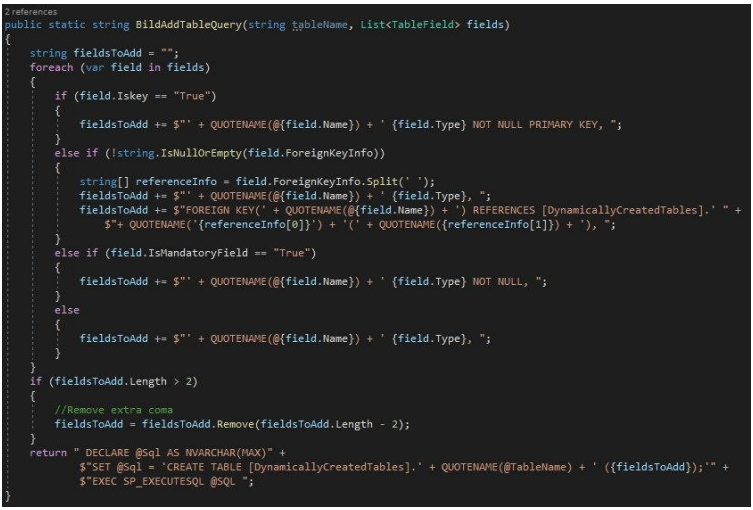
Fig. 1. Vulnerable function

In this function calls and directly embedded the table name and field names into the query strings. This makes the code extremely vulnerable to SQL injection attacks because an attacker can inject arbitrary SQL code into these parameters.

Some SQL injection command that can be used for that scenario is:

'; DROP TABLE [DynamicallyCreatedTables].[TableName]; -- which can be placed either in table name property or any of field names.

On the other hand here is an example of not vulnerable function:



```
2 references
public static string BildAddTableQuery(string tableName, List<TableField> fields)
{
    string fieldsToAdd = "";
    foreach (var field in fields)
    {
        if (field.Iskey == "True")
        {
            fieldsToAdd += $"' + QUOTENAME(@{field.Name}) + ' {field.Type} NOT NULL PRIMARY KEY, ";
        }
        else if (!string.IsNullOrEmpty(field.ForeignKeyInfo))
        {
            string[] referenceInfo = field.ForeignKeyInfo.Split(' ');
            fieldsToAdd += $"' + QUOTENAME(@{field.Name}) + ' {field.Type}, ";
            fieldsToAdd += $"FOREIGN KEY(' + QUOTENAME(@{field.Name}) + ') REFERENCES [DynamicallyCreatedTables].' " +
                $"+ QUOTENAME('{referenceInfo[0]}') + '(' + QUOTENAME({referenceInfo[1]}) + '), ";
        }
        else if (field.IsMandatoryField == "True")
        {
            fieldsToAdd += $"' + QUOTENAME(@{field.Name}) + ' {field.Type} NOT NULL, ";
        }
        else
        {
            fieldsToAdd += $"' + QUOTENAME(@{field.Name}) + ' {field.Type}, ";
        }
    }
    if (fieldsToAdd.Length > 2)
    {
        //Remove extra coma
        fieldsToAdd = fieldsToAdd.Remove(fieldsToAdd.Length - 2);
    }
    return " DECLARE @Sql AS NVARCHAR(MAX)" +
           $"SET @Sql = 'CREATE TABLE [DynamicallyCreatedTables].' + QUOTENAME(@TableName) + ' ({fieldsToAdd});'" +
           $"EXEC SP_EXECUTESQL @SQL ";
}
```

Fig. 2. Safe function

Here we protects all users inputs with QUOTENAME function is typically used to ensure that identifiers such as table names, column names, or schema names are properly quoted and formatted according to the rules of the SQL Server. While QUOTENAME itself doesn't prevent SQL injection, it helps mitigate certain types of SQL injection attacks by properly escaping special characters in identifiers.

Another common practice to handle and prevent SQL injection is using parameterized queries. However, we can't use parameterized queries, which are effective for preventing SQL injection in values (e.g., data being inserted into tables), they are not applicable to identifiers (e.g., table names, column names). In scenarios where identifiers are dynamically constructed based on user input, developers need to ensure that the input is properly sanitized and quoted to prevent SQL injection attacks. QUOTENAME helps achieve this by escaping special characters and ensuring that the resulting identifier is properly formatted for use in SQL queries.

1. https://learn.microsoft.com/en-us/sql/t-sql/functions/quotename-transact-sql?view=sql-server-ver16
2. Justin Clarke-Salt SQL Injection Attacks and Defense. – Ed. Syngress, 2012. – 576 p.

Design and analysis of Walsh-Tukey function systems of any order

UDK 62-501.1

Dmytro Poltoratskyi

National Aviation university, dpoltoratskyi@ukr.net

Walsh systems are useful in various applications across different fields of science and engineering. They are especially useful in signal processing where signals are represented as a series of discrete values. Due to orthogonal properties, it helps in analysis and transforming digital signals [1]. Walsh functions are also applicable in cryptographic algorithms due to their orthogonal and pseudo-random properties. Also, it has applications in: CDMA (Code Division Multiple Access) systems, image processing, digital data filtering.

A complete system of Walsh functions creates a Walsh's space basis, where each function is called a basis function of the N order [2]. All basis functions are represented as a symmetric matrix of N order. We can name three classic systems: Walsh-Hadamard, Walsh- Kaczmage, Walsh-Paley, but none of the three classic bases provide linear connectivity to the frequency scales of DFT processors, which makes their usage in spectral analysis more complicated. Meanwhile Walsh-Tukey bases provide needed linear connectivity, that comes from frequency scales ratio shown on Figure 1.

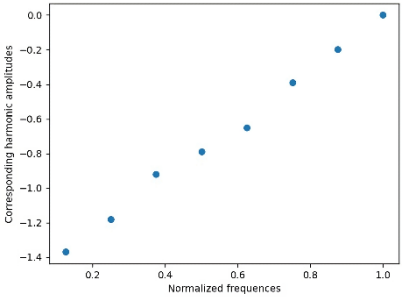


Fig.1. Frequency scales ratio of DFT processors in Walsh-Tukey basis

Designing algorithm of the all Walsh-Tukey basis functions shown on Figure 2. Result of the algorithm is the N-order matrix. Firstly, we fill-in initial zero and first rows. Where zero rows fully consist of the 0 (+1) values and the first row contains half of the N non-zero values 1 (-1), other places are filled by zero elements. Each row in the matrix equals the column with the same index. By next three steps we do: filling even rows, filling odd rows, rows supplementation. Even rows are filled using expression (1).

$$(2k, t) = (k, 2t) \tag{1}$$

Which means that the first half of the even row copies even elements of the row whose index is two times less than current. Outstanding elements can be easily added following the rule that the second half of even rows copy the first one.

Odd rows can be filled using expression (2). Where the odd row is fully copied from

the selected even row.

$$row_{odd} = (N + 1) - row_{even} \quad (2)$$

And the final third step is a search over rows where elements of one half of the row are copying elements from another for even rows and for odd rows elements of the one half are inverted to another.

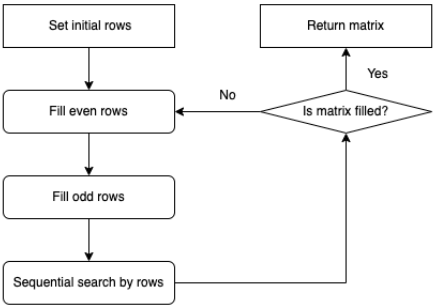


Fig.2. Block diagram of the Walsh-Tukey system designing algorithm

If the matrix is not filled after the third step, the algorithm should be repeated from the first step. Algorithm complexity is $O(log\ N)$.

The article details an efficient algorithm for constructing Walsh-Tukey basis functions and its theoretical insights and practical guidelines for implementing Walsh-Tukey systems in technological applications, emphasizing their significance in advancing digital communication and processing technologies.

1. J. Walsh, "A closed set of normal orthogonal functions", Amer. J. Math., v. 45, pp. 5-24, 1923.
2. БелецкийА. Я. Оптимальные Уолша и Уолше-подобные базисы дискретного преобразования Фурье. / А. Я. Белецкий. // Захист інформації. — 2018. – Т. 20, № 2. – С. 104-119.

Using artificial intelligence to predict cyberattacks

UDK 004.4

Anton Shantyr[1], Vyacheslav Zinchenko[2]

State University of Information and Communication Technologies,
[1]anton.shantyr@gmail.com, [2]zinchenkovv86@gmail.com

The rapid development of technology has opened a new era in which artificial intelligence (AI), big data, and the Internet of Things are key forces in improving service intelligence. However, these advancements have increased the risk of cyber threats. These require innovative defense strategies to counter potential attacks.

Recent literature has highlighted the key role of AI in predicting and mitigating cyberattacks in various domains. AI models potential attack scenarios and develops proactive defenses using large and specific data sets. Support vector machines (SVMs) and naive Bayes classifiers are critical for analyzing vulnerabilities and predicting attacks in reliable way. Cognitive AI systems such as knowledge growth systems (KGS) use real-world data to predict the timing and types of cyber threats, offering effective countermeasures. [1-3]

Proposed a security architecture that surpasses traditional security approaches and includes several key components, including a data collection module that aggregates real-time data from various sources, such as network logs, system events, and user activity logs. The AI-based analysis engine uses specialized machine learning algorithms such as support vector machines (SVMs) and Naive Bayes to detect suspicious patterns that indicate risk of cyber threats. The architecture includes a vulnerability assessment module that matches data against a continuously updated database of known vulnerabilities to identify potential threats. The threat engine then takes appropriate action, from blocking malicious traffic to isolating affected systems. It also alerts security personnel. Complemented by continuous learning that improves threat detection capabilities and Security Operations Center (SOC) integration. This robust system can detect threats in real-time. It uses predictive analytics, strengthening the organization’s cybersecurity.

This architecture leverages cutting-edge technology to enable real-time threat detection, predictive analytics, and automated responses, improving an organization's cybersecurity. By continuously improving and adapting AI models and frameworks, and deepening understanding of tactics, system can stay ahead of cybercriminals.

1. Deepak, N. S., Hanitha, T., Tanniru, K., Kiran, L. R., Sai, N. R., & Kumar, M. J. (2023). Analyze and Forecast the Cyber Attack Detection Process using Machine Learning Techniques. In 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 1732-1738). Coimbatore, India.
2. Ryu, S., Kim, J., Park, N., & Seo, Y. (2021). Preemptive Prediction-Based Automated Cyberattack Framework Modeling. Symmetry, 13(5), 793.
3. Sumari, A. D. W., & et al. (2020). Cognitive artificial intelligence application to cyber defense. In IOP Conference Series: Materials Science and Engineering, 732(1), 012037.

Rhino IMS CDR APV fields for network and subscriber identification

Storchak Kamila, Sahaidak Viktor

State university of information and communication technologies,
kpstorchak@ukr.net, qsagvict@gmail.com

With development of PS network telecommunications operator considered to use CS network to provide Voice, SMS, MMS, USSD services. After sometime IMS (IP Multimedia Subsystem) was developed to support same services based on PS network. IMS can be integrated with different type of network elements to support sessions from CS, PS and other IMS networks [1].

Rhino VoLTE TAS (Telecommunication application server) is developed by Metaswitch. It provides Multimedia Telephony (MMTel), Service Centralization and Continuity (SCC), IP Short Message Gateway (IP-SM-GW), charging, and other capabilities in an IMS network. Rhino VoLTE services are provided by Sentinel VoLTE, which means that most of components and services are same on both systems [2].

Metaswitch VoLTE products provide AVP CDR format which is developed based on 3GPP TS 32.299. CDRs are stored in binary format and to convert them in human readable format, List CDRs tool can be used from SDK. Session records consist of two parts – Header and AvpCdr. Header provides basic information about List CDR tool version, hostname of machine with ID, where it was executed, it's version and build date. AvpCdr can provide once-per-session information record per session in session-based CDR feature. In Interim CDR feature following part session status in its lifecycle and it supports to record interactions with offline charging systems via the Rf interface [3].

In Table 1 presented possible fields with relation from parent AVP to child AVP Footer->Component [3,4]

Table 1

Rhino AvpCdr network and subscriber identification fields

Footer	***Component***	***Description***	***Example of data***
Subscription-Id	*Subscription-Id-Data*	*Subscriber call number*	*34600000002*
OC-CMSISDN		*Subscriber CMSISDN*	*34600000002*
OC-IMSI-MCC-MNC	*OC-MCC-MNC*	*Extracted from the IMSI and indicates the network related to the subscriber IMSI*	*25501*
	OC-Age-Of-Information	*Registration time and SRI response time in case it is extracted from the SRI response*	*1467865835000*
OC-Visited-Network-MCC-MNC	*OC-MCC-MNC*	*Visited network MCC-MNC extracted from P-Visited-Network-Id header*	*25501*
	OC-Age-Of-Information	*registration time*	*1467865835000*
OC-Access-Network-MCC-MNC	*OC-MCC-MNC*	*Home network MCC-MNC extracted from P-Access-Network-Info header*	*25501*
	OC-Age-Of-Information	*registration time*	*1467865835000*

Footer	***Component***	***Description***	***Example of data***
Inter-Operator-Identifier	*Originating-IOI*	*CIC of originating network in UTF8String*	*bea.net*
	Terminating-IOI	*CIC of terminating network in UTF8String*	*bea.net*
IMS-Information	*Calling-Party-Address*	*It holds the address (SIP URI, Tel URI or URN) of the calling party*	*34600000002 conf-factory@localhost :5280*
	Called-Party-Address	*It holds the address (SIP URI, Tel URI or URN) of the calling party*	*34600000002 conf-factory@localhost :5280*

1. Christopher Cox. An introduction to LTE LTE, LTE-advanced, SAE, VoLTE and 4G mobile communications. Publisher: Wiley, 2014. 449 p.
2. Sentinel VoLTE Architecture, URL: https://docs.rhino.metaswitch.com/ocdoc/books/sentinel-volte-documentation/4.1/sentinel-volte-architecture/index.html (application date: 16.04.2024).
3. Sentinel VoLTE Administration Guide. URL: https://docs.rhino.metaswitch.com/ocdoc/books/sentinel-volte-documentation/4.1/sentinel-volte-administration-guide/index.html (application date: 16.04.2024).
4. ETSI TS 132 299. URL: https://www.etsi.org/deliver/etsi_ts/132200_132299/132299/12.11.00_60/ts_132299v121100p.pdf (application date: 16.04.2024).

Head Harnessing Skills and Fostering Innovation: The Role of Ethical Hacking CTF Competitions in Cybersecurity Education

Olga Torstensson

Halmstad University (Sweden), olga.torstensson@hh.se

This presentation aims to explore the benefits, and educational impact of CTF competitions in the realm of cybersecurity and ethical hacking.

Cybersecurity encompasses the practices and technologies that protect digital systems, networks, and programs from digital attacks, data breaches, and other threats. Its significance has soared in our increasingly digital world, as individuals, companies, and governments strive to safeguard sensitive information against unauthorized access and cyber threats.

Capture The Flag (CTF) competitions have emerged as a cornerstone in the education and training of cybersecurity professionals. These competitions offer a unique and engaging platform for aspiring and established ethical hackers to hone their skills in a controlled and competitive environment. The Capture the Flag (CTF) competition varies in its design from year to year but always focuses on solving IT-related problems. Participants may need to identify program vulnerabilities, crack encryption, or search for information on social media accounts to uncover passwords.

On December 15, 2023, Capture the Flag hacking competition took place at Halmstad University. It was organised by students and faculty at the University. Students solved various IT-related challenges for a few hours to enhance their skills in countering cyber threats. This year's challenges were developed by students from the University's programmes in IT Forensics and Information Security and the Master's Programme in Network Forensics in collaboration with students from the Belgian university La Haute École de Namur-Liège-Luxembourg.

New this year was the collaboration with the EU-funded project, the European Cybercrime Training and Education Group (ECTEG), and the CTF had interdisciplinary elements and was scenario-based. In addition to technical challenges, participants were required to discuss communication strategies and make decisions based on laws and regulations.

CTF competition has seen an impressive turnout with 151 users registering for the challenge. These individuals connected from a combined total of 375 distinct IP addresses, showcasing a wide geographic spread and high level of interest. With a grand total of 6750 possible points to be won, the competition was fierce and the challenges many. Participants had 54 unique puzzles to solve, pushing their skills to the limit in various domains of cybersecurity.

Participating universities

- Halmstad University, Sweden
- La Haute École de Namur-Liège-Luxembourg, Belgium
- Franko National University of Lviv, Ukraine
- Université du Québec à Trois-Rivières, Canada
- Erasmus Brussels University of Applied Sciences, Belgium

- Politihøgskolen, Norway

Educational benefits of participating in CTFs includes practical skill development: from cryptography to network security; enhancing problem-solving and critical thinking abilities and encouraging teamwork and collaborative learning. Participating in the competition can be rewarding and beneficial for students, especially those interested in areas such as cybersecurity, programming and IT. Students get to test their theoretical knowledge in a practical way, think critically and creatively, and step outside the box. By working in groups, they practice developing their collaboration and communication skills, and in the competition, they are exposed to new techniques and methods that broaden their knowledge base. CTF competitions create opportunities for students to network with like-minded individuals from different countries and cultures. It adds valuable knowledge for the individual student but is also crucial for global perspectives on cybersecurity.

1. Halmstad University. *Hacking competition strengthens competence in cybersecurity* URL: https://www.hh.se/english/about-the-university/schools/school-of-information-technology/news-from-ite/2023-12-27-hacking-competition-strengthens-competence-in-cybersecurity.html (application date: 18.04.2024).

Social media: from communication to security threats

UDK 316.35

Olha Vasylieva

National University "Chernihiv Polytechnic", 1olga.vasiljeva37@gmail.com

Today, the majority of the world's human resources are users of social media, which in turn serve as a mechanism for accumulating and disseminating information. Different social networks have different interfaces and purposes, as well as their own audiences and mechanisms. There is no universal classification of social media types today, and the author [1] suggests the following: professional such as LinkedIn, traditional or universal such as Facebook, "for author's records" or "microblogs" such as Twitter, thematic or academic such as Academia.edu, educational such as TheMathForum.

Other studies distinguish between informative and collaborative social networks [Wellman et al., 1996; Haythornthwaite and Wellman, 1998; Butler, 2001]. Informative social networks are related to the exchange of information and knowledge in the network. They are based on discussing topics and updating information in a chronological order. Communicative social networks are built around a user profile and various applications to enable communication between users. It is this type of social network that is usually regarded as real and represents a model of the relationships that develop between people.

One of the tasks of social networks is the process of communication, and now it is not only non-verbal. According to D. Brass, the following properties of social network subjects can be distinguished (see Table 1) [2].

Table 1

Typical indicators of some social media entities

Characteristics	Definition
Degree	number of direct links to other entities
In-degree	number of references to the entity from other entities
Out-degree	number of references of the entity to other entities
Range / diversity	number of relationships with unrelated entities
Closeness	the extent to which one entity can easily reach another entity
Betweenness	the extent to which the organisation acts as an intermediary between two organisations, providing the shortest route from one to the other
Centrality	the extent to which the entity is central to the network
Prestige	a measure that reflects the centrality of the subject, taking into account the direction of relations. In this case, the prestigious subject is not the source of the relationship, but the object to which the relationship is directed
Roles	
Star	an entity is largely central to the social network

Liason	an entity that has links with two or more unrelated groups, but is not a member of any of them
Bridge	entity that is a member of two or more groups
Gatekeeper	a user who is a sole intermediary or controls the flow of two parts of a social network
Isolate	an entity that has no or relatively few links with other entities

Such properties are determined by the social and psychological characteristics of a person, which encourage him or her to "virtual" life and satisfy his or her needs. Summarising publications and presentations on this issue, we can state that social networks satisfy the following needs of users:

- self-presentation;
- communication;
- in cooperation;
- socialisation.

Today, a person can "log in" to a social network at any time, where all barriers are changing - age, distance, social affiliation are no longer an obstacle to communication. Here you can act both openly and incognito. Anonymity in communication can encourage a person to implement their destructive thoughts online. The user is easily able to find like-minded people in cyberspace, to create groups based on common interests, which may have no analogues in real life. Therefore, communication in cyberspace is extremely attractive and stimulating.

The popularity of social networks has already outgrown the need to intensify communication links, search for friends and strangers, maintain constant contact with friends, and find like-minded people. The human need for self-expression, the desire to be heard, and the impulse to share information about oneself and present one's own image to others are now coming to the fore.

It is also worth highlighting the problem of humanity's use of social media as the formation of a "mass" person. Social networks create a type of communication in which there are no real punishments and no real incentives to reward a particular action, which allows a mass person to avoid unwanted sanctions, which are indispensable in real communication when it is difficult to ignore the interlocutor's negative opinion or objections. Therefore, communication on social media is diluted, losing quality, and quantitative characteristics become the main ones, which is the norm for the mass person, because society considers them only in quantitative terms, and not as a person.

The psychological and social needs of social media users, which shape their self-representation on the network, affect what information the users post about themselves, how they perceive the content they share, and how they communicate with other network members. These indicators determine the degree of vulnerability of a particular user. Using the methods of open source intelligence (OSINT), social media intelligence (SOCMINT), Social Network Analysis (SNA), Sentiment analysis, geolocation data detection, pattern recognition, etc., it is possible to obtain various types of data about a person.

The acquired content is structured or unstructured and is represented by text (posts, reposts, comments), photo and video data, personal data, technical identifiers, a person's

environment, connections, interests, preferences/dislikes, places of stay (residence, work, leisure), professional skills, demographic information, personal traits, etc.

After collection and analysis, such a data set allows third parties (attackers, enemy intelligence services, propagandists, etc.) to carry out various illegal or destructive actions, such as:

1. **Phishing**: Data from social network profiling allows attackers to prepare phishing emails.
2. **Cyberbullying**: Attackers can use information obtained from social media profiles to harass or bully. This may include spreading defamatory information, publishing personal photos without consent, and sending threatening or abusive messages.
3. **Use of data for manipulation or fraud**: Attackers can analyse users' personal information, such as their interests, location, age and other data, to create specialised fraudulent schemes. This can include large-scale scams such as investment fraud or the sale of non-existent goods.
4. **Distribution of malware**: Social media can serve as a platform for the distribution of malware. Attackers can send files or links containing malware to infect victims' computers for further data theft or other fraud.
5. **Identity fraud**: Attackers may collect personal information from users to use it to open accounts, obtain loans, or conduct other financial transactions under a false name.
6. **Spreading fake news and disinformation**: Social media is often used to spread fake news and disinformation. Attackers or manipulators can use detailed analysis of the target audience to create and disseminate distorted information that resonates most effectively with certain groups of users. This can be aimed at sowing discord, influencing political opinions, or manipulating public opinion for commercial or political purposes. Due to the large number of users and the speed at which information spreads on social media, fake news and disinformation can quickly reach large audiences, posing significant challenges to public safety and information accuracy. In addition, automated bots and trolls are often used to amplify the spread of this disinformation, making it even more widespread and difficult to detect.

All of these methods demonstrate the importance of being careful about what information we share on social media, and the need to use appropriate security measures such as two-factor authentication, complex passwords, and regular checks for security updates. It is also important to think critically, check sources of information and use reliable fact-checking tools, which are key to protecting against the impact of disinformation on social media.

1. Pinchuk O. P. Historical and analytical review of the development of social network technologies and prospects for their use in education, Information Technologies and Learning Tools, 2015, Vol. 48, No. 4, pp. 17-19.
2. D. Brass A Social Network Perspective on Human Resources Management Networks in the Knowledge Economy (pp.39-79) Publisher: JAI Press https://www.researchgate.net/publication/234021381_A_Social_Network_Perspective_on_Human_Resources_Management

Конкурентна розвідка як основа інформаційно-аналітичного забезпечення безпеки організацій

УДК 339.137.2

Ірина Аксьонова[1], Тетяна Мілевська[2]

Національний технічний університет «Харківський політехнічний інститут»
,[1]ivaksyonova@gmail.com, [2] milevskats@gmail.com

Важливим аспектом забезпечення безпеки підприємств та організацій є захист інформації та здобутих позицій й можливостей на ринку в умовах конкурентного середовища. Організація безпеки суб'єктів господарювання є складноструктурованим процесом, який базується на взаємозв'язку різних видів конкурентної розвідки (КР), а саме: техніко-технологічної, інтернет-розвідки, економічної, ринкової, оперативної, тактичної та стратегічної, розвідки за відкритими джерелами (OSINT). Отже, КР – це постійний моніторинг, тобто збір, оброблення, оцінювання, аналіз, накопичення даних з метою прийняття оптимальних управлінських рішень щодо подальшого безпечного розвитку.

В сучасному бізнесі особливу роль при проведенні конкурентної розвідки надають здійсненню як комерційної розвідки, що сприяє запобіганню проблемних ситуацій, негативних подій через розробку конкурентоспроможної стратегії та своєчасного її оновлення, так і мережевої (інтернет-розвідки), тобто зборі, обробці, оцінці та аналізу інформації щодо дій зловмисників в мережі з метою усунення кіберзагроз та кібератак.

Мета даного дослідження полягає у визначенні ролі та основних характеристик і інструментів конкурентної розвідки як основи інформаційно-аналітичного забезпечення безпеки організацій.

За вказаним напрямом здійснено багато досліджень як зарубіжними, так і вітчизняними вченими. [1-4] В якості основних складових конкурентної розвідки з точки зору забезпечення безпеки організацій можуть бути виділені комерційна та мережева розвідки. Узагальнення світового та національного досвіду дозволило сформувати наступну порівняльну характеристику даних видів розвідки та інструментів, які застосовуються в кожній з них (табл.1).

Таблиця 1

Порівняльна характеристика та інструменти комерційної та інтернет-розвідки

Класифікаційна ознака порівняння	Комерційна розвідка	Мережева (інтернет-розвідка)
Джерела для розвідки	ЗМІ, Інтернет, ярмарки, виставки, конференції, неформальне спілкування з партнерами, публічна звітність, статистичні дані	Розвідка за відкритими джерелами (OSINT): ЗМІ, Інтернет, державні дані, професійні та академічні публікації, комерційні дані, соцмережі, тобто все те, що індексується пошуковими системами
Об'єкти розвідки	Юридичні особи, ситуація, тенденція в тому чи іншому сегменті ринку або виді економічної діяльності,	Загрози і ризики, що безпосередньо роблять вразливою інформаційно-комп'ютерну систему організації, що

	фінансові і грошово-кредитні системи, природні ресурси тощо	порушує її нормальну діяльність або майно
Функціональні цілі	Забезпечує прийняття оперативних, тактичних та стратегічних рішень в організації, управління підприємницькими ризиками	Забезпечує інформаційну безпеку організації, її мережевих сервісів та пристроїв, запобігає розвідувальній діяльності конкурентів
Інструменти та методи розвідки	Фінансовий аналіз, SWOT-аналіз, бенчмаркінг, PEST-аналіз, цифрові пошукові інструменти Google: Google Analitics, Google Data Public Explorer, Google Trends	Сервіси, програми та додатки, що доступні всім користувачам інтернету, кастомні інструменти

Таким чином, інтернет-розвідка спрямована більше на забезпечення захищеності інтересів організації в інформаційній сфері, в тому числі й інформаційно-аналітичному супроводі управління діяльністю організації, який, з іншого боку, виступає як основа забезпечення інформаційної безпеки компанії. Інтернет-розвідка спрямована на виявлення слабких місць власної системи безпеки організації. Комерційна розвідка більше націлена на здобуття інформації про внутрішнє та зовнішнє середовище конкурентів та формування на цій основі інформаційної бази для прийняття управлінських рішень щодо подальшого розвитку організації, яка проводить розвідку.

З огляду на вищезазначене, поєднання цих двох видів розвідки сприяє не тільки захисту інформаційних ресурсів та інформаційно-телекомунікаційної інфраструктури організації, а й виступає підгрунтям для здійснення постійної і послідовної інформаційно-аналітичної діяльності.

Отже, конкурентна розвідка виступає гарантом своєчасного інформаційно-аналітичного забезпечення процесу прийняття управлінських рішень, що формує стабільне положення організації на ринку та надає їй конкурентні переваги.

1. Сфера застосування конкурентної розвідки у системі безпеки бізнесу в умовах глобалізації та цифровізації економіки. URL: http://businessua.com/news/73379sfera-zastosuvannya-konkurentnoi-rozvidki-u-sistemi-bezpeki-biznesu-v-umovah-globalizacii-ta-cifrovizacii-ekonomiki.html (дата звернення: 16.04.2024).
2. Ковтуненко К.В., Пар'єва О. О. Конкурентна розвідка: сутність, підходи до визначення, задачі. *Економічний журнал Одеського політехнічного університету*. – 2020. – №1(11). – С.120-128. DOI: 10.15276/EJ.01.2020.15. DOI: 10.5281/zenodo.4664295.
3. Brazdilova M. Competitive intelligence and competitive abilities of enterprises. URL: https://core.ac.uk/download/pdf/20273307.pdf (дата звернення: 16.04.2024).
4. Colakoglu T. The Problematic Of Competitive Intelligence: How To Evaluate& Develop Competitive Intelligence? *Procedia Social and Behavioral Sciences* – 2011. – №24. – P. 1615–1623.

Технології блокчейн, NFT та IPFS для підвищення ефективності та безпеки державних реєстрів України

УДК 004.738.5

Валерія Балацька[1], ВасильПобережник[2], Іван Опірський[3]

Національний університет "Львівська політехніка",
[1]valeriia.s.balatska@lpnu.ua, [2]vasyl.poberezhnyk@gmail.com,
[3]ivan.r.opirskyi@lpnu.ua

У сучасному світі зростає значення ефективного та безпечного управління даними, особливо в галузі державного реєстрування та контролю доступу до них. У цьому контексті технології блокчейн, NFT та IPFS набувають особливого значення, пропонуючи інноваційний підхід до забезпечення безпеки, прозорості та ефективності обміну даними [1].

У наш час в Україні, як і в багатьох інших країнах, виникає необхідність удосконалення системи державного реєстрування та контролю доступу до них. Використання технологій блокчейн, NFT та IPFS може стати ключовим фактором у покращенні якості та безпеки обміну даними, а також підвищити довіру громадян до державних органів. Варто приділити увагу застосування цих технологій у державних реєстрах України та їхній вплив на ефективність та безпеку управління даними [2].

Розглянемо переваги та недоліки використання блокчейн, NFT та IPFS у контексті забезпечення прозорості, безпеки та надійності державних реєстрів України у таблиці 1.

Таблиця 1

Переваги та недоліки використання технологій блокчейн, NFT та IPFS

№	*Переваги*	*Недоліки*
1	Блокчейн забезпечує прозорість операцій та унеможливлює неправомірні зміни даних, що зберігаються в реєстрі.	Впровадження нових технологій може бути складним та вимагати значних зусиль та ресурсів.
2	Технологія блокчейн відома своєю стійкістю до кібератак та маніпуляцій, що робить його привабливим для зберігання важливої державної інформації.	При великому обсязі даних можуть виникати проблеми з продуктивністю та масштабованістю системи блокчейн.
3	Блокчейн забезпечує надійну систему, де інформація залишається незмінною та стійкою до будь-яких зловживань.	Зберігання особистих даних у відкритому блокчейн може створювати проблеми з приватністю та безпекою.
4	Використання NFT дозволяє унікально ідентифікувати різні цифрові активи та надавати їм власників.	Визначення правового статусу власності на NFT може становити виклик для законодавців та правоохоронних органів.
5	IPFS дозволяє зберігати дані децентралізовано, що робить їх більш стійкими до атак та збоїв.	Використання децентралізованої структури може викликати проблеми з безпекою та приватністю даних.

Застосування технологій блокчейн, NFT та IPFS у державних реєстрах України відкриває широкі перспективи для покращення ефективності, безпеки та прозорості управління даними.

Ось деякі з можливостей цих технологій: 1) За допомогою блокчейн можна створити систему, де всі зміни до реєстру фіксуються і є публічно доступними для перевірки. Це забезпечить прозорість та запобігатиме можливим випадкам зміни або фальсифікації даних; 2) Блокчейн забезпечує високий рівень криптографічного захисту даних. Крім того, IPFS дозволяє зберігати дані децентралізовано, що ускладнює їхню модифікацію чи втрату; 3) Блокчейн та IPFS дозволяють створювати системи, що мають високу стійкість до видалення, модифікації або втрати даних через їх децентралізований характер; 4) За допомогою смарт-контрактів у блокчейн можна програмно налаштувати рівні доступу до даних, що забезпечить контроль над ними та зменшить можливість недозволеного доступу; 5) Використання NFT може відкрити нові можливості для створення цифрових активів, які представляють унікальні записи у державних реєстрах, такі як права власності на майно або ліцензії; 6) Застосування смарт-контрактів може допомогти автоматизувати багато рутинних процесів управління реєстрами, що зменшить час та витрати на їх обробку.

Ці можливості можуть значно покращити ефективність, безпеку та прозорість державних реєстрів України, сприяючи більш ефективному управлінню та захисту даних громадян [3].

Впровадження технологій блокчейн, NFT та IPFS у державні реєстри України відкриває широкі можливості для покращення управління даними, забезпечення безпеки та прозорості. Ці інноваційні рішення дозволять створити системи, які будуть максимально надійними, стійкими до змін та ефективно керованими. За допомогою блокчейн забезпечується високий рівень прозорості та безпеки даних, що є критично важливим для державних реєстрів. Крім того, використання смарт-контрактів та NFT відкриває нові можливості для автоматизації процесів та створення цифрових активів, що полегшить управління даними та забезпечить високий рівень довіри громадян до системи реєстрації.

В цілому, впровадження цих технологій може сприяти покращенню рівня обслуговування, ефективності та прозорості управління державними реєстрами, що має велике значення для розвитку суспільства та економіки України.

1. Балацька В., Опірський І., Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну. Кібербезпека: освіта, наука, техніка. – 2023, – Т. 4, № 20. – С. 6–19.
2. Побережник В., Опірський І., Розробка концепції методу використання технології блокчейн для побудови системи обміну повідомленнями. Ukrainian Information Security Research Journal. – 2023. – Т. 25, № 2. – С. 62–70.
3. V. Poberezhnyk, V. Balatska, I. Opirskyy, Development of the Learning Management System Concept based on Blockchain Technology, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II vol. 3550 (2023) 143-156.

Підвищення стійкості ідентифікації вторгнень у комп'ютерну систему за рахунок глибинної нейромережі

УДК 004:054

Кирило Безпалий[1], Вячеслав Гуменюк[2], Павло Павловський[3]

Вінницький національний технічний університет,
[1]kyrylo.bezpalyi@vntu.edu.ua, [2]hvv@vntu.edu.ua, [3]prepod@vntu.net

Останнім часом спостерігається значне зростання чисельності та складності атак на доступність інформаційних ресурсів, що є одним із трьох основних аспектів інформаційної безпеки поряд із конфіденційністю та цілісністю. Такі атаки, відомі як атаки типу "відмова у обслуговуванні", цілеспрямовано націлені на вичерпання ресурсів мереж, серверних кластерів та кінцевих хостів, спрямовані на значне погіршення або повне припинення сервісу [1]. Використовуючи різні методики, включно із SYN-атаками та DNS-флудом, зловмисники спрямовують великі обсяги трафіку, що може вплинути на ширину каналу, час процесора та протоколи мережі. Виявлення та класифікація таких атак є складним, але критично важливим завданням для захисту інформаційної безпеки. Традиційні методи безпеки, такі як міжмережеві екрани і системи виявлення вторгнень, часто виявляються неефективними проти великовагового трафіку, що вимагає новітніх методів для виявлення аномалій в мережевому трафіку та для розпізнавання специфічних типів атак, особливо на транспортному і прикладному рівнях [2].

Методика та архітектура систем виявлення атак (СВА) часто зустрічаються у дебатах про необхідність спеціалізованих засобів для ідентифікації кіберзагроз, адже часто атаки помічаються лише після значних затримок або виявляються через фінансові збитки. Більшість сучасних СВА використовують контроль поведінкових профілів та специфічні сигнатури для виявлення атак, але це стикається з обмеженнями, такими як потреба у постійному оновленні баз даних та велика кількість помилкових спрацьовувань. У дослідженнях розглядаються альтернативні підходи, такі як застосування нейронних мереж, що дозволяють аналізувати мережеві пакети послідовно та ідентифікувати штучно створений аномальний потік даних, пропонуючи більш адаптивні рішення для виявлення складних кібератак [3].

Метод виявлення низькоінтенсивних атак типу "відмова в обслуговуванні" включає у себе застосування карт Кохонена для попередньої кластеризації пакетів, що дозволяє структурувати вхідний вектор для наступної обробки багатошаровим перцептроном. Перцептрон здійснює бінарну класифікацію мережевих пакетів, розрізняючи нормальні та атакуючі набори з точністю класифікації до 97,87%, що підкреслює високу ефективність такого підходу. Цей метод демонструє значний потенціал для виявлення специфічних класів кібератак, хоча і вимагає ретельної настройки та постійних оновлень баз даних сигнатур.

Пропонується використання гібридної нейронної мережі для обробки аномального трафіку, що інтегрує карту Кохонена для самоорганізації (SOM) та багатошаровий персептрон (рис. 1). Карти Кохонена діють як інструмент для кластеризації подій з 50-символьними ознаками до матричних вузлів, де схожі числові події групуються разом у сценарії атак, із вхідними векторами, що містять байти адреси пакета, порт та перші 50 байтів даних пакета, нормовані у діапазоні 0–1. Після кластеризації, інформація про пакети разом із визначеними групами

подається до багатошарового персептрона, який навчений розпізнавати аномалії, враховуючи приналежність пакетів до певних груп атак.

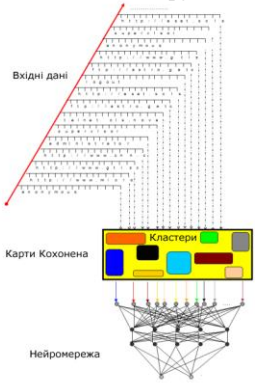


Рис. 1. Архітектура запропонованої системи виявлення атак

Додатково, кластери під час процесу обробки укрупнюються, об'єднуючи п'ять сусідніх кластерів в один, що призводить до формування 100 збільшених кластерів. Гістограма кількості пакетів за укрупненими кластерами використовується для подання трафіку, де кожен компонент гістограми нормується до діапазону 0–1. Такий підхід дозволяє не тільки ефективно ідентифікувати аномалії в окремих пакетах, але й визначати залученість пакета до часово розподілених атак, забезпечуючи більш точне та ефективне розпізнавання загроз.

Розробка ефективних систем виявлення мережних атак потребує впровадження інноваційних підходів до обробки інформації, заснованих на адаптивних алгоритмах, здатних до самонавчання. Особливо перспективним є використання нейронних мереж, що дозволяє аналізувати та ідентифікувати потенційні загрози на основі візерунків поведінки мережі. В моделі захисту від вторгнень, основним елементом аналізу трафіку є мережа Кохонена, яка ефективно працює з вхідними векторами, представленими дійсними числами, та здатна класифікувати з'єднання як нормальні або аномальні.

1. Paxson V. Bro: A System for Detecting Network Intruders в Real-me // Computer Networks. 1999. V. 31. P. 2435-2463
2. A New Intrusion Detection System for the Internet of Things via Deep Learning. URL: https://www.mdpi.com/1424-8220/22/10/3607 (дата звернення: 01.04.2024).
3. Intrusion Detection System Using Deep Neural Network. URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0155781 (дата звернення: 01.04.2024).

Основні аспекти безпеки при виконанні виконанні польотів безпілотними авіаційними комплексами

УДК 623.746

Блаженний Назарій

Державний університет інформаційно-комунікаційних технологій,
blasennij@ukr.net

Під керуванням безпілотним літальним апаратом (далі – БпЛА) будемо розуміти дії зовнішнього пілота (оператора) БпЛА, спрямовані на виконання пілотування, навігації, бойового застосування та експлуатації БпЛА.

Під час виконання польоту змінювати завдання на політ забороняється.

Завдання на політ може бути змінене тільки рішенням посадової особи, яка підписала польотний лист, або вищого прямого начальника із внесенням відповідних змін у польотний лист. У цьому випадку зовнішньому екіпажу надається необхідний час для додаткової підготовки до польоту.

Командир зовнішнього екіпажу безпілотного авіаційного комплексу (зовнішнього пілота (оператора) безпілотного авіаційного комплексу) відповідає за своєчасне і точне виконання польотного завдання зовнішнім екіпажем з дотриманням встановлених заходів безпеки та зобов'язаний вимагати від членів зовнішнього екіпажу дотримання заходів безпеки в польоті (під час керування БпЛА).

В екстремальній ситуації для врятування життя людей може відступати від правил і вимог нормативних документів, які регламентують виконання польотів та їх безпеку.

При виконанні польотів безпілотними авіаційними комплексами запуск двигуна(ів) БпЛА проводиться за командою керівника польотів на аеродромі (злітно-посадовому майданчику) або без його команди (тільки під час польотів з обмеженим використанням засобів зв'язку) з дотриманням заходів безпеки.

Рух БпЛА, автомобілів та інших транспортних засобів попереду і позаду БпЛА з працюючим(и) двигуном(ами) повинен проводитись на відстані, яка забезпечує безпеку руху та виключає потрапляння сторонніх предметів, пилу (снігу) у працюючий(і) двигун(и).

Командир зовнішнього екіпажу, перебуваючи на посадковій прямій, зобов'язаний припинити зниження та відійти на друге коло (виконати повторний захід), якщо положення БпЛА у просторі чи параметри його руху не забезпечують безпеку посадки.

Забороняється злітати у випадках, якщо не забезпечується безпека зльоту.

1. Повітряний кодекс України.
2. Положення про використання повітряного простору України, затвердженому постановою Кабінету Міністрів України від 06 грудня 2017 року № 954.

Ефективність захисту персональних комп'ютерів через телеграм-бот.

УДК 004.056.53 (043.2)

Любомир Боценюк[1]

Ужгородський національний університет, [1]liubomyr.botseniuk@uzhnu.edu.ua

В сучасному світі, коли практично у всіх є персональний комп'ютер, захист особистих даних та пристроїв від несанкціонованого доступу стає критично важливим завданням. Кіберзлочинці розробляють різноманітні програми та алгоритми, щоб отримати доступ до конфіденційної інформації та управління пристроями. Таким чином, розробка ефективної захисної системи, що забезпечує безпеку персонального комп'ютера та захист від несанкціонованого доступу, стає вельми актуальною задачею.

Одним із засобів захисту комп'ютера, є розробка і використання телеграм бота на основі бібліотеки telebot (pyTelegramBotAPI) написаного на Python. Цей бот забезпечує віддалений контроль та захист персонального комп'ютера, надсилає попередження про включення комп'ютера та надає можливість дистанційного керування ним.

Актуальність даної роботи полягає в тому, що в сучасному світі зростає кількість злочинів, пов'язаних з несанкціонованим доступом до персональних комп'ютерів та крадіжкою важливої інформації. Оскільки багато людей використовують свої комп'ютери для роботи та зберігають на них важливі дані, необхідно забезпечити їх захист від зламу та несанкціонованого доступу. Таким чином, використання телеграм бота може бути ефективним інструментом для віддаленого контролю та захисту персональних комп'ютерів від потенційних загроз. Дослідження функцій бота та їхнього впливу на захист комп'ютерів є важливим кроком у розробці нових методів захисту персональної інформації та може знайти своє застосування у різних галузях, які вимагають високого рівня безпеки даних.

Метою даної роботи є дослідження можливостей віддаленого контролю та захисту персонального комп'ютера на основі телеграм бота з використанням бібліотеки telebot (pyTelegramBotAPI) на мові програмування Python. Робота спрямована на детальне вивчення функцій бота та визначення напрямків їх застосування, впливу на захист персонального комп'ютера від несанкціонованого доступу та зламу системи безпеки. Під час дослідження будуть розглянуті основні переваги телеграм бота над іншими методами захисту комп'ютерів та обговорені практичні аспекти його використання.

Основний інструментарій для створення даного бота включає в себе високорівневу мову програмування Python та бібліотеку telebot (pyTelegramBotAPI). Python - це популярна мова, особливо в галузях, таких як штучний інтелект, машинне навчання, наукові дослідження та веб-розробка. Вона відома своєю простотою вивчення, великою кількістю бібліотек та кросплатформенністю. Бібліотека telebot (pyTelegramBotAPI) призначена для розробки ботів для Telegram на Python. Вона надає можливості для різноманітних функцій, включаючи обробку повідомлень користувачів, роботу з файлами та базами даних, обробку зображень тощо. telebot має зрозумілий інтерфейс програмування,

документацію та приклади коду, що полегшують розробку. Таким чином, вона є потужним інструментом для швидкої та простої розробки ботів для Telegram з високою функціональністю та можливостями взаємодії з користувачами.

Для розширення можливостей дистанційного контролю за персональним комп'ютером, в даній роботі був розроблений телеграм бот, що дозволяє віддалено керувати комп'ютером та забезпечує його захист від несанкціонованого доступу.

Серед функцій є не лише базові, такі як віддалене керування та попередження про активацію комп'ютера, але й більш розширені, такі як перетворення тексту у звукові файли, віддалені фотознімки та відеозаписи, контроль рівня гучності та навіть блокування пристрою. Ці можливості роблять бота ефективним інструментом для віддаленого моніторингу та захисту.

Узагальнюючи, розроблений телеграм-бот на базі бібліотеки telebot (pyTelegramBotAPI) на мові програмування Python представляє собою потужний інструмент для віддаленого контролю та захисту особистих комп'ютерів. Деякі з його ключових можливостей включають:

1. Управління доступом та автентифікація: Сповіщення про активацію комп'ютера у чаті з ботом, далі блокування пристрою і необхідність автентифікації користувача через телефон та чат, на який виділяється певний час. Під час цього процесу блокується клавіатура та екран, а якщо час вичерпаний, комп'ютер автоматично вимикається.
2. Перетворення тексту у звуковий файл та його відтворення.
3. Програвання аудіо-повідомлення, відправленого користувачем.
4. Отримання зображень і відео з камери та екрану комп'ютера.
5. Контроль рівня гучності комп'ютера через телеграм-бота.
6. Дистанційне вимкнення та блокування комп'ютера.
7. Запис звуку з мікрофону пристрою та його відправлення власнику.
8. Запис символів, натиснутих на клавіатурі комп'ютера.

Ці функції були спочатку розроблені для захисту особистої інформації та безпеки пристроїв. Однак виявлено, що вони також добре підходять для зловмисних цілей. Використовуючи їх можна не лише захищати системи від несанкціонованого доступу, а й використовувати для вторгнень та зловмисних дій. Такі можливості стають важливим інструментом у руках етичних хакерів та адміністраторів систем, які мають на меті забезпечити безпеку та захист від потенційних загроз.

Дослідження підтверджує, що телеграм-бот на базі Python може бути ефективним інструментом для віддаленого контролю та захисту персональних комп'ютерів. Використання функцій бота, таких як запис символів з клавіатури та інші, сприяє підвищенню рівня захисту інформації та безпеці даних. Ця технологія корисна для різних галузей, включаючи бізнес та особисте використання. Проте, слід пам'ятати про можливе втручання у приватне життя користувачів і дотримуватися відповідального використання відповідно до законодавства.

Вплив користувацьких інтерфейсів на безпеку інформації

УДК 004.5 (043.2)

Буковецький Василь[1], Михайло Різак[2]

[1]Карпатський університет ім. Августина Волошина, bukovetsky@outlook.com,
[2]Ужгородський національний університет, mykhailo.rizak@uzhnu.edu.ua

В уяві багатьох людей безпека інформації — це щось пов'язане з написанням файлів, мережевим обладнанням, налаштуванням політик безпеки та різними алгоритмами шифрування. Можна посперечатись, що безпека інформації це в першу чергу робота з людьми та розуміння їхньої поведінки. Саме люди будуть користуватися розробленими системами захисту, програмним забезпеченням та іншим.

В історії є чимало прикладів, коли використання незрозумілих інтерфейсів користувача могло приводити навіть до фатальних наслідків.

Для оцінки впливу користувацького інтерфейсу було вибрано функціонал ревізії у програмному забезпеченні яке використовується для продажу автозапчастин та використовується магазинами по всій території України. Телеметрія показувала, що інколи клієнти при використанні цього програмного модулю часто відкривали ревізію, яка по замовчуванню завжди була з нульовою кількістю нарахованого товару. Якщо їх бажання було скасувати ревізію, замість прийняття нульових результатів, іноді вони вибирали не ту дію що хотіли, і приймали результат ревізії: 0 товарів на складі. Виконання такої дії знищувало всі дані про товар підприємства і потребувало подальшого відновлення даних.

Інтерфейс програмного забезпечення до внесення змін мав вигляд таблиці зі списком поточних товарів ревізії та двох кнопок: «Скасувати ревізію» та «Прийняти зміни». При натисканні кожної з кнопок виводилось попередження з поясненням результату виконання цієї операції. Не можна сказати, що це поганий інтерфейс чи заплутаний. Всього дві кнопки та додаткове підтвердження, яке мало б уберегти від випадкових дій. Тим не менш, 3.2% ревізій потребували процедури відновлення даних.

Для перевірки результатів різних підходів до організації інтерфейсу було використано метод А/Б тестування, де кожному клієнту випадав випадковий варіант інтерфейсу. Дані про інтерфейс зберігались разом із даними ревізії. Збір даних виконувався протягом двох місяців.

Зміна в інтерфейсі	**% відновлень**	**Загальна к-сть ревізій**
Інтерфейс без змін	2.9	312
Зміна кольору кнопки «Скасувати» на червоний	2.6	323
Додавання додаткового попередження при прийманні змін	2.6	341

Додавання додаткового попередження при прийманні змін із затримкою в 3 секунд	1.6	293
Два попередження із затримкою та інформацією про кількість товарів на які буде прийнято зміни	1.0	296
Вимога ввести слово «ПІДТВЕРДЖУЮ» у поле вводу, якщо кількість товарів які буде змінено більше ніж 95%	0.3	320

Виміри показали, що зміни в інтерфейсі користувача можуть мати значний вплив на поведінку людей. Це проілюстровано в табл. 1. З результатів видно, що найбільший вплив на розуміння користувачем наслідків виконання деструктивної дії має зміна інтерфейсу на такий, що заставить виконати його незвичну дію, яка займе більший час ніж зазвичай.

Генерація зображень в завданнях стеганографічного захисту

УДК 621.395.7 (043.2)

Андрій Варениця[1], Дмитро Пелешко[1,2], Олена Винокурова[2]

[1]Національний університет Львівська Політехніка,
andrii.varenytsia.mknssh.2023@lpnu.ua ,
[2]Львівський національний університет ім. Івана Франка,
dmytro.peleshko@lnu.edu.ua, olena.vynokurova@lnu.edu.ua

Хоча застосування методів комп'ютерного зору принесло чимало успіхів у вирішенні різних задач, деякі елементи процесу є добре відомі, зокрема ті, що стосуються архітектури моделей, вибору параметрів та навчання, а також тонкої настройки гіперпараметрів. Тим не менш, збір і анотація даних залишаються критично важливими компонентами, які продовжують ставити виклики. Цей процес часто є найдовшим, найбільш затратним і складним. Необхідність збору даних незмінно важлива для створення точних та надійних моделей, що використовуються в реальних умовах. Дослідники прагнуть розширити існуючі набори даних за допомогою технік аугментації, щоб забезпечити нові та різноманітні зображення для підвищення здатності моделі до узагальнення. Проте багато традиційних методів аугментації обмежуються лише внесенням змін до вже наявних зображень [2].

У сфері обробки природної мови, що є частиною машинного навчання, вже існує практика використання аугментації існуючих наборів даних або створення нових за допомогою передових мовних генеративних моделей [1]. Цей підхід вже активно використовується фахівцями по всьому світу. У випадку з сферою комп’ютерного зору, такий підхід ще не набув популярності через проблему синтезу якісного і реалістичного зображення без генеративних артефактів, що є більш складною задачею, що потребує певні модифікації до процесу генерації чи архітектури моделі, щоб знизити процент пошкоджених чи далеких від реальності зображень.

Метою роботи є створення рішення, яке дозволить генерувати якісні зображення для аугментації і доповнення існуючих наборів даних для їх подальшого використання в завданнях стеганографічного захисту. Окрім того, ця система може слугувати для автоматизації збирання даних, усуваючи потребу в ручному створенні та анотації даних.

Завдяки новітнім рішенням у сфері генеративного штучного інтелекту ми можемо не тільки модифікувати, але й створювати повністю нові зображення. Лідером в сфері генерації зображень на даний момент являються латентні дифузійні моделі (LDM) [3]. Ці нейромережі функціонують в латентному просторі з меншою розмірністю. Такий підхід вдається завдяки використанню автоенкодера, який перетворює деталізовані дані в латентний простір, де дифузійний процес може сконцентруватись на семантичних характеристиках зображень, мінімізуючи увагу до деталей. Вагомим удосконаленням у порівнянні з попередніми архітектурами стало підвищення швидкості тренування та прогнозування, що було досягнуто завдяки інтеграції латентного простору та зниження розмірності даних під час навчання (Рис. 1).

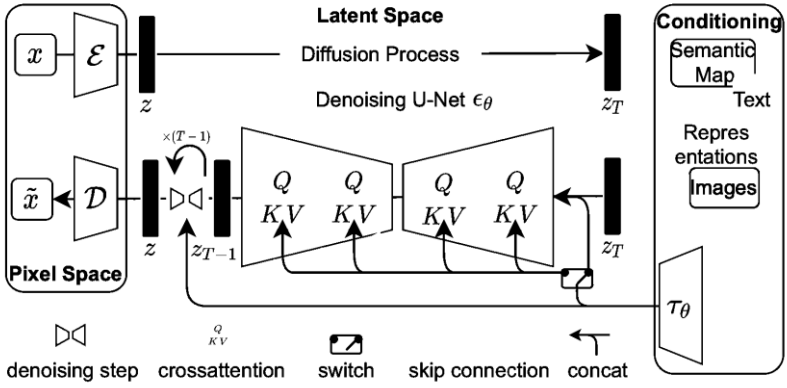


Рис.1. Архітектура латентної дифузійної моделі

Часто однією з проблем у дослідженнях стеганографії є відсутність великих і різноманітних наборів даних. Використання дифузійних моделей для створення синтетичних зображень може допомогти розширити доступні набори даних, що забезпечує кращі умови для розвитку і валідації нових стеганографічних технологій.

Також дифузійні моделі для генерації зображень ми можемо використовувати і для вдосконалення методів стеганографії з допомогою яких ми можемо створювати більш реалістичні носії для стеганографічних даних, тим самим збільшуючи непомітність вбудованої інформації.

Наостанок генеративні моделі можуть бути використані для проведення тренування і валідацію довільних стеганографічних систем. Синтезовані зображення можуть використовуватися для тренування алгоритмів машинного навчання, які виявляють або аналізують стеганографічні дані. Це може включати в себе класифікацію зображень на основі наявності або відсутності стеганографічних вставок, допомагаючи в розвитку кращих інструментів для виявлення атак і потенційно шкідливих маніпуляцій.

1. J. Ye et al., “LLM-DA: Data Augmentation via Large Language Models for Few-Shot Named Entity Recognition.” arXiv, Feb. 22, 2024. URL: http://arxiv.org/abs/2402.14568 (дата звернення: 11.04.2024)
2. T. Kumar, A. Mileo, R. Brennan, and M. Bendechache, “Image Data Augmentation Approaches: A Comprehensive Survey and Future directions.” arXiv, Mar. 11, 2023. URL: http://arxiv.org/abs/2301.02830 (дата звернення: 11.04.2024)
3. R. Rombach, A. Blattmann, D. Lorenz, P. Esser, and B. Ommer, “High-Resolution Image Synthesis with Latent Diffusion Models.” arXiv, Apr. 13, 2022. URL: http://arxiv.org/abs/2112.10752 (дата звернення: 11.04.2024)

Методи та засоби мінімізації ризиків привілейованих облікових засобів в інформаційних системах

УДК 004.056.52

Петро Венгерський[1], Андрій Ребець[2]

[1]ЛНУ, [2]Intellias, [1]petro.venherskyy@lnu.edu.ua, [2]andrii.rebets@intellias.com

Сучасний кіберпростір тісно пов'язаний з аутентифікацією та авторизацією користувачів за допомогою облікових записів. Тому існує широкий перелік ризиків інформаційної безпеки (ІБ), похідних від облікових записів, паролів, ключів аутентифікації тощо. Ще більший ризик несуть так звані привілейовані (адміністративні) облікові записи (ПОЗ) через наявність розширеного доступу в інформаційних системах. Зокрема згідно з останнім дослідженням [1] компанії Verizon, 95% підтверджених інцидентів ІБ, пов'язаних з неналежним використання привілейованого доступу, призвели до витоку конфіденційної інформації.

Яскравим прикладом інциденту, який мав суттєві наслідки і вплив на Україну, є потужна хакерська атака проросійських кіберзлочинців на найбільший телекомунікаційний оператор «Київстар» у грудні 2023 року. Зважаючи на наслідки атаки, зловмисники змогли отримати привілейований доступ до ядра мережі і сервісів компанії і нанести руйнівну шкоду.

З огляду на актуальність тематики, метою дослідження є аналіз методів та засобів управління ПОЗ в інформаційних системах, які дають можливість суттєво знизити ймовірність реалізації пов'язаних загроз і уникнути інциденти ІБ. Розглянемо основні методи управління ПОЗ, які мінімізують ризики ІБ.

Реєстр ПОЗ. В залежності від розміру та можливостей організації, такий реєстр може наповнюватися і редагуватися вручну або за допомогою спеціалізованих систем – директорій користувачів (Microsoft Active Directory, Microsoft Entra тощо). В ньому повинна міститися актуальна інформація про власника облікового запису, перелік і рівень доступу в системах, час та дата останнього аудиту доступу. Також використання директорій дає можливість управління життєвим циклом облікових записів – створення, зберігання, внесення змін, деактивація.

Розділення облікових записів в залежності від функцій. Хорошою практикою є наявність у користувачів, які здійснюють адміністрування систем, додаткових облікових записів з обмеженим доступом для здійснення операцій, які не вимагають привілейованого доступу. Це мінімізує ризик компрометації ПОЗ.

Застосування принципу гранулярного доступу. Важливо розділяти привілейований доступ в залежності від обов'язків, покладених на користувачів. Замість наявності одного адміністратора, відповідального за управління всіма наявними інформаційними системами і пристроями, необхідно розділити доступ в залежності від ролі, яку виконує користувач – адміністратор серверного обладнання, адміністратор робочих станцій, адміністратор мережі тощо.

Ведення журналу подій. Збір і аналіз подій використання привілейованих облікових записів дає можливість відстеження та аналізу дій користувачів в системах, виявлення аномальних подій та фактів неавторизованого доступу і реєстрацію та опрацювання інцидентів ІБ з метою виявлення і запобігання загроз. Для централізації та автоматизації обробки зібраної інформації доцільно використовувати спеціалізовані системи – SIEM (Security Information and Event

Management), які дають можливість зібрати події з різних систем, провести ретельний аналіз та аудит і реєструвати та опрацьовувати інциденти ІБ.

Аудит доступу. Регулярна перевірка поточного рівня доступу користувачів в системах дає можливість виявити надмірний чи неактуальний доступ і виправити ці недоліки. Це сприяє дотриманню принципу мінімального необхідного доступу.

Суттєвий контроль і управління ПОЗ забезпечить впровадження спеціалізованих інформаційних систем – Privileged Access Management (PAM), які дають можливість виявляти і реєструвати ПОЗ, забезпечують життєвий цикл, ведуть детальний журнал використання ПОЗ і дій користувачів, надають фунціонал безпечного віддаленого доступу з можливістю ізоляції сесій та моніторингу, забезпечують можливість виявлення аномальної поведінки.

На рис. 1 наведений результат впровадження перерахованих вище методів і засобів в ІТ аутсорсинговій компанії чисельністю близько 3000 працівників за останні три роки. У 2021 році відбулося впровадження методів, у 2022 – злагодження і вдосконалення процесів, у 2023 – впроваджено систему PAM, яка дозволила додатково скоротити кількість виявлених порушень за результатами повторного аудиту.

Рис.1. Ефективність впровадження методів і засобів управління ПОЗ на кількість пов'язаних порушень політики ІБ

Отже, запропоновані в дослідженні методи та засоби мінімізації ризиків ПОЗ в інформаційних системах дозволяють суттєво зменшити кількість пов'язаних порушень політики ІБ і, відповідно, знизити ймовірність реалізації загроз та інцидентів ІБ.

1. Verizon 2024 Data Breach Investigations Report. URL: https://verizon.com/dbir (дата звернення: 18.04.2024)

Підхід до вибору стратегії застосування методів протидії кібератакам

УДК 621.395.7 (043.2)

Сергій Веретюк[1], Катерина Молодецька[2]

Поліський національний університет,
[1]kateryna.molodetska@polissiauniver.edu.ua, [2]mail2@nau.rdu.ua

Зростання кількості кібератак свідчить про динамічний характер взаємодії в кіберпросторі між кіберзлочинцями та системами кіберзахисту. Більшість існуючих систем, підходів та стандартів стикаються з певними обмеженнями, такими як застосування статичних моделей, відсутність урахування спільної еволюції стратегій та відсутність синхронізованого налаштування, що не враховує динамічний характер кібератак і захисту. Постійна коеволюція вимагає від захисників не лише реактивної, але й прогнозованої стратегії.

Ефективний захист передбачає синхронізацію стратегій на різних рівнях захисту, включаючи мережевий, рівень застосунків та фізичний захист, для ефективного запобігання вразливостям. Застосування динамічних моделей дозволяє краще розуміти та передбачати змінність в діях кіберзлочинців і захисників, що допомагає вчасно реагувати на потенційні загрози. Нарешті, стратегічне планування є ключовим елементом в розробці майбутніх стратегій захисту, дозволяючи захисникам адаптуватися до швидких змін у загрозах та технологіях.

Таким чином, пошук нових адаптивних динамічних підходів до забезпечення ефективного кіберзахисту об'єктів інформаційної діяльності є актуальним науковим завданням.

Дослідження спрямоване на розроблення підходу до підвищення ефективності стратегічного планування заходів із забезпечення кібербезпеки об'єктів інформаційної діяльності в умовах динамічного антагоністичного середовища.

Нехай є набір методів протидії кібератакам на об'єкт інформаційної діяльності

$$M = \{m_i\},\ i \in [1; N]. \quad (1)$$

Кожний метод формалізовано трьома параметрами $\{P, T, C\}$, де:

P_i – потенціал протидії, тобто здатність методу адекватно протидіяти окремому типу кібератаки або її складовій *i*-того методу протидії кіберзагрозі;

T_i – час імплементації *i*-того методу або час перехідного процесу від початку дії методу;

C_i – вартість застосування *i*-того методу.

Стратегією протидії $S_j = \{m_{j,i}\}$ називатимемо довільний набір методів, який ефективно протидіє кіберзагрозі Z_j. У свою чергу кіберзагрозу Z_j будемо описувати параметром збитків L_i.

Ефективністю *i*-того методу E_i визначимо через наступне співвідношення

$$E_i = \frac{P_i}{T_i C_i}. \quad (2)$$

Тоді загальну ефективність стратегії S_j формалізуємо через величину

$$E_{s_j} = \sum E_{ij}, \quad (3)$$

де E_{ij} – ефективність застосування *i*-того методу в *j*-тій стратегії.

Опишемо загальні втрати від потоку атак таким співвідношенням

$$L_{\text{заг}} = \lambda\tau L_A\left(1 - E_j^*\right), \quad (4)$$

де E_j^* – нормована відносно 1 ефективність обраної стратегії, λ- інтенсивність потоку атак (пуассонівського потоку подій).

Тоді принцип вибору стратегії повинен забезпечувати мінімізацію $L_{\text{заг}}$

$$\lambda\tau L_A\left(1 - E_j^*\right) \to min \quad (5)$$

за таких умов

$C_j = \sum C_i < C_{max}$ – обмеження на вартість;

$P_j = \sum P_i < P_{max}$ – обмеження, які накладаються на потенціал методу;

$T_j < T_{max}$ – обмеження по часу;

$C_j < \lambda\tau L_{A\tau}$ – виконання умови доцільності, а саме використовувати стратегію, якщо вартість її реалізації менша за втрати від кібератак.

Вираз (5) можемо переписати як

$$\lambda\tau L_A\left(1 - \frac{E_j}{E_{max}}\right) \to min,$$

де E_{max} – максимальна ефективність обраної стратегії.

При фіксованих значеннях $L_A, \lambda, \tau, E_{max}$ задача зводиться до мінімізації співвідношення

$$E_{max} - E_j \to min. \quad (6)$$

Для вирішення скористаємось методом Лагранжа. Розв'язок системи диференціальних рівнянь, отриманих шляхом диференціювання рівняння Лагранжа дасть можливість визначити параметри $\{P, T, C\}$ оптимальної стратегії S_j для протидії кіберзагрозі Z_j за критерієм ефективності за сукупністю показників: потенціалу методів, що входять до стратегії, вартості та часу реагування цих методів. Отже, розуміння коеволюції засобів здійснення кібератаки та методів кіберзахисту надає можливість дослідити та спрогнозувати зміни в системі «загроза-захист» на макрорівні.

1. Van der Kleij, Rick, et al. Developing decision support for cybersecurity threat and incident managers. *Computers & Security*. – 2022. – 113:102535.
2. Yevseiev S., Hryshchuk R., Molodetska K., Nazarkevych M. and others. Modeling of security systems for critical infrastructure facilities: monograph. Kharkiv: PC Technology Center, 2022. 196 p.
3. Yin, Yimin. Information Security and Risk Control Model Based on Plan-Do-Check-Action for Digital Libraries. *Journal of Cyber Security and Mobility*. – 2024. – PP. 305–326.
4. Lippert, Kari J., Robert Cloutier. Cyberspace: a digital ecosystem. *Systems*. – 2021. – 9.3: 48.
5. Fedushko, S., Molodetska, K., Syerov, Y. Analytical method to improve the decision-making criteria approach in managing digital social channels. *Heliyon*. – 2023. – 9(6). – e16828.

Обмін шифрованими повідомленнями в командному рядку

УДК 621.395.7 (043.2)

Віталій Власов[1]

Львівський національний університет імені Івана Франка,
[1]vitaly.vlasov@lnu.edu.ua

Безпечний обмін повідомленнями набуває все більшої актуальності протягом останніх років. Наскрізне шифрування повільно, але впевнено було впроваджене у всіх домінуючих системах обміну повідомленнями, таких як Facebook Messenger, WhatsApp, Telegram, і т.д.

Signal (Сигнал) був одним із перших застосунків, побудованих навколо ідеї приватності повідомлень. У Сигналі було вперше імплементовано декілька новітніх протоколів шифрування, таких як Double Ratchet, Extended Triple Diffie-Hellman, і, нещодавно, Post-Quantum Extended Diffie-Hellman [1].

Усі перелічені вище застосунки мають мобільні та десктопні/веб версії. Тим не менше, в останні роки відбувся значний прогрес у розвитку можливостей текстових користувацьких інтерфейсів, зокрема, термінальних емуляторів. Серед них слід згадати мультиплексери, розширену підтримку клавіатури, підтримку зображень, і т. д. Зважаючи на широке використання терміналів у сучасній розробці програмного забезпечення, є сенс покращити підтримку обміну повідомленнями в інструментарії розробника.

Існує декілька застосунків такого типу,: зокрема Tinode, декілька клієнтів для протоколу Matrix, і модульний клієнт WeeChat. Тим не менше, певна комбінація функціональностей наразі не представлена в жодному з клієнтів:

- наскрізне шифрування по замовчуванню
- децентралізація
- підтримка передачі зображень

Автором запропонований та розробляється застосунок із наступною архітектурою:

- Низькорівнева мережева бібліотека – libp2p [2]
- Рівень обміну повідомленнями – Waku [3]
- Безпечний протокол чату – Status protocol [4]
- TUI-бібліотека: notcurses [5]

Додатково, передбачено можливість скриптування із використанням Lua. Застосунок підтримує як повноекранний режим, так і використання як утиліти в командному рядку, зокрема, в цілях тестування та налаштування децентралізованих вузлів.

1. Signal Protocol Specifications. URL: https://www.signal.org/docs/
2. Libp2p protocol. URL: https://libp2p.io
3. Waku specs. URL: https://docs.waku.org
4. Status protocol. URL: https://status.app/specs/status-1to1-chat
5. Notcurses TUI library. URL: https://notcurses.com

З історії української авіаційної промисловості. 1919–1926 рр.

УДК 94.(477) "191/192": 355.48.623.746.

Валерій Ворожко

Національний авіаційний університет, ГДА СБУ, wp06vv@gmail.com

Нині Україна протистоїть потужним зусиллям своїх ворогів, мета яких – ліквідація української державності та знищення українців. Сучасні політичні виклики зумовлюють необхідність об'єктивного аналізу історичних аспектів функціонування «державного організму» України та його подальшої трансформації в сучасну вільну і демократичну країну.

Метою даної роботи є недопущення рецидивів минулого пов'язаних із загрозами для Української держави остаточно втратити пріоритети у науково-технологічному забезпеченні розвитку вітчизняної галузі авіабудування.

Після захоплення більшовиками влади почалася конфіскація робітничими колективами, органами влади авіаційних підприємств у їхніх власників. Спочатку більшовики вважали, що пролетарські маси, «озброєні» революційною свідомістю, швидко налагодять виробничий процес, створять нові види літаків, що забезпечать «перемогу світової пролетарської революції». Натомість після уведення «робітничого керівництва» почався спад виробництва і трудової дисципліни. Для недопущення остаточного розпаду промисловості, більшовики почали процес її одержавлення. Націоналізовані заводи авіаційної промисловості у 1919 р. об'єднали у Головне правління об'єднаних заводів авіаційної промисловості (Головавіа). У 1920 р. до складу Головавіа увійшли українські авіаційні заводи – «Дека» в Олександрівську (нині Запоріжжя) та «Анатра» в Одесі. Рада військової промисловості 9 вересня 1920 р. видала наказ про організацію в Києві «Державного авіаційного заводу № 12» (ДАЗ № 12). Завод створили на базі майстерень Київського політехнічного інституту та розформованого в серпні 1920 р. «Київського авіапарку». Водночас, для ремонту літаків, що належали Морським силам Чорного моря, у Севастополі сформували «Гідробазу морської авіації Чорного моря». Водночас частина авіаційних підприємств увійшли до Правління фабрично-заводських підприємств військово-повітряних сил «Промповітря», створеного у 1921 р. ДАЗ № 12 увійшов, серед інших авіапідприємств до «Промповітря» та отримав нову назву «Ремповітря-6». Із 1926 р. він мав назву «завод № 43» і був орієнтований на ремонт авіатехніки, що перебувала на озброєнні частин Українського військового округу. До «Промповітря» увійшла і «гідробаза морської авіації Чорного моря», отримавши нову назву «Ремонтні авіаційні майстерні № 2»,(завод № 45). У червні 1921 р. Головавіа ліквідували. Авіапідприємства підпорядкували Авіавідділу № 4 Головного управління військової промисловості(ГУВП) Вищої ради народного господарства (ВРНГ), а у січні 1925 р. авіапідприємства перейшли у підпорядкування Державного тресту авіапромисловості (Авіатрест) у складі ВРНГ.

Авіатрест знаходився під пильним наглядом чекістів, які вважали за необхідне контролювати весь спектр діяльності Авіатресту: від конструкторських креслень та технологічних процесів до політичної благонадійності науковців, конструкторів, робітників. Так, у лютому 1926 р. начальник Особливого відділу ОДПУ Я. Ольській за підсумками перевірок діяльності «Авіатресту» у 1925 рр. направив доповідну

записку до ВРНГ та ЦК ВКП(б), в якій зазначалося про невиконання виробничої програми підприємствами «Авіатресту», що відбувалося внаслідок «бюрократичного й безпланового ставлення керівництва «Авіатресту» до заводів». Ольський акцентував увагу, що «правління тресту слабке і неавторитетне, у тресті панує неорганізованість й “безшабашність”». Він скаржився, що їхні неодноразові вказівки на невдалий підбір особового складу керівництвом ГУВП ігнорувалися. Також, на його думку, підозрілим було «орієнтування на закордонні зразки авіатехніки».

У вересні 1925 р. на базі ремонтних майстерень АТ "Укрповітрошлях" був створений "Авіазавод ім. Раднаркому УСРР" (№ 135). Розвиток авіапромисловості України в першій половині 1920-х рр. характеризувався з одного боку, ліквідацією старих заводів. З іншого боку з’явилися нові заводи в Києві і Харкові. Виробництво було зведено до мінімуму, підприємства займалися в основному ремонтом.

В умовах російської агресії Україна як фронтир між цивілізованим світом й авторитарно-тоталітарними режимами, зобов’язана швидко розвивати власну авіаційну промисловість, зробити її ефективною відповідно до потреб Сил оборони.

Використання алгоритмів CCC/UMAC для вдосконалення протоколу SSL/TLS

УДК 004.056.53

Алла Гаврилова[1], Ірина Аксьонова[2]

Національний технічний університет «Харківський політехнічний інститут», [1]alla.havrylova@khpi.edu.ua, [2]iryna.aksonova@khpi.edu.ua

В основі вдосконалення протоколу SSL/TLS використовуються комплексовані алгоритми на основі постквантових алгоритмів, які дають змогу забезпечити виконання послуг безпеки з урахуванням усунення вразливостей, що базуються на використанні фази рукостискання [1]. На сучасному етапі використовуються дві версії протоколу SSL/TLS версій v.1.2 і v.1.3. Їхня архітектура складається з двох протоколів: I – протокол рукостискання (призначення – автентифікація та обмін ключами); II – протокол запису, за яким усі вихідні повідомлення шифруються секретним ключем, встановленим під час рукостискання, зашифровані повідомлення передаються від Клієнта до Сервера, а Сервер перевіряє отримані зашифровані повідомлення на наявність змін та у разі відсутності змін, зашифровані повідомлення розшифровуються за допомогою секретного ключа.

Щоб гарантувати, що зашифроване повідомлення не було змінено під час передавання, протоколи TLS v.1.3 використовують автентифіковане шифрування (режим AEAD) [2, 3]. Версії стека протоколу SSL/TLS не є постквантовими алгоритмами і не можуть гарантувати необхідний рівень безпеки в умовах появи повномасштабного квантового комп'ютера. Для забезпечення послуг безпеки та усунення вразливостей у фазі рукостискання протоколу SSL/TLS запропоновано передавати тільки параметри рівняння кривої, а також за необхідності вектори ініціалізації на модифікованих еліптичних кодах (MEC) [3].

Таким чином, для формування ключових даних як на стороні Сервера, так і на стороні Клієнта достатньо передати тільки коефіцієнти *a1, a2, a3, a4, a5, a6*, тобто бінарну послідовність із п'яти символів. При цьому обидві сторони зможуть сформувати необхідні матриці і бути готовими до обміну інформацією. Крім цього, немає необхідності використовувати додаткові несиметричні алгоритми (Діффі-Хеллмана, RSA) для передавання ключових даних для симетричного алгоритму (у запропонованому випадку використовуються несиметричні криптосистеми зі швидкістю криптоперетворень, які можна порівняти із симетричними криптоалгоритмами). На рис. 1 представлено вдосконалену схему протоколу SSL/TLS [3].

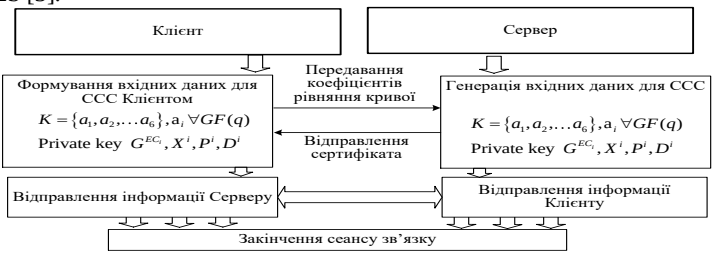


Рис. 1. Вдосконалена схема протоколу SSL/TLS

При необхідності “відновлення” сеансу в режимі 0-RTT також немає необхідності забезпечувати обмін ключовими даними та частиною зашифрованого коду для перевірки правильності визначення ключа, що розділяється [2]. Клієнту достатньо відправити тільки коефіцієнти кривої для того, щоб сервер визначив ключові дані для крипто-кодових конструкцій (ССС). Використання вектора помилки *e* під час передавання інформації дає змогу його розглядати як сеансовий ключ для кожного окремого пакета, що істотно підвищує рівень стійкості. Це усуває можливі вразливості replay attack і дає змогу забезпечити необхідний рівень безпеки (досконала пряма секретність). Використання несиметричних криптоалгоритмів (постквантових алгоритмів – ССС Мак-Еліса на МЕС та збиткових кодах (DC) [3]), “спрощує” обмін ключами і не вимагає додаткових енергетичних (обчислювальних) витрат на використання несиметричних криптоалгоритмів. Крім цього, використання завадостійких кодів дає змогу “варіювати” показником вектора помилки *e* (сеансовий пароль для кожного пакета) і забезпечувати або підвищення рівня стійкості, або підвищення рівня достовірності.

Таким чином, запропоноване удосконалення найпоширенішого протоколу забезпечення послуг безпеки на транспортному рівні SSL/TLS на постквантових алгоритмах – ССС на МЕС (з укороченням та/або подовженням) [3] дозволить істотно знизити “можливості” відомих вразливостей на протокол SSL/TLS. При цьому забезпечується необхідний рівень безпеки в постквантовий криптоперіод, обчислювальних та енерогоємнісних вимог до використання в кіберфізичних системах на основі смарт-технологій.

1. Yevseiev S., Gavrilova A., Tomashevsky B. and other. Research of crypto-code designs construction for using in post quantum cryptography. Development Management. – 2018. – vol. 4, iss. 4. – P. 26-39.
2. Havrylova A., Tkachov A., & Shmatko A. Development of a pseudo-random substrate for the UMAC algorithm on crypto-code constructions. *Information Protection And Information Systems Security 2021*" November 11–12, 2021, LVIV, UKRAINE. 2021. P. 49 – 50.
3. Yevseiev S., Havrylova A., Milevsky and other. Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies. – 2023. – №3/9 (123). – P. 33-48.

Система моніторингу периметра об'єкта критичної інфраструктури

УДК 004.056

Олександр Галущенко[1], Володимир Лужецький[2]

Вінницький національний технічний університет,
[1]mamr3379@gmail.com, [2]v.luzhetskyi@vntu.edu.ua

Захист об'єктів критичної інфраструктури набуває особливої актуальності в теперішній час. Тому значна увага приділяється створенню систем забезпечення кібербезпеки, що призначені для запобігання, своєчасного виявлення та протидії загрозам безпеці об'єктам критичної інфраструктури з використанням кіберпростору; усунення умов, що їм сприяють, та причин їх виникнення.

Процес забезпечення безпеки великих за площею об'єктів критичної інфраструктури (великі промислові об'єкти, електростанції, морські порти та ін.)базується на використанні комплексу технічних систем і заходів, метою яких є виявлення та попередження несанкціонованого проникнення в заборонену зону. Ці системи мають забезпечувати багатофакторний контроль ближніх та дальніх рубежів.

У доповіді розглядається система моніторингу периметра об'єкта критичної інфраструктури, яка використовує особливості Wi-Fi технології бездротової мережі з пристроями на основі сімейства стандартів IEEE 802.11.

Використання бездротових технологій надає багато переваг і забезпечує гнучкість в побудові бізнес-процесів. Особливо це стосується управління рухомими об'єктами, складської логістики та об'єктів, де неможливо або складно організувати дротову мережу.

Основна задача моніторингу полягає у:

- визначенні координат пристроїв з модулями Wi-Fi, що працюють як точка доступу;
- визначенні часу їх появи в зоні, що підлягає моніторингу;
- створення історії їх переміщень.

Для розв'язання даної задачі потрібно знати координати всіх точок доступу на планеті та здійснювати моніторинг радіоефіру навколо об'єкта критичної інфраструктури.

Будь-який мережевий пристрій має свій унікальний ідентифікатор у вигляді MAC-адреси. Теоретично існує понад 281 трильйон унікальних MAC-адрес. Ця кількість дозволяє забезпечити унікальність ідентифікаторів для всіх мережевих пристроїв у світі. Глобальна система моніторингу створює базу координат всіх пристроїв на планеті та здійснює їх прив'язку до карти.

Метод визначення координат пристроїв передбачає реалізацію таких дій. Створюється віртуальне середовище, в якому кожна віртуальна машина формує унікальний набір характеристик (fingerprinting), який ніколи більше не буде застосовуватися. До геопровайдерів надсилається запит виду: «Я увімкнувся, бачу тільки один пристрій з MAC-адресою ****, скажи, де я». Якщо надходить відповідь з координатами пристрою за MAC-адресою ****, то дані записуються в базу і віртуальна машина змінює свої характеристики для наступного запиту. Якщо

відповіді немає, то псевдовипадковим чином формується наступна MAC-адреса і робиться запит. Це виконується до тих пір, поки не буде отримано відповідь.

Будь-який пристрій, що працює в стандарті IEEE 802.11, обмінюється технічною інформацією з іншими пристроями, які розташовані поруч. Це необхідно для визначення завантаженості каналів і перемикання самих точок доступу на менш завантажені канали. Ще цей механізм використовується для більш точної геолокації. Мобільний пристрій, який хоче визначити свою геолокацію, збирає отримані дані: MAC-адресу точки доступу Wi-Fi, SID та LAC базових станцій операторів мобільного зв'язку, рівень сигналу в точці вимірювання та передає ці дані геопровайдеру. Геопрвайдер повертає координати розташування пристроїв, що бачить пристрій, якому потрібно визначити свої координати.

Для створення глобальної системи моніторингу використано хмару AMAZON AWS, 1500 орендованих серверів з 36 одночасно працюючими потоками. Така система забезпечує можливість здійснювати моніторинг всіх MAC-адрес на планеті кожні 24 години. Завдяки чому можна відстежувати переміщення пристроїв з однієї локації в іншу.

Локальна система моніторингу здійснює моніторинг радіоефіру навколо об’єкта критичної інфраструктури використовуючи дані, отримані від глобальної системи моніторингу, та від вимірювального комплексу. Дані від глобальної системи моніторингу запитуються шляхом виділення певної зони на карті. Результатом виконання запиту є набір координат, які доступні для оброблення в межах зазначеної зони.

Для моніторингу радіоефіру використовуються нерухомі та рухомі вимірювальні пристрої. Це забезпечує побудову радіоефірної карти місцевості навколо об’єкта критичної інфраструктури. Аналіз такої карти дає можливість виявити:

- аномальні пристрої, власники яких шукають підходи до території, що охороняється, але не потрапляють у поле зору камер відео спостереження;
- однакові пристрої біля різних об’єктів критичної інфраструктури;
- різні пристрої, що раніше підключалися до точки доступу з одним ім'ям мережі.

Таким чином, поєднання цих двох систем моніторингу дозволяє своєчасно виявляти:

- осіб, які проводять негласне спостереження за об'єктами критичної інфраструктури або за працівниками;
- спроби злому Wi-Fi мереж та перехоплення трафіку клієнтів цих мереж;
- спроби сканування мережі критичної інформаційної інфраструктури хакерами та місця фізичного розташування хакера при підключенні до мережі Wi-Fi;
- переміщення осіб у темний час доби в зонах поганої видимості камер відеоспостереження.

Аналіз методів оцінки кібербезпеки програмного забезпечення

УДК 621.395.7:004.05

Роман Гамрецький[1], Віктор Гнатюк[2]

Національний авіаційний університет,
[1]45391@stud.nau.edu.ua, [2]viktor.hnatiuk@npp.nau.edu.ua

Оцінка кібербезпеки програмного забезпечення (ПЗ) є важливим компонентом загальної стратегії оцінки якості ПЗ. Така оцінка дозволяє ідентифікувати потенційні слабкі місця та вразливості, зменшити ризики безпеки та забезпечити дотримання стандартів.

Кібербезпека в ПЗ стосується захисту ПЗ від навмисних атак або випадкових загроз, які можуть призвести до несанкціонованого доступу, зміни, викрадення або знищення цифрових активів. Врахування кібербезпеки у процесі оцінки якості ПЗ дозволяє розробникам ідентифікувати і усунути вразливості на ранніх етапах розробки, що забезпечує створення більш безпечного та надійного продукту. Аналіз методів оцінки кібербезпеки ПЗ дозволяє визначити складність, механізм та результативність їх застосування.

Серед ключових методів, які застосовуються для оцінки безпеки програмних продуктів можна виділити наступні:

- статистичний аналіз – Static Application Security Testing (SAST);
- динамічний аналіз - Dynamic Application Security Testing (DAST);
- аналіз залежностей – Software Composition Analysis (SCA);
- тестування на проникнення – Penetration Testing.

Статичний аналіз передбачає перевірку коду програми на наявність вразливостей без самого виконання коду. Цей метод виявляє помилки у коді, такі як буферні переповнення, SQL ін'єкції та інші поширені вразливості, які можуть бути використані зловмисниками [1]. Перевагою метода є висока швидкість аналізу та можливість інтеграції з процесом розробки ПЗ. А недоліком є те, що метод не може виявити вразливості, які залежать від контексту виконання програми.

Існують інструменти які допомагають автоматизувати статичний аналіз, серед яких можна виділити такі як SonarQube, Fortify, Checkmarx [2].

Динамічний аналіз включає тестування ПЗ в реальному часі під час його виконання. Цей метод здатний виявити вразливості, які не можуть бути виявлені статичним аналізом, включаючи проблеми з конфігурацією та виконанням [3]. Перевагою методу є виявлення вразливостей, які проявляються тільки під час виконання програми. В порівнянні з статичним аналізом, метод вимагає більше ресурсів та часу за рахунок потреби в контексті для виконання програми.

Серед популярних інструментів виділяють наступні: ZAP, Burp Suite.

Аналіз залежностей фокусується на ідентифікації уже відомих вразливостей в сторонніх бібліотеках які використовуються в програмі [4]. Цей метод виявляє вразливості в залежностях, які могли бути включені у програму з зовнішніх джерел, а також покращує управління версіями залежностей.

Серед популярних інструментів для аналізу залежностей є Black Duck, WhiteSource, Snyk .

Тестування на проникнення включає активні спроби "проникнути" у систему або програму з метою виявлення неочевидних вразливостей. Це може включати

ручні атаки або автоматизовані системи для імітації дій зловмисника. Таке тестування дозволяє імітувати реальну поведінку зловмисників, що в порівнянні з попередніми методами дозволяє ідентифікувати інші типи вразливостей.

Серед інструментів які використовують спеціалісти в тестуванні на проникнення є Metasploit, Nmap, Wireshark, ZAP та інші.

Для забезпечення високого рівня кібербезпеки, важливо інтегрувати оцінку кібербезпеки безпосередньо у процеси розробки ПЗ. Це можна здійснити за допомогою:

- неперервної інтеграції (CI) та неперервного розгортання (CD), де тести на кібербезпеку виконуються автоматично на кожному етапі розробки;
- регулярних оновлень політик безпеки і вимог, які враховують зміни у зовнішніх умовах та загроза;
- тренінгів і освітніх програм для розробників, щоб підвищити їх обізнаність у сфері кібербезпеки та здатність ідентифікувати потенційні вразливості.

Деякі з перелічених інструментів (SonarQube, ZAP і тп.) представляють комплексні рішення та дозволяють використовуючи комбінації із різних методів. В тому числі, перевіряючи загальну якість коду ПЗ, а не тільки визначаючи вразливості.

Кожен із розглянутих методів має свої переваги та недоліки. Найбільшою перевагою для методів SAST, DAST, SCA є можливість їх автоматизації, що дозволяє постійно тримати під контролем певну групу вразливостей.

Лише комбінація методів дозволяє провести глибокий і всебічний аналіз безпеки ПЗ, мінімізувати ризики та забезпечити необхідний рівень захисту. Використання комплексу методів оцінки кібербезпеки дозволяє не тільки виявляти та усувати вразливості, але й забезпечує розробку ПЗ, яке може ефективно протистояти зовнішнім та внутрішнім загрозам, гарантуючи його надійність і безпеку для кінцевих користувачів.

1. Basutakara, B. S., Jayanthi, D., A review of static code analysis methods for detecting security flaws, *J. Univ. Shanghai Sci. Technol./Shanghai Ligong Daxue Xuebao*, vol. 23, no. 06, pp. 647–653, 2021.
2. Lenarduzzi, V., Pecorelli, F., Saarimaki, N., Lujan, S., Palomba, F., A critical comparison on six static analysis tools: Detection, agreement, and precision, *J. Syst. Softw*., vol. 198, no. 111575, p. 111575, 2023.
3. Trofymenko, O., Dyka, A., Loboda, Y., Analysis of web application testing tools, *Cybersecurity*, vol. 4, no. 20, pp. 62–71, 2023.
4. Vera, Fernando, et al. "Profile of Vulnerability Remediations in Dependencies Using Graph Analysis." *arXiv preprin*t arXiv:2403.04989 (2024).

Частота оновлення маркерів доступу при використанні OAuth 2.0 технології

УДК 004.9

Микола Герцюк[1], Дмитро Новостройний[2]

Державний університет інформаційно-комунікаційних технологій,
gertsiuk@gmail.com[1], digitaldut2022@gmail.com[2]

Одним з найкращих протоколу для аутентифікації користувача до системи є протокол OAuth 2.0. Таке судження може бути зроблене виходячи з аналізу логіки роботи та популярності використання даного протоколу. Зокрема, даний протокол забезпечує можливість проведення валідації сесії, використовуючи маркери доступу(далі токени), які мають визначений час валідації, та час від часу мають бути перегенеровані. Такий підхід робить низькою можливість перехоплення та використання токену зловмисниками. Однак, налаштування часу життя такого маркеру є доволі важливою складовою, оскільки впливає на рівень безпеки інформаційної системи. Аналіз різних інформаційних систем, як Google[1], Facebook[2], Azure[3] та інших систем, що використовує OAuth 2.0 показав, що токени мають наступний час життя:

- короткі: мають час життя від 5 хвилин до 1 години;
- довгі: від 8 годин до 30 днів.

Короткі токени мають наступні переваги для інформаційної системи:

- низький ризик витоку інформації. Токени, що мають короткий час життя дозволяють зменшити ризик в разі, якщо потраплять до рук зловмисників. Очевидно, якщо токен дійсний лише обмежений час, зловмисники матимуть менше часу на його використання в своїх цілях перед тим, як строк їхньої дії буде недоступний;
- менеджмент доступу. Короткий час життя токенів сприяє кращому контролю за доступом користувача до інформаційної системи. Такий підхід дозволить змусити користувачів отримувати токени частіше. Таким чином, адміністратори систем зможуть більш динамічно реагувати на зміну прав доступу та актуалізувати дані користувачів в сесіях.

Водночас, короткі токени мають деякі недоліки, що негативно впливають на функціонування системи:

- збільшене навантаження на сервери авторизації. Короткий час життя токену означає часте оновлення їх. У випадку з великою кількістю користувачів, навантаження на сервер авторизації зростає. Оскільки сервер авторизації є ключовим в будь-якій інформаційній системі, що має функціонал авторизації, продуктивність всієї системи погіршується;
- складність управління сеансами користувачів. Оскільки короткий час життя токенів означає часте їх оновлення, розробники повинні описувати більш складну логіку управління сеансами користувачів. Таким підхід, наприклад, змусить їх створювати окремі таймери в клієнтських складових системи для оновлення, і відмовитись від більш простої логіки оновлення «за запитом»;

– підвищений обсяг трафіку мережі. Часте оновлення токенів означає велику кількість запитів, що можуть призводити до неминучого збільшення трафіку в мережі і викликати проблеми навантаження мережі.

Аналізуючи переваги та недоліки, можна зробити висновок, що короткі токени є більш безпечними, однак вони негативно впливають на продуктивність системи.

Довгий час життя токенів має наступні переваги:

– невисоке навантаження на сервери. Невелика частота оновлення токенів не призводить високого навантаження на сервер авторизації;
– невисоке навантаження на трафік. Низька частота запитів на оновлення токенів не перевантажує сервер авторизації великою кількістю запитів. Відповідно, не спричиняє високе навантаження на трафік.

Однак, існують і недоліки такого підходу:

– збільшений ризик безпеки. В разі заволодіння токеном зловмисниками такий токен стає компрометованим на довгий час. Таким чином існує ризик втрати великої кількості даних;
– складніше управління правами доступу. Довгий час життя токену вимагає в системних адміністраторів враховувати дану характеристику при змінах прав доступу, або інших метаданих, що робить управління користувачами ускладненим та більш статичним процесом.

Аналіз довгих токенів показав, що хоча продуктивність інформаційної системи покращується, безпека даних погіршується.

Існує, також варіант використовувати середній час життя токенів, що має значення від 1 до 8 годин. Такий варіант є прийнятним, як «золота середина» між безпекою та навантаженням на інформаційні системи.

Врахувавши вищеописані переваги та недоліки різних часів життя токенів можна дійти таких висновків:

– якщо безпека інформаційної системи є пріоритетною, потрібно використовувати якнайкоротший час життя токену. Однак, потрібно обов'язково враховувати це при розробці та розгортанні інформаційної системи;
– якщо продуктивність системи повинна бути на першому місці і безпека не є важливою, довгий час життя є найсприятливішим вибором.
– якщо продуктивність системи та безпека є однаково важливими факторами, варто обирати середній час життя токену.

Більш точні значення для різних градацій токенів, зазвичай, обираються індивідуально для кожної інформаційної системи, та мають враховувати велику кількість факторів самої системи.

1. Google for Developers - from AI and Cloud to Mobile and Web. URL: https://developers.google.com/ (дата звернення: 16.04.2024).
2. Meta Developer Documentation | Meta APIs, SDKs Guides. URL: https://developers.facebook.com/docs?locale=en_US (дата звернення: 15.04.2024).
3. Authorize access to REST APIs with OAuth 2.0 - Azure DevOps | Microsoft Learn. URL: https://learn.microsoft.com/en-us/azure/devops/integrate/get-started/authentication/oauth?view=azure-devops (дата звернення: 17.04.2024).

4. Access Tokens - OAuth 2.0 Simplified. URL: https://www.oauth.com/oauth2-servers/access-tokens/ (дата звернення: 17.04.2024).

Кібербезпека колісних транспортних засобів: регламенти ООН

УДК 004.056

Віктор Горицький, Анна Дорошенко

Державне підприємство «Державний автотранспортний науково-дослідний і проектний інститут», gorytski@ukr.net, ad990820@gmail.com

Автомобільна промисловість останні роки стикається з радикальною зміною парадигми в частині інтелектуалізації автомобілів: зі швидкими темпами інтелектуалізації та підключеності колісних транспортних засобів (КТЗ), які підвищують загальну безпеку КТЗ, спостерігається і зростаюча залежність від електроніки, підключеності, насиченості інформаційно-комунікаційними технологіями (ІКТ), що породжує іншу небезпеку – кібернетичну, що породжує проблему кібербезпеки автомобіля.

Ця проблема, як і інші подібні у сфері захисту інформації, вирішується шляхом регламентації, стандартизації, оцінки відповідності (сертифікації), акредитації органів з оцінки відповідності, їх нотифікації (призначення) тощо.

В статті досліджено поточний стан та подальший розвиток зазначеного комплексу міжнародного регулювання в сфері кібербезпеки автомобіля.

Сьогодні у світі формується декілька стандартів та регламентів, які регулюють кібербезпеку автомобіля, що додатково сприяє розгортанню рішень щодо кібербезпеки у всіх, зокрема і підключених автомобілях.

ООН 24 червня 2020 року ухвалила документ WP.29 ЄЕК, який регулює питання кібербезпеки. WP.29 діє у 54 країнах, у тому числі ЄС.

Регламенти ООН юридично забезпечені. Якщо країна або регіон приймає регламент WP.29, то всім виробникам комплектуючих, що діють у ній, потрібен доказ відповідності для проходження обов'язкової сертифікації та подальшого права роботи на ринку. У Європі проходження обов'язкової сертифікації потребує взаємного визнання відповідності нормам на рівні всього автомобіля. Якщо виробник отримує сертифікат на автомобіль певного типу в одній країні ЄС, може продавати таку модель у всіх країнах ЄС без подальших перевірок.

Регламент WP.29 складається з двох основних директив з кібербезпеки автомобілів. Докладніше про них далі.

Перший документ норми ООН щодо кібербезпеки, у рамках документа WP.29 – UN Regulation No. 155. У документі основна увага приділяється кібербезпеці та системам управління кібербезпекою (CSMS).

Визначення WP.29 CSMS: під CSMS розуміється систематичний підхід на основі оцінки ризиків, який визначає організаційні процеси, зони відповідальності та управління для правильного трактування ризиків, пов'язаних з кіберзагрозами транспортних засобів та із захистом транспортних засобів від кібератак.

У документі CSMS добре розглянуті загрози, пов'язані з кібербезпекою, наведено великий перелік уразливостей та методів атаки. Додаток 5 містить 10 сторінок з описом уразливостей, розподілених по безлічі категорій. У першій з

таблиць, наведених нижче, узагальнено погрози та вразливості. Існує 6 типів загроз і безліч типів уразливостей (29) з безліччю прикладів (67), перелічених у документі *CSMS.*

Другий документ норми ООН щодо кібербезпеки, в рамках документа WP.29 – UN Regulation No. 156. Другий регулюючий документ стосується процесів оновлення програмного забезпечення та систем керування такими оновленнями (SUMS).

Визначення WP.29 SUMS: Система управління оновленнями програм – це систематичний підхід, що визначає, які організаційні процеси та процедури повинні відповідати вимогам щодо доставки програмних оновлень згідно з цим регулюючим документом.

Нова регулююча норма ООН про універсальні передумови до оновлень програм та систем управління оновленнями програм застосовується до автомобілів, робота яких залежить від оновлення програмного забезпечення. Ця норма також стосується трейлерів та сільськогосподарської техніки, а також пасажирського транспорту, фургонів, вантажівок та автобусів.

UN Regulations: WP29, ECE155, ECE156 — Правила ООН про однакові положення щодо офіційного затвердження транспортних засобів щодо кібербезпеки та їх систем управління кібербезпекою. Вимоги наказують отримання сертифікату відповідності для компанії та Vehicle Type Approval для кожної моделі автомобіля. Без цих сертифікатів з 2024 року продавати автомобілі у низці країн буде неможливо.

Рис. 1. Процес впровадження вимог щодо кібербезпеки автомобіля

Виконання вимог Правил ООН підтверджується двома документами:

1. Сертифікат CSMS – Cyber Security Management System (сертифікат, що підтверджує наявність системи керування кібербезпеки у OEM). Сертифікат видається на OEM загалом та діє протягом 3-х років.
2. Сертифікат VTA - Vehicle Type Approval (сертифікат, що підтверджує те, що автомобіль розроблений з урахуванням вимог кібербезпеки (SDLC). Сертифікат видається на весь термін життя кожного окремої моделі.

1. https://unece.org/sites/default/files/2024-03/R156e%20%282%29.pdf
2. https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf

Задачі кібербезпеки в хмарних обчисленнях.

Давиденко А.М.

Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, davidenkoan@gmail.com

Сучасність, хмари кібербезпека. Сучасний світ зрозумів що потрібні обчислювальні потужності не завжди потрібні. Тому з'явилися хмари, але на відміну від інтернету вони зразу будуються в захищеному варіанті. Але основне протиріччя пов'язане з вартістю заходів кібербезпеки які суттєво збільшує собівартість технологічних або бізнес процесів на відміну від головної мети отримання прибутку або досягнення мінімальної собівартості. Розглянемо як вирішують цю проблему гравці ринку надання хмарних послуг.

Хмарні провайдери організовують на базі обраних платформ хмарні сервіси, які надалі здаються в оренду бізнесу. Таке рішення забезпечує користувачам по всьому світу доступ до високопродуктивних ресурсів для створення власної інфраструктурі.

Розрізняють приватні та публічні хмари. З нашої точки зору більш цікави саме публічні. Існує три підходи до надання послуг :

IaaS (Infrastructure as a Service) — інфраструктура як сервіс;

PaaS (Platform as a Service) – платформа як сервіс;

SaaS (Software as a Service) – програмне забезпечення як сервіс.

В першому варіанте постачальник послуги надає в оренду обчислювальні ресурси. Це може бути сукупність віртуальних машин, сховищ даних, мережевих елементів різних типів. За допомогою IaaS користувач може швидко розгортати копії ОС, запускаючи віртуальні копії ряду програмних пакетів. У цьому випадку немає потреби розгортати власну інфраструктуру. Все необхідне надається постачальником IaaS. При цьому таке середовище є гнучким та масштабованим.

В другому PaaS – це один із способів надання клієнту готового програмного середовища. Одночасно надаються інструменти для тонкого налаштування такого середовища. Елементами PaaS є апаратне забезпечення, операційна система, СУБД, проміжне ПЗ, інструменти тестування та розробки.

Третій варіант SaaS використовується розробниками програмних застосунків з наданням віддаленого доступу до продукту. Відомім прикладом SaaS може бути Microsoft Office 365. Корпорація Microsoft надає за моделлю SaaS доступ клієнтам до MS Office Suite (Office Web Apps).

Найбільш вагома частка ринку хмарних послуг приблизно 2/3 це Amazon Web Services, Microsoft Azure та Google Cloud . AWS перший, Microsoft має велику клієнтську базу, Google активно зростає доганяючи перших.

Компанія AWS пропонує під заголовком «Безпека, ідентифікація та відповідність вимогам» 23 продукти які забезпечують ідентифікацію, керування доступом, моніторинг та аудит, захист даних в транзите та спокої, кожна функція захисту має різні варіанти від простих та дешевих, до коштовних але досить надійних та зручних рішень. Ефективність рішення залежить від досвіду та наявного бюджету користувача. Інтересним є рішення пов'язане з розподілом

обов'язків між компанію та користувачем просте ознайомлення з ним вже значно підвищує безпеку користувача.

Головним лозунгом компанії Microsoft є «комплексний та економічно ефективний захист». Вона пропонує: захист за допомогою ШІ; єдину платформу заходів безпеки, яка поєднує можливості розширеного виявлення та реагування (XDR) і керування захистом інформації (SIEM); посилення безпеки обробки та збереження даних за допомогою багатошарової системи захисту; засобі ідентифікації та автентифікації для контролю та розмежуванню доступу; засобі забезпечення повній видимості та комплексному захисту робочих навантажень; засобі моніторингу та аналізу ризиків.

Головним лозунгом компанії Google є «передовий підхід до захисту й забезпечення відповідності вимогам». Вона пропонує: автоматизовані засоби захисту на основі штучного інтелекту Google, щоб запобігати атакам і забезпечувати безперебійну роботу; засобі для оперативного виявлення, сортування й усування загроз; хмарні додатки на базі глобальної інфраструктури Google; засобі налаштування доступу до даних усередині організації і поза її межами; політику шифрування даних на боці клієнта; систему штрафів за недотримання вимог, використовування несертифікованих рішень.

Існує також багато окремих сервісів. Перелічимо найбільш популярні.

Dropbox - хмара доступна для користувачів практично всіх популярних ОС. Недорогий сервіс для зберігання різноманітних файлів увійшов до рейтингу не тільки завдяки універсальності: є в нього інші позитивні якості.

Google Диск - зручний варіант для зберігання різних файлів, якими можна ділитися з іншими користувачами. Гугл Диск — один із найзахищеніших і зручніших сервісів.

Microsoft OneDrive - віртуальне сховище файлів та файлообмінник, запущений ще у 2007 році.

iCloud Drive - інформаційний інтернет-сейф від Apple встановлено на всіх «яблучних» гаджетах: треба тільки створити облік.

Mega - перспективний хмарний файлообмінник від Kim Dotcom — компанії, відомої всьому світу дітищем Megaupload. Про сервіс відгукуються добре не тільки завдяки щедрості творців, але і внаслідок інших приємних характеристик.

pCloud - створене швейцарською компанією сховище файлів набуло популярності внаслідок країни-творця: вона відома своїм трепетним ставленням до конфіденційності.

Підсумуючи можна визначити компанії розуміють зазначене в початку огляду протиріччя. Вони перекладають його вирішення на бік клієнта, але пропонують широкий спектр інструментарію, це **засобі штучного інтелекту**, **ідентифікації та автентифікації**, **моніторингу** та **автоматизації реагування на інциденті кібербезпеки**.

Тенденції та виклики у навчанні з кібербезпеки

УДК 004.056.5 (355.4)

Максим Делембовський[1], Денис Калениченко[2]

[1]Київський національний університет будівництва і архітектури, delembovskyi.mm@knuba.edu.ua, [2]Київський національний університет імені Тараса Шевченка, denys.kalenychenko.student@knu.ua

Сучасний світ цифрових технологій постійно розвивається, а з ним і загрози кібербезпеки стають все складнішими та різноманітнішими. Ця динаміка ставить перед освітніми інституціями низку викликів у підготовці кваліфікованих фахівців у галузі кібербезпеки. Тематика зосереджується на аналізі основних тенденцій, таких як адаптація курсів до найновіших технологічних загроз, використання інтерактивних та іммерсивних технологій для підвищення ефективності навчання. Також в роботі розглядаються ключові виклики, включаючи нестачу кваліфікованих викладачів, потребу в постійному оновленні навчальних матеріалів, а також проблеми зі збалансуванням теоретичних знань та практичних навичок. Дана тематика спрямована на визначення шляхів оптимізації навчального процесу, щоб випускники могли ефективно реагувати на кіберзагрози в реальному світі [1-3].

Освітній ланшафт з кібербезпеки формується швидкою еволюцією загроз та технологічних досягнень, представляючи складний набір викликів та тенденцій, які викладачі та фахівці повинні долати.

Однією з основних тенденцій, що спостерігається, є інтеграція штучного інтелекту (AI) та машинного навчання (ML) в навчальні програми з кібербезпеки. Освітні заклади все частіше використовують ці технології для забезпечення більш адаптивного навчального досвіду, який налаштовує навчальний контент відповідно до потреб учня. Цей підхід не лише робить процес навчання ефективнішим, але й допомагає підготувати студентів до реальних сценаріїв, де AI та ML відіграють значущу роль у виявленні загроз та реагуванні на них [4].

Однак, є і значні виклики. Швидкий темп технологічних змін вимагає, щоб навчальний контент постійно оновлювався, щоб залишатися актуальним, що становить логістичний та фінансовий виклик для багатьох установ. Крім того, зростаюча складність кіберзагроз вимагає відповідного розвитку навчання та інструментів, доступних для професіоналів кібербезпеки, роблячи важливим для освітніх програм йти в ногу з потребами індустрії [5].

Більше того, Всесвітній економічний форум підкреслює важливість антиципації майбутніх викликів кібербезпеки. Вони вважають, що поле кібербезпеки повинно адаптуватися до середовища, де довіра стає все рідкіснішою, а технологічна цілісність є вирішальною. Вони також прогнозують, що освіта з кібербезпеки повинна зосереджуватися не лише на захисті, а й на підтримці стійкості та здатності відновлюватися після кіберінцидентів[1-3].

Загалом, поки галузь освіти з кібербезпеки розвивається завдяки введенню нових технологій та методологій,она також стикається з постійним викликом адаптації до швидко змінюваного ландшафту загроз. Ця динаміка вимагає постійних інвестицій у освітні ресурси, інноваційні методики навчання та

прогресивний підхід до розробки навчальних програм, щоб ефективно підготувати наступне покоління фахівців з кібербезпеки.

Для вирішення викликів у навчанні з кібербезпеки можна застосувати кілька стратегій:

1. Регулярне оновлення навчальних матеріалів для відображення найновіших технологічних інновацій та кіберзагроз. Це забезпечує, що студенти вивчають актуальні техніки та методи кібербезпеки.
2. Інтеграція штучного інтелекту та машинного навчання для створення адаптивних навчальних платформ, які відповідають індивідуальним потребам студентів, підвищуючи ефективність навчання.
3. Надання студентам доступу до практичних лабораторій та симуляцій, що дозволяють їм застосовувати теоретичні знання в реальних сценаріях, підвищуючи їх готовність до роботи.
4. Співпраця між різними дисциплінами, такими як комп'ютерні науки, інженерія та право, для створення всебічних освітніх програм, що включають різні аспекти кібербезпеки.
5. Стимулювання неперервного навчання серед професіоналів у галузі кібербезпеки через сертифікації та регулярні тренінги для підтримки їхніх знань на високому рівні.
6. Підтримка глобальної співпраці між освітніми закладами та індустрією для обміну кращими практиками та розробки спільних навчальних ініціатив.

1. Шестаковська Т.Л. Аналіз тенденцій та викликів впливу цифрових технологій на публічне управління. Economic Synergy, 2023, 2: 8-22.
2. Бучма О.В.; Гнинюк Р.Ю. Особливості сучасного стану кібербезпеки України. 2018. PhD Thesis. НПУ імені МП Драгоманова.
3. Essien N.P.; Ekaiko U.A. Cyber security: trends and challenges toward educational development in 21st century. Asia-Africa Journal of Education Research, 2022, 2: 141-156.
4. #CybersecurityAwarenessMonth - The Evolution of Cybersecurity Education. (б. д.). Cybersecurity Certifications and Continuing Education | ISC2. https://www.isc2.org/Insights/2023/10/Evolution-of-Cybersecurity-Education
5. An Executive View of Key Cybersecurity Trends and Challenges in 2023. (б. д.). ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2023/an-executive-view-of-key-cybersecurity-trends-and-challenges-in-2023
6. 7 trends that could shape the future of cybersecurity in 2030. (2023, 3 березня). https://www.weforum.org/agenda/2023/03/trends-for-future-of-cybersecurity/

Параметрична оптимізація законів руху портального маніпуляційного робота

УДК 531.8+62-50

Мирослав Демидюк[1, 2], Богдан Проць[2]

[1]*Інститут прикладних проблем механіки і математики ім. Я.С.Підстригача НАН України,*
[2]*Львівський національний університет імені Івана Франка,*
myroslav.demydyuk@lnu.edu.ua, bohdan.prots@lnu.edu.ua

Актуальність дослідження зумовлена постійною потребою в удосконаленні наявних та створенні нових зразків маніпуляційних роботів із високими експлуатаційними показникам. *Мета* дослідження – побудувати алгоритм та комп'ютерну програму для оптимізації законів руху маніпуляційного робота портального типу. Запропонована розробка розвиває підхід параметричної оптимізації в розв'язуванні задач оптимального керування робототехнічними системами [1–3].

Розглядаємо портальний робот, що виконує плоскопаралельний рух у вертикальній площині O_1XY (рис.1). Основними складниками робота є каретка G та дволанковий маніпулятор O_1O_2B. Каретка G під дією сили F поступально переміщається вздовж горизонтальної балки 1, встановленої на вертикальних колонах 2 і 3. Колони своїми нижніми кінцями закріплені на нерухомій основі. До каретки з допомогою циліндричного шарніра O_1 приєднаний дволанковий маніпулятор, ланки якого з'єднані між собою циліндричним шарніром O_2. На кінці другої ланки встановлено захоплювач із вантажем. Поворот ланок маніпулятора відбувається під дією моментів сил u_1, u_2, прикладених відносно осей шарнірів O_1, O_2. Тертям у системі нехтуємо, захоплювач (з вантажем) моделюємо точковою масою m (у точці B).

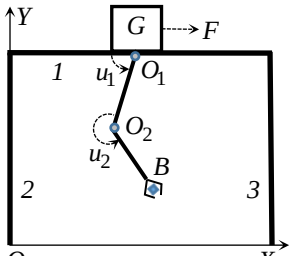


Рис.

Рівняння руху портального робота являють собою систему трьох нелінійних звичайних диференціальних рівнянь другого порядку, які описують зміну узагальнених координат $x(t)$, $\alpha(t)$, $\beta(t)$ під дією керувань $F(t)$, $u_1(t)$, $u_2(t)$. Тут $x(t)$ – відстань від осі OY до полюса O_1, $\alpha(t)$, $\beta(t)$ – кути відхилення ланок O_1O_2, O_2B від вертикалі (осі OY).

Нехай маніпулятор на проміжку часу $[0,T]$ виконує транспортну операцію – переносить вантаж із заданого початкового положення в задане кінцеве:

$$x(\tau)=x_\tau,\ \alpha(\tau)=\alpha_\tau,\ \beta(\tau)=\beta_\tau,\ \dot{x}(\tau)=\dot{\alpha}(\tau)=\dot{\beta}(\tau)=0,\ \tau=0,T, \qquad (1)$$

де T, $(x_\tau,\alpha_\tau,\beta_\tau)\big|_{\tau=0,T}$ – задані сталі параметри транспортної операції, крапкою

над змінними позначено диференціювання за часом t. Сформулюємо таку задачу оптимального керування.

Задача 1. Визначити оптимальні керування $F^*(t)$, $u_1^*(t)$, $u_2^*(t)$, $t \in [0,T]$, які забезпечать виконання маніпулятором транспортної операції (1) з мінімальним значенням функціонала

$$E = \int_0^T [F^2(t) + u_1^2(t) + u_2^2(t)]dt \tag{2}$$

Квадратичний функціонал типу (2) часто використовують у задачах оптимізації робототехнічних систем. За певних припущень такий функціонал опосередковано оцінює енерговитрати на переміщення системи [3].

З огляду на нелінійність рівнянь руху портального робота та взаємозалежність між його узагальненими координатами використаємо для побудови субоптимального розв'язку *задачі 1* метод параметричної оптимізації [1, 2]. Згідно із цим методом подамо узагальнені координати механічної системи у вигляді суми кубічного полінома та скінченного тригонометричного ряду

$$q_i = \sum_{k=0}^{3} p_{ik} t^k + \sum_{k=1}^{n} (a_{ik} \cos k\frac{2\pi}{T} t + b_{ik} \sin k\frac{2\pi}{T} t), \quad i = \overline{1,3}, \tag{3}$$

де $q_1 = x(t)$, $q_2 = \alpha(t)$, $q_3 = \beta(t)$, $\{p_{ik}\}_{k=0}^{3}$ – коефіцієнти, які визначаємо з умов транспортної операції (1), $\{a_{ik}\}_{k=1}^{n}$ – коефіцієнти, які знаходимо у вигляду розв'язку допоміжної задачі нелінійного програмування, n – заданий параметр.

Узагальнені швидкості та прискорення робота обчислюємо диференціюванням (3) за часом t. Далі, використовуючи підхід обернених задач динаміки, після підставлення параметризованих функцій (3) у рівняння руху робота отримуємо параметризоване сімейство шуканих керувань, що в кінцевому підсумку зводить вихідну *задачу 1* до задачі мінімізації $\tilde{E}(\mathbf{z}) \xrightarrow[\mathbf{z}]{} \min$. Тут $\tilde{E}(\mathbf{z})$ – функція коефіцієнтів параметризації $\mathbf{z} = (a_{ik};\ k = \overline{1,n},\ i = \overline{1,3})$, яку отримуємо після підставлення параметризованих керувань у функціонал (2).

Запропонований алгоритм реалізовано на мові програмування Java в програмному середовищі Intellij IDEA Ultimate. Проведено серію числових розрахунків, результати яких підтвердили ефективність методу параметричної оптимізації керованого руху досліджуваного портального робота.

На рис. 2 – рис. 4 показані графіки отриманих субоптимальних характеристик портального робота з такими параметрами: маса каретки рівна 10 кг, ланки мають кільцевий поперечний переріз зі сталими зовнішнім 0.1 м і внутрішнім 0.094 м діаметрами та сталою густиною матеріалу 7850 кг/м3, довжини ланок 0.8 м і 0.6 м (відповідно маси ланок рівні 5.74 кг та 4.30 кг). Масу захоплювача (з вантажем) задавали рівною 1 кг.

Параметри транспортної операції: $x_0 = 1$ м, $\alpha_0 = -\pi/4$, $\beta_0 = 0$, $x_1 = 5$ м, $\alpha_1 = 0$, $\beta_1 = \pi/4$, $T = 10$ с.

У параметричному представленні (3) покладали $n = 8$, відповідно кількість

параметрів оптимізації становила 48. Для мінімізації функції $\widetilde{E}(\mathbf{z})$ використовували алгоритм циклічного покоординатного спуску з початковим значенням $\mathbf{z}=0$. Точність за параметрами оптимізації та значенням цільової функції задавали 10^{-6} і 10^{-3}.

У результаті розрахунків отримали мінімальне значення $\widetilde{E}^{*}=107.5$, що є меншим приблизно у 2.5 рази від початкового значення $\widetilde{E}(\mathbf{z})_{|\mathbf{z}=0}=269.4$.

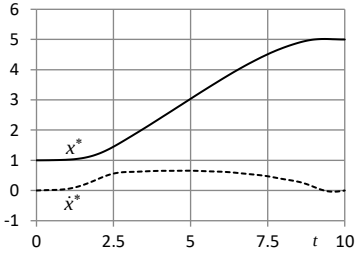


Рис. 2. Закон руху і швидкість каретки

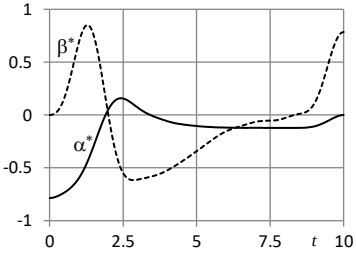


Рис. 3. Закон обертального руху ланок маніпулятора

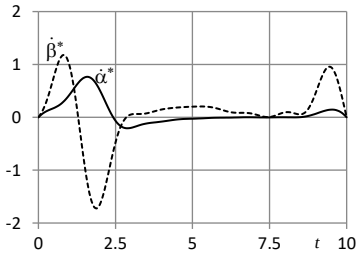


Рис. 4. Кутова швидкість ланок маніпулятора

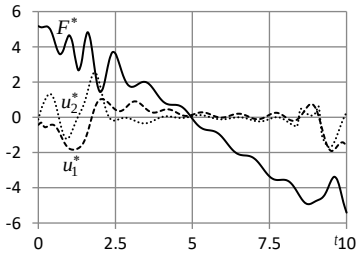


Рис. 5. Керування портального робота

1. Demydyuk M.V. Parametric optimization of four-link close-chain manipulator with active and passive actuators. *J. of Mathematical Sci*. – 2010. – 168, No. 5. – P. 746–758.
2. Demydyuk M. V., Hoshovs'ka N.V. Parametric optimization of the transport operations of a two-link manipulator. *J. of Mathematical Sci*. – 2019. – 238, Is. 2. – P. 174–88.
3. Demydyuk M.V., Lytwyn B.A. Optimization of the parameters of feet and the laws of motion of bipedal walking robots. *J. of Mathematical Sci*. – 2023. – 270, Is. 1. – P. 214–236.

Методи виявлення вторгнення в IT інфраструктуру

УДК 07.01.02

Дмитро Денисюк[1], Олег Савенко[2],
Антоніна Каштальян[3]

Хмельницький національний університет, [1]denysiuk@khmnu.edu.ua ,
[2]savenko_oleg_st@ukr.net,[3]yantonina@ukr.net

IT інфраструктура представляє собою комплекс систем, обладнання та програм, що необхідні для операційного функціонування інформаційних технологій у певній організації чи компанії. Ця інфраструктура включає в себе сервери, системи зберігання даних, мережеве обладнання, програмне забезпечення, засоби комунікацій та інструменти забезпечення безпеки, спрямовані на забезпечення обміну, зберігання та обробку інформації всередині організації. Згідно з звіту за 2023 рік компаній у сфері кібербезпеки CiscoTalos[1] і SonicWall[2], зафіксовано тенденцію у використанні зловмисного програмного забезпечення (ЗПЗ), спрямованого на вбудовування програм-майнерів, атаки на мережеві пристрої та шифрування даних в інфраструктурі організацій з метою вимагання викупу. Ці типи вторгнень отримали значний розвиток завдяки інтенсивному застосуванню штучного інтелекту (ШІ), що дозволило прискорити процес розробки шкідливого програмного забезпечення. Використання ШІ у кібератаках дозволяє зловмисникам автоматизувати та ускладнювати методики атак, застосовуючи технології машинного навчання для аналізу, адаптації та вдосконалення їхніх атакуючих стратегій.

З розвитком атак на основі ШІ почався розвиток методів виявлення вторгнень, які базуються на машинному навчанні. Найпоширеніші методи виявлення вторгнень включають навчання з учителем[3], навчання без учителя[3], гібридні[3] та мета-навчання[3]. Навчання з учителем використовує набір позначених даних для навчання моделі класифікації. Навчання без учителя спирається на непозначені дані, використовуючи методи кластеризації або виявлення аномалій. Гібридні методи комбінують підходи навчання з учителем та без учителя для досягнення кращої ефективності. Мета-навчання використовується для автоматичної настройки параметрів моделей виявлення вторгнень на основі змін у середовищі або типах атак. Хоча машинне навчання є ефективним інструментом для виявлення вторгнень, важливо зауважити, що воно не гарантує абсолютної ефективності. У таблиці 1 наведено порівняльний аналіз методів машинного навчання[4], спрямованих на виявлення вторгнень. В ній продемонстровано, як залежать характеристика виявлення вторгнень, від вибору методу машинного навчання. Крім того, важливо розуміти, що різні моделі машинного навчання можуть мати різні сильні та слабкі сторони в контексті виявлення вторгнень. Наприклад, деякі моделі можуть бути більш ефективними виявлення аномалій, тоді як інші можуть бути краще пристосовані для виявлення певних типів атак. Правильний вибір моделі може бути важливим для досягнення високої точності та надійності системи виявлення вторгнень. Таким чином, враховуючи особливості конкретного середовища та характеристики потенційних загроз, важливо обирати модель, яка найкращим чином відповідає потребам захисту інформації.

Таблиця 1

Порівняльний аналіз методів навчання для виявлення вторгнень

Характеристика	Навчання з учителем	Навчання без учителя	Гібридні методи	Мета-навчання
Використання позначених даних	Так	Ні	Залежить від моделі	Залежить від моделі
Використання непозначених даних	Ні	Так	Так	Так
Потреба в експертному втручанні	Ні	Можливо	Залежить від моделі	Можливо
Здатність виявляти нові атаки	Слабка	Можливо	Залежить від моделі	Можливо
Ефективність у виявленні аномалій	Висока	Висока	Залежить від моделі	Залежить від моделі

З таблиці 1 видно, що методи машинного навчання є потужним інструментом для створення систем виявлення вторгнень. Вони володіють здатністю адаптуватися до різних видів атак та аномалій, що може виявитися критичним у великих обсягах даних. Однак, оскільки зловмисники постійно вдосконалюють свої методи, наявна потреба у постійному вдосконаленні механізмів виявлення вторгнень для ефективного протидії новим загрозам.

Подальше дослідження спрямоване на створення системи виявлення вторгнень, яка буде виявляти backdoor у IT інфраструктурі. Ця система буде заснована на аналізі файлів, що завантажуються на сервер, з метою виявлення у них команд для виконання зловмисних дій. Додатково буде проведено дослідження для ідентифікації потенційних вразливостей та розроблено методи для їхнього ефективного усунення.

1. CiscoTalos. URL: https://blog.talosintelligence.com/content/files/2023/12/2023_Talos_Year_In_Review.pdf (дата звернення: 20.04.2024)
2. SonicWall. URL: https://www.sonicwall.com/medialibrary/en/white-paper/2024-cyber-threat-report.pdf (дата звернення: 20.04.2024)
3. Kolhar M., Aldossary SM. A Deep Learning Approach for Securing IoT Infrastructure with Emphasis on Smart Vertical Networks. *Designs*, 2023, 7.6: 139.
4. Zhukov I., Okhrimenko T., Balakin S., Chaikovska O., Sulkowski K. Risk assessment in critical infrastructure computer networks. *CEUR Workshop Proceedings*. 2023. p. 272-277.

Математична модель для аналізу інформаційних потоків в соціокіберфізичних системах

УДК 004.056

Наталія Дженюк [1], Максим Толкачов [2]

Національний технічний університет "Харківський політехнічний інститут",
[1]natalidzh16@gmail.com, [2]maksymtolkachov@gmail.com

Природа динамічних фізичних середовищ ставить під сумнів здатність соціокіберфізичних систем до адекватного управління фізичними активами у різноманітних ситуаціях. Отже, проектування соціокіберфізичних систем повинно гарантувати не тільки надійну автономію, але й стійкість у експлуатації та безпеку. Запропонований метод базується на інтеграції специфічних (змішаних) загроз через поєднання технічних кіберзагроз і методів соціальної інженерії.

Аналіз публікацій останніх років дозволяє зробити висновок, що під час створення соціокіберфізичних систем і систем, які забезпечують безпечне їх функціонування, недостатньо досліджені питань, пов'язаних з інформаційними процесами соціальної складової, а також семантичними елементами переданої інформації. Тому вказані питання аналізу сприйняття, оцінки, обміну та обробки інформації є актуальними і пояснюють необхідність розробки методик оцінки цих процесів.

Набори даних із різних сфер зазвичай містять семантичні дані, визначені за широким набором атрибутів, між якими існують різні ступені кореляції.

Ми зосереджуємося на виявленні об'єктів даних, які демонструють аномальну поведінку за підмножиною атрибутів, названих поведінковими, у відношенні до інших, названих контекстними. Основний вклад полягає у розробці моделі для опису законів кореляції, прихованих у розподілах даних між парами поведінкових та контекстних атрибутів. Вводиться ймовірнісний показник, спрямований на оцінку спостережуваних об'єктів на основі того, наскільки їхні дії відхиляються від виявлених законів кореляції [1].

Кореляція між зазначеними атрибутами існує як на рівні топології, так і на рівні семантичного змісту наборів даних, а також у часовому аспекті. Таким чином, результатом цього етапу стане набір кластерів даних, корельованих між собою. Ці кластери вказують на події, які корелюють одна з одною за часовими, семантичними та топологічними показниками.

Математичну модель цього процесу можна розглядати як модель, з використанням якої необхідно визначити маніпулятивні фактори на основі спостережуваних моделей переконань або думок цільової аудиторії [2].

Припустимо, що у нас є потік інформації, що складається з набору N повідомлень. Кожне повідомлення характеризується набором атрибутів, що описують його зміст, контекст, семантичні ознаки. Семантичні ознаки, що вилучені з інформації джерела, дозволяють моделювати особисті характеристики користувача. Кожне повідомлення може бути представлене у вигляді вектора ознак, де кожна ознака – це бінарна змінна, яка вказує на наявність або відсутність певної характеристики.

Також визначимо набір шаблонів M або шаблони, що охоплюють ключові характеристики повідомлень, пов'язаних з певними темами.

Для аналізу ентропії інформаційного потоку та вилучення відповідних даних може бути використаний метод, такий як порівняння зі зразком або кластеризація. Це дозволяє ідентифікувати повідомлення, які відповідають шаблонам з бібліотеки. Бібліотеку шаблонів можна представити у вигляді матриці P, де кожен рядок відповідає певному шаблону, а кожен стовпець – певній функції:

Щоб визначити повідомлення, схожі на шаблони у нашій бібліотеці, ми можемо представити повідомлення у вигляді векторів функцій та обчислити їхню схожість з кожним шаблоном, використовуючи такі міри, як косинусна схожість чи схожість Жаккара. Наприклад, представляючи повідомлення у вигляді вектора M, його косинусну схожість з кожним шаблоном у нашій бібліотеці обчислюється наступним чином:

$$similarity(M, P_i) = \frac{dot(M,P_i)}{(norm(M) \cdot norm(P_i))} \quad (1)$$

де $dot(M, P_i)$ – скалярное произведение векторов M и P_i,
$norm(M)$ и $norm(P_i)$ – евклидовы нормы векторов M и P_i.

Ця міра подібності може бути використана для визначення k найкращих шаблонів, які найкраще відповідають кожному з повідомлень, і використовувати їх для витягування відповідних даних чи ідей. Наприклад, якщо повідомлення найбільше відповідає зразку політики, можна зробити висновок, що воно містить політичний контент, і додати його до бази даних політичних повідомлень.

Таким чином, побудована математична модель дозволяє аналізувати ентропію інформаційних потоків та витягувати відповідні дані з використанням бібліотеки шаблонів, що можуть бути корисні для розуміння динаміки розповсюдження інформації та розробки ефективних заходів втручання або протидій.

Запропонований підхід у майбутньому сприятиме покращенню контролю та управління в галузі кібербезпеки, забезпечуючи врахування різних аспектів, включаючи соціальні та сприйняттєві фактори.

1. Fabrizio Angiulli, Fabio Fassetti, Cristina Serrao, Anomaly detection with correlation laws, Data & Knowledge Engineering, Volume 145, 2023, 102181, ISSN 0169-023X, https://doi.org/10.1016/j.datak.2023.102181.
2. Yevseiev, S., Dzheniuk, N., Tolkachov, M., Milov, O., Voitko, T., Prygara, M., Shpak, O., Voropay, N., Volkov, A., & Lezik, O. (2023). Development of a multi-loop security system of information interactions in socio-cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 5(9 (125), 53–74. https://doi.org/10.15587/1729-4061.2023.289467

Розробка алгоритму автентифікації на основі криптокодової конструкції Мак-Еліса

УДК 004.056.5

Сергій Дунаєв[1], Вадим Стеценко[2]

Національний Технічний Університет "Харківський Політехнічний Інститут", [1]serg.dynaev@gmail.com, [2]4all2dream@gmail.com

Автентифікація - це процес перевірки та підтвердження ідентичності користувача, системи або пристрою. Головною метою аутентифікації є забезпечення впевненості у тому, що суб'єкт, який намагається отримати доступ до системи або ресурсу, дійсно той, за кого себе видає. Процес аутентифікації може включати в себе різні методи та засоби перевірки ідентичності, такі як введення пароля, використання біометричних даних (наприклад, відбитків пальців або скану обличчя), використання токенів або смарт-карт, а також двофакторну автентифікацію. Автентифікація є важливою складовою частиною системи безпеки та доступу до інформації в будь-якій області, включаючи комп'ютерні мережі, фінансові транзакції, мобільні пристрої, фізичний доступ до приміщень та інші.

Використання постквантових алгоритмів, таких як крипто-кодові конструкції Мак-Еліса/Нідеррайтера [1,2] на різних типах кодів, забезпечує необхідний рівень стійкості, швидкості та вірогідності інформації в постквантовій епохи та забезпечує їх практичне застосування на ресурсообмежених пристроях.

Для забезпечення послуги автентичності між абонентами *А* та *Б* в доповіді пропонується використовувати еліптичний код *(25,19,3)*, з елементами з поля $GF(2^4)$, *n,k,d* параметри коду дають йому змогу виправляти одну помилку з поля $GF(2^4)$. Структурна схема автентифікації на основі теоретико-кодовій конструкції Мак-Еліса представлена на рисунку1.

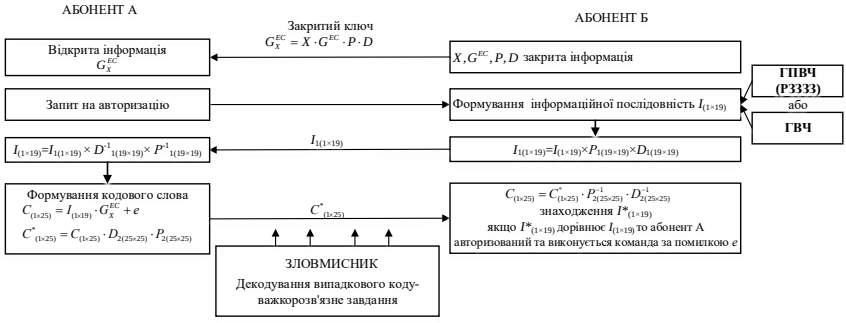


Рис.1. Структурна схема автентифікації на основі теоретико-кодовій конструкції Мак-Еліса для коду *(25,19,3)*

Запропонований процес автентифікації складається з наступних кроків:

1. Абонент *А* посилає пакет із запитом на авторизацію.

2. Абонент *Б* використовуючи генератор псевдовипадкових чисел або генератор випадкових чисел формує двійкову послідовність з 76 біт.

3. Отримане число з 76 біт абонент *Б* перетворює на інформаційну послідовність $I_{(1\times19)}$ з елементами поля $GF(2^4)$, за рахунок використання мультиплексорів.

4. Абонент *Б* проводить перетворення інформаційній послідовності $I_{(1\times19)}$ за рахунок використання діагональної матриці $D_{1(19\times19)}$ та перестановочної матриці $P_{1(19\times19)}$ та відправляє отримане повідомлення абоненту *А* $(I_{1(1\times19)}=I_{(1\times19)}\times P_{1(19\times19)}\times D_{1(19\times19)})$.

5. Абонент *А* отримавши повідомлення $I_{1(1\times19)}$ проводить зворотне перетворення $I_{(1\times19)}=I_{1(1\times19)}\times D^{-1}{}_{1(19\times19)}\times P^{-1}{}_{1(19\times19)}$.

6. Абонент *А* формує додатковий сеансовий ключ – *е* (вектор помилки, який може відповідати деякій команді абонента *Б*). Вектор помилки може приймати значення з поля $GF(2^4)$, тобто включати в себе до 15 команд.

7. Абонент *А* формує кодове слово з помилкою та відправляє абоненту *Б*. Для ускладнення роботи зловмисника отримане кодове слово $C_{(1\times25)}=I_{(1\times19)}\times G^{EC}{}_X+e$ (перемножує з діагональною матрицею $D_{2(25\times25)}$ та перестановочною матрицею $P_{2(25\times25)}$ та відправляє отримане кодове слово $C^*_{(1\times25)}=(I_{(1\times19)}G^{EC}{}_X+e)\times D_{2(25\times25)}\times P_{2(25\times25)}$ абоненту *Б*.

8. Абонент *Б* отримавши кодове слово $C^*_{(1\times25)}$ проводить зворотне перетворення $C_{(1\times25)}=C^*_{(1\times25)}\times P^{-1}{}_{2(25\times25}\times D^{-1}{}_{2(25\times25))}$.

9. Отримавши кодове слово $C_{(1\times25)}$ абонент *Б*, на підставі швидкого алгоритму розкодування Берлекемпа-Мессі виконується знаходження вектора помилки *е* та інформаційне слово $I^*_{(1\times19)}$. Якщо $I^*_{(1\times19)}$ дорівнює $I_{(1\times19)}$ то абонент *Б* виконує команду згідно з помилкою *е*.

Запропонована схема автентифікації на основі конструкції Мак-Еліса дозволяє забезпечити необхідний рівень послуг конфіденційності, цілісності та автентичності. Такий підхід забезпечує необхідний рівень захищеності послуг безпеки, а використання різних завадостійких кодів, дозволяє з урахуванням рівня секретності інформації забезпечити її зниження енергоємності та підвищити оперативність передачі інформації.

1. R.J. McEliece. A Public-Key Criptosystem Based on Algebraic Theory // DGN Progres Report 42 – 44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114 – 116.
2. H. Niederreiter. Knapsack-Type Cryptosystems and Algebraic Coding Theory. // Probl. Control and Inform. Theoty. – 1986. – V. 15. – P. 19 – 34.

Розробка методу генерації зображень на основі заданого текстового опису для обходу водяних знаків

УДК 621.395.7 (043.2)

Максим Житніков[1], Дмитро Пелешко[1,2], Олена Винокурова[2]

[1]Національний університет "Львівська Політехніка", maksym.zhytnikov.mknssh.2023@lpnu.ua
[2]Львівський національний університет ім. Івана Франка, dmytro.peleshko@lnu.edu.ua, olena.vynokurova@lnu.edu.ua

Водяні знаки - це поширений метод захисту авторських прав і прав власності на цифрові зображення шляхом вбудовування ледь помітного знаку або візерунка, який ідентифікує автора або законного власника. Однак цей метод іноді може бути перешкодою, особливо у випадках, де візуальна цілісність зображення має першорядне значення. Тому зростає інтерес до розробки технологій, які можуть генерувати зображення, обходячи водяні знаки або захищаючи від них [1]. Генеративні алгоритми можуть створювати абсолютно нові зображення. Ця здатність робить їх ідеальними для створення зображень, які природним чином уникають будь-яких водяних знаків, які зазвичай наносяться на оригінальні роботи.

Метод генерації зображень на основі заданого текстового опису може зробити значний внесок у вирішення проблеми обходу цифрових водяних знаків кількома способами. По-перше, ці архітектури призначені для генерування нових зображень з текстових описів [2]. Цей процес за своєю суттю дозволяє уникнути прямого дублювання будь-яких існуючих зображень, на які можуть бути нанесені водяні знаки. Оскільки згенеровані зображення є оригінальними творіннями, вони не переносять жодних вбудованих водяних знаків, по суті, обходячи водяний знак без необхідності його видалення. По-друге, гнучкість і творчий підхід, які пропонують моделі перетворення тексту в зображення, дозволяють створювати зображення таким чином, що водяні знаки стають неефективними. Наприклад, якщо водяний знак зазвичай розміщується в певній області зображення, модель можна навчити генерувати зображення з ключовими візуальними елементами, що займають ці області, природно, приховуючи будь-який водяний знак, який може бути доданий пізніше. Загалом, технологія генерації зображень на основі заданого тексту пропонує універсальне рішення проблеми цифрового водяного маркування шляхом створення оригінального контенту, який не порушує права авторів оригінальних зображень, зберігаючи при цьому естетичні та функціональні якості зображень.

Доволі популярним вирішенням проблеми генерації зображень на основі заданого тексту є архітектура [3]. Запропонований метод підтримує генерацію зображень на основі заданого класу (conditional generation) та сегментації-маски. Основним її недоліком є відсутність можливості генерації зображень на основі заданого вхідного тексту.

У даній роботі пропонується модифікація архітектури [3] таким чином, що стає можливою генерація зображень на основі заданого тексту. На рисунку 1, представлена модифікована архітектура, яка дозволить генерувати зображення на основі заданого тексту.

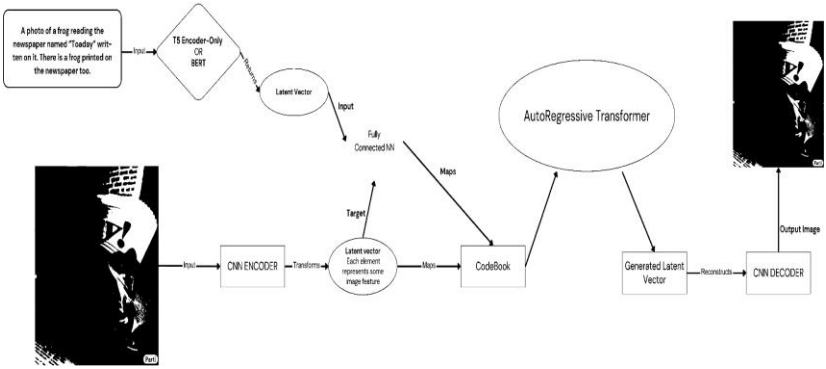


Рис.1. Модифікація архітектури [1]

На рисунку 1 відображається модульна архітектура, яка поєднює авторегресивний трансформер та VQ-GAN [3, 4]. VQ-GAN складається з двох частин: VQ-VAE в ролі генератора, та класичного конволюційного дискримінатора. Генерація зображення відбувається шляхом трансформації вхідного зображення, використовуючи конволюційний енкодер, у латентне векторне представлення. Кожен елемент латентного вектора відображає певну характеристку-особливість зображення, таку як, наприклад, наявність ока чи голови. Далі, цей латентний вектор співставляється із codebook [3, 5], яка була отримана в результаті тренування VQ-GAN. Дана codebook містить дискретні латентні вектори, кожен з яких відповідає за певний елемент який може бути представлений на зображенні.

Отримані латентні вектори співставляються з найближчими дискретними латентними векторами з codebook. Далі на основі цих латентних дискретних кодів, трансформер авторегресивно генерує зображення, представлене у вигляді латентних кодів-харектеристик, які подані як дискретні вектори у codebook [2]. Цей авторегресивний підхід, де генерація кожної частини зображення послідовно залежить від попередньо згенерованих частин, забезпечує послідовність і контекстуальну узгодженість вихідних даних. Далі конволюційний декодер генерує вже повноцінне зображення, використовуючи латентні вектори характеристик зображення, які згенеровані авторегресивним трансформером.

Під час генерації зображення на основі вхідного текстового опису, використовується енкодер-частина T5 text-to-text трансформера, який перетворює вхідний текстовий опис у латентний вектор, який, у свою чергу, чітко охоплює всі текстові залежності та деталі наявні у вхідному текстовому описі. Далі використовується натренована повнозв'язна нейронна мережа, яка трансформує латентний вектор вхідного текстового опису, отриманий від T5 енкодера, у формат, співставний із латентним вектором, отриманим від конволюційного енкодера. Таким чином, латентний вектор зображення і латентний вектор відповідного

текстового опису будуть приблизно однаковими. Після цього латентний вектор текстового опису співставляється із дискретними латентними векторами із codebook, подається у трансформер, який, у свою чергу, авторегресивно генерує дискретні латентні вектори вихідного зображення. В результаті, конволюційний декодер реконструює повноцінне вихідне зображення.

Розроблений метод генерації зображень на основі текстового опису показує великий потенціал у обході цифрових водяних знаків. Використання комбінації генеративних алгоритмів, таких як T5, VQ-GAN та авторегресивного трансформера, дозволяє створювати візуально привабливі та унікальні зображення, що ефективно уникають стандартних методів водяного маркування. Це становить значний крок у забезпеченні цифрової безпеки зображень, одночасно зберігаючи їх естетичну цінність і доступність для широкої публіки.

1. Huiwen Chang, Han Zhang, Jarred Barber, AJ Maschinot, Jose Lezama, *et al.* Muse: Text-To-Image Generation via Masked Generative Transformers arXiv, Jan. 2, 2023. Accessed: Apr. 29, 2024. [Online]. Available: https://arxiv.org/abs/2301.00704
2. Jiahui Yu, Yuanzhong Xu, Jing Yu Koh, Thang Luong, *et al.*, Scaling Autoregressive Models for Content-Rich Text-to-Image Generation. arXiv, Jun. 21, 2022. Accessed: Apr. 21, 2024. [Online]. Available: http://arxiv.org/abs/2206.10789
3. Patrick Esser, Robin Rombach, Björn Ommer Transformers for High-Resolution Image Synthesis. arXiv, Jun. 23, 2021. Accessed: Apr. 21, 2024. [Online]. Available: http://arxiv.org/abs/2012.09841
4. Shiyue Cao, Yueqin Yin, Lianghua Huang, Yu Liu, Xin Zhao, Deli Zhao and Kaiqi Huang., Efficient-VQGAN: Towards High-Resolution Image Generation with Efficient Vision Transformers. arXiv, Oct. 09, 2023. Accessed: Apr. 21, 2024. [Online]. Available: http://arxiv.org/abs/2310.05400
5. Long Zhao, Zizhao Zhang, Ting Chen, Dimitris N. Metaxas, Han Zhang. Improved Transformer for High-Resolution GANs. arXiv, Dec. 23, 2021. Accessed: Apr. 21, 2024. [Online]. Available: http://arxiv.org/abs/2106.07631

Автоматизоване керування та планування маршрутів для БпЛА

УДК 004.89:629.735

Ігор Жуков[1], Сергій Балакін[2] , Богдан Долінце[3]

Національний авіаційний університет[1], Україна zhuia@ukr.net,
Інститут менеджменту і стратегій[2] , Україна bpys@i.ua,
Інститут менеджменту і стратегій [3], Україна b.dolintse@gmail.com

Використання інструментів Matlab для автоматизованого складання та візуалізації маршрутів польотів дозволяє детально планувати та оцінювати траєкторію безпілотних літальних апаратів (БпЛА) [1]. Керування польотом здійснюється за допомогою алгоритму планування переміщення та управління рухом, який регулює швидкість, кути нахилу, курс та інші параметри польоту БпЛА, забезпечуючи точне виконання заданого маршруту.

Для створення плану польоту були визначені початкові умови, включаючи координати початку та завершення місії, обмеження за мінімальною та максимальною висотою польоту над поверхнею, а також перелік завдань на політ, які включають 4 об'єкти, навколо яких БпЛА повинен виконати круговий обліт [2].

Для генерації операціоналізованого польотного завдання (рис. 1) розроблено алгоритм автоматичного планування та складання операційного плану польоту. У наведеному фрагменті коду програми ініціалізується початкова точка маршруту, а потім забезпечується автоматизований зліт до заданої висоти, визначеної на основі визначених мінімальної та максимальної висот польоту. Програма обробляє кожну цільову точку на заданому маршруті, встановлюючи кругові обльоти навколо кожної з них та задаючи тривалість статичного зависання над цими точками.

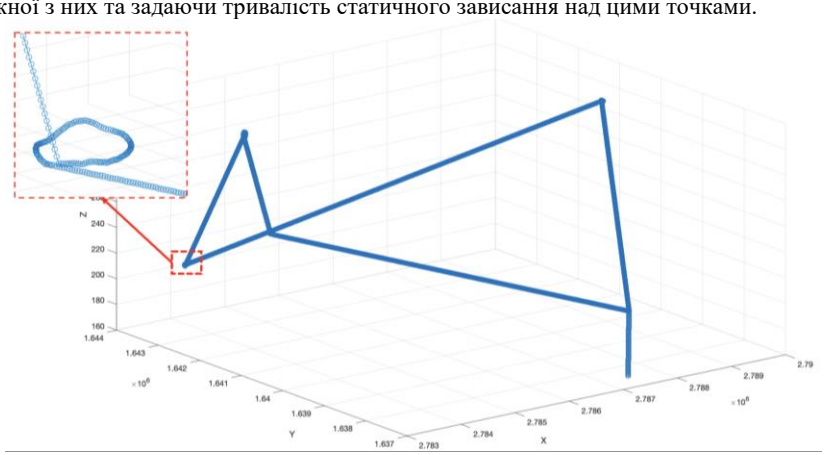


Рис. 1. Візуалізація операціоналізованого плану польоту для БпЛА створеного за допомогою Matlab.

Після обльоту точок, БпЛА летить до наступних цілей, дотримуючись безпечної висоти. По завершенні місії відбувається посадка на кінцеву точку. Програма ідеально підходить для точного планування маршрутів у сферах аерофотозйомки, моніторингу та картографування. Для отримання карт висот по маршруту

використовували Google Maps Elevation API та скрипт, що опрацьовує дані для кожної точки маршруту. Модель симуляції польоту БпЛА інтегрує дані з різних систем позиціонування для аналізу поведінки в різних умовах. Використання реалістичних даних дозволило створити деталізовану тривимірну модель польоту з урахуванням корекції позиціонування, карти висот та реального рельєфу місцевості (рис. 2).

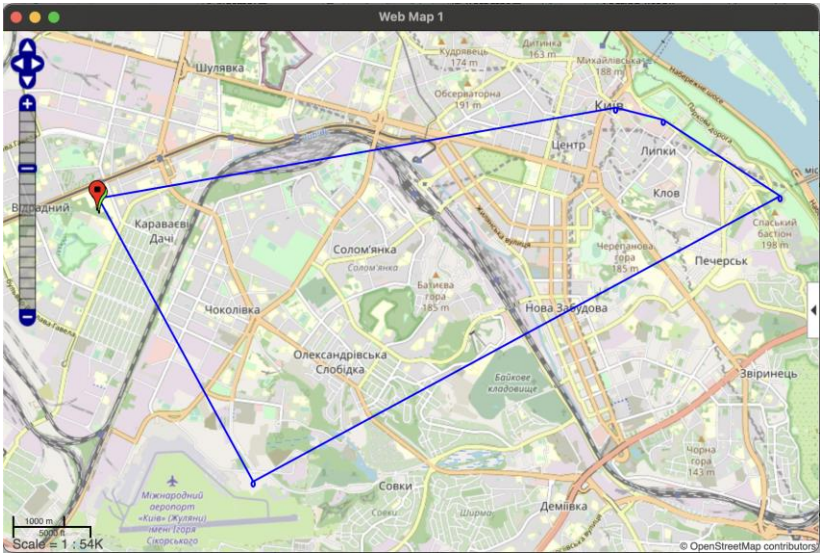


Рисунок 2. Генерація траєкторії польоту для виконання місії БпЛА з прив'язкою до реальної карти місцевості.

Для оптимізації та ефективного керування польотом БпЛА в реальних умовах прольоту точок та проходження місії, визначено допуск для проходження плану польоту - 2 м, складено маршрут з центрами кіл, які проходять через точки маршруту з відстанню не більше 1 м. Отриманий оптимізований план польоту дозволяє сформувати масив керуючих сигналів для управління польотом БпЛА. Алгоритмом генерації масиву управляючих сигналів обробляється отриманий операціоналізований план польоту для забезпечення ефективного та оптимального управління БпЛА під час польоту. Шляхом інтеграції отриманих керуючих сигналів можна отримати фактичні значення зміни швидкості та прискорення БпЛА, які дозволяють керувати його переміщенням у просторі під час виконання місії. На кожній ітерації алгоритм обчислює вектор напрямку між поточною та наступною точками, з якого отримують евклідову відстань між точками, для обчислення кутових відхилень та прискорень у тривимірному просторі.

Для підвищення точності управління та позиціонування БпЛА використовується алгоритм калібрування датчиків Micro-Electro-Mechanical Systems (MEMS). Він коригує систематичні похибки, забезпечуючи надійність та

точність роботи. Алгоритм оцінює похибки акселерометра та гіроскопа перед місією, що дозволяє отримати точні дані для обчислень. Після калібрування алгоритм коригує вимірювання Inertial Navigation System (INS), що дозволяє точно відобразити рух БпЛА. Етап інтеграції перетворює дані прискорення в оцінки швидкості та положення, що дозволяє отримати динамічну траєкторію переміщення та точне позиціонування [3]. Включення алгоритму базового калібрування датчиків системи MEMS і корекції систематичних похибок INS перед місією знизило загальний рівень похибок.

Для підвищення точності даних курсового спрямування, що вимірюються магнітометром, додатково застосовується цифровий фільтр експоненціального ковзного середнього (EMA). Отримана інформація є більш стабільним і надійним джерелом даних для позиціонування та керування БпЛА [4].

Для оцінки ефективності системи позиціонування БпЛА порівнюють її з сучасними системами, що інтегрують бортову INS та Global Navigation Satellite Systems (GNSS) з оптимальною фільтрацією (фільтр Калмана) що моделює роботу системи при оцінці інформації про положення та швидкість. Фільтр працює в циклі, оновлюючи оцінки з кожним новим набором вимірювань, прогнозуючи та коригуючи стан системи. Під час моделювання похибки не накопичуються з часом, а стабілізуються на низьких рівнях, що дозволяє ефективно компенсувати їх в математичній моделі системи, яка набуває стійкості, криві значень параметрів стабілізуються на рівнях близьких до 0.

Таким чином, мета включення корекції та калібрування досягнута: створено стабільну систему з постійними параметрами, а тривалість перехідних процесів становить 5-8 с, що відповідає вимогам. Для підвищення точності системи можна видалити коливання в кривих після стабілізації за допомогою додаткової обробки інформації та фільтрів.

1. Dolintse B.I. Architecture of Integrated Navigation Systems with enhanced Coordinate Accuracy and Fault Detection. Problems of Informatization and Control. 2023. V. 2. No. 74. P. 31–37.
2. Zhukov I., Dolintse B. Enhancing Accuracy of Information Processing in Onboard Subsystems of UAVs. Technology Audit and Production Reserves. 2023. V. 5. No. 2(73). P. 6–10.
3. Zhukov I, Okhrimenko I, Balakin S, Chaikovska S and Sulkowski O. Risk assessment in critical infrastructure computer networks. CEUR Workshop Proceedings. 2023. V. 3421, P. 272–277.
4. Zhukov I. Implementation of integral telecommunication environment for harmonized air traffic control with scalable flight display systems. 2010. Aviation, V. 14, No. 4. P. 117-122.

Використання блокчейн-технології для підвищення безпеки від SQL ін'єкцій

УДК 004.056

Ірина Замрій[1], Іван Шахматов[2]

Державний університет інформаційно-комунікаційних технологій,
1irinafraktal@gmail.com, 2ivan.shakhmatov@gmail.com

Загроза SQL-ін'єкцій залишається актуальною проблемою у сфері веб-розробки, оскільки вони виявляють вразливості систем і дозволяють зловмисникам отримувати несанкціонований доступ до даних [1-2]. Цей вид атак полягає у введенні шкідливого SQL-коду через інтерфейс користувача, що може призвести до ннесанкціонованого доступу, витоку або втрати інформації. Зловмисники активно шукають слабкі місця у захисті для того, щоб отримати доступ до конфіденційної інформації, видалити критично важливі дані або навіть заволодіти контролем над серверами.

Модель BlockchainSQLSecure є рішенням для забезпечення безпеки SQL, яке поєднує технології блокчейн та фільтр Блума для виявлення та запобігання SQL ін'єкціям. Унікальність полягає в тому, що модель не обмежується лише відстеженням стандартних сценаріїв SQL-ін'єкцій, а замість цього використовує блокчейн для надійного зберігання інформації про попередні запити. Це дозволяє створити журнал стійкий до змін з можливістю перевірки у будь-який момент з метою забезпечення безпеки даних.

Розроблена модель не потребує великих обчислювальних ресурсів для своєї роботи і може легко інтегруватися у наявні системи. Фільтр Блума, у свою чергу, забезпечує високу швидкість і ефективність обробки, що робить його ідеальним для роботи з великими обсягами даних. У моделі BlockchainSQLSecure ключовим аспектом є визначення схожості між SQL-запитами для ефективного виявлення та запобігання спробам SQL-ін'єкцій. Для досягнення цієї мети використовується формула відстані Жаккара:

$$d(X, Y) = \frac{\sum_{i=1}^{n} X_i Y_i}{\sum_{i=1}^{n} X_i^2 + \sum_{i=1}^{n} Y_i^2 - \sum_{i=1}^{n} X_i Y_i} \quad (1)$$

де X_i, Y_i – координати векторів X та Y відповідно.

Ідентифікація між двома SQL-запитами відбувається за формулою (1), де значення, що прямує до 1, вказує подібність, а значення, що прямує до 0, вказує на відмінність. Ця відстань є важливим елементом алгоритму видалення дублікатів даних на основі фільтра Блума і підвищує ефективність і точність моделі. Метрика дозволяє швидко визначити, чи є новий SQL-запит варіантом вже існуючого SQL-запиту, що містить потенційну спробу ін'єкції. Використання відстані Жаккара в поєднанні з фільтром Блума підвищує ефективність і точність системи у виявленні та запобіганні SQL-ін'єкцій.

Запропонована UML-діаграма (рис. 1) показує класову структуру інноваційної системи, яка поєднує в собі функції обробки SQL-запитів, управління блокчейн-

транзакціями, контролю дій користувачів та використання фільтру Блума для оптимізації запитів. Розроблена UML-діаграма містить п'ять основних класів: User, SQLQuery, BlockchainManager, AuditLogger та BloomFilter, кожен з яких відіграє важливу роль у функціонуванні системи та встановленні взаємозв'язків, залежностей між класами.

Розробка системи на мові програмування Python дозволила прийняти принципи чистого кодування, забезпечивши якість, легкість розуміння та можливість подальшого розширення проекту. Архітектура системи була розроблена у вигляді модулів та класів, що забезпечило чітку структуру та розподіл обов'язків.

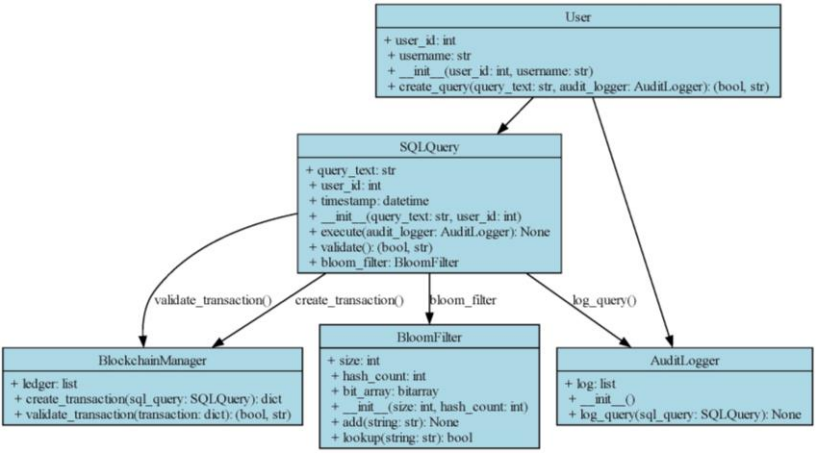


Рис. 1 UML-діаграма класів для системи управління базою даних та блокчейн-транзакціями

Створена система демонструє високий рівень структурованості, безпеки та ефективності. Використання UML-схеми дозволило нам ретельно спланувати архітектуру системи, визначивши ключові компоненти та їх взаємодію. Кожен клас відіграє унікальну роль, що сприяє створенню цілісної та надійної системи.

1. Tanrıverdi M., Tekerek A. Implementation of Blockchain Based Distributed Web Attack Detection Application. Feminist Press at CUNY. 2021. 102 p.
2. Alghawazi M., Alghazzawi D., Alarifi S., Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review. *Journal Cybersecurity and Privacy*, 2022, 2(4), pp. 764-777.

Using blockchain technology to improve security against SQL injections

UDK 004.056

Iryna Zamrii[1], Ivan Shakhmatov[2]

State University of Information and Communication Technologies,
[1]irinafraktal@gmail.com, [2]ivan.shakhmatov@gmail.com

The threat of SQL injections remains an actual problem in the field of web development, as they reveal system vulnerabilities and allow attackers to gain unauthorized access to data [1-2]. This type of attack consists of injecting malicious SQL code through the user interface, which can lead to unauthorized access, leakage or loss of information. Attackers are actively looking for weak points in protection in order to gain access to sensitive information, delete critical data or even gain control over servers.

The BlockchainSQLSecure model is a SQL security solution that combines blockchain technology and a Bloom filter to detect and prevent SQL injections. What's unique is that the model is not limited to tracking standard SQL injection scenarios, but instead uses blockchain to securely store information about previous queries. This allows you to create a log that is resistant to changes and can be checked at any time to ensure data security.

The developed model does not require large computing resources for its work and can be easily integrated into existing systems. The Bloom filter, in turn, provides high processing speed and efficiency, which makes it ideal for working with large volumes of data. In the BlockchainSQLSecure model, a key aspect is the identification of similarities between SQL queries to effectively detect and prevent SQL injection attempts. To achieve this goal, the Jacquard distance formula is used:

$$d(X, Y) = \frac{\sum_{i=1}^{n} X_i Y_i}{\sum_{i=1}^{n} X_i^2 + \sum_{i=1}^{n} Y_i^2 - \sum_{i=1}^{n} X_i Y_i} \quad (1)$$

where X_i, Y_i are the coordinates of vectors X and Y respectively.

The identification between two SQL queries is by formula (1), where a value leading to 1 indicates similarity and a value leading to 0 indicates relativity. This distance is an important element of the algorithm for removing duplicate data based on the Bloom filter and increases the efficiency and accuracy of the model. The metric allows you to quickly determine whether a new SQL query is a variant of an existing SQL query that contains a potential injection attempt. Using the Jacquard distance in combination with the Bloom filter increases the efficiency and accuracy of the system in detecting and preventing SQL injections.

The proposed UML diagram (Fig. 1) shows the class structure of the innovative system, which combines the functions of processing SQL queries, managing blockchain transactions, monitoring user actions, and using the Bloom filter to optimize queries. The developed UML diagram contains five main classes: User, SQLQuery, BlockchainManager, AuditLogger and BloomFilter, each of which plays an important role in the functioning of the system and establishment of relationships and dependencies between classes.

The development of the system in the Python programming language made it possible to

adopt the principles of clean coding, ensuring quality, ease of understanding and the possibility of further expansion of the project. The system architecture was developed in the form of modules and classes, which ensured a clear structure and division of responsibilities.

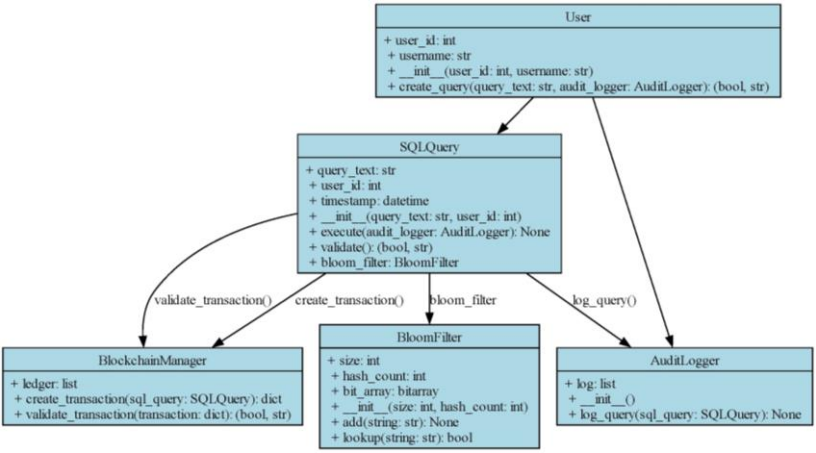


Fig. 1 UML class diagram for database management system and blockchain transactions

The created system demonstrates a high level of structure, security and efficiency. Using the UML diagram allowed us to carefully plan the architecture of the system, identifying the key components and their interactions. Each class plays a unique role that contributes to the creation of a complete and reliable system.

1. Tanrıverdi M., Tekerek A. Implementation of Blockchain Based Distributed Web Attack Detection Application. Feminist Press at CUNY. 2021. 102 p.
2. Alghawazi M., Alghazzawi D., Alarifi S., Detection of SQL Injection Attack Using Machine Learning Techniques: A Systematic Literature Review. *Journal Cybersecurity and Privacy*, 2022, 2(4), pp. 764-777.

Математична модель оцінки захищеності хмарних сервісів

УДК 004.056.5

Євгенія Іванченко[1], Ірина Лозова[2],
Євгеній Педченко[3], Марі Петровська[4],
Ігор Іванченко[5]

*Національний авіаційний університет, 1evivancenko@gmail.com,
2illozovaya@gmail.com, 3ympedchenko@gmail.com,
4pmarisha2004@gmail.com, 5igor-p-l@gmail.com*

Оцінюючи тенденції розвитку українського, польського та інших світових ринків, спостерігається факт, що використання виключно хмарних обчислень, за версією The Next Platform [1] та Gartner [2] за 2023, зросла до 44%, а використання гібридної інфраструктури (поєднання хмарних та наземних обчислень) становить 18% та виключно наземні обчислення становлять 38%, що робить постачальників хмарних сервісів лідером в сфері надання обчислювальної інфраструктури.

Проте, актуальною залишається проблема забезпечення захищеності та попередження витоку чи компрометації персональних даних, що розташовуються на ресурсах хмарних сервісів. Відповідно на дослідження компанії Veritis [3] за 2023 рік було визначено 10 найкритичніших проблем з безпекою у хмарних обчисленнях, що були виявлені у 83% компаній, аудит яких було проведено. До основних проблем було віднесено наступні проблеми з Cyber Security: некоректність конфігурацій; можливість отримання несанкціонованого доступу до ресурсів хмарних сервісів; можливість витоку чи втрати даних тощо

Метою даної роботи є представлення узагальненої математичної моделі оцінки захищеності хмарних сервісів в залежності від їх типів та особливостей їх використання в сучасному кіберпростір.

Новизною в даному випадку буде розробка узагальненої математичної моделі оцінки захищеності хмарних сервісів шляхом визначення типів хмарних сервісів, до яких буде застосовуватися розроблена математична модель. Також, в розробленій узагальненій математичній моделі представлено залежність типів хмарних сервісів та їх параметрів оцінки. На основі отриманих результатів буде розроблено структурно узагальнену математичну модель оцінки захищеності хмарних сервісів.

На сьогоднішній день популярність використання хмарних сервісів тільки набирає оберти і важливо не забувати про їх захищеність. Найпопулярнішими типами хмарних сервісів на сьогоднішній день є: Infrastructure-as-a-Service (IaaS), Containers-as-a-Service (CaaS), Platform-as-a-Service (PaaS), Function-as-a-Service (FaaS) та Service-as-a-Service (SaaS), - детальніше про аналіз даних сервісів можливо дізнатися в статті [4] за 2022 рік. Додатково, використовуючи результати дослідження, описані в статті [4], ви маєте змогу дізнатися про вразливості та атаки, що актуальні для хмарних сервісів та додатків, що розташуються на ресурсах хмарних сервісів.

Опираючись на різноманітність типів хмарних сервісів, було прийнято рішення розробити математичну модель, що буде основою для побудови системи проведення аудиту кожного із вище описаних хмарних сервісів, з метою оцінки їх стану захищеності. Задля зручності оцінки хмарних сервісів, скористаємося

розробленою архітектурою Sacha Roger [5], що описує кожну складову хмарного сервісу, саме:

- **Network module** – модуль управління мережевими налаштуваннями,
- **Storage module** – модуль управління дисковим простором,
- **Servers module** – модуль управління серверним обладнанням,
- **Virtualization module** – модуль управління системи віртуалізації,
- **Operation System module** – модуль управління операційною системою,
- **Container Technology module** – модуль управління системи контейнеризації,
- **Runtime module** – модуль управління доступність сервісу,
- **Application module** – модуль управління розгорнутими додатками на базі операційної системи чи контейнеру,
- **Data module** – модуль управління даними, що генеруються розгорнутими додатками.

Важливо розуміти, що від точності проведеного аудиту безпекових налаштувань використовуваного хмарного сервісу залежить захищеність даних та точність надання рекомендацій для підвищення захищеності додатків, що функціонують в хмарі. Саме тому, для проведення якісної та комплексної оцінки стану захищеності різного роду марних сервісів було розроблено математичну модель, що складається з 11 параметрів кортежу, та описує ключові моменти, що містять в собі набір питань та рекомендацій, які застосовуються до таких типів хмарних сервісів, як: IaaS, CaaS, PaaS, FaaS та SaaS. Для побудови узагальненої математичної моделі було використано позначення «CSP», що розшифровується, як «Cloud Service Provider», та означає «Постачальник хмарних сервісів».

Загальний вигляд математичної моделі можливо представити у вигляді узагальненого кортежу [6]:

$$\boldsymbol{CSP} = \left\{ \bigcup_{i=1}^{n} \boldsymbol{CSP}_i \right\} = \left\{ \boldsymbol{CSP}_1, \boldsymbol{CSP}_2 ..., \boldsymbol{CSP}_n \right\}, \quad (1)$$

де, $\boldsymbol{CSP}_i \subseteq \boldsymbol{CSP}$ $(i = \overline{1,n})$ – ключовий компонент кортежної моделі характеристик, що демонструє *i*-й ідентифікатор параметра оцінки хмарних сервісів, *n* – їх кількість.

Наприклад, при *n* = 11, математична модель для кортежу (1) буде виглядати наступним чином:

$$\boldsymbol{CSP} = \left\{ \bigcup_{i=1}^{n} \boldsymbol{CSP}_i \right\} = \left\{ \boldsymbol{CSP}_1, \boldsymbol{CSP}_2, \boldsymbol{CSP}_3, ..., \boldsymbol{CSP}_7, ..., \boldsymbol{CSP}_{11} \right\} = \left\{ \boldsymbol{GP, N, S, SR, V, OS, CT, R, A, D, RE} \right\}, \quad (2)$$

Де $\boldsymbol{CSP}_1 = \boldsymbol{GP} = \text{"}\boldsymbol{General\ Points\ module}\text{"}$, $\boldsymbol{CSP}_2 = \boldsymbol{N} = \text{"}\boldsymbol{Network\ module}\text{"}$,

$\boldsymbol{CSP}_3 = \boldsymbol{S} = \text{"}\boldsymbol{Storage\ module}\text{"}$, $\boldsymbol{CSP}_4 = \boldsymbol{SR} = \text{"}\boldsymbol{Server\ module}\text{"}$,

$\boldsymbol{CSP}_5 = \boldsymbol{V} = \text{"}\boldsymbol{Virtualization\ module}\text{"}$, $\boldsymbol{CSP}_6 = \boldsymbol{OS} = \text{"}\boldsymbol{Operation\ System\ \ module}\text{"}$,

$\boldsymbol{CSP}_7 = \boldsymbol{CT} = \text{"}\boldsymbol{Container\ Technology\ module}\text{"}$, $\boldsymbol{CSP}_8 = \boldsymbol{R} = \text{"}\boldsymbol{Runtime\ module}\text{"}$,

$CSP_9 = A =$ "***Application module***", $CSP_{10} = D =$ "***Data module***",

$CSP_{11} = RE =$ "***Requirements' module***".

В табл. 1 представлено залежність кожного параметру кортежу та типу хмарного сервісу, до якого застосовується представлена оцінка захищеності.

Таблиця 1. Залежність параметрів від типу хмарного сервісу

№	Параметр	IaaS	CaaS	PaaS	FaaS	SaaS
1	$CSP_1 = GP =$ "***General Points module***"	+	+	+	+	+
2	$CSP_2 = N =$ "***Network module***"	+	+	+	+	+
3	$CSP_3 = S =$ "***Storage module***"	+	+	+	+	+
4	$CSP_4 = SR =$ "***Server module***"	+	+	+	+	+
5	$CSP_5 = V =$ "***Virtualization module***"	+	+	+	+	+
6	$CSP_6 = OS =$ "***Operation System module***"	-	+	+	+	+
7	$CSP_7 = CT =$ "***Container Technology module***"	-	+	+	+	+
8	$CSP_8 = R =$ "***Runtime module***"	-	-	+	+	+
9	$CSP_9 = A =$ "***Application module***"	-	-	-	+	+
10	$CSP_{10} = D =$ "***Data module***"	-	-	-	-	+
11	$CSP_{11} = RE =$ "***Requirements' module***"	+	+	+	+	+

В роботі, шляхом використання теоретико-множинного підходу та параметрів оцінки хмарних сервісів – представлено математичну модель на базі кортежного підходу, що надалі надасть можливість оцінити стан захищеності даних, що зберігаються та обробляються на ресурсах харних сервісів. Використовуючи представлену узагальнену математичну модель, в подальшому відкривається можливість детального представлення кожного із елементів кортежної моделі і побудови фінального варіанту структурної схеми, що буде в основі розробленого програмного застосунку та використовуватиметься для оцінки стану захищеності хмарних сервісів.

1. Morgan T.P. Cloud Spending Curtailed, On Premises Spending Heading Into Recession [Electronic resource] / T.P. Morgan // TheNextPlatform. — Mode of access: https://www.nextplatform.com/2023/04/03/cloud-spending-curtailed-on-premises-spending-heading-into-recession/ (date of access: 10.01.2024). — Cloud Spending Curtailed, On Premises Spending Heading Into Recession.
2. Strategic Cloud Platform Reviews and Ratings [Electronic resource] : Gartner Peer Insights. — Mode of access: https://www.gartner.com/reviews/market/cloud-infrastructure-and-platform-services (date of access: 12.01.2024). — What are Strategic Cloud Platform Services?
3. All You Need to Know About Top 10 Security Issues in Cloud Computing [Electronic resource] : Veritis. — Mode of access: https://www.veritis.com/blog/top-10-security-issues-in-cloud-computing/ (date of access: 14.01.2024). — All You Need to Know About Top 10 Security Issues in Cloud Computing.
4. Pedchenko Y. Analysis of modern cloud services to ensure cybersecurity [Electronic resource] / Y. Pedchenko, Y. Ivanchenko, I. Ivanchenko, I. Lozova, D. Jancarczyk, P. Sawicki // Procedia Computer Science. — 2022. — Vol. 207. — P. 110-117. — Mode of access: https://www.sciencedirect.com/science/article/pii/S1877050922009164 (date of access: 17.01.2024). — Analysis of modern cloud services to ensure cybersecurity.
5. Roger S. IaaS vs. CaaS vs. PaaS vs. FaaS vs. SaaS — What's the difference? [Electronic resource] / S. Roger // Medium. — Mode of access: https://stample.com/link/stamples/5ff3d43b60b2acfb9eb5ceb6/iaas-vs-caas-vs-paas-vs-faas-vs-saas-whats-the-difference (date of access: 17.01.2024). — IaaS vs. CaaS vs. PaaS vs. FaaS vs. SaaS — What's the difference?
6. Корченко О.Г. Системи захисту інформації : монографія / О.Г. Корченко. — К, 2004. — 264 с. — Режим доступу: https://scholar.google.com/scholar?cluster=6804965558680208678&hl=en&oi=scholarr (дата звернення: 18.01.2024) . — Системи захисту інформації: Монографія.

Аналіз поняття кіберстійкості критичної інфраструктури

УДК 004. 056

Євгенія Іванченко[1], Олександр Корченко[2], Наталія Вишневська[3], Ігор Іванченко[4]

Національний авіаційний університет, Державний університет інформаційно-комунікаційних технологій
yevheniia.ivanchenko@npp.nau.edu.ua, ihor.ivanchenko@npp.nau.edu.ua, nataliia.vyshnevska@npp.nau.edu.ua

У зв'язку зі збільшенням кількості кібератак та інцидентів на об'єкти критичної інфраструктури перед спеціалістами постає проблема підвищення ефективності заходів безпеки, які будуть в змозі забезпечити надійну та безперебійну роботу об'єктів критичної інфраструктури в цілому. Тому поняття кіберстійкість, управління кіберстійкістю, забезпечення кіберстійкості, оцінювання кіберстійкості набувають подальшої актуалізації. Тому актуальною задачею є аналіз поняття кіберстійкості критичної інфраструктури. Метою роботи є аналіз понять кіберстійкості для критичних інформаційних інфраструктур.

Так в [2] кіберстійкість – це здатність організації забезпечити розвиток діяльності (стійкість підприємства) за рахунок готовності до кіберзагроз, можливості реагування на них, засобів відновлення після кібератак. Кіберстійка організація здатна адаптуватися до відомих і невідомих криз, загроз, несприятливих факторів та викликів. У кінцевому підсумку кіберстійкість дозволяє підприємству процвітати за умов негативних чинників (кризи, пандемії, фінансової нестабільності тощо) і характеризується критеріями – відновлення після збоїв, стійкість.

Для забезпечення кіберстійкості пропонуються застосовувати комплексний аналітично керований підхід, в основі якого лежить тріада – Безпека, Ризики та Керівництво, що дозволить протистояти кібератакам, при цьому керуючись документом NCSI «Підвищення національної кіберстійкості» [3] і характеризується критеріями – керівництво NCSI, підготовка до атаки, протистояння.Кіберстійкість банківської системи [4] визначається як властивість інформаційної інфраструктури банку забезпечувати функціонування його бізнес-процесів, продуктом яких є банківські та фінансові послуги, під час кібератак і кіберінцидентів, яка має постійно підтримуватися органами управління банку шляхом організації управління кіберризиками та впровадження заходів кіберзахисту. Тож в [4] кіберстійкість характеризується критеріями – безпека (захист), ризики, протистояння.

В джерелі [5] кіберстійкість визначається як спроможність національної системи протидіяти кіберзагрозам, зокрема кібертероризму, кібердиверсіям, кібератакам стосовно національної інформаційної інфраструктури.Так в [6] одним із ключових аспектів створення кіберстійкості є розуміння природи загроз, з якими стикаються організації. Отже в [6] кіберстійкість характеризується такими критеріями – ризики, внутрішні і зовнішні загрози.У [7] кіберстійкість визначається як інтегральний показник і характеризується кібернадійністю, яка відображає можливість виконувати свої завдання в складній системі управління критичною інфраструктурою в умовах інформаційних деструктивних впливів.Європейський

центральний банк поняття кіберстійкості формулює як спроможність захисту електронних даних і систем від кібератак, а також відновлювати бізнес-операції у випадку успішної атаки [8] і характеризується такими критеріями, як відновлення після збоїв, безперервність сервісів, захист електронних даних.

У NIST SP 800-172 [9] кіберстійкість визначається як здатність передбачати, протистояти, відновлюватися та адаптуватися до несприятливих умов, стресів, атак чи компрометації систем, які використовують кіберресурси або підтримуються ними, що відповідає наступним критеріям: відновлення після збоїв, підготовка до атаки, зниження можливих наслідків атаки, управління та захист, запобігання.

В документі [10] кіберстійкість визначається, як здатність системи або інформаційної інфраструктури до оперативності реагування та адаптації до кіберзагроз, включаючи атаки, помилки, вразливості та відмови, збереження конфіденційності, цілісності та доступності інформації в умовах кібератаки, при виникненні кіберінцидентів або непередбачуваних змін та відповідає наступним критеріям: відновлення після збоїв, безперервність сервісів, зниження можливих наслідків атаки.

Згідно з [11], кіберстійкість – це здатність підготуватися до «несприятливих умов», таких як кібератаки та інциденти, які загрожують конфіденційності, доступності або цілісності цифрових активів компанії, реагувати на них, відновлюватися та адаптуватися до них.

Застосовуючи проактивний комплексний підхід до кібербезпеки [11] можна сказати що кіберстійкість – це не лише технології, бо співробітники відіграють ключову роль у забезпеченні цілісності систем і організацій і, у разі порушення безпеки, вони забезпечують належну реакцію організації на інцидент та характеризується наступними критеріями: відновлення після збоїв, керівництво NSCI «Підвищення національної кіберстійкості», підготовка до атаки.

IT Governance [12] пропонує розглядати кіберстійкість як здатність організації захищати, виявляти, реагувати на кібернетичні дії та відновлюватися після них. Завдяки стійкості, організації можуть пом'якшити вплив атаки та забезпечити ефективну роботута характеризується такими критеріями, як відновлення після збоїв, адаптування до відомих і невідомих криз, управління та захист.

В [13], кіберстійкість означає здатність організації виявляти, реагувати та швидко відновлюватися після інцидентів інформаційної безпеки, характеристики кіберстійкості наступні: відновлення після збоїв, ризики, виявлення.Тихоокеанська північно-західна національна лабораторія [14] підтримує концепцію захисту системи, яка базується на припущенні, що системи повинні мати можливість продовжувати роботу та/або швидко відновлюватись у разі порушення віртуальних каналів [14]. Так в [14] характеристики кіберстійкості наступні: відновлення після збоїв, протистояння, виявлення.

Mimecast визначає кіберстійкість [15] як цілісний підхід до забезпечення кібербезпеки, який полягає у здатності подолати кібератаки та відновлюватися після них. Це запобіжний захід проти людських помилок, уразливості програмного забезпечення, апаратних проблем і неправильних налаштувань. У [15] характеристиками кіберстійкості є відновлення після збоїв, підготовка до атаки, протистояння.У [16] Кіберстійкість означає здатність постійно виконувати

задуманий результат, незважаючи на несприятливі кіберподії. Так в [16] основною характеристикою кіберстійкості є підготовка до атаки.

Джерело [17] визначає кіберстійкість як здатність організації постійно досягати запланованих бізнес-результатів, незважаючи на несприятливі кіберподії. Таким чином в [17] за критерії кіберстійкості приймається: відновлення після збоїв, безперервність сервісів, підготовка до атаки, зниження можливих наслідків атаки, цільовий час (точка) відновлення.У [18] стійкість передбачає вжиття заходів для ефективного виявлення, реагування та відновлення, якщо зловмиснику вдасться порушити захист кібербезпеки. Тож у [18] критеріями кіберстійкості є відновлення після збоїв, ризики, підготовка до атаки, зниження можливих наслідків атаки, протистояння, управління та захист, виявлення.

Кіберстійкість у [19] відноситься до здатності організації продовжувати бізнес-операції, незважаючи на інциденти кібербезпеки або втрату даних. Так у [19] критеріями кіберстійкості є наступні: надійність (кібернадійність), аутентифікація користувача\програми, філософія довіри\недовіри, кількість та типи інтеграцій з провідними постачальниками рішень безпеки.

Підвищення кіберстійкості є ключовим елементом робочої програми FSB (рада з фінансової стабільності) [20] щодо забезпечення фінансової стабільності. Таким чином, у [20] критеріями кіберстійкості є відновлення після збоїв, внутрішні, зовнішні загрози.Для того, щоб організація стала стійкою до атак, необхідно змінити спосіб мислення, який змінить сприйняття ризиків та потенційних наслідків [21]. Так в [21] критерії кіберстійкості є наступні: відновлення після збоїв, підготовка до атаки, зниження можливих наслідків атаки.В [22] кіберстійкість визначається як здатність до збереження та відновлення функціональності та життєздатності інформаційних систем і даних внаслідок кіберінцидентів, а також адаптивність до змін у внутрішніх та зовнішніх умовах і відповідає наступним критеріям: відновлення після збоїв, підготовка до атаки, зниження можливих наслідків атаки, виявлення.

ENISA [23] визначає кіберстійкість як можливість організацій та систем відновлюватися після кібератак та інших кіберінцидентів, а також пропонує застосовувати заходи для запобігання таким інцидентам і відповідає наступним критеріям: відновлення після збоїв, запобігання. Схема визначення кіберстійкості від CyberResilienceReview (CRR) [24] визначає кіберстійкість як здатність адаптуватись до негативних впливів і кіберзагроз, включаючи атаки, помилки та надзвичайні ситуації тощо, а також можливість системи відновлюватись після виникнення інциденту. Тобто в [24] за критерії кіберстійкості приймаються: відновлення після збоїв, адаптація до відомих і невідомих криз. В [25] кіберстійкість – це здатність системи або мережі залишатися операційними та забезпечувати доступ до необхідних ресурсів в умовах кібервпливу, кібертероризму, кібершпигунства та інших кіберзагроз і відповідно кіберстійкість відповідає критеріям – надійність (кібернадійність) та кібервпливи.

У роботі [26-28] кіберстійкість визначається як здатність системи, бізнесу, організації передбачати, витримувати, відновлюватись і розвиватися в умовах деструктивних дій, кібератак на інформаційні ресурси, які являються критичними для функціонування. Тобто критеріями кіберстійкості є відновлення після збоїв, зниження можливих наслідків атаки, виявлення, запобігання, стримування,

готовність до кіберзагроз. [29] кіберстійкість визначається як здатність протистояти зовнішнім загрозам, викликаними кіберризиками, відновлюватися та адаптуватися до них. В [30] поняття кіберстійкості описується як здатність системи протистояти кібератакам, збоям і продовжувати працювати в погіршеному стані для виконання своєї місії.

Так компанія [31] визначає кіберстійкість як здатність готуватися до кібератак і витоків даних, реагувати на них і відновлюватися після них, продовжуючи при цьому ефективно працювати. У [31] виділяють чотири елементи кіберстійкості: управління та захист (сюди входить розвиток здатності виявляти, оцінювати та керувати кіберризиками, пов'язаними з мережами та інформаційними системами, у тому числі ризиками сторонніх та четвертих постачальників); виявлення та попередження (цей елемент передбачає використання безперервного моніторингу безпеки та управління поверхнями атак для виявлення аномалій та потенційних витоків даних до того, як буде завдано значної шкоди); реагування та відновлення (цей елемент передбачає впровадження адекватного планування реагування на інциденти для забезпечення безперервності бізнесу, навіть якщо система стала жертвою кібератаки); керування та забезпечення безпеки (останнім елементом є забезпечення того, щоб програма кіберстійкості контролювалася з боку керівництва організації). Отже, в [31] критеріями кіберстійкості є відновлення після збоїв, безпека (захист), зниження можливих наслідків атаки, протистояння, кібервпливи.

В [32] кіберстійкість означає здатність підприємств знижувати ризик пошкодження своїх даних та операцій, а також відновлюватися неушкодженими після атаки. Так в [32] критеріями кіберстійкості є відновлення після збоїв, зниження можливих наслідків атаки, протистояння, управління та захист. В [33] досліджена модель зрілості потенціалу – перша у галузі хмара для забезпечення стійкості даних Druva. В [33] кіберстійкість відповідає наступним критеріям – стійкість, безперервність сервісів, підготовка до атак. Джерело [34] зазначає, що кіберстійкість – це спроможність обчислювальної системи швидко відновлювати систему у випадку виникнення несприятливої ситуації. В [34] основними критеріями кіберстійкості є відновлення після збоїв, ризики, керівництво NSCI «Підвищення національної кіберстійкості», безперервність сервісів, управління та захист, виявлення.

У [35] було проведено дослідження постраждалих клієнтів, які не мали базових елементів керування безпекою та критично важливих елементів для підвищення кіберстійкості корпоративних систем. Результати ґрунтуються на взаємодії клієнтів із корпорацією Microsoft за минулий рік за показниками, які ґрунтуються на показниках вразливостей системи. В [35] основними критеріями кібербезпеки є безпека (захист), надійність (кібернадійність).

Для досягнення поставленої мети визначено множину критеріїв, що характеризують поняття кіберстійкості. (табл. 1):

Таблиця 1

Критерії визначення кіберстійкості

№ з.п	Номер джерела	Крітерії (К)																								
		Резервування	Відновлення після збоїв	Безпека (захист)	Ризики	Керівництво NSCI «Підвищення національної	Внутрішні, зовнішні загрози	Стійкість	Безперервність сервісів	Підготовка до атаки	Зниження можливих наслідків атаки	Адаптація до відомих і невідомих криз	Національний індекс кіберзрізки	Глобальний індекс кібербезпеки	Національний індекс кіберпотужності	Надійність (кібернадійність)	Захист електронних даних	Протистояння	Управління та захист	Виявлення	Аутентифікація користувача\програми	Філософія довіри\недовіри	Частота виконання певних операцій	Цільовий час (точка) відновлення	Кількість та типи інтеграцій з провідними	Готовність до кіберзагроз	Управління кіберризиками
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	2	23	24	25	26
1.	[1]	+	+	+				+	+	+	+	+				+										+	
2.	[2]		+					+																			
3.	[3]					+				+								+									
4.	[4]			+	+													+									
5.	[5]												+	+	+												+
6.	[6]				+		+																				
7.	[7]															+											
8.	[8]		+						+								+										
9.	[9]		+							+	+							+									
1	[10]		+						+		+																
1	[11]		+			+				+																	
1	[12]		+									+								+							
1	[13]		+		+															+							
1	[14]		+															+		+							
1	[15]		+							+								+									
1	[16]									+																	
1	[17]		+						+	+	+													+			
1	[18]		+		+					+	+							+	+	+							
1	[19]															+					+	+			+		
2	[20]		+				+																				+
2	[21]		+					+		+	+																
2	[22]		+							+	+									+							
2	[23]		+																								
2	[24]		+																								
2	[25]															+											
2	[26]		+								+															+	
2	[27]		+								+															+	

2	[28]		+							+														+	
2	[29]		+								+														+
3	[30]																+		+						
3	[31]			+						+							+								
3	[32]									+							+	+							
3	[33]						+	+	+																
3	[34]				+	+		+										+	+						
3	[35]			+											+										

Отже, проведений аналіз поняття кіберстійкості, на основі якого була сформована тридцятиоднокомпонентна множина критеріїв, дозволить сформулювати дефініцію "кіберстійкості" для подальшого використання в задачах кібербезпеки та захисту інформації. Отримана дефініція кіберстійкості може послужити основою для розробки методів та моделей оцінювання рівня кіберстійкості.

1. SPILNO [Electronic resource] spilno.org//Mode ofaccess:// https: // spilno.org /article/kiberstiikist-scho-tse-yak-zabezpechyty-ta-yak-upravlyaty //(date ofaccess: 20.12.2023).
2. INTRACOM-UKRAINE [Electronic resource] intracom-ukraine.com//Mode of access:// https://www.intracom-ukraine.com/cyber-security-cyber-resilience//(date of access: 20.12.2023).
3. EGA [Electronic resource] ega.ee// Mode of access://https://ega.ee/uk/publication/ncsi-pidvishhennya-natsionalnoyi-kiberstijkosti//(date of access:20.12.2023).
4. ПЛАТФОРМА ЛІГА:ЗАКОН [Electronic resource]ips.ligazakon.net//Mode of access: //https://ips.ligazakon.net / document / TM065903 / (date ofaccess: 20.12.2023).
5. Онищенко С.В., Глушко А.Д., Маслій О.А. Кіберстійкість як основа національної безпеки України/ Innovations and prospects of world science : Proceedings of XI International Scientific and PracticalConference, Vancouver, Canada, 22-24 June 2022.Vancouver: Perfect Publishing, 2022. С. 551-556.
6. ts2 [Electronic resource] ts2.space // Mode of access://https://ts2.space/uk/%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D1%81%D1%82%D1%96%D0%B9%D0%BA%D1%96%D1%81%D1%82%D1%8C//(date of access: 20.12.2023).
7. Мальцева І. Р., Черниш Ю. О., Овсянніков В. В. Аналіз методик оцінки кіберстійкості критичноїінфраструктури. Кібербезпека: освіта, наука, техніка :електронне наукове видання. 2021. N 12. С.29-35. Режим доступу:http://ek.kubg.edu.ua/cgibin/irbis64r_17/cgiirbis_64.exe?LNG=&Z21ID=&I21DBN=KUBG&P21DBN=KUBG&S21STN=1&S21REF=3&S21FMT=fullwebr&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21LOG=1&S21P03=K=&S21STR=%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D1%81%D1%82%D1%96%D0%B9%D0%BA%D1%96%D1%81%D1%82%D1%8C//(date of access: 20.12.2023).

8. CB[Electronicresource]ecb.europa.eu//Modeofaccess://https://www.ecb.europa.eu/paym/cyberresilience/ html/index.en.html#:~:text=Cyber%20resilience%20refers%20to%20the,case%20of%20a%20successful%20attack//(date of access: 20.12.2023).
9. NIST [Electronic resource] csrc.nist.gov//Mode ofaccess://https://csrc.nist.gov/glossary/term/ cyber_resiliency//(date of access: 20.12.2023).
10. Спеціальна публікація NIST 800-53B "NISTCybersecurity Framework [Electronic resource]csrc.nist.gov//Mode of access: //https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/ SP_800_53_5_1_1 /home// (date of access: 20.12.2023).
11. SPLUNK [Electronic resource] splunk.com//Modeof access:// https://www.splunk.com/en_us/blog/learn/ cyber-resilience.html // (date of access: 20.12.2023).
12. itgovernance [Electronic resource]itgovernance.co.uk//Modeof access://https://www.itgovernance.co.uk/(date of access: 20.12.2023).
13. CISCO [Electronic resource] www.cisco.com//Modeof access://https://www.cisco.com/c/en/ us/solutions/hybrid-work/what-is-cyber-resilience.html// (date of access: 20.12.2023).
14. PNNL [Electronic resource] pnnl.gov//Mode ofaccess://https: // www.pnnl.gov /explainer-articles/ cyber-resilience(date of access: 20.12.2023).
15. MIMECAST [Electronic resource] mimecast.com//Mode of access://https://www.mimecast.com/content/cyber-resilience/(date of access: 20.12.2023).
16. SPRINGER LINK [Electronic resource] link. springer.com//Mode of access://https://link. springer.com/chapter/10.1007/978-3-319-16486-1_31//(date of access: 20.12.2023).
17. Deborah, B., Graubart, R. (2011), “Cyber ResiliencyEngineering Framework”, MITRE Report, p. 37.
18. COHESITY [Electronic resource] cohesity.com//Mode of access://https://www.cohesity.com/glossary/cyber-resilience//(date of access: 20.12.2023).
19. THALESGROUP [Electronic resource] thalesgroup.com//Mode of access://https://www.thalesgroup.com/en/cyber-resilience//(date of access: 20.12.2023).
20. FSB [Electronic resource] fsb.org // Mode of access:// https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/cyber-resilience//(date of access: 20.12.2023).
21. DELOITTE [Electronic resource] deloitte.com //Mode of access: // https://www.deloitte.com/ ua/en/pages/risk/solutions/cyberresilience.html//(dateof access: 20.12.2023).
22. [22] ISO/IEC 27032:2012 [Electronic resource] iso.org//Mode of access:// https://www.iso.org/ru/standard/76070.html (date of access: 20.12.2023).
23. ENISA [Electronic resource] enisa.europa // Modeof access:// www.enisa.europa.eu (date of access: 20.12.2023).

24. CyberResilienceReview [Electronic resource] cisa.gov//Mode of access:// https://www.cisa.gov/resources-tools/services / cyber-resilience-review-crr (dateof access: 20.12.2023).
25. Шиповський В. Система показників оцінюваннякіберстійкості інформаційних систем об'єктів критичної інфраструктури. Захист Інформації, Том25, № 1, Січень-Березень 2023. С. 37-45.
26. Juan F. Carías, SaioaArrizabalaga, LeireLabaka andJosuneHernantes. Cyber Resilience Progression Model. Applied Scitnces. 2020. Vol.10(21), 7393.
27. R.S. Ross, R. Graubart, D. Bodeau, R. McQuaid, SystemsSecurityEngineering: CyberResiliencyConsiderationsfortheEngineeringofTrustworthySecureSystems.(National Institute of Standards and Technology,Gaithersburg, MD), NIST Special Publication (SP)800-160, 2019, Vol. 2. // Mode of access://https://doi.org/10.6028/NIST.SP.800-160v2. (date of access: 20.12.2023).
28. Brian West. Data Breach Preparation and Response.Breaches Are Certain, Impact Is Not. 2016, pp. 167-185. //Mode of access://https://doi.org/10.1016/B978-0-12-803451-4.00007-1 (date of access: 20.12.2023).
29. Benoît Dupont, Clifford Shearinga, Marilyne Bernier,Rutger Leukfeldt. The tensions of cyber-resilience:From sensemaking to practice. Computers & SecurityVolume 132, September 2023, 103372//Mode of access: // https:// doi.org/10.1016/j.cose.2023.103372//(date of access: 20.12.2023).
30. Carlos Espinoza-Zelaya, Young Bai Moon. Framework for enhancing the operational resilience ofcyber-manufacturing systems against cyber-attacks.Manufacturing Letters. Volume 35, Supplement, August 2023, pp 843-850. //Mode of access: //https: //doi.org / 10.1016/j.mfglet.2023.07.004// (date of access: 20.12.2023).
31. UPGUARD [Electronic resource] upguard.com//Mode of access://https://www.upguard.com/blog/cyber-resilience//(date of access: 20.12.2023).
32. ZERTO [Electronic resource] zerto.com //Mode ofaccess://https://www.zerto.com/resources/a-to-zerto/cyber-resilience (date of access: 20.12.2023).
33. DRUVA [Electronic resource] druva.com //Mode ofaccess:// https://www.druva.com/glossary/what-iscyber-resilience//(date of access: 20.12.2023).
34. TECHTARGET [Electronic resource] techtarget.com // Mode of access: // https: //www.techtarget.com/whatis / definition / cyber-resilience // (date ofaccess: 20.12.2023).
35. MICROSOFT [Electronic resource] microsoft.com// Mode of access://https://www.microsoft.com/uk-ua /security / business/ microsoft-digital-defensereport-2022-cyber-resilience (date of access: 20.12.2023).

Афінний шифр зсуву в системі залишкових класів

УДК 004.056.55

Михайло Касянчук[1], Микола Карпінський[2], Михайло Голембйовський[3]

Західноукраїнський національний університет, [1]kasyanchuk@ukr.net, [3]mykhailo.2097@gmail.com

На даний час надійний захист інформаційних потоків стає надзвичайно важливим завданням. Як правило, воно вирішується за допомогою криптографічних методів. Для збільшення швидкодії алгоритмів шифрування використовуються різні способи. Одним з них є розпаралелення процесу обчислень за допомогою системи залишкових класів (СЗК) [1]. Тому мета нашої роботи полягає у розробці афінного шифру зсуву на основі СЗК.

Афінному шифру зсуву відповідає формула $x2=(x+s) \bmod n$, де x та $x2$ – числові коди букв відкритого та зашифрованого тексту відповідно, $0<s<n$ – ключ для шифрування, n – кількість букв в алфавіті. У найпростішому способі числовим кодом букви є її порядковий номер в алфавіті, починаючи з нуля. Розшифрування відбувається згідно таких виразів: $x=(x2+s2) \bmod n=(x2-s) \bmod n$, де $s2=n-s$ – ключ для розшифрування. Недоліком такого шифру є примітивний зв'язок між ключами. Усунути цей недолік дозволяє СЗК.

Відомо, що у СЗК будь-яке натуральне число N можна представити у вигляді залишків b_i від ділення N на натуральні попарно взаємно прості числа p_i, які називаються модулями: $b_i=N \bmod p_i$. Для відновлення десяткового числа із його залишків, як правило, використовується китайська теорема про залишки (КТЗ): $N=\left(\sum_{i=1}^{k} m_i M_i b_i\right) \bmod P$ $P=\prod_{i=1}^{k} p_i$, де $m_i = M_i^{-1} \bmod p_i$, $M_i = P/p_i$, k - кількість модулів. Крім цього, повинна виконуватися умова $N<P$.

Отже, обидва абоненти таємно вибирають модулі p_i та відповідні їм ключі s_i. Відкритий текст розбивається на блоки згідно останньої умови. Після пошуку залишків при діленні одного з блоків на модулі p_i відбувається їх зсув на різну величину для різних модулів: $b_i = (b_i + s_i) \bmod p_i$. Конкатенацію отриманих b_i «неправильних» залишків можна використовувати як зашифроване повідомлення, яке розшифровується згідно формул $b_i = (b_i + s_i) \bmod p_i = (b_i - s_i) \bmod p_i$ $s_i = p_i - s_i$, де , та КТЗ.

Стійкість шифру значно підвищиться, коли відновити десяткове число на основі $N' = \left(\sum_{i=1}^{k} m_i M_i b_i'\right) \bmod P$ «неправильних» залишків: N'. Тоді шифртекстом є число $b_i = N' \bmod p_i$. При розшифруванні спочатку треба знайти «неправильні» залишки , і далі на основі КТЗ обчислити відкрите повідомлення.

1. Kasianchuk M.M., Yakymenko I.Z., Nykolaychuk Y.M. Symmetric Cryptoalgorithms in the Residue Number System. *Cybernetics and Systems Analysis*. – 2021. – Vol. 57(2). – P. 329–336.

Метод захищеного зберігання медичних даних за допомогою розмежування прав доступу та блокчейну

УДК 004.056

Вікторія Клиш, Владислава Ланова, Юрій Баришев

Вінницький національний технічний університет, vklysh71@gmail.com, lanovaia02y@gmail.com, yuriy.baryshev@vntu.edu.ua

Медичні дані – це важлива інформація, підвищені вимоги до захисту якої регламентуються низкою законів та підзаконних нормативно-правових актів. Крім того, відповідно до GDPR за розголошення персональних даних передбачаються штрафи [1], тому актуально покращувати систему захисту інформацію в медичних закладах.

Аналіз інформаційних джерел показав недостатній рівень захисту цілісності та доступності в системі охорони здоров'я України. Водночас застосування відомих практик інших країн ускладнюється відмінностями у законодавчому регулюванні та правилах документообігу. Саме тому, актуально розробити метод захисту медичних даних, який дозволить покращити рівень їх захисту шляхом внесення змін до використовуваної в Україні інформаційної системи в галузі медицини. Розв'язання цього завдання було поставлено метою даного дослідження. Для досягнення мети передбачається покращення системи розмежування прав доступу та способу зберігання даних.

Аналіз джерел показав, що метод автентифікації повинен бути зручним для користувача та мати можливість інтегруватися з іншими системами.

Аналіз поширених методів [2] дозволив виявити такі фактори автентифікації:

- традиційний логін та пароль;
- токени;
- біометричні дані;
- одноразові паролі;
- апаратні пристрої.

Внаслідок проведеного аналізу було обрано найкращим методом для медичних установ автентифікація на основі токенів, а саме JWT.

Застосування JWT дозволить гранулювати доступ, тобто тільки авторизовані користувачі, такі як лікарі та медичні сестри, можуть отримувати доступ до конфіденційних даних про пацієнтів, додаючи додаткові атрибути, які дозволять підвищити рівень захищеності.

JWT складається з трьох частин: заголовка (Header), тіла (Payload) і підпису (Signature). Згідно зі стандартом RFC 7519 [3], який описує формат та правила використання JWT, заголовок описує криптографічні операції, також можуть міститися додаткові параметри, у тілі - атрибути користувачів та додаткові дані, та підпис, що використовується для підтвердження того, що маркер JWT не було модифіковано або змінено під час передавання.

Кожен токен містить унікальний ідентифікатор, ім'я користувача, термін дії, роль та робочу станцію, що дозволяє системі точно визначити права доступу та обмеження для кожного окремого користувача.

Адміністратор, який має повноваження у системі, створює токен для лікаря, враховуючи його потреби та рівень доступу. Коли лікар потребує доступу до системи, він спочатку вводить свій логін, пароль та токен на веб-сайті. Після успішної перевірки логіна та пароля система переходить до перевірки створеного токена. Після успішної перевірки токена система надає лікареві доступ до необхідних функцій та ресурсів у межах встановлених обмежень. Такий підхід забезпечує високий рівень безпеки та контролю над доступом до медичної інформації.

Серед моделей розмежування прав доступу обрано ABAC та RBAC, що дозволить призначити потрібні дозволи ролі “лікар” та додаткові параметри за допомогою ABAC: термін дії та робочі станції, з яких відбувається автентифікація користувача.

Запропонований метод автентифікації користувачів передбачається використовувати в поєднання з системою зберігання даних на основі гібридизації технологій розподіленого реєстру та реляційної бази даних [4].

Для доведення концепції предметною областю було обрано сімейну медицину, а саме процес видавання електронних направлень на додаткові обстеження.

Було розроблено базу даних, в яку передбачається записувати дані, що вимагають підвищених вимог щодо захисту конфіденційності. Також було розроблено смарт-контракти для Ethereum-подібного блокчейну, який використовується як контейнер для даних, що потребують підвищених вимог до захисту цілісності та доступності. Для покращення захисту даних, які потребують як захисту конфіденційності, так і цілісності, вирішено записувати в блокчейн геш-значення цих даних, які зберігаються в базі даних.

Таким чином, поєднання запропонованого методу розмежування прав доступу та методу зберігання даних дозволяють покращити захист в медичних інформаційних системах, при цьому не впливаючи на процеси документообігу та організації взаємодії з пацієнтами.

1. K. Hjerppe, J. Ruohonen, V. Leppanen The General Data Protection Regulation: Requirements, Architectures, and Constraints, *IEEE 27th Int. Requirements Eng. Conf.*, Jeju Island, Korea (South), 23–27 sept. 2019. IEEE, 2019, URL: https://doi.org/10.1109/re.2019.00036 (accessed: 02.04.2024).
2. S. Z. S. Idrus, E. Cherrier, C. Rosenberge, J.-J. Schwartzmann. A Review on Authentication Methods. Australian Journal of Basic and Applied Sciences. 7. p. 95-107. URL: https://hal.science/hal-00912435/document (accessed: 02.04.2024).
3. RFC 7519: JSON web token (JWT). IETF Datatracker. URL: https://datatracker.ietf.org/doc/html/rfc7519 (accessed: 02.04.2024).
4. Ю. В. Баришев, В. С. Ланова. Метод захищеного зберігання медичних даних на основі реляційної бази даних та блокчейну, Наукові Праці ВНТУ, № 3, 2023. 8 с. URL: (дата звернення: 02.04.2024)

Метод ідентифікації вторгнень на основі алгоритму визначення самоподібності трафіку та алгоритмів нечіткої логіки

УДК 004.77

Юрій Кльоц[1], Наталія Петляк[2]

Хмельницький національний університет, [1]klots@khmnu.edu.ua, Національний авіаційний університет, [2]npetlyak@khmnu.edu.ua

Аналіз мережевого трафіку у відкритих мережах ускладнений: різноманітністю джерел трафіку; динамічним середовищем; новими сервісами, програмами та пристроями. При цьому такі мережі є основними цілями для зловмисних дій: розповсюдження шкідливого програмного забезпечення, фішингові атаки, несанкціоновані дії щодо третіх осіб. Наявні IDS/IPS-системи через неоднорідність трафіку дають велику кількість помилкових спрацювань, глибока перевірка кожного пакету дає додаткову затримку й впливає на продуктивність мережі. А впровадження та налаштування таких систем вимагає значних апаратних ресурсів.

Метою даної роботи є розробка методу ідентифікації вторгнень на основі алгоритму визначення самоподібності трафіку та алгоритмів нечіткої логіки задля виявлення зловмисного вихідного трафіку у комп'ютерній мережі, який мінімізує помилкові спрацювання із мінімальним впливом на продуктивність роботи мережі.

Аналіз мережевого трафіку доцільно здійснювати у кілька етапів: 1) формування сигнатури із потоку; 2) перевірка сигнатури на самоподібність; 3) якщо самоподібний, то можна продовжувати з'єднання; 4) якщо ж потік класифіковано як не самоподібний, то варто виконувати перевірку потоку засобами нечіткої логіки на наявність зловмисних дій [1]; 5) у разі визначення потоку як нормального засобами НЛ, то можна продовжувати з'єднання; 6) у разі визначення потоку як зловмисного засобами НЛ, то потрібно блокувати з'єднання; 7) перевірка наступного потоку даних. Узагальнену схему аналізу потоків даних представлено на рис.1.

Рис.1. Узагальнена схема аналізу потоків мережевого трафіку

Самоподібний потік мережевого трафіку (DF) має задовольняти наступну

умову, порівнюючи дані із сформованої сигнатури [2]:

$$DF = \begin{cases} Pr \in Pr_{ss} \\ Ps \in Ps_{ss} \\ Pd \in Pd_{ss} \\ IPd \in IPd_{ss} \\ SFs \in SFs_{ss} \\ SFd \in SFd_{ss} \\ IFs \in IFs_{ss} \end{cases} \quad (1)$$

де Pr_{ss} – множина самоподібних протоколів, Ps_{ss} – множина самоподібних портів джерела, Pd_{ss} – множина самоподібних портів отримувача, IPd_{ss} – множина самоподібних IP-адрес отримувача, SFs_{ss} – множина самоподібного розміру пакетів від джерела, SFd_{ss} – множина самоподібного розміру пакетів від отримувача, IFs_{ss} – множина самоподібної інтенсивності трафіку від джерела.

Деталізована схема аналізу потоків мережевого трафіку засобами НЛ представлена на рис.2.

Рис.2. Схема аналізу потоків мережевого трафіку засобами НЛ

Даний метод дозволить поетапно здійснювати перевірку трафіку на наявність зловмисного. При цьому користувачі із нормальним трафіком не будуть відчувати часових затримок, а при наявності не самоподібного трафіку буде здійснено додатково ряд перевірок для правильної ідентифікації.

1. Y. Klots, N. Petliak and V. Titova, "Evaluation of the efficiency of the system for detecting malicious outgoing traffic in public networks," *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Athens, Greece, 2023, pp. 1-5
2. Petliak, N., Klots, Y., Titova, V., Cheshun, V., Boyarchuk, A. Signature-based Approach to Detecting Malicious Outgoing Traffic. CEUR Workshop Proceedings, 2023, 3373, pp. 486–506

Протидія витоку конфіденційної інформації шляхом аналізу та виявлення програм-шпигунів

УДК 004.056.58

Олександр Ковальов[1], Тетьяна Матьовка[2]

Ужгородський Національний Університет, [1]kovalov23@gmail.com, [2]rtanyusha17@gmail.com

В період активного розвитку інформаційних технологій проблема збереження конфіденційності є надзвичайно актуальною. На сьогоднішній день існують декілька тисяч різновидів шкідливих програм, які працюють за різними алгоритмами. Однак їх всіх об'єднує факт того, що вони створюються спеціалізовано для несанкціонованого користувачем модифікування, знищення, блокування та копіювання інформації, порушуючи роботу комп'ютера та комп'ютерних мереж. Існує вид шкідливих програм, які здатні нанести значної шкоди конфіденційності інформації і при цьому вони залишаються непомітними навіть для спеціалізованих програм. Мова йде про програмних шпигунів (spyware). Для виявлення в системі програмного шпигуна слід використовувати спеціалізоване програмне забезпечення, яке спрямоване на виявлення саме цього виду загроз. Однак навіть вони не можуть гарантувати повної безпеки. У даній роботі описано основні типи програмних шпигунів та розроблено Spyware типу "системний монітор", завданням якого є збір користувацької інформації з можливістю подальшої її обробки та передачі. Ефективність роботи розробленої програми продемонстровано на основі зібраних даних та від'ємних результатів сканування системи спеціалізованими програмними засобами. Розглянуто особливості роботи програмних шпигунів та проведено аналіз їх поведінки, результати якого можуть бути використані при розробці імовірнісних методів пошуку програм досліджуваного типу.

Важливою загрозою безпеці, яка сьогодні зачіпає багатьох користувачів Інтернету є шпигунське програмне забезпечення [7, 8]. Шпигунське ПЗ - це шкідливе програмне забезпечення, яке намагається непомітно відстежувати поведінку користувачів, записувати їх звички під час веб-серфінгу або красти їх конфіденційні дані, такі як логіни та паролі. Як правило, зібрана інформація відправляється назад розповсюджувачу шпигунських програм, де вона використовується для цільової реклами або в маркетингових дослідженнях. Це відрізняє їх від інших типів шкідливих програм, таких як віруси та хробаки, які зазвичай прагнуть поширитися на інші системи та завдати їм шкоди [6].

Оскільки проблема шпигунських програм загострилася, був введений ряд комерційних рішень, спрямованих на виявлення і видалення небажаних шпигунських програм. Ці інструменти схожі на антивірусні продукти в тому, що вони ідентифікують відомі екземпляри шпигунських програм, порівнюючи бінарне зображення невідомих зразків з базою даних відомих сигнатур [9].

Часто ці сигнатури генеруються вручну шляхом аналізу відомих зразків шпигунських програм (що є досить складним завданням, врахувати те що кожного дня доводиться аналізувати сотні нових випадків). На жаль, засоби виявлення

шпигунських програм страждають від відомих недоліків детекторів які працюють на основі сигнатур, таких як постійна необхідність оновлення бази даних сигнатур і неможливість ідентифікувати раніше невідомі зразки. Зауважимо, що основним недоліком сигнатурних методів є те, що вони також часто не можуть впоратися із простими методами обфускації коду.

Оскільки методи виявлення на основі сигнатур мають суттєві недоліки, основним нашим завданням є розробити програмний засіб для виявлення в системі підозрілих програмних процесів, поведінка яких відповідає програмам типу Spyware. До функціоналу розроблюваної програми входять моніторинг наявних в системі програм та процесів, файлової системи та мережевої активності. Першим кроком у цьому напрямку є розробка та аналіз стійкості до виявлення засобами захисту програмного шпигуна з метою отримання даних стосовно поведінки даного типу програм і виявлення його можливих вразливостей.

1. J. Yan, Y. Qi and Q. Rao, "Detecting malware with an ensemble method based on deep neural network", Secur. Commun. Netw., vol. 2018, Mar. 2018.
2. P. Wang and Y.-S. Wang, "Malware behavioural detection and vaccine development by using a support vector model classifier", J. Comput. Syst. Sci., vol. 81, no. 6, 2015.
3. R. Islam, R. Tian, L. M. Batten and S. Versteeg, "Classification of malware based on integrated static and dynamic features", J. Netw. Comput. Appl., vol. 36, no. 2, 2013.
4. Ladakis E., Koromilas L., Vasiliadis G., Polychronakis M., Ioannidis S. "You Can Type, but You Can't Hide: A Stealthy GPU-based Keylogger." In Proceedings of the 6th European Workshop on System Security. EuroSec, Prague, Czech Republic, April 2013.
5. Hassell J., Campbell T.: "Windows Vista: Beyond the Manual"; Apress,. New York (2007).
6. Steven D. Gribble Alexander Moshchuk, Tanya Bragin and Henry M. Levy. A CrawlerBased Study of Spyware on the Web. In Proceedings of the Annual Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2006.
7. Combating Spyware: H.R. 29, the SPY Act : Hearing Before the Committee on Energy and Commerce, House of Representatives, One Hundred Ninth Congress, First Session, January 26, 2005.
8. Thompson, R. Why Spyware Poses Multiple Threats to Security. Communications of the ACM 48, 8 (2005).
9. Saroiu, S., Gribble, S., Levy, H. Measurement and Analysis of Spyware in a University Environment. In Usenix NSDI (2004).

Використання узагальнених матриць Галуа і Фібоначчі у потокових шифрах

УДК 621.395.7 (043.2)

Арсен Ковальчук[1], Анатолій Білецький[2]

Національний авіаційний університет, [1]kovalchuk.arsen1@gmail.com, [2]abelnau@ukr.net

У доповіді розглянуто різні варіанти побудови двійкових генераторів псевдовипадкових послідовностей (ПВП) і алгоритмів потокового шифрування інформації на основі так званих узагальнених матриць Галуа і Фібоначчі. Терміни «матриця Галуа» і «матриця Фібоначчі» запозичена з теорії криптографії, в якій широко використовують генератори ПВП на регістрах зсуву з лінійними зворотними зв'язками (РЗЛЗЗ) за схемою Галуа і Фібоначчі [1]. За допомогою матриць Галуа і Фібоначчі можна програмно обчислити такі ж самі бінарні послідовності, як і послідовності, які формують відповідні класичні РЗЛЗЗ-генератори ПВП.

Класичні матриці Галуа і Фібоначчі належать підмножині сильно розряджених матриць, тоді як узагальнені до підмножині щільних матриць. Перехід від класичних до узагальнених матричних генераторів ПВП супроводжується розширенням різноманіття генераторів, що призводить до істотного підвищення їхньої криптостійкості. Даний ефект досягається як за рахунок збільшення числа елементів, що утворюють матриці, так і за рахунок того, що узагальнені матриці синтезуються не тільки на основі примітивних породжувальних поліномів, а й на основі поліномів, які зовсім не обов'язково (як у класичних варіантах) є примітивними.

Матриці Галуа $\boldsymbol{G}$ і Фібоначчі $\boldsymbol{F}$ пов'язані оператором правостороннього транспонування (позначається символом $\perp$), що здійснює поворот матриці щодо допоміжної діагоналі. Якщо матриці $\boldsymbol{G}$ і $\boldsymbol{F}$ піддати класичному (лівосторонньому) транспонуванню (позначається символом T), то отримуємо так звані сполучені матриці Ґалуа та Фібоначчі.

Класичним генераторам і їхнім матричним еквівалентам притаманний істотний недолік, який полягає в тому, що вони схильні до атаки Берлекемпа-Мессі (БМ). Узагальнені матричні генератори ПВП вільні від атаки БМ. Остання властивість є наслідком такої особливості алгоритму БМ. Цим алгоритмом злому класичних РЗЛЗЗ-генераторів ПВП вирішується завдання обчислення єдиного невідомого - примітивного полінома, що породжує генератор. Для варіантів узагальнених матричних генераторів ПВП виникає необхідність у визначенні двох невідомих параметрів: як неприводного полінома, так і утворювального елемента, що спільно породжують узагальнену матрицю. Така проблема виявляється нерозв'язною для алгоритму Берлекемпа-Мессі [2], оскільки він призначений для обчислення лише одного невідомого параметра.

Результати досліджень узагальнено для розв'язання задач синтезу генераторів ПВП над полем Галуа непарних характеристик.

Розроблені матричні генератори ПВП стали основою побудови алгоритмів потокового шифрування інформації, один із варіантів якого наведено на рис. 1.

Результати статистичних випробувань шифру пакетом NIST STS підтвердили високу ефективність криптографічного захисту вихідних текстів.

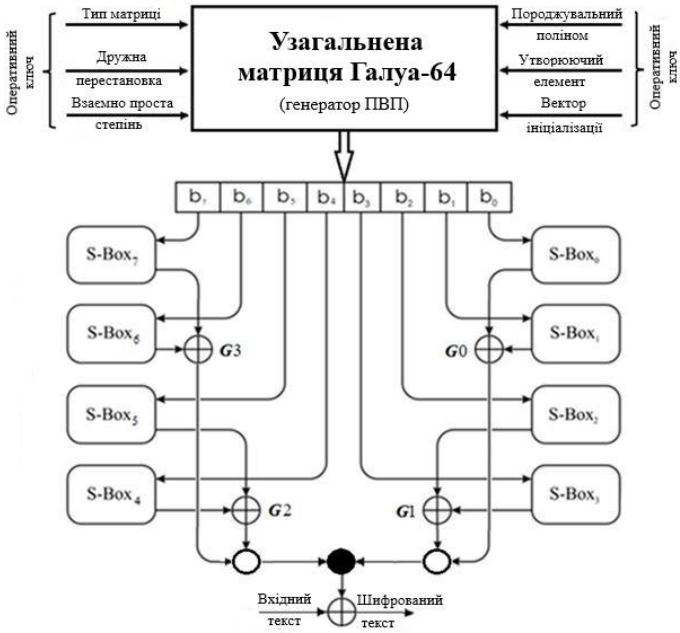


Рис. 1. Структурно-логічна схема поточного шифру

Оператори ○ та ● незалежно один від одного реалізують перетворення: порозрядного складання(0) або конкатенації (1) так, що шифруючи гама приймає значення наведене на рис. 2.

№	○	●	Перетворення	Довжина гами
1	0	0	$(G_0 \oplus G_1) \oplus (G_2 \oplus G_3)$	1 байт
2	0	1	$(G_0 \oplus G_1) \| (G_2 \oplus G_3)$	2 байта
3	1	0	$(G_0 \| G_1) \oplus (G_2 \| G_3)$	2 байта
4	1	1	$(G_0 \| G_1) \| (G_2 \| G_3)$	4 байта

Рис. 2. Варіанти шифрування гами

1. Anatoly Beletsky. Generalized Galois-Fibonacci Matrix Generators Pseudo-Random Sequences. *I. J. Computer Network and Information Security*, 2021, 6, pp. 57-69.
2. Anatoly Beletsky. Generalized Galois and Fibonacci Matrices in Cryptographic Applications. *WSEAS Transactions on Circuits and Systems*, Vol. 21, 2022, pp. 1-19.

Сучасні методи соціотехнічних атак

УДК 004.056.53(045)

Анна Корченко[1], Кирило Давиденко[2],

[1,2]Національний технічний університет «Дніпровська політехніка»,
[1]annakor@ukr.net, [2]kirilldavy@gmail.com

Стрімкий розвиток інформаційних технологій та зростаючий обмін даними через Інтернет відкривають нові можливості, але при цьому збільшують загрози для безпеки. Попит на цифрові послуги також породжує нові види кіберзлочинності, такі як шахрайство, крадіжка особистих даних і фішинг. Швидкий обмін даними в Інтернеті також збільшує ризики кібершпигунства, коли конфіденційна інформація може бути вкрадена або перехоплена.

Останнім часом спостерігається збільшення застосування соціального інжинірингу як ефективного методу кібератак. Оскільки людина є найбільш уразливим ланцюжком у системі кібербезпеки, кіберзлочинці активно використовують соціотехнічні методи. Розуміння цих методів дозволяє розробляти ефективні заходи захисту для користувачів і організацій.

Тому, аналіз сучасних методів соціотехнічних атак є ключовим елементом стратегії кібербезпеки, який допомагає забезпечити захист від неперервно зростаючих загроз та є актуальним науковим завданням, яке стоїть перед науковою спільнотою.

Згідно з провідними дослідженнями, серед найбільш поширених методів соціотехнічних атак можна виділити такі: фішинг, водопій, атака китобоя, під приводом, атаки приманка і послуга за послугу, голосовий фішинг, медова пастка, задні двері, смішинг, спір фішинг та інші. Однак в цих публікаціях не сформован повний опис характеристик, що визначають кожен з цих методів соціотехнічних атак.

Аналіз відповідних методів сприятиме більш глибокому розумінню різноманітних аспектів соціотехнічних атак і допоможе у розробці ефективних стратегій протидії їм.

Тому, на базі відомих досліджень [1-4] з подальшим їх узагальнюванням проведемо аналіз сучасних методів соціотехнічних атак (СМСА) за наступними критеріями:

1. За часовим аспектом СМСА поділяються на спонтанні (СП-атаки) та попереднього планування (ППЛ-атаки).

2. За галузевою афіліацією СМСА поділяються на атаки на корпоративний сектор (КС-атаки) та атаки на громадські установи (ГУ-атаки).

3. За взаємодією з політикою безпеки СМСА поділяються на постполітизаційні (ПП-методи) та деполітизаційні (ДП-методи) методи.

4. За ініціалізацією СМСА поділяються на умовні (УМ-атаки) та безумовні (БМ-атаки) атаки.

5. За типом звернення СМСА поділяються на аверсні (АВ-методи) і реверсні (РВ-методи).

6. За інструментарієм СМСА поділяються на програмні (ПМ-методи), апаратні (АМ-методи) та нетипові (НМ-методи) методи.

7. За порушенням характеристик безпеки СМСА поділяються на три типи: К-дієві, Ц-дієві та Д-дієві.

8. За ступенем важкості СМСА поділяються на прості (П-атаки), складні (С-атаки) та системні (СС-атаки).

9. За реляційними ознаками СМСА поділяються на чотири типи: мономономні (ММ-атаки), полімономні (ПМ-атаки), монополічні (МП-атаки) та поліполічні (ПП-атаки).

10. За типом атакованого джерела СМСА поділяються на чотири категорії: ЕК-джерельні (експерт), ЛГ-джерельні (легковажна особа), КН-джерельні (люди-контактери), ВП-джерельні (випадкова людина), а тип атакованого джерела визначається залежно від рівня інформованості особи, що піддається атаці.

11. За типом доступу до інформації СМСА поділяються на відкритого (ВК-доступу), умовно відкритого (УВ-доступу), конфіденційного (КН-доступу) та секретного (СК-доступу) доступу.

12. За дистанційністю СМСА поділяються на локальні (КТ- локальні, ПР-локальні, РМ-локальні, ЗД-локальні) та віддалені (Т-віддалені, МТ-віддалені, РП-віддалені).

13. За маніпулюванням СМСА поділяються на шість категорій, що включають риси людської натури: авторитетність (АВ-маніпулювання), прихильність (ПР-маніпулювання), взаємність (ВМ-маніпулювання), відповідальність (ВД-маніпулювання), соціальність (СЦ-маніпулювання) та обмеженість (ОБ-маніпулювання).

14. За типом соціотехніка СМСА поділяються на ті які виконуються хакерами (ХК-виконавчі), пенетрейшн-тестерами (ПТ-виконавчі), шпигунами (ШГ-виконавчі), злодіями ідентичності (ЗІ-виконавчі), незадоволеними співробітниками (НС-виконавчі), шахраями (ШХ-виконавчі), рекрутерами (РК-виконавчі), продавцями (ПР-виконавчі), з використанням віддалених комбінацій (ВК-виконавчі) та методи що націлені на конкретний сектор (СК-виконавчі), що ранжуються за специфікою діяльності і спрямовані на урядовців (УР-виконавчі), лікарів (ЛР-виконавчі), психологів (ПС-виконавчі), юристів (ЮР-виконавчі) тощо.

15. За масштабом СМСА поділяються на локальні (ЛК-атаки) та глобальні (ГБ-атаки) атаки.

Також, на базі запропонованого аналізу СМСА та набору критеріїв можна описати приклад здійснення соціотехнічної кібератаки.

Далі, приведемо загальний опис процесу звичайної соціотехнічної атаки, яка може мати свої унікальні особливості в залежності від цілей, методів і засобів зловмисника та включає наступні кроки:

Крок. 1. Дослідження цілі. Зловмисник починає з дослідження своєї цілі, будь то компанія, окрема особа або організація. Він збирає інформацію про цільову особу або організацію, таку як контактні дані, роль в організації, соціальні мережі тощо.

Крок. 2. Підготовка соціальної інженерії. Зловмисник розробляє стратегію впливу на цільову особу. Це може включати створення підроблених електронних

листів, створення фальшивих акаунтів у соціальних мережах або підготовку підроблених веб-сайтів.

Крок. 3. Виконання атаки. Зловмисник виконує заплановану атаку, яка може включати відправлення фішингових електронних листів з вимогою введення конфіденційної інформації, перехоплення даних або навіть використання соціальних інженерних методів для отримання доступу до системи.

Крок. 4. Експлуатація отриманої інформації. Після успішного здійснення атаки зловмисник може використовувати отриману інформацію для різних цілей, таких як крадіжка конфіденційних даних, використання цільових систем для здійснення подальших атак або навіть вимагання викупу за повернення доступу до скомпрометованих систем.

Крок. 5. Приховання слідів. На останньому етапі зловмисник може намагатися приховати свої сліди, щоб уникнути виявлення та відповідальності за атаку.

Запропонований аналіз СМСА за рахунок розширення існуючих класифікацій відповідних методів та додавання нових критеріїв, як от часовий аспект, галузева афіліація, взаємодія з політикою безпеки, дистанційність, ініціалізація, інструментарій, маніпулювання, порушення характеристик, реляційні ознаки, ступінь важкості, тип атакованого джерела, тип доступу, тип звернення, тип соціотехніка, масштаб, дозволить враховувати зазначені критерії при виборі відповідних засобів протидії соціотехнічним атакам та розробляти ефективні заходи захисту для користувачів та організацій, що є важливою складовою стратегії кібербезпеки для забезпечення захисту від постійно зростаючих кіберзагроз.

1. Класифікація методів соціального інжинірингу / О.Г. Корченко, Є.В. Паціра,Д.А. Горніцька // Захист інформації. – 2007. – №4 (36). – С.37-45.
2. О. Г. Корченко, Д. А. Горніцька, та А. Ю. Гололобов, «Розширена класифікація методів соціального інжинірингу», Безпека інформації, т. 20, № 2, с. 197-205, 2014.
3. Д. А. Горницька, А. Г. Корченко, В. П. Харченко, «Система соціально-технічних атак в інформаційному середовищі», II Міжнародна науково-практична конференція «Проблеми економіки та менеджменту на залізничному транспорті», Київ, 2007, с. 137-138.
4. Анна Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019 – 361 с.

Створення захищеного протоколу передачі даних для БПЛА.

УДК 263.61

Віктор Котетунов

ДержНДІ технологій кібербезпеки, v.kotetunov@gmail.com

Створення національного захищеного протоколу передачі даних для безпілотних літальних апаратів залишається актуальною задачею, зокрема в умовах постійного удосконалення сучасних засобів та методів РЕБ. Використання БПЛА в зоні бойових дій наразі є одним із значущім фактором досягнення успіху ведення сучасного бою. Кількість, різноманітність, види модіфікацій БПЛА, які використовуються постійно зростають з кожним місяцем. Актуальними на дани час для використання є БПЛА від аматорських з невеликою дальністю та тривалістю польоту призначених для фото та відео зйомки до БПЛА військового призначення призначених для розвідки та наведення артилерійських розрахунків.

Збільшення інсцендентів перехоплення управління та проблем РЕБ ускладнює захист каналів зв‘язку з БПЛА за допомогою криптоалгоритмів та використання протоколів стійких до радіоперешкод. Актуалізуються дослідження методів виявлення та перехоплення БПЛА, що порушують кордони зон, що контролюються.

В сьогоднішніх умовах дуже активно використовують протокол передачі пакетів DSMX та спосіб перехоплення дрону, що використовує дану пакетну технологію за допомогою атаки за часом.

DSMX протокол [1] – це один з протоколів передачі даних по радіоканалу, використовується при передачі на частоті 2,4 ГГц. Це базова частота але на сьогоднішній день можливо використовувати і інші частоти. Переваги даної технології у великій кількості каналів передачі даних та у прогресивному алгоритмі кодування та зміни каналів. У разі завади на певній частоті даний алгоритм роботи протоколу швидко змінить частоту передачі, що дозволить не втрачати зв‘язку між передавачем та приймачем.

При формуванні радіосигналу використовуються псевдовипадкове перестроювання робочої частоти (FHSS), множинний доступ з кодовим розділенням каналів (CDMA), метод прямої послідовності для розширення спектру (DSSS) та Гаусівська частотна маніпуляція (GFSK).

Технологія пакетної передачі DSMX має серйозну вразливість до атаки за часом. Ключовим для реалізації даної атаки є відсутність криптографічного шифрування пакетів даних. Програмно-визначальна радіосистема дозволяє реалізувати даний спосіб атаки для будь-якої пакетної технології, що не має достатнього рівня захисту інфраструктури. Тем не менш саме ця технологія виглядає перспективною для розробки на її базі національного захищеного протоколу передачі даних

1. FPV Protocols Explained (CRSF, SBUS, DSHOT, ACCST, PPM, PWM and more) // OscarLiang. URL: https://oscarliang.com/rc-protocols/ (дата звернення 19.04.2024).

Модель піринговой мережі для захищеної корпоративної комунікації

УДК 621.395.7 (043.2)

Михайло Кренцін[1], Леонід Куперштейн[2]

Вінницький національний технічний університет,
[1]mishatron98@gmail.com, [2]kupershtein.lm@gmail.com

Забезпечення безпеки комунікації стає ключовим завданням для успішного функціонування будь-якого підприємства в цифрову епоху. Особливу важливість має забезпечення безпеки каналів зв'язку, оскільки вони є основою для передачі важливої інформації та збереження конфіденційності. Щоб визнати цифровий зв'язок безпечним, важливо враховувати кілька ключових принципів, включаючи шифрування, аутентифікацію, збереження цілісності, конфіденційність та доступність [1]. Без належного захисту можуть виникнути різноманітні загрози, такі як витік цінних даних чи порушення конфіденційності.

На сучасному етапі розвитку існує множина систем комунікації, деякі є загального призначення, а інші спеціалізовані для корпоративного використання. Більшість таких систем базуються на клієнт-серверній архітектурі [2], де центральний сервер відповідає за аутентифікацію, шифрування, забезпечення цілісності тощо. Однак існують численні вразливості та потенційні атаки, спрямовані на центральний сервер, що може призвести до перебоїв у роботі та неможливості здійснення комунікації.

На відміну від традиційного клієнт-серверного підходу до створення інформаційно-комунікаційних систем, існують децентралізовані (пірингові, P2P мережі). Порівняно з клієнт-серверними системами, P2P мережі мають свої переваги, такі як самоорганізованість, стійкість до відмов при втраті зв'язку з вузлами, можливість ресурсного обміну без прив'язки до конкретних адрес, швидше копіювання інформації через використання декількох джерел одночасно, ефективне використання пропускної здатності та гнучке розподілення навантаження [3]. Тому розробка захищеної моделі піринговой мережі для корпоративної комунікації є актуальною задачею на сьогоднішній день.

Проаналізувавши існуючі топології пірингових мереж було визначено, що і структурована мережа, і неструктурована мають свої переваги та недоліки. Також розглянувши моделі комунікацій вузлів у пірингових мережах, було визначено, що найгнучкішою та сприятливою до вирішення задач сьогодення (захищена комунікація між працівниками підприємства) є гібридна модель (така, що містить центральний сервер для певних дій, але комунікація вузлів здійснюється децентралізовано). Проте, федеративна модель має теж ряд переваг, якими не можна нехтувати [4]. Таким чином пропонується модель мережі, що поєднує у собі переваги вищеописаних (рис. 1). Мережа є гібридно-федеративною та частково структурованою.

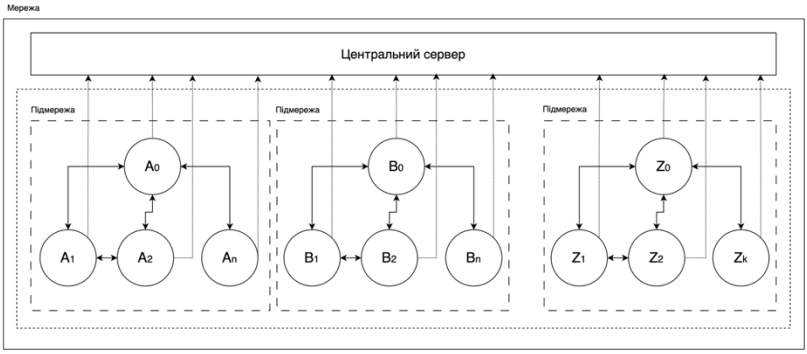


Рис.1. Структурна модель пірингової мережі

Основними елементами мережі є центральний сервер та децентралізовані підмережі. Загалом, множина підмереж складає мережу N, де $N = \{A, B, \dots, Z\}$. $A = \{A_0, A_1, A_2, \dots, A_n\}$, де n є кількістю вузлів у підмережі A; $B = \{B_0, B_1, B_2, \dots, B_m\}$, де m є кількістю вузлів у підмережі B; $Z = \{Z_0, Z_1, Z_2, \dots, Z_k\}$, де k є кількістю вузлів у підмережі Z. Умовно сегменти мережі представляють собою незалежні відділи підприємства, вузли у підмережі – співробітників певного відділу, а мережа загалом – підприємство. Таким чином, це дозволяє здійснювати захищений обмін цінними даними всередині підприємства та ізолювати дані кожного відділу (наприклад, бухгалтерія та відділ розробки).

Центральний сервер відповідає за перший етап аутентифікації учасників у мережі з метою запобігання доступу зловмисникам, які можуть використовувати різноманітні атаки, такі як DoS та DDoS, а також "Людина посередині". Цей підхід не забезпечує абсолютної захищеності від зловмисників, але допомагає зменшити негативний вплив на працездатність децентралізованої мережі. Крім того, сервер містить лише службову інформацію про наявні вузли, таку як ідентифікаційні дані та токени доступу, і не зберігає конфіденційну інформацію, наприклад, криптографічні ключі.

Підмережі функціонують як автономні мережі, поки не виникає необхідність у спільному вузлі для двох федерацій. У такому випадку дві федерації об'єднуються в єдину. Це розділення на підмережі сприяє підвищенню стійкості загальної мережі до потенційних атак зловмисників, оскільки до моменту взаємодії федерацій дії зловмисника не можуть вплинути на інші частини мережі, що допомагає запобігти порушенню стабільності та доступності, наприклад, через атаки "Атака відтоку" або "Ботнет".

У випадку виявлення одним вузлом $A_i \in A$ будь-якої підозрілої або зловмисної активності деякого вузла $B_j \in B$, вузол додається до чорного списку, тому до вузла B_j дані надходитимуть, в від нього – ні. Коли чорний список оновлюється, то ця інформація надсилається усім вузлам федерції. Вузол, що є у чорному списку не може сам себе видалити з нього. Видалення певного вузла $B_j \in B$ з чорного списку можливе лише тоді, коли протягом певного періоду $t, t \in (0; M_{max}]$, де M_{max} – максимальний час (у мілісекундах) перебування вузла у чорному списку. Час M_{max}

збільшується за геометричною прогресією ($M_{max} = 1 * 2^{(n-1)}$, де n – кількість разів, що вузол було додано у чорний список, $n > 0$) для цього ж вузла, якщо він знову опиняється у чорному списку. Це сприятиме зменшенню внутрішнього негативного трафіку в мережі, оскільки зловмисні вузли будуть перебувати в чорному списку все довше і, відповідно, не матимуть можливості передавати дані. Такий підхід допоможе захистити мережу від зловмисних дій атакуючого і забезпечить стабільну роботу інших частин мережі.

Безпосередня комунікація вузлів є лише частковим захистом від зловмисника. Дані, що передаються повинні бути зашифровані надійним алгоритмом, аби унеможливити компрометацію цих даних у випадку, коли один із вузлів все ж виявиться зловмисним. Саме тому модель пірингової мережі передбачає так зване наскрізне шифрування (End-to-end encryption, E2EE) – спосіб передачі даних, в якому доступ до даних, що передаються мають лише ті вузли, які передають та приймають ці дані. Найпоширенішим алгоритмом шифрування, що використовуються у сучасних протоколах E2EE є Діффі-Геллмана [5].

Отже, була розроблена структурна модель пірингової мережі, яка використовує гібридну федеративну структуру. Ця модель об'єднує основні елементи федеративної та децентралізованої та клієнт-серверної архітектур, використовуючи центральний сервер для вирішення певних задач. Модель враховує процеси ініціації та управління з'єднаннями між вузлами, забезпечуючи ефективність та високий рівень безпеки. Модель оптимізована для захисту від потенційних загроз, таких як атаки на конфіденційність або цілісність даних під час встановлення з'єднань. Структурна модель взаємодії між вузлами у федераціях враховує складні аспекти комунікації та забезпечує безпечну передачу даних за рахунок наскрізного шифрування. Вона спрямована на ефективне управління та моніторинг комунікаційного процесу для забезпечення безпеки та реагування на можливі виклики, пов'язані з зовнішніми атаками або внутрішніми загрозами.

1. Guardian Digital Inc. The Importance of Secure Communication in Today's Business World. LinkedIn: Log In or Sign Up. URL: https://www.linkedin.com/pulse/importance-secure-communication-todays-business-world/ (date of access: 16.04.2024).
2. Zmerzlyi I. Клієнт-серверна архітектура та ролі серверів. Medium. URL: https://medium.com/@IvanZmerzlyi/клієнт-серверна-архітектура-та-ролі-серверів-9893d8048229 (дата звернення: 16.04.2024).
3. Куперштейн Л.М., Кренцін М.Д., Маліновський В.І. Аналіз методів підвищення захищеності пірингових мереж. Міжнародна науково-практична конференції “Інформаційні технології та комп’ютерне моделювання”, м. Івано-Франківськ, 6-8 липня 2023 р. с. 135-137
4. Qureshi H. P2P Networking. NAKAMOTO. URL: https://nakamoto.com/p2p-networking (date of access: 16.04.2024).
5. Schillinger, F., Schindelhauer, C. (2019). End-to-End Encryption Schemes for Online Social Networks. In: Wang, G., Feng, J., Bhuiyan, M., Lu, R. (eds) Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2019. Lecture Notes in Computer Science(), vol 11611. Springer, Cham. https://doi.org/10.1007/978-3-030-24907-6_11

Особливості застосування методів протидії змагальним атакам в системах виявлення вторгнень

УДК 004.056.5

Олександр Кручінін[1], Володимир Святошенко[2], Дмитро Тимофєєв[3]

НТУ «Дніпровська політехніка», [1]kruchinin.o.v@nmu.one, [2]sviatoshenko.v.o@nmu.one, [3]tymofieiev.d.s@nmu.one

Одним із ефективних засобів протидії мережним атакам є системи виявлення вторгнень (англ. Intrusion Detection System, IDS). Однак, зі збільшенням складності та різноманітності атак, системи виявлення вторгнень стикаються зі складними задачами адаптації та ефективної протидії. Для вирішення цих задач застосовують методи машинного навчання для системи виявлення вторгнень. Це відкриває нові можливості для підвищення ефективності виявлення атак, але водночас створює потенційні вразливості. Наявність цих вразливостей створює умови для реалізації змагальних атак на системи виявлення вторгнень на основі машинного навчання.

Метою даної роботи є аналіз факторів, які обумовлюють особливості застосування методів протидії змагальним атакам на системи виявлення вторгнень та вплив на їх подальший розвиток.

За результатами класифікації та аналізу змагальних атак на системи виявлення вторгнень можна зробити висновок, що деякі види змагальних атак мають достатньо великий вплив на ефективність IDS. Слід зазначити, що більшість досліджень змагальних атак виконана для систем розпізнавання зображень. Тому для подальших досліджень треба враховувати наступне.

1) У розпізнаванні зображень основною ознакою, що використовується для збурення противника, є пікселі зображення. Однак у мережній безпеці існує велика варіативність типів ознак, які можуть бути використані, і, таким чином, обсяг збурень для ворожих атак значно збільшується.

2) Атаки в мережній безпеці відрізняються від комп'ютерного зору, оскільки розглядаються об'єкти даних, а не зображення. Як наслідок, збурені функції є більш різноманітними та неоднорідними.

Аналіз методів протидії атакам на системи виявлення вторгнень виявив схожу ситуацію. Тільки частина методів протидії може бути застосована саме для захисту IDS. Тобто, на сьогодні є певні успіхи в розробці універсальних засобів захисту, але дослідження в області мережної безпеки потребують розвитку. Можна сформулювати наступні рекомендації щодо вдосконалення та застосування самих IDS та методів протидії змагальним атакам:

1) Використання ансамблів моделей, а саме – інтеграція кількох моделей машинного навчання та поєднання різних стратегій ідентифікації.

Переваги:

- покращення загальної точності за рахунок комбінування прогнозів декількох моделей для виправлення помилок одна одної;
- різні моделі можуть вчитися на різних складових даних і робити помилки в різних областях вхідного простору;
- підвищення стійкості до шуму та зміненню даних завдяки «голосуванню» або усередненню прогнозів;

- зниження ризику перенавчання за рахунок незалежності моделей;
- підвищення стійкості до змагальних атак (змагальні атаки часто розробляються так, щоб впливати на конкретні моделі ML)
- використання моделей, що спеціалізуються на різних типах даних (наприклад: мережний трафік, логи серверів).

Недоліки:

- складність реалізації порівняно з одиночними моделями;
- підвищені вимоги до обчислювальних ресурсів та енергоспоживання;
- збільшення затримки у виявленні та реакції на атаки;
- збільшення трудомісткості налаштування та оновлення;
- наявність небезпеки «голосування більшості».

Таким чином, використання ансамблів моделей доцільно використовувати в IDS, які насамперед вимагають покращення робастності та інтегральної міри резільєнтності.

2) Зменшення ознак або редукція розмірності даних дозволяє зменшити обсяг даних і при цьому зберегти важливу інформацію.

Переваги:

- зменшення кількості ознак може значно знизити час навчання та класифікації моделі;
- усунення незначних ознак може допомогти зменшити вплив шуму на модель IDS;
- ускладнення реалізації змагальних атак за рахунок зменшення можливості маніпулювати всіма ознаками;
- спрощення моделі та зменшення вимог до обчислювальних ресурсів та енергоспоживання;
- зменшення кількості ознак може значно знизити час навчання та класифікації моделі;
- системи з редукцією розмірності можуть бути більш гнучкими та адаптованими для впровадження в різні середовища, що дозволяє масштабувати IDS відповідно до потреб безпеки, що змінюються.

Недоліки:

- можлива втрата важливих ознак, які є критичними для виявлення специфічних типів атак;
- вибір ознак для редукції розмірності вимагає глибокого розуміння даних і потенційних атак;
- існує ризик, що модель навчиться виявляти лише відомі шаблони атак.

Таким чином, використання зменшення ознак доцільно використовувати в IDS, які насамперед вимагають покращення наступних показників: відсоток використання ресурсів, часові показники, пропускна здатність мережі, наприклад для IoT.

Слід зазначити, що представлені методи по суті є діаметрально протилежні за характеристиками та можуть буть використані як базові при розробці нових методів.

Визначення важливих параметрів систем захисту інформації у захищених інформаційних мережах передачі даних

УДК 004.056

Олександр Лаптєв, Юлія Хохлачова,
Абдуллах Аль-Далваш, Наталія Вишневська

Національний авіаційний університет yuliiahohlachova@gmail.com

Одним із першочергових завдань, що передують оцінці безпеки конфіденційного зв'язку, є завдання вибору показників захищеності інформації. Ця система показників має відображати всі вимоги до захисту інформації, структуру МЗ, технологію та умови обробки, зберігання і передавання інформації в ній, а також ураховувати можливості супротивника з добування інформації.

Вибір показників оцінювання безпеки конфіденційного зв'язку є складним дослідницьким завданням і в постановочному плані належить до сфери ухвалення рішення. Складність вибору показників, що дають змогу дати адекватну оцінку захищеності інформації, визначається:

— необхідністю контролю великої кількості засобів і об'єктів захисту, а також заходів, спрямованих на забезпечення безпеки конфіденційного зв'язку;

— випадковістю зовнішніх впливів і внутрішніх змін у системі обробки інформації та системі її захисту;

— відсутністю аналогів показників, що враховують специфіку МЗ і особливості її функціонування;

— необхідністю отримання не тільки якісної, а й кількісної оцінки захищеності інформації.

Узагальнений підхід до побудови інтегрального показника безпеки інформації в системі Q можна представити у вигляді послідовності таких кроків.

1. Формується вектор $X = (x1, \dots, xn)$ вихідних характеристик системи, що обробляє конфіденційну інформацію, кожна з яких є необхідною, а всі вони разом достатні для повного, всебічного контролю та оцінювання ступеня захищеності даної конфіденційної інформації.

2. Формується вектор $Q = (q1, \dots, qm)$ окремих комплексних показників захищеності, що являють собою функції $q_i(x)$, $i = l, \dots, m$ вектора початкових характеристик $x=(x_1,\dots,x_n)$ та які оцінюють різні складові захищеності досліджуваної системи з використанням m різних критеріїв.

3. Формується вектор $H = (h1, \dots, hk)$ параметрів захищеності, що характеризує значення кожного окремого показника $q_i(x)$.

4. Визначається значення вектора $W=(w_1\dots,w_m)$, де $w_1\dots,w_m$ – *вагові* коефіцієнти, що визначають значущість окремих показників $q_{1,\dots,}q_m$ для інтегральної оцінки Q і задають ступінь впливу окремих показників $q_{1,\dots,}q_m$ на цю оцінку.

5. Обирається вид синтезуючої функції $Q(q)$, що зіставляє вектору окремих показників $Q^{=}(q_{1,\dots,}q_m)$ інтегральну оцінку Q (значення Q інтегрального показника $Q(q)$), яка характеризує ступінь захищеності інформації досліджуваної системи загалом Q:

$$Q = Q(q) = Q(q; w), w = (w1, \dots, wm). \quad (1)$$

На рис. 1 наведено загальну схему визначення показників захищеності інформації в МЗ. Під час оцінювання безпеки найчастіше необхідні значення показників, узагальнених за якимось одним індексом - певною категорією порушника, певним каналом витоку інформації, певним компонентом МЗ. Узагальнення може здійснюватися і на основі будь-якого екстремального стану захищеності.

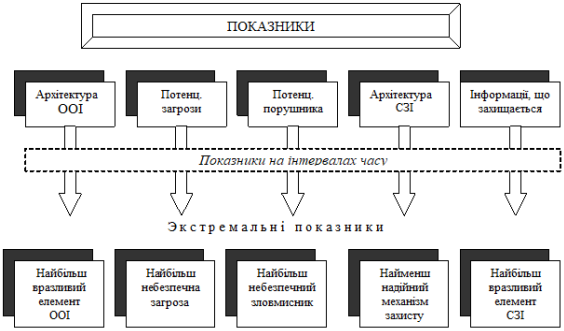


Рис. 1. Схема визначення показників безпеки інформації

Основними параметрами, що визначають показники захищеності інформації, є:

— кількість та характеристики тих структурних компонентів МЗ, в яких оцінюється захищеність інформації;

— кількість і характеристики дестабілізуючих факторів, які потенційно можуть проявитися і негативно вплинути на інформацію, що захищається;

— кількість та характеристики застосовуваних механізмів захисту інформації;

— число та категорії осіб, які потенційно можуть бути порушниками правил доступу та обробки інформації, що захищається;

— види інформації, що захищається.

Велике значення для оцінки захищеності інформації має часовий інтервал щодо якого оцінюється захищеність. Незважаючи на те, що час є категорією суто безперервної, для цілей його як параметр захищеності можна структурувати, виділивши інтервали для аналізу та оцінки рівня захищеності інформації. Такі інтервали можна поділяти:

— на дуже малі – інтервали, які можна вважати точками;

— малі – інтервали, які не можна зводити до точки, але процеси, що відбуваються, на яких щодо розв'язуваних завдань можна вважати однорідними;

— великі – інтервали, які не можна вважати малими, але за якими заздалегідь можна визначити стан кожного структурного компонента на кожному малому інтервалі;

— дуже великі – інтервали, для яких не може бути виконана умова великих інтервалів, але за якими з достатньою точністю все ж таки можна спрогнозувати послідовність та зміст функціонування основних компонентів системи захисту інформації;

— нескінченно великі – інтервали, для яких неможливо виконати умову існування дуже великих інтервалів.

Існують три методологічні підходи до вирішення задачі оцінки захищеності інформації: суто емпіричний, суворо теоретичний та теоретико-емпіричний.

Сутність *емпіричного підходу* полягає в тому, що на основі тривалого збору та обробки фактичних даних про реальні прояви загроз інформації та розміри збитків, які при цьому мав місце, чисто емпіричним шляхом встановлюються залежності між потенційно можливим збитком та коефіцієнтами, що характеризують частоту прояву відповідної загрози та значення наявного за її прояві розміру шкоди. Розглянемо підходи, що розвиваються в цих моделях.

Вихідною посилкою розробки моделей є майже очевидне припущення, з одного боку, у разі порушення захищеності інформації завдається певний збитки, з іншого - забезпечення захисту інформації пов'язані з витрачанням коштів. Очікувана повна вартість захисту може становити суму, що складається з видатків на захист та втрат від її порушення.

Для визначення рівня витрат, що забезпечують необхідний рівень захищеності інформації, необхідно принаймні знати, по-перше, повний перелік загроз інформації, по-друге, потенційну небезпеку для інформації кожної з загроз і, по-третє, розміри витрат, необхідних для нейтралізації кожної із загроз.

Строго теоретичний підхід ґрунтується на тому посиланні, що потенційно можливі прояви загроз та розміри потенційно можливої шкоди є випадковими подіями, а тому можуть бути охарактеризовані законами розподілу та числовими характеристиками. Приклад даного підходу розглянуто у [42] на основі динамічної моделі оцінки потенційних загроз. Сенс даної моделі на змістовному рівні може бути представлена таким чином:

1. Введено поняття «середній коефіцієнт можливого прояву загрози» кожного типу — 1. Функція розподілу має визначатися з урахуванням обробки статистичних *даних*, зібраних у процесі реального функціонування МЗ.

2. Зроблено припущення, що кількість проявів загрози r_t протягом фіксованого періоду часу залежить лише від тривалості періоду спостереження та середнього коефіцієнта прояву, внаслідок чого для числа проявів загроз справедливим визнано розподіл Пуассона:

$$P(\overline{r} = r/\lambda) = \frac{(\lambda t) r e^{-\lambda t}}{r!}. \qquad (2)$$

3. За рядом значень числа загроз, отриманих для інтервалів різної тривалості, розподіл середнього коефіцієнта представлений у вигляді гамма-розподілу з параметрами.

4. На основі інтегрування двох названих вище розподілів отримано безумовний розподіл ймовірностей числа проявів загрози за певний період часу.

Викладки для оцінки очікуваної шкоди виглядають так:

— спочатку розглядається середня шкода від прояву загроз і приймається нормальна функція її розподілу;

— за даними спостереження за проявами загроз і розміром шкоди, що мала місце, на декількох інтервалах часу різної тривалості коригуються параметри розподілу середньої шкоди;

— виділяючи невизначені параметри з функції розподілу ймовірностей збитків, будують остаточний розподіл розміру очікуваних збитків.

Теоретико-емпіричний підхід певною мірою ґрунтується на синтезі основних положень емпіричного та теоретичного підходів. Цей синтез полягає в тому, що на основі теоретико-імовірнісних методів будуються моделі, необхідні для визначення та прогнозування показників захищеності, а на основі збору та обробки статистичних даних, отриманих у ході теоретичних досліджень та практичних розробок проблем захисту інформації, формулюються вихідні дані, необхідні для практичного використання моделей.

Розглянемо одні з методів оцінки безпеки інформації на ЗСЗ, що належать до теоретико-емпіричного підходу.

Комплексним показником оцінки безпеки при цьому обраний рівень безпеки інформації, що обробляється та зберігається в системі, що характеризує можливість надати достатню протидію виникненню КНПІ та ПНЦІ та визначається як ймовірність забезпечення захисту інформації *($P_{зі}$)* у системі, що розглядається:

$$P_{ЗІ} = P_{кнпі} P_{пнці}, \tag{3}$$

де, $P_{кнпі}$ – ймовірність захисту інформації від витоку КНПІ;

$P_{пнці}$ – ймовірність забезпечення цілісності інформації.

Забезпечити захист від розглянутих видів загроз можна, вирішивши, як зазначалося вище, комплекс завдань захисту. Для вирішення цих завдань мають бути обрані типові методи та засоби. Рівень безпеки інформації зрештою визначається здатністю застосовуваних засобів захисту перекрити характерні для об'єкта КНПІ та усунути ПНЦІ.

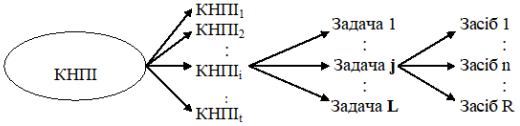


Рис. 2. Структура вирішення проблеми перекриття КНПІ системи

Імовірність захисту інформації на об'єкті від витоку КНПІ визначається безліччю таких каналів *{K}*, притаманних для даного об'єкта.

Виходячи з припущення про незалежність випадків виникнення каналів, значення $P_{кнпі}$ можна виразити як

$$P_{кнпі} = \prod_{i=1}^{K} P_{кнпі_з}. \tag{4}$$

Проблему перекриття КНПІ можна вирішити реалізацією різних видів завдань із множини *{L}*, характерного для КНПІ;

$$P_{кнпі} = 1 - \prod_{j=1}^{L} (1 - P_{\varsigma_j}), \tag{5}$$

де $P_{\varsigma j}$ – ймовірність забезпечення безпеки перекриття і-го КНПІ при вирішенні j-го завдання захисту інформації. Це можна зробити різними засобами з безлічі наявних на об'єкті *{R}*:

$$P_{\varsigma_j} = 1 - \prod_{i=1}^{R} (1 - P_{\tilde{N}D_n}), \tag{6}$$

де $P_{ЙД\ n}$ – ймовірність забезпечення безпеки *n*-м засобом захисту інформації.

Аналогічні залежності можна сформулювати й у розрахунку $P_{кнпі}$. Розрахунок даних ймовірностей може здійснюватися за відомими методиками на основі статистичних оцінок коефіцієнтів безпеки, що виражають відношення поточного значення небезпечного сигналу до значення, що нормується, для відповідного каналу витоку інформації.

Таким чином, розглянуто можливість кількісного визначення інтегрального показника, що характеризує ступінь безпеки інформації на об'єкті та визначається ймовірністю витоку інформації з урахуванням усіх факторів, що значно впливають на його формування. На основі цього показника проводиться оцінка стану системи захисту інформації.

На закінчення необхідно сказати, що розглянуті моделі в основному використовуються не просто для отримання конкретних значень показників уразливості, а для оцінки поведінки цих значень при варіюванні істотно значущими вихідними даними у можливих діапазонах їх змін.

Інша модель оцінки може бути заснована на теорії ігор, що передбачає побудову оптимальних стратегій поведінки двох протиборчих сторін, Припустимо, що зловмисник витрачає *x* коштів з метою подолання механізму захисту, створення якого витрачено *y* коштів. Очікувана кількість інформації, яку отримує зловмисник, є деяка функція *I(x,y)*. Якщо далі *f(n)* є цінністю для зловмисника т одиниць інформації, а *g(n)* – сумарні витрати на створення та заощадження цього ж числа одиниць інформації, то чистий прибуток зловмисника виражатиметься як

$$V(x,y) = f[I(x,y)] - x, \tag{7}$$

а втрати

$$u(x,y) = g[I\{x,y)] + y. \tag{8}$$

Побудова оптимальних стратегій буде зводитись до отримання максимально можливого прибутку з боку зловмисника та мінімізації втрат з боку захисників інформації. Природним продовженням моделей оцінки загроз є моделі нейтралізації цих загроз, тобто захисту. Одними із найбільш розроблених є моделі систем розмежування доступу. До цього типу моделей відноситься п’ятивимірна модель безпеки. Для формального опису процесу доступу до даних в умовах захисту введено п’ять таких множин: U-список зареєстрованих користувачів; R-набір наявних у системі ресурсів, що містять або обробляють конфіденційну інформацію; S – безліч можливих станів ресурсів; E-набір операцій над ресурсами; A – перелік можливих повноважень користувачів.

Вводиться поняття «область безпеки» як декартовий добуток перелічених множин:

$$D = U\,A\,R\,S\,E. \tag{9}$$

В області безпеки можуть бути виділені підобласті, що відповідають окремим користувачам, окремим ресурсам тощо. Будь-який запит на доступ може бути описаний чотиривимірним кортежем

$$q = (u,r,s,e), \tag{10}$$

де $u \in U$, $r \in R$, $s \in S$, $e \in E$.

Запит отримує право на доступ лише в тому випадку, якщо він потрапляє у відповідну сферу безпеки. Малюнок 3 ілюструє реалізацію даної моделі для опису доступу співробітника *N* до копіювання інформації 1_K, що має гриф «Секретно».

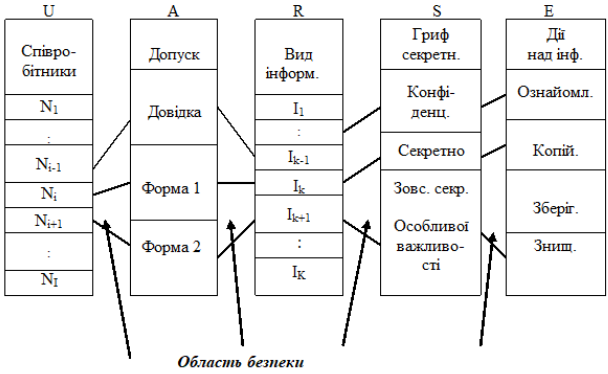


Рис. 3. Структура п’ятивимірної моделі доступу до інформації

Розглянуті вище моделі дозволяють визначати поточні та прогнозувати майбутні значення всіх показників уразливості інформації для будь-яких компонентів МЗ, будь-якої їх комбінації та будь-яких умов життєдіяльності системи.

Щодо адекватності моделей тим реальним процесам, для імітації яких вони призначаються, слід зробити два суттєві зауваження:

1) практично всі моделі побудовані в припущенні незалежності тих випадкових подій, сукупності яких утворюють складні процеси захисту інформації на сучасних МЗ;

2) для забезпечення роботи моделей необхідні великі обсяги таких вихідних даних, переважна більшість яких нині відсутня, а формування їх пов'язане з великими труднощами.

Розглянемо коротко істота наведених зауважень та визначимо порядок використання моделей у умовах. Зауваження перше; допущення незалежності випадкових подій, що відбуваються у системах захисту інформації. Основними подіями, що імітуються в моделях визначення показників уразливості, є прояв дестабілізуючих факторів на інформацію, що захищається, і вплив використовуваних засобів захисту на дестабілізуючі фактори. При цьому зроблено такі припущення (причому в аналітичних – у явному вигляді):

— потенційні можливості прояву кожного дестабілізуючого фактору не залежать від прояву інших;

— кожен із зловмисників діє незалежно від інших;

— негативний вплив на інформацію кожного з дестабілізуючих факторів не залежить від такого ж впливу інших факторів;

— негативний вплив дестабілізуючих факторів на інформацію в одному будь-якому компоненті МЗ може призвести лише до вступу на входи пов'язаних з ним компонентів інформації з порушеною захищеністю і не впливає на такий самий вплив на інформацію в цих компонентах;

— кожний із засобів захисту має нейтралізуючий вплив на дестабілізуючі фактори та відновлюючий вплив на інформацію незалежно від такого ж впливу інших;

— сприятливий вплив засобів захисту в одному компоненті ЗСЗ лише знижує ймовірність надходження на входи пов'язаних з ним компонентів інформації з порушеною захищеністю та не впливає на рівень захищеності інформації у самих цих компонентах.

Друге зауваження стосується забезпечення моделей необхідними вихідними даними. Вище вже неодноразово зазначалося, що з практичного використання моделей визначення показників уразливості необхідні великі обсяги різноманітних даних, причому переважна більшість із них нині відсутні.

Сформулюємо тепер рекомендації щодо використання моделей, розроблених у рамках розглянутих вище припущень маючи на увазі, що це використання, забезпечуючи вирішення завдань щодо аналізу, синтезу та управління в системах захисту інформації, не повинно призводити до істотних похибок.

Перша та основна рекомендація зводиться до того, що моделями повинні користуватися кваліфіковані фахівці – професіонали в галузі захисту інформації, які могли б у кожній конкретній ситуації вибрати найбільш ефективну модель та критично оцінити ступінь її адекватності одержуваним рішенням.

Друга рекомендація Полягає в тому, що моделі треба використовувати не просто для отримання конкретних значень показників уразливості, а для оцінки поведінки цих значень при варіюванні істотно значущими вихідними даними у можливих діапазонах їх змін.

Третя рекомендація зводиться до того що, що з оцінки адекватності моделей, вихідних даних, і одержуваних рішень треба якнайширше залучати кваліфікованих і досвідчених експертів.

Нарешті, четверта рекомендація у тому, що з ефективного використання моделей треба безупинно виявляти підвищену турботу про вихідних даних, необхідні забезпечення моделей під час вирішення завдань із захисту. Істотно важливою при цьому є та обставина, що переважна кількість вихідних даних має високий ступінь невизначеності. Тому треба не просто формувати необхідні дані, а перманентно їх оцінювати та уточнювати.

Припустимо, що якість функціонування СЗІ описується сукупністю приватних критеріїв, які необхідно мінімізувати $K = \langle K_1, \vec{K}_2, ..., K_m \rangle$. Знайдемо відносні відхилення приватних критеріїв від екстремальних (мінімального та максимального) значень:

$$K^i_{\max} = \frac{K_i(СЗИ) - K_i^{\min}(СЗИ)}{K_i^{\max}(СЗИ)}, \quad i = \overline{1,m}. \tag{11}$$

Тоді обрана СЗІ залишатиметься оптимальною за сукупністю приватних критеріїв, якщо вони характеризуються сукупністю відносних відхилень, які є найменшими значеннями. Позначивши оптимальний варіант системи захисту інформації Со, запишемо у формалізованому вигляді це завдання таким чином:

$$K_{\max}(C_0) < K_{\max}(C), \; C, C_0 \in \mathrm{M}_{CD}, \tag{12}$$

де $K_{\max} = \max\{K_i\}$, $i = \overline{1,m}$ - найбільше з відносних відхилень, що розраховуються за формулою (3.11); $C_{сд}$ – безліч СЗІ (суворо допустимих), сукупності умов, які задовольняють застосування та обмеження на структуру та значення основних параметрів. До умов застосування СЗІ належать, наприклад, діапазон робочих температур, глибина захисту тощо. Запропонований критерій відрізняється тим, що дозволяє оцінювати СЗІ в діапазоні можливих відхилень приватних критеріїв і завдяки цьому додатково враховує ступінь погіршення одних параметрів СЗІ за рахунок поліпшення інших.. Однак, якщо $K_i^{\min}$ « $K_i^{\max}$, при використанні цього критерію може статися, що перевага буде віддана такій СЗІ з пари існуючих, яка за незначного кращого (меншого) значення одного показника якості має значно гірші інші показники порівняно з відповідними показниками якості іншої СЗІ. У такому разі критерій, що розглядається, має такий самий недолік, як і критерії, наведені в роботах. З огляду на це модифікований мінімаксний критерій, який доцільно використовувати при виборі оптимального варіанту із сукупності СЗІ однакового технологічного виконання.

Мінімаксний критерій (3.12) можна навести також у вигляді:

$$K_p = f_p(K_1,\ldots,K_i,\ldots,K_m) = \min,\ C \in C_{СД}, \tag{13}$$

де

$$f_p(K_1,\ldots K_i,\ldots K_m) = \max \frac{K_i - K_1^{\min}}{K_1^{\max}},\ldots, \frac{K_i - K_i^{\min}}{K_i^{\max}},\ldots, \frac{K_m - K_m^{\min}}{K_m^{\max}} \tag{14}$$

Система захисту інформації Со, що визначається рішенням задачі (13), (14) і буде оптимальною. З формули (13) слід, що мінімаксний критерій можна вважати різновидом критерію, заснованого на мінімізації результуючої цільової функції, вид якої відповідає виразу (14).

З залежностей (13) і (14) бачимо, що мінімаксний критерій забезпечує найкраще (найменше) значення із сукупності найгірших (найбільших) нормованих показників якості. Тому всі окремі показники якості СЗІ повинні бути приведені до стаціонарного вигляду. Показник якості K_i вважатиметься стандартним, якщо він задовольняє умові $K_i \geq 0$, де $i = \overline{1,m}$, і що менше величина K_i, краще обраний варіант СЗІ. Якщо будь-який показник якості K_i^* не є стандартним, його завжди можна привести до вигляду . Наприклад, якщо невід'ємний показник якості може змінюватися в межах $K_{i\min}^* \leq K_i^* \leq K_{i\max}^*$ і чим більша величина K_i^*, тим краще СЗІ, то як еквівалентний йому стандартний показник якості необхідно вибрати величину $K_i = K_{i\max}^* - K_i^*$ або (за умови $K_{i\max} \to \infty$) $K_i = 1/K_i^*$. Таким чином, K_i^* є стандартним показником якості, що дає можливість здійснювати порівняння СЗІ в різних умовах експлуатації або порівнювати різні системи, які працюють на одному об'єкті, між собою.

Ефективність та проблеми використання кібернавігаційних та кіберпросторових методів у розслідуванні кіберзлочинів

УДК 004.67

Марина Ларченко

Національний університет «Чернігівська політехніка»,
Ніжинський державний університет імені Миколи Гоголя,
urlinka2006@gmail.com

Використання кібернавігаційних та кіберпросторових методів у розслідуванні кіберзлочинів є ключовим етапом у боротьбі з кіберзлочинністю. Вони дозволяють збирати докази, необхідні для успішного проведення розслідування та притягнення злочинців до відповідальності [1].

Кібернавігація включає в себе використання різних цифрових технологій, таких як GPS, IP-адреси, мережеві протоколи тощо, для визначення місцезнаходження та руху користувачів у кіберпросторі [2]. Кіберпростір, у даному контексті, включає в себе інтернет, комп'ютерні мережі, віртуальні середовища та інші цифрові платформи.

Однією з основних переваг кібернавігаційних та кіберпросторових методів у розслідуванні кіберзлочинів є їх здатність забезпечувати детальну інформацію щодо місцезнаходження, дій та взаємодій злочинців у віртуальному середовищі [3]. Вони дозволяють слідчим встановлювати маршрути та зв'язки між різними суб'єктами кібернавігації, а також виявляти цифрові сліди, які можуть бути використані для ідентифікації злочинців та підтвердження їх дій.

Під час розслідування кіберзлочинів відомими кіберполіцейськими організаціями та службами безпеки в усьому світі використовуються різноманітні кібернавігаційні та кіберпросторові методи, серед яких можна виділити наступні [4, 5]:

IP-аналіз: Включає в себе вивчення IP-адрес, які використовуються зловмисниками, для виявлення їхнього місцезнаходження та маршрутів.

Цифровий форензічний аналіз: Полягає у зборі, аналізі та інтерпретації цифрових доказів, таких як файли журналів, метадані та інші цифрові сліди, залишені зловмисниками.

Використання веб-стежачів та куки: Використовуються для відстеження дій користувачів у мережі та збору інформації про їхню активність та звички.

Методи аналізу мережевого трафіку: Дозволяють виявити незвичайну активність в мережі, а також виявити атаки, що здійснюються через мережу.

Використання геолокаційних технологій: Зокрема, використання GPS-даних або інших методів визначення місцезнаходження для виявлення фізичного місцеперебування зловмисників.

Аналіз мережевих протоколів: Полягає у вивченні протоколів, що використовуються для комунікації в мережі, для виявлення аномальних патернів або поведінки.

Використання соціальних медіа: Аналіз активності у соціальних мережах та форумах для виявлення злочинців, їхніх контактів та зв'язків.

Основною метою сучасних досліджень у цій сфері має бути встановлення наскільки ефективно застосовуються кібернавігаційні та кіберпросторові методи в

розслідуванні кіберзлочинів, а також розгляд проблем, що виникають у цьому процесі. Ключові питання, які потребують вирішення систематизовані нижче в таблиці 1.

Таблиця 1

Факторно-інформаційна таблиця ефективності та проблем використання кібернавігаційних та кіберпросторових методів у розслідуванні кіберзлочинів

Фактор	***Опис***	***Ключові аспекти***
Ефективність	Оцінка ефективності використання кібернавігаційних та кіберпросторових методів у виявленні кіберзлочинів	Співвідношення успішних розслідувань до загальної кількості випадків
Методи та інструменти	Аналіз методів та інструментів, які використовуються для збору та аналізу цифрових слідів у кіберпросторі	Популярність та ефективність різних інструментів
Проблеми точності та достовірності даних	Виявлення та аналіз проблем, пов'язаних з точністю та достовірністю кібернавігаційних даних у розслідуванні кіберзлочинів	Частота та серйозність помилок у навігаційних даних
Приватність та етичні аспекти	Розгляд викликів та обмежень, пов'язаних з приватністю та етичними аспектами використання кібернавігаційних та кіберпросторових методів	Законність та моральність використання отриманих даних

Згідно з аналізом, проведеним у рамках статті, підтверджено, що кібернавігаційні та кіберпросторові методи є ключовими інструментами для виявлення, аналізу та розслідування кіберзлочинів. Вони також дозволяють збирати докази, необхідні для притягнення злочинців до відповідальності. Наявні проблеми вимагають постійного вдосконалення методів, а також розробки відповідного законодавства та етичних стандартів для забезпечення прав та приватності користувачів.

1. Clarke, R. A., & Knake, R. K. Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins. 2010. 140 p.
2. Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press is an imprint of Elsevier, 2011. 837 p.
3. Goodall, J. Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices. IGI Global, 2016. 275 p.
4. Nelson, B., Phillips, A., & Steuart, C. Guide to Computer Forensics and Investigations. Cengage Learning, 2018. 688 p.
5. Rogers, M. Network Forensics: Tracking Hackers through Cyberspace. Prentice Hall, 2019. 545 p.

Вплив соціальних мереж на інформаційну безпеку

УДК 004.77

Світлана Легомінова[1], Юрій Якименко[2],
Михайло Запорожченко[3]

Державний університет інформаційно-комунікаційних технологій,
[1]chiarasvitlana77@gmail.com, [2]yakum14@ukr.net,
[3]zaporozhchenkomm@gmail.com

Сучасні соціальні мережі повністю змінили спосіб комунікації, налагодження зв'язків та обміну інформацією по всьому світу. Ці платформи пропонують численні переваги, включаючи миттєве спілкування, можливості для нетворкінгу та доступ до широкого спектру інформаційних та розважальних ресурсів. Завдяки цьому користувачі можуть бути в курсі подій, що відбуваються з їхніми друзями, родичами та іншими людьми, та всього, що відбувається в їхньому оточенні.

Однак разом з цими перевагами з'являються і значні загрози для інформаційної безпеки та приватності користувачів. Соціальні мережі часто збирають значні обсяги як персональних даних, таких як дата народження, номер телефону тощо, так і особистої інформації, включаючи вподобання користувачів, їхню поведінку та взаємодію. Ці дані часто використовуються для таргетованої реклами та персоналізації контенту, але вони також викликають занепокоєння щодо порушення конфіденційності та несанкціонованого доступу.

Крім того, поширення фейкових новин, дезінформації та кіберзагроз у соціальних мережах створює серйозні виклики для інформаційної безпеки. Зловмисники використовують соціальні мережі для поширення неправдивої інформації, маніпулювання громадською думкою та здійснення кібератак, таких як фішинг або розповсюдження шкідливого програмного забезпечення. Так, наприклад, за результатами дослідження [1], проведеному в 2023 році, було виявлено, що більшість українців вірять інформації, викладеній в соціальних мережах (рис. 1).

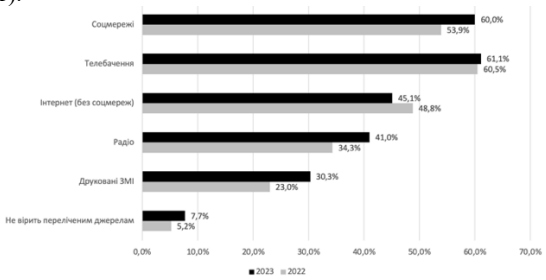


Рис.1. Джерела інформації, яким довіряють користувачі

Особливо привабливою платформою для зловмисників з точки зору планування кібератак на організації, в т.ч. з використанням соціальної інженерії, є LinkedIn, яка стала надзвичайно популярною завдяки своїй унікальній спрямованості на професійний нетворкінг та розвиток кар'єри. LinkedIn надає користувачам можливості для пошуку компаній, колег та демонстрації своїх навичок і досягнень за допомогою докладних профілів, а також платформу для спілкування та обміну

знаннями з колегами, наставниками та потенційними роботодавцями. Роботодавці та рекрутери також використовують платформу для розміщення оголошень про вакансії, відбору кандидатів та пошуку потенційних працівників, в яких нерідко вказуються вимоги до кандидата, особливості системи, з якою йому доведеться працювати, використовувані технології і т.д., що може стати цінною інформацією для кіберзлочинця, який планує атаку на цю організацію.

Таким чином, незважаючи на свою популярність і корисність, LinkedIn також створює певні загрози для інформаційної безпеки. По-перше, як і будь-яка інша онлайн-платформа, LinkedIn є вразливою до витоку даних, коли інформація користувачів, така як адреси електронної пошти, паролі та особисті дані, може бути скомпрометована. У минулому LinkedIn стикався з інцидентами безпеки, що призводили до витоку даних користувачів.

По-друге, кіберзлочинці можуть націлюватися на користувачів LinkedIn за допомогою фішингових електронних листів або повідомлень, представляючись рекрутерами або колегами, щоб обманом змусити їх розкрити конфіденційну інформацію або перейти за шкідливим посиланням, що може призвести до крадіжки особистих даних, фінансових втрат або зараження шкідливим програмним забезпеченням [2]. Також існує занепокоєння щодо того, як LinkedIn та сторонні розробники можуть використовувати або зловживати даними користувачів для цілей, на які користувачі не давали своєї згоди. Це піднімає питання про конфіденційність даних, прозорість та етичні практики.

Незважаючи на ці ризики, LinkedIn залишається цінним інструментом для професійного спілкування та кар'єрного зростання за умови, що користувачі вживають необхідних заходів для захисту своєї інформації та конфіденційності.

Таким чином, щоб зменшити ризики, пов'язані з використанням зловмисниками соціальних мереж для отримання інформації про користувача або для розповсюдження дезінформації чи шкідливого програмного забезпечення, користувачі повинні бути пильними щодо своєї діяльності в соціальних мережах, регулярно переглядати налаштування конфіденційності та з обережністю ділитися особистою інформацією. Крім того, компанії, що розробляють соціальні мережі, повинні надавати пріоритет конфіденційності користувачів та інвестувати в надійні заходи безпеки, включаючи шифрування, анонімізацію даних і суворий контроль доступу, щоб захистити дані користувачів і ефективно протидіяти кіберзагрозам.

1. Media consumption habits of Ukrainians: the second year of full-scale war. URL: https://www.oporaua.org/en/polit_ad/24796-mediaspozhivannia-ukrayintsiv-drugii-rik-povnomasshtabnoyi-viini-24796 (дата звернення: 18.04.2023).
2. Jason Edwards. The dynamics of social media security: threats, privacy, and the future. URL: https://www.linkedin.com/pulse/dynamics-social-media-security-threats-privacy-future-dr-jason-4kfzc?trk=public_post (дата звернення: 18.04.2023).

Ефективність алгоритмів машинного навчання для виявлення аномалій у фінансових операціях

УДК 621.395.7 (043.2)

Юрій Лісовський[1]

Львівський національний університет імені Івана Франка,
[1]yuralisovskiy98@gmail.com

Оплата товарів чи послуг в мережі Інтернет стає буденністю. Кількість платежів, які проходять в онлайні зростає і цим користуються шахраї. Зловмисники намагаються привласнити чужі кошти, які зберігаються на банківських картках. Для мінімізації втрат банки та фінансові компанії впроваджують системи протидії. Оскільки, шахраї завжди еволюціонують, класичні алгоритми захисту можуть бути не ефективними. Наприклад, використовуючи заздалегідь визначені набори правил, система захисту не зможе виявити раніше невідомі ознаки, які вказують на шахрайство, бо такого правила просто немає в списку.

Моделі штучного інтелекту дають можливість передбачити набагато більше можливих комбінацій ознак, які можуть вказувати на те, що операція є шахрайською, ніж уже згадані набори правил. Використання машинного навчання дає можливість будувати більш ефективні системи захисту.

Ключовою відмінністю від багатьох задач класифікації є сильна незбалансованість даних, на яких потрібно навчати модель. Більшість операцій є звичайними, і лише дуже мала частка з них – шахрайськими.

Метою роботи є порівняння ефективності моделей машинного навчання для виявлення шахрайства серед фінансових операцій різних типів.

Для порівняння було вибрано два звичайних алгоритми: логістична регресія [1] і метод опорних векторів [2], та два ансамблевих: випадковий ліс [3] та екстремальне градієнтне підсилювання (XGB) [4].

У зв'язку з обмеженістю доступу до даних фінансових установ, для навчання моделі було використано набір синтетично створених операцій [5]. У таблиці 1 подано список параметрів, що містить набір, а також їх опис. Набір даних було перевірено на відсутність пропущених значень, категоріальні параметри перетворено у числові, вилучено зайві параметри та прибрано частину даних, для яких присутні лише звичайні операції. Перевірку якості натренованих моделей було виконано за допомогою матриці невідповідностей, а також наступних метрик: влучності (1), повноти (2) та F-міри (3):

$$precision = \frac{TP}{TP+FP}, \tag{1}$$

$$recall = \frac{TP}{TP+FN}, \tag{2}$$

$$f\ score = \frac{2 \times precision \times recall}{precision+recall}, \tag{3}$$

де TP – кількість істинно-позитивних прикладів, які виявила модель, FP – кількість хибно-позитивних, та FN – кількість хибно-негативних.

Таблиця 1

Параметри оригінального набору синтетичних даних

step	Кількість годин, що пройшли від початку симуляції: 1, 2,
type	Тип операції: CASH-IN, CASH-OUT, DEBIT, PAYMENT та TRANSFER
amount	Сума операції
nameOrg	Ідентифікатор рахунку ініціатора операції
oldBalanceOrg	Баланс на рахунку ініціатора перед операцією
newBalanceOrig	Баланс на рахунку ініціатора після операції
nameDest	Ідентифікатор рахунку отримувача
oldBalanceDest	Баланс на рахунку отримувача перед операцією
newBalanceDest	Баланс на рахунку отримувача після операції
isFraud	1 – операція шахрайська, 0 – справжня
isFlaggedFraud	1 – спроба переказу на суму більшу, ніж 200.000, 0 – у іншому випадку

Для аналізу та обробки набору даних було використано бібліотеку *pandas* [6], реалізацію алгоритмів було використано з бібліотек *scikit-learn* [7] та *xgboost* [8].

Результати, отримані в ході навчання та тестування, наведено у таблиці 2. З таблиці видно, що усі моделі добре вміють виявляти об'єкти класу більшості, і лише XGB має високу точність виявлення обох класів.

Таблиця 2

Порівняння ефективності моделей

Алгоритм	Влучність	Повнота	F-міра
Logistic Regression	0.913	0.485	0.633
Support Vector Machine	0.870	0.485	0.623
Random Forest	0.999	0.479	0.648
Extreme Gradient Boosting	0.952	0.947	0.950

1. Tolles J., Meurer W. J. Logistic regression: relating patient characteristics to outcomes, Jama, 316(5), 2016. 533-534 pp.
2. Cortes C., Vapnik V. Support-vector networks, Machine Learning, 20, 1995. 273–297 pp.
3. Breiman L. Random Forests. Machine Learning. 45 (1), 2001. 5–32 pp.
4. Wade C. Hands-On Gradient Boosting with XGBoost and scikit-learn. Birmingham: Packt Publishing Ltd., 2020. 117-121 pp.
5. Synthetic Financial Datasets For Fraud Detection. URL: https://www.kaggle.com/datasets/ealaxi/paysim1 (accessed: 15.11.2023)
6. Бібліотека *pandas* для мови програмування Python. URL: https://pandas.pydata.org/ (дата звернення: 23.12.2023)
7. Бібліотека *scikit-learn* для мови програмування Python. URL: https://scikit-learn.org/ (дата звернення: 23.12.2023)
8. Бібліотека *xgboost* для мови програмування Python. URL: https://github.com/dmlc/xgboost (дата звернення: 23.12.2023)

Кіберполігон кафедри твердотільної електроніки та інформаційної безпеки УжНУ

УДК 004.056:378.16 (043.2)

Богдан Маліцький[1], Сергій Калкутін[2], Василь Різак[3]

Ужгородський національний університет, [1]bohdan.malitskyi@uzhnu.edu.ua, [2]serhii.kalkutin@uzhnu.edu.ua, [3]vrizak@uzhnu.edu.ua

Кібербезпека є однією з найважливіших областей у сучасному цифровому світі, де зростання числа кібератак ставить під загрозу особисті, корпоративні та національні інтереси. В цьому контексті кафедра твердотільної електроніки та інформаційної безпеки (далі – ТЕІБ) Ужгородського національного університету створила кіберполігон, який служить як важливий інструмент для практичної підготовки у боротьбі з кіберзагрозами. Цей кіберполігон дозволяє користувачам здобувати реальний досвід роботи з кібератаками та оборонними стратегіями в контрольованому та безпечному середовищі.

Метою даної розробки є створення нового кіберполігону на базі існуючих напрацювань на кафедрі ТЕІБ та їх розширення за допомогою нового обладнання, програмного забезпечення та сценаріїв.

Завдяки підтримці агентства США з міжнародного розвитку USAID, ми змогли оновити матеріально-технічну базу наявного полігону кібербезпеки, а також розширити її за допомогою додавання нових компонентів.

Кіберполігон – це комплексна гейміфікована система, реалізована для моделювання реалістичних сценаріїв кібератак та фізично поділяється на сектори для команди атаки (red team) та команди захисту (blue team). Основне завдання цієї команди полягає в проникненні в мережу на основі знайдених під час сканування вразливостей, закріплення в комп'ютерах, які знаходяться в цій мережі, а також в отриманні доступу до певної інформації. Основне завдання цієї команди це постійний моніторинг, документування та в окремих випадках безпосереднє втручання в дії команди атаки (блокування учасників від команди атаки в мережі).

Специфіка завдань для кожної з команд може відрізнятись в залежності від сценаріїв. Наразі користувачі полігону можуть працювати з базовим сценарієм роботи, заснованим на особливостях та вразливостях операційної системи Metasploitable 2. У співпраці з компанією UnderDefense розробляються та поступово впроваджуються три нові сценарії роботи полігону різного рівня складності. Основними вимогами до сценаріїв є наближеність до реального світу та проблем, з якими фахівець із кібербезпеки може зіткнутись під час роботи.

Кіберполігон постійно проходить тестування здобувачами освіти нашої кафедри та оновлюється відповідно до зауважень та результатів роботи користувачів. Діапазон застосування розробки є широким і враховує майбутні залучення фахівців із кібербезпеки, державних службовців, ветеранів бойових дій, а також посадових осіб органів самоврядування.

Шифрування з надійними ключами в асиметричних алгоритмах

УДК 003.26:511.41

Юлія Мисло[1], Михайло Пагіря[2]

Ужгородський національний університет,
[1]julia.mislo@uzhnu.edu.ua, [2]mykhaylo.pahirya@uzhnu.edu.ua

В сучасному інформаційному світі особливо важливою є проблема збереження конфіденційність даних, які передаються від одного абонемента до іншого. Найбільш важлива інформація пересилається учасниками обміну у зашифрованому вигляді. Для шифрування використовуються алгоритми як із симетричними, так із асиметричними ключами. Кожен класів алгоритмів має свої переваги та недоліки, а також сферу свого використання. В останні десятиліття широкої популярності набули алгоритми із асиметричним ключем, оскільки вони ґрунтуються на важко розв'язувані математичні задачі зокрема на задачі факторизації великих чисел. На криптосистеми із асиметричним ключем донині покладається велика надія.

З іншого боку, бурхливий розвиток інформаційних технологій безпосередньо пов'язаний із зростанням потужностей сучасних комп'ютерів. Це дозволяє проводити так звані лобові атаки на нових підкласах важко розв'язуваних задач. Щоб убезпечити себе від подібних несподіванок, доводиться проводити додатковий аналіз алгоритмів, які використовуються.

Ланцюгові дроби використовують при розв'язанні задач з різних розділів сучасної математики та її застосувань. В задачах теорії чисел, наприклад, ланцюгові дроби утворюють підґрунтя для аналізу надійності шифрів з асиметричними ключами.

Відомо [1,2], що при використанні одного із найбільш вживаних алгоритмів з асиметричним ключем --- алгоритму RSA, функція шифрування визначається наступним чином $E(x)=x^e \pmod n$, де модуль n рівний добутку двох великих простих чисел p та q, $n=pq$, які утворюють таємну частину ключа. Варто зауважити, що задача факторизації числа n належить до складних, важко розв'язуваних задач теорії чисел і перевершує за складністю задачу про перевірку числа на простоту. З іншого боку, і секретний ключ d в функції дешифрування $D(c)=c^d \pmod n$ знайти не легше, якщо залишається невідоме значення функції Ойлера $\varphi(n)=(p-1)(q-1)$.

Щоб виконати факторизацію числа n використовують метод пробних ділень, який вимагає $O(n^{1/2})$ двійкових операцій, ***ρ-метод Полларда,*** який здатний знайти один із співмножників після виконання $O(n^{1/4}(\log n)^3)$ двійкових операцій, ***метод Ферма***, який особливо ефективний у випадку, коли співмножники близькі, метод факторних баз, що вимагає виконання $O(\exp(C(r \log r)^{1/2}))$ двійкових операцій. На метод факторних баз спирається спосіб відшукання співмножників числа за допомогою розвинення числа в ланцюговий дріб, який ґрунтується на теоремі Лагранжа.

Метод дослідження стійкості алгоритмів з асиметричними ключами, який використовує результати з теорії ланцюгових дробів на прикладі алгоритму RSA розглянуто в роботі [3]. Якщо зроблені додаткові припущення про складові секретної частини ключа, тобто, якщо $q < p < 2q$, $d < n^{1/4}/3$, $e < \varphi(n)$, то можна відшукати розвинення відношення складових відкритої частини ключа e/n у правильний ланцюговий дріб і один із канонічних знаменників ланцюгового дробу

буде секретним ключем ***d*** для RSA шифру. Для того, щоб здійснити реалізацію алгоритму необхідно виконати перевірку ***O(ln n)*** підхідних дробів.

Було проведено дослідження розглянутих методів факторизації таємних складових ключів [4], здійснено порівняння по часу виконання кожного із методів. Це дозволяє виробити певні рекомендації щодо вибору надійних таємних складових ключів шифрування.

1. N.Koblitz A Course in Number Theory and Cryptography. 2-nd ed. Springer Science & Business Media, 1994.
2. M. Cozzens, S. J. Miller The Mathematics of Encryption: an Elementary Introduction. American Mathematical Society. Mathematical World 29, 2013.
3. M. Wiener Cryptanalysis of short RSA secret exponents *// IEEE Transactions on Information theory* 36.3 (1990): 553-558.
4. Ю.М. Мисло, М.М. Пагіря Криптоаналіз асиметричних ключів алгоритмами ланцюгових дробів. // ITSec: Безпека інформаційних технологій: матеріали XII Міжнар. наук.-техн. конф., (м. Ужгород, 2-4 трав. 2023 р.) Київ: НАУ, 2023. С. 36.

Методологія побудови багатоконтурної системи безпеки у соціокіберфізичних системах

УДК 004.056. 5/.6/.7

Станіслав Мілевський[1], Сергій Євсеєв[2], Ірина Аксьонова[3]

Національний технічний університет «Харківський політехнічний інститут», [1]milevskiysv@gmail.com, [2]Serhii.Yevseiev@gmail.com, [3] ivaksyonova@gmail.com

Революційні зміни інфокомунікаційних та комп'ютерних мереж дозволили сформувати об'єднання в єдиний інформаційно-кібернетичний простір, систем на основі смарт-технологій, та зумовили формування соціокіберфізичних систем та перегляд об'єктів критичної інфраструктури. Як наслідок, суттєво зріс і спектр загроз для національної безпеки держави загалом. Ключовою і найбільш потенційно небезпечною є загроза зриву чи взяття під віддалений контроль процесів управління в соціокіберфізичних системах. При цьому під соціокіберфізичною системою розуміється еволюційне комплексування смарт-технологій із соціальними мережами месенджерами.

Наслідки у разі відсутності чи недосконалості механізмів забезпечення безпеки у соціокіберфізичній системі можуть мати колосальний та незворотний характер,. Вирішення всього комплексу питань, пов'язаних із забезпеченням кібербезпеки, інформаційної безпеки та безпеки інформації у соціокіберфізичній системі має вирішуватися в комплексі та нерозривно одне від одного. Просте комплексування сил і засобів у кожному окремому випадку задля забезпечення безпеки соціокіберфізичних системах (об'єктах критичної інфраструктури) є недоцільним, як із практичної, так і наукової точок зору. Відсутність інших альтернативних підходів спонукає нагальну необхідність у вирішенні проблеми, що склалася – підвищення захищеності інформації в соціокіберфізичних системах на основі нових невідомих до сьогодні підходів. Такий підхід потребує переформатування механізмів побудови систем захищеності елементів інфраструктури та потребує врахування побудови багатоконтурних систем захисту інформації на основі постквантових алгоритмів [1–5].

На рис. 1 представлено структурну схему методології побудови багатоконтурної системи захисту інформації. Основною відмінністю від відомих підходів є можливість синтезу як експертного, так і системного аналізу цільових загроз на соціокіберфізичні системи, а й можливість об'єктивної оцінки поточного стану захищеності інформації. Такий підхід дозволяє своєчасно реагувати на можливі зміни (модифікації) цільових загроз, а також враховувати їхню синергію та гібридність, можливість комплексування з методами соціальної інженерії. Пропоновані практичні рішення щодо забезпечення послуг безпеки на основі постквантових алгоритмів дозволяють забезпечити необхідний рівень стійкості конфіденційної інформації з різними рівнями їх секретності.

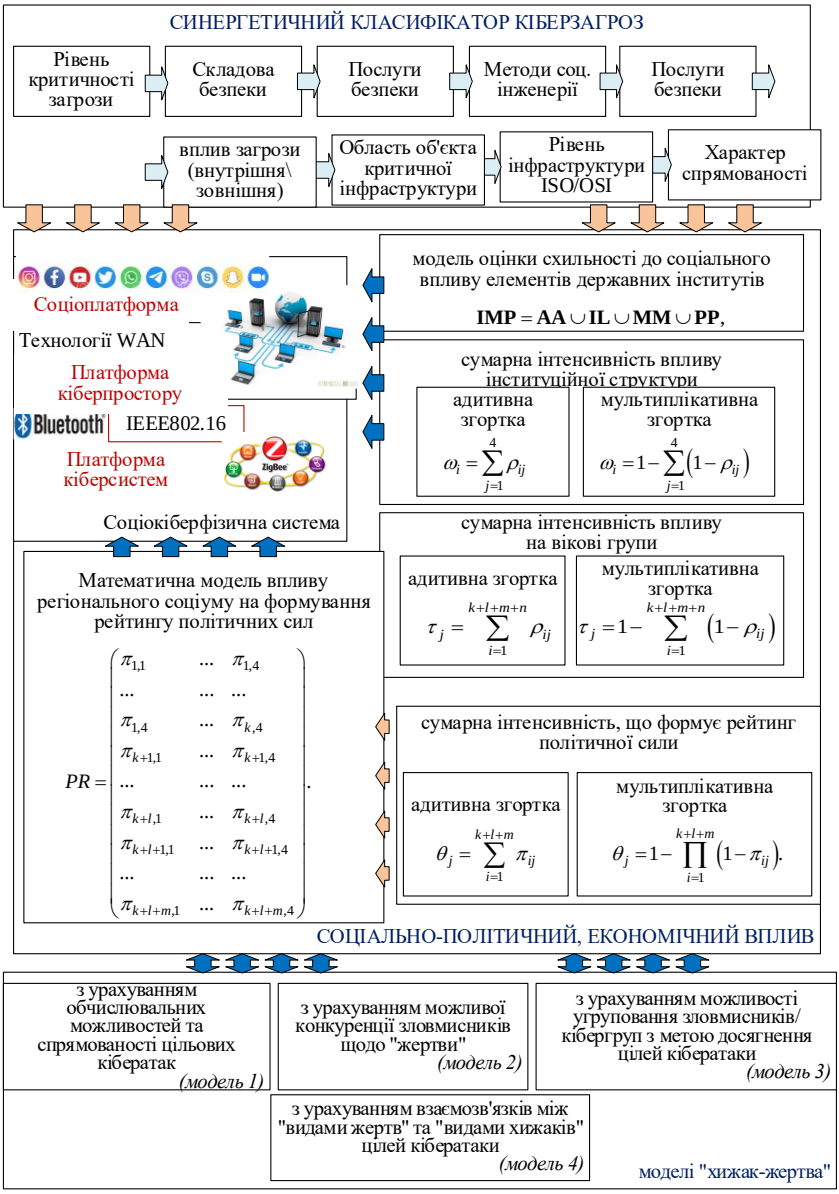


Рис.1. Структурна схема побудови системи оцінки поточного стану багатоконтурної системи захисту

Аналіз використання різних перешкодостійких кодів у крипто-кодових конструкціях та аналіз технологій побудови соціокіберфізичних систем на основі смарт-технологій показав, що використання різних кодів дозволяє диференціювати основні показники криптосистем та враховувати рівень таємності інформаційних ресурсів. Такий підхід дозволить знизити не тільки обчислювальні та ємнісні витрати, але й підвищити рівень безпеки за рахунок різних модифікацій та вибору завадостійких кодів. Даний механізм знизить можливість зламування крипто-кодових конструкцій та забезпечити необхідний рівень безпеки. Подано методологію побудови багатоконтурних систем захисту інформації, яка забезпечує об'єктивність оцінки поточного стану захищеності елементів інфраструктури соціокіберфізичних систем. Побудова багатоконтурної системи захисту на основі постквантових алгоритмів дозволить забезпечити необхідний рівень безпеки з урахуванням кількості секретності інформаційних ресурсів, їхньої циркуляції та зберігання.

1. Serhii Yevseiev, Oleksandr Milov, Nataliia Dzheniuk, Maksym Tolkachov, Tetiana Voitko, Mykhailo Prygara, Natalia Voropay, Oleksandr Shpak, Andrii Volkov, Oleksandr Lezik. Development of a multi-loop security system of information interactions in socio-cyberphysical systems. Eastern-European Journal of Enterprise Technologies. 2023. 5/9 (125). P. 53–74
2. Nataliia Dzheniuk, Serhii Yevseiev, Bogdan Lazurenko, Oleksandr Serkov, Oleg Kasilov. Methods of information systems protection. Advanced Information Systems. 2023. Vol. 7, No. 4, P.80-85
3. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
4. Khoroshko V.O., Pavlov I.M., Bobalo Y.Ya., Dudykevich V.B. and others. Design of complex information protection systems. – Lviv: Ed. Lviv Polytechnic, 2020. – 320 pp.
5. Olexander Shmatko, Serhii Herasymov, Yurii Lysetskyi, Serhii Yevseiev, Oleksandr Sievierinov, Tetiana Voitko, Andrii Zakharzhevskyi, Alexander Nesterov, Kyrylo Bondarenko. Development of the synthesis method of the automated acceptance system in the management of information security channels. Eastern-European Journal of Enterprise Technologies. 2023. 6/9 (126). P. 39–49.

Тенденція до змінювання парадигми забезпечування кібербезпеки

УДК 004[738.5::(056.53+413.4)]

Володимир Мохор[1], Олександр Бакалинський[1], Ярослав Дорогий[2,3], Василь Цуркан[1,3]

[1]ІПМЕ ім. Г.Є. Пухова НАН України, v.mokhor@gmail.com, baov@meta.ua
[2]ДонНТУ, argusyk@gmail.com
[3]КПІ ім. Ігоря Сікорського, v.v.tsurkan@gmail.com

Кіберпростір визначається як складне віртуальне середовище, що утворюється унаслідок взаємодіяння людей, програмного забезпечення і послуг у Інтернеті [1]. Дана глобальна мережа використовується людьми, суспільством, організаціями, націями для здійснювання цифрових і голосових комунікацій. Цим обумовлюється необхідність задоволення потреб в збереженості насамперед властивостей конфіденційності, цілісності, доступності інформації [1, 2]. Тож забезпечуванням кібербезпеки охоплюється діяльність зі встановлювання і підтримування безпеки в кіберпросторі.

Типово серед основних засад кібербезпеки виокремлювалося забезпечування інформаційної безпеки, безпеки програм і мереж, безпеки глобальної мережі Інтернет. Кожен зі зазначених складників направлявся на покращення корисності та функційності кіберпростору. Водночас попри існування такого підґрунтя кібербезпека тлумачилася *окремим різновидом* забезпечування збереженості властивостей конфіденційності, цілісності, доступності інформації. І, як наслідок, *не ототожнювалася* з інформаційною безпекою, безпекою програм і мереж, безпекою глобальної мережі Інтернет [1]. Тому кібербезпека характеризувалася збереженням конфіденційності, цілісності та доступності інформації у кіберпросторі. Разом з тим, нині спостерігається тенденція до змінювання даної парадигми в напрямі захищання людей, суспільства, організацій, націй від кіберризиків. Кібербезпека *включає в себе* забезпечування веббезпеки, безпеки мереж та Інтернету. Глобальною мережею утворюється середовище для обмінювання інформацією. З одного боку, цьому сприяє об'єднання через неї серверів, комп'ютерів та інших апаратних пристроїв. Тоді як з іншого – використання вебзастосунків і вебсервісів для реалізування зазначеного обміну. Тому забезпечування кібербезпеки *зводиться до* збереження конфіденційності, цілісності та доступності інформації в глобальній мережі Інтернет [2].

Отже, парадигма забезпечування кібербезпеки змінюється з огляду на включеність у неї веббезпеки, безпеки мереж та Інтернету. Вона направлена на, по-перше, збереження конфіденційності, цілісності та доступності інформації при її зберіганні в цифровій формі у комп'ютерах, сховищах і мережах. По-друге, забезпечування безпеки підключених до глобальної мережі Інтернет систем.

1. ISO/IEC 27032:2012. Information Technology. Security techniques. Guidelines for cybersecurity. [From 2012-07-16]. URL: https://www.iso.org/standard/ 44375.html (accessed on: 18.04.2024).
2. ISO/IEC 27032:2023. Cybersecurity. Guidelines for Internet security. [From 2023-06-28]. URL: https://www.iso.org/standard/76070.html (accessed on: 18.04.2024).

Проекти Європейського Союзу для безпеки Інтернету речей

УДК 004.056:004.738.5:061-1 ЄС Тетяна Мужанова[1], Віталій Тищенко[2]

Державний університет інформаційно-комунікаційних технологій,
[1]muzanovat@gmail.com, [2]tvs5vetal@gmail.com

Пристрої Інтернету речей (IoT) відіграють ключову роль у забезпеченні стійкості мереж і збереженні конфіденційності й безпеки даних. Але зростаюча тенденція до ускладнення загроз кібербезпеці викликає потребу в більш надійних структурах безпеки для пристроїв і мереж IoT.

Усвідомлюючи нагальність вирішення цієї проблеми, у 2020 році Єврокомісія представила комплексну Стратегію кібербезпеки ЄС для цифрової декади, в якій, зокрема окреслено шлях до поширення Інтернету безпечних речей. Так, Стратегія передбачає формування й дотримання вимог безпеки на внутрішньому ринку продуктів і послуг ЄС, що містять цифрові елементи, в т.ч. IoT, впровадження прозорих рішень безпеки й сертифікації, стимулювання безпечних продуктів і послуг IoT без шкоди для їх продуктивності [1].

На виконання поставлених у Стратегії завдань Єврокомісія започаткувала так званий кластер безпеки проектів IoT, спрямований на усунення недоліків пристроїв і мереж шляхом розробки безпечних і модульних інфраструктур, які можна інтегрувати в нові та існуючі рішення для сфер охорони здоров'я, догляду за людьми похилого віку, виробництва, постачання продуктів харчування, енергетики і транспорту. Цей кластер складається з 8 проектів, на реалізацію яких ЄС передбачив фінансування обсягом 40 млн. євро (приблизно 5 млн. євро кожен) [2].

На рис. 1 показано перелік цих проектів. Розглянемо детальніше призначення кожного з них.

Рис.1. Проекти ЄС щодо безпечного Інтернету речей

SecureIoT - це спільний проект компаній у сфері послуг і безпеки IoT, який на основі кількох платформ і мереж розумних об'єктів реалізує низку прогностичних служб безпеки IoT. SecureIoT має забезпечити конкретні механізми збору даних, моніторингу і прогнозних механізмів безпеки, які стануть основою для надання інтегрованих послуг з оцінки ризиків, аудиту нормативної відповідності, а також підтримки для розробників IoT.

Проект *SEMIoTICS* спрямований на розробку керованої шаблонами структури, побудованої на існуючих платформах IoT, щоб забезпечити безпечне й надійне спрацьовування й напівавтономну поведінку в додатках IoT, в т.ч. промислових.

Проект має підтримувати міжрівневу інтелектуальну динамічну адаптацію різнорідних "розумних об'єктів, мереж і хмар, розробляти й інтегрувати розумні програмовані мережі й механізми семантичної взаємодії.

DevOps ENACT є спільною ініціативою. Рух DevOps просуває використання набору інструментів розробки ПЗ, які забезпечують якість послуг і одночасно розвиток складних систем, сприяють швидким інноваціям і простоті у використанні. ENACT створив засоби підтримки платформи, давши можливість DevOps розробити надійні рішення для систем IoT з високим рівнем безпеки і стійкості в умовах їх спільного впровадження.

Проект *IoTCrawler* сфокусований на сумісності між платформами, реконфігураційних рішеннях для інтеграції даних і послуг, безпечних алгоритмах з урахуванням конфіденційності й механізмах для сканування, індексування та пошуку в системах IoT.

BRAIN-IoT зосереджується на складних сценаріях, де активація й управління спільно підтримуються групою систем IoT. Мета полягає у створенні структури й методології, що підтримує спільну "розумну" поведінку в повністю децентралізованих, комбінованих і динамічних об'єднаннях різнорідних платформ IoT.

Проект *SOFIE* вирішив проблему фрагментації IoT через об'єднання, до якого будь-яка платформа IoT може приєднатися, створивши адаптер. Проект реалізує конфіденційність, забезпечуючи наскрізну безпеку, управління ключами, авторизацію, підзвітність і можливість перевірки.

CHARIoT має на меті вдосконалення сучасних технологій IoT шляхом використання методу проектування й когнітивної обчислювальної платформи, що підтримує уніфікований підхід до конфіденційності, надійності й безпеки систем IoT, що сприяє високому рівню безпеки і цілісності промислового IoT.

У рамках проекту *SerIoT* розроблено структуру IoT на основі адаптивної "розумної" програмно-визначеної мережі із захищеними маршрутизаторами, розширеною аналітикою і зручною візуальною аналітикою, оптимізував безпеку на платформах і в мережах у цілісний, багаторівневий спосіб.

Отже, беручи до уваги ключову роль Інтернету речей у забезпеченні стійкості мереж і збереженні конфіденційності й безпеки даних, керівництво ЄС започаткувало кластер безпеки проектів IoT, спрямований на розробку безпечних і модульних інфраструктур IoT. Завдяки використанню модульного підходу з відкритим вихідним кодом, який дозволяє повторно використовувати модулі в інших рішеннях для більш широкого спектру програм, досягнуто значних успіхів у реалізації проектів кластеру.

1. The EU's Cybersecurity Strategy for the Digital Decade. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018 (дата звернення: 20.04.2024)
2. Secure solutions for the Internet of Things. URL: https://digital-strategy.ec.europa.eu/en/policies/secure-internet-things (дата звернення: 20.04.2024).

Виклики та стратегії кібербезпеки цифрових послуг для широкого застосування

УДК 004.056

Марія Навитка

Львівський державний університет безпеки життєдіяльності, m.navytka@ldubgd.edu.ua

У сучасному світі, де технології розвиваються швидкими темпами, цифрові послуги стають невід'ємною частиною нашого повсякденного життя. Від банківських операцій до управління охороною здоров'я, цифровізація послуг зробила доступнішими та зручнішими багато аспектів життя для широкого кола споживачів. Цифрові послуги для населення включають широкий спектр програм та платформ, які спрощують повсякденне життя громадян, надають доступ до важливої інформації та допомагають взаємодіяти з урядовими та комерційними організаціями.

Однак, разом з розширенням цифрових можливостей, збільшується і ризик кібератак, що ставить під загрозу конфіденційність, доступність та цілісність цих послуг. Забезпечення безпеки цифрових послуг важливе не тільки для захисту конфіденційності та даних користувачів, але й для підтримки довіри і репутації компанії серед споживачів. Безпечні цифрові послуги — це цифрові продукти та сервіси, які втілюють в собі принципи кібербезпеки для захисту даних, систем і приватності своїх користувачів. Основна мета таких послуг полягає у наданні безпеки і надійності при використанні цифрових технологій.

Управління інцидентами в галузі цифрових послуг вимагає специфічного підходу, що враховує широкий спектр потенційних загроз і викликів. Розглянемо декілька ключових аспектів, на які потрібно звернути увагу при управлінні інцидентами в цій сфері.

1. Для швидкого їх виявлення використовують авангардні систем моніторингу та аналізу для раннього виявлення незвичайних активностей або потенційних загроз. Запроваджується налаштування тривог, що базуються на конкретних критеріях та індикаторах компрометації.

2. При систематизації інцидентів йде розробка чіткої системи класифікації інцидентів для визначення їх серйозності та пріоритетності реагування, та реалізація процедур оцінювання впливу на конфіденційність, цілісність та доступність даних.

3. В комунікаційних стратегіях акцентують на розробці чітких комунікаційних лініях для зв'язку з усіма зацікавленими сторонами, включаючи керівництво, користувачів та потенційних регуляторів. Інформувати користувачів і клієнтів у випадку інцидентів, що можуть вплинути на їхню приватність чи дані.

4. В реагуванні на інциденти використовувати готові плани реагування на них для мінімізації шкоди та швидкого відновлення послуг. Проводити технічний аналіз та форензики для визначення джерела інциденту та способів його усунення.

5. Впроваджувати зміни у системи та процедури для запобігання повторенню подібних інцидентів та реалізовувати стратегії відновлення для повернення до нормальної операційної діяльності.

6. Проводити детальний аналіз після завершення інциденту для виявлення слабких місць системи та можливостей для покращення. Обов'язково зберігати всі дані про інциденти для майбутнього аналізу та як вхідні дані для тренінгів і навчань.

7. Регулярно проводити навчання персоналу методам виявлення, реагування та поводження під час кіберінцидентів. Запровадити освіту користувачів та клієнтів щодо основ безпеки та важливості захисту своїх даних.

8. Задіювати підтримку юридичних радників для визначення відповідальності та вимог у випадках кіберінцидентів. Здійснювати оцінку відповідності дій компанії законодавчим та регулятивним вимогам після інциденту.

Звертаючи увагу на ці аспекти, організації зможуть більш ефективно управляти кіберінцидентами, мінімізуючи їхній вплив на бізнес та підтримуючи довіру своїх користувачів.

На сьогодні цифрові послуги стають все більш взаємопов'язаними та централізованими, важливість кібербезпеки не можна недооцінювати. Однак, за допомогою стратегічного підходу та використання комплексних рішень, ці виклики можуть бути подолані. Перш за все, розуміння специфіки загроз, з якими можуть зіткнутися підприємства, які надають цифрові послуги, є критично важливим для розробки ефективних механізмів захисту. Застосування багаторівневого захисту, постійні аудити та оновлення, шифрування даних та освіта та тренінги для співробітників повинні бути стандартною практикою.

Завершуючи, необхідно підкреслити важливість розроблення стратегій реагування на інциденти як фундаментального аспекту забезпечення цифрової безпеки. Ефективне впровадження планів відповіді на кіберзагрози, які враховують змінність кіберпейзажу, є критичним для збереження довіри користувачів та оперативної стабільності.

З огляду на це, важливо, що всі зацікавлені сторони — від розробників і урядових агентств до освітніх установ і кінцевих користувачів — зобов'язані колаборувати для підтримки більш безпечного та резилієнтного цифрового середовища, яке слугує важливим елементом соціальної стабільності та економічного прогресу.

1. Закон України від 10.08.2023 № 3321-IX, «Про цифровий контент та цифрові послуги». https://zakon.rada.gov.ua/laws/show/3321-20#Text
2. Жаворонок, А., Лопащук, І. (2024). Цифровізація соціальної сфери в контексті забезпечення економічної безпеки держави. Економічний простір, (189), 253-258. https://doi.org/10.32782/2224-6282/189-45.
3. Хаустова, М. Г. (2023). Вигоди, ризики та проблеми цифровізації суспільства: загальнотеоретичний аспект. Аналітично-порівняльне правознавство, (5), 753-759

Методи Data Science для підтримки прийняття рішень щодо прогнозування кібератак в інформаційних системах

УДК 004.853 (043.2)

Олена Негоденко[1], Віталій Негоденко[2]

Державний університет інформаційно-комунікаційних технологій,
[1]negodenkoav@gmail.com, Київський столичний університет імені Б. Грінченка
[2]v.nehodenko.asp@kubg.edu.ua

Протягом останніх десятиліть велика увага приділяється методам Data Science для вирішення проблем безпеки. Так, для виявлення вторгнень та шкідливих програм, фішинг і атаки на відмову в обслуговуванні використовують методи машинного навчання, статистичного навчання, інтелектуального аналізу даних і обробки природної мови. Крім того, кібербезпека також стає серйозною проблемою для організацій, частково через руйнівне поширення інцидентів у кібератаках, таких як витоки даних у Equifax, Verizon, Gmail та Instagram.

Інші загрози кібербезпеки, які викликають серйозне занепокоєння, включають перевантаження даних, фальшиві сповіщення, невідомі дані, обмежені ресурси та труднощі з інтеграцією та оркестровкою. Крім того, зловмисники постійно адаптуються до методів виявлення та активно прагнуть використовувати нові вразливості. Зважаючи на складність і динамічний характер кіберзагроз, автоматизація аналітики на основі даних, а саме підтримка прийняття рішень щодо прогнозування кібератак в інформаційних системах набуває важливого значення для дослідження [1].

В першу чергу кібербезпека має справу з різними типами кіберзлочинів, але важливо визначити подібність існуючих кіберзлочинів за допомогою інтелектуального аналізу даних і технологій машинного навчання. Алгоритми машинного навчання можуть допомогти навчити систему виявляти аномалії, конкретні шаблони для прогнозування кібератак. Інтелектуальний аналіз даних відіграє вирішальну роль у забезпеченні прогностичного рішення для виправлення можливих кіберзлочинів і методів дії та дослідження системи захисту від них. Методи Data Science дозволяють системі аналізувати приховані знання та навчати експертну систему сповіщенню та процесу прийняття рішень [2].

Загальний підхід для прогнозування та ефективного виявлення аномалій та кібератак в реальному часі включає комплексну систему на основі штучного інтелекту та аналітики даних.

Першим кроком є вибір відповідних моделей машинного навчання для використання в системі виявлення аномалій та передбачення кібератак. Серед яких виділяють класичні моделі, такі як метод опорних векторів (SVM), навчання з учителем (нейронні мережі), навчання без учителя (методи кластеризації), або нові моделі, які використовують глибинне навчання (Deep Autoencoder Network та інші.)

Після вибору моделей необхідно оптимізувати їх параметри для максимізації точності передбачення та мінімізації помилок. А саме налаштування гіперпараметрів моделей, таких як розмір шарів нейронної мережі, швидкість навчання (learning rate), коефіцієнти регуляризації та інші. Даний процес також включає використання методів перехресної перевірки (cross-validation) та оптимізації на основі результатів та вибір оптимальних функцій втрат.

Для ще кращої ефективності використовують ансамблеві моделі, які комбінують кілька моделей машинного навчання для зниження помилок та підвищення стійкості передбачення Рис.1.

Ансамблеві моделі	**Bagging (Bootstrap Aggregating)**
	Random Forest
	Boosting
	Stacking (Stacked Generalization)
	Градієнтний бустинг (Gradient Boosting)

Рис.1 Ансамблеві моделі машинного навчання для зниження помилок та підвищення стійкості прогнозування

Багато даних у сфері кібербезпеки можуть бути незбалансованими, з великою кількістю зразків нормальної поведінки та обмеженою кількістю зразків аномальної поведінки. Для ефективного використання моделей машинного навчання необхідно враховувати незбалансування та використовувати відповідні техніки обробки даних (Undersampling, Oversampling, SMOTE, Weighting, ансамблі методи та використання F1-метрик та матриці помилок).

Після розробки моделей важливо провести оцінку їх ефективності та якості прогнозування, що реалізується через розрахунок метрик якості, таких як точність, чутливість, специфічність, F1-оцінка, а також перехресна перевірка стійкості моделей та уникнення перенавчання [3].

Оскільки кіберзагрози постійно еволюціонують, тому важливо надавати системі можливість навчатися на нових даних та вдосконалювати моделі з часом. Тому важливо включати автоматизований процес оновлення моделей на основі нової інформації про загрози.

1. Abomhara M, Geir M. Køien. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. J Cyber Secur Mob.– 2015 – V. 4(1). – P. 65 – 88.
2. Chayal, N.M., Patel, N.P. Review of Machine Learning and Data Mining Methods to Predict Different Cyberattacks. Data Science and Intelligent Applications. Lecture Notes on Data Engineering and Communications Technologies, 2021. 305 p.
3. J. Song, H. Takakura, Y. Okabe and K. Nakao, “Toward a more practical unsupervised anomaly detection system”, Information Sciences, vol. 231, (2013), p. 4-14.

Дослідження методів апроксимації неявно заданих кривих в комп'ютерній графіці

УДК 621.395.7 (043.2)

Михайло Олексин[1], Петро Венгерський[2]

Львівський національний університет імені І. Франка,
[1]mykhailo.oleksyn@lnu.edu.ua, [2]petro.venherskyy@lnu.edu.ua

Електронні пристрої з графічними дисплеями вже давно стали підручними засобами чи не для кожного, а тому звідусіль оточують нас в повсякденному житті. А відтак точне та ефективне відображення неявно заданих кривих є одним з важливих елементів комп'ютерної графіки.

У питанні ефективного розбиття площини для апроксимації неявно заданих кривих непогано себе зарекомендував метод інтервального аналізу. У поєднанні з критерієм глобальної параметризації [1] він дає непогані результати пошуку коренів рівняння та побудови множини інтервалів, в межах яких знаходиться крива, що описується функцією.

Для пошуку інтервалів перетину функцією глобально параметризованих областей оригінально використовується метод Ньютона:

$$X_{n+1} = \left(x_n - \frac{f(x_n)}{f'(X_n)}\right) \bigcap X_n \,, x_n \epsilon X_n$$

В даній роботі пропонується натомість використати метод типу Рунге [2]:

$$X_{n+1} = \left(x_n - \frac{f(x_n)}{\frac{1}{4}f'(x_n) + \frac{3}{4}f'(x_n + \frac{2}{3}(X_n - x_n))}\right) \bigcap X_n \,, x_n \epsilon X_n$$

та порівняти кількість ітерацій та час виконання обох алгоритмів.

Наведемо псевдокод методу, що шукає корені рівняння тим, чи іншим з вище перерахованих методів:

```
For index from 0 to max_iterations-1
    m = midpoint(current_interval)
    Increment global iterations counter
    Compute next_interval:
      next_runge_interval = (1/4)*df(m) + (3/4)*i_df(m + (2/3)*(current_interval -
m))
      next_newton_interval = i_df(current_interval)
    Compute next_interval:
      next_interval = m - (f(m) / next_interval)
    Update current_interval:
      current_interval = intersection of next_interval and current_interval
    If current_interval exists and width(current_interval) is less than tolerance
      Break loop
    If current_interval exists and has more than one subinterval
      Recursively apply interval_method on each subinterval
      Collect results in intervals
      If intervals are empty, return None
      Return intervals
    Return None
```

Для проведення обрахунків було вибрано наступну неявно задану криву:

$$x^2 + y^2 + \cos(2\pi x) + \sin(2\pi y) + \sin(2\pi x^2)\cos(2\pi y^2) = 1$$

Інтервал, на якому проводилися розрахунки – [-5.1, 5.1] для обох координат. Для більшої точності порівняльних характеристик задану криву було побудовано 5000 разів для кожного методу.

На рисунку 1 продемонстровано графік кількості ітерацій для обох методів.

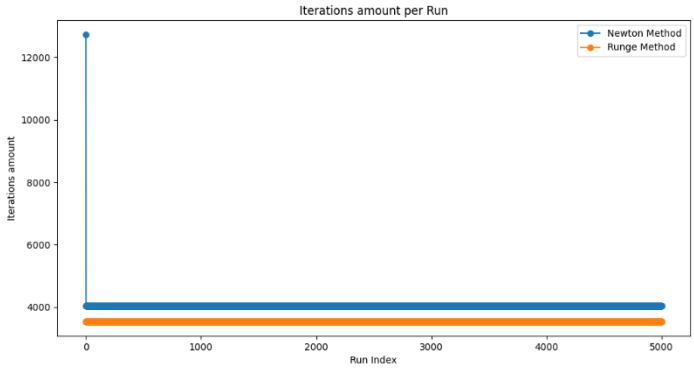


Рис.1. Кількість ітерацій для кожного методу

На рисунку 2 продемонстровано мінімальний, максимальний та середній час виконання програми для обох методів.

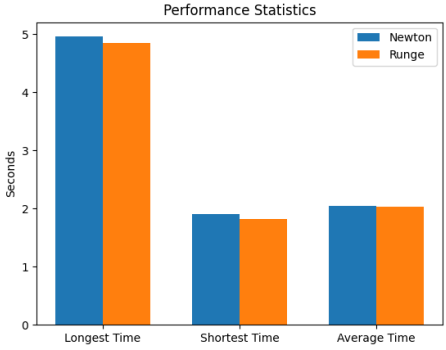


Рис.1. Час виконання для кожного методу

1. John M. Snyder, “Interval analysis for computer graphics”. Computer Graphics, 26(2):121-130, 1992.
2. Сеньо П.С., Венгерський П.С., Вирішення систем нелінійних рівнянь за допомогою модифікованого методу типу Рунге, *Інтервальні обчислення*.4(6):59-65, 1992

Поширення радіохвиль та його особливості як методика подолання природніх перешкод для телекомунікаційних сиситем

УДК 621.395.7 (043.2)

Володимир Пархоменко[1], Андрій Щепак[2], В'ячеслав Пархоменко[3]

Державний університет інформаційно-комунікаційних технологій,
[1]k27pine@gmail.com, [2]k27pine@gmail.com, [3]k27pine@gmail.com

Стабільний зв'язок в сучасних телекомунікаційних системах має надзвичайну важливість з різних точок зору. По-перше, стабільний зв'язок забезпечує безперервну та надійну комунікацію між людьми, компаніями та пристроями. Він гарантує, що інформація може бути передана швидко та ефективно, що особливо важливо в сферах екстрених ситуацій, медичних послуг, фінансів та багатьох інших галузях, де навіть найменша перерва в зв'язку може мати серйозні наслідки [1].

По-друге, стабільний зв'язок є основою для розвитку інновацій та нових технологій. Багато інноваційних рішень та послуг, таких як Інтернет речей (IoT), хмарні технології, віртуальна реальність та інші, базуються на здатності пристроїв до постійного та стабільного зв'язку між собою та інтернетом.

По-третє, стабільний зв'язок впливає на ефективність бізнесу та економічний розвиток. Він дозволяє компаніям збільшувати продуктивність, зменшувати час, необхідний для обробки даних та прийняття рішень, а також сприяє зменшенню витрат та підвищенню якості послуг.

Отже, стабільний зв'язок є невід'ємною складовою сучасних телекомунікаційних систем, який забезпечує безперервну та ефективну комунікацію, сприяє розвитку нових технологій та інновацій, а також впливає на ефективність та конкурентоспроможність різних галузей економіки.

Частота коливань електромагнітних хвиль грає важливу роль у визначенні їх фізичних властивостей. Це відноситься до таких аспектів, як довжина хвилі, проникнення в речовину, ефекти розсіювання та відбивання, а також ефективність зв'язку.

Низька частота коливань відповідає довшим довжинам хвиль, тоді як висока частота - коротшим. Це впливає на здатність хвиль проникати в різні матеріали. Низькі частоти мають кращу здатність проникнення через перешкоди, тоді як високі можуть бути поглинуті або розсіяні на поверхні об'єктів. Частота також впливає на ефекти розсіювання та відбивання. Висока частота може призводити до більшої розсіювання, тоді як низька - до відбивання. Це може мати важливе значення для забезпечення стійкості зв'язку та якості передачі даних.

У телекомунікаційних системах різні частоти можуть мати різний ефект на ефективність зв'язку, залежно від умов та потреб. Розуміння цих властивостей допомагає оптимізувати телекомунікаційні системи та забезпечувати стабільний та надійний зв'язок.

Важлива формула, яка використовується для опису енергії (E) електромагнітної хвилі, залежить від її частоти:\

E = h * f

де:

h - стала Планка

f - частота хвилі у герцах (Гц).

Ця формула показує, що енергія електромагнітної хвилі пропорційна її частоті. Чим вища частота хвилі, тим більше її енергія. Наприклад, рентгенівське випромінювання має високі частоти, що робить його дуже енергетично зарядженим і придатним для використання в медичних обстеженнях, де потрібна велика проникність та роздільна здатність.

Частота сигналу впливає на огибання навколо Землі через довжину хвилі та геометрію планети. Сигнали з низькою частотою, які мають довгі хвилі, зазвичай мають кращу здатність огинати поверхню Землі. Такі сигнали можуть легше подолати перешкоди, такі як гори або будівлі, та досягати далеких областей.

Стає очевидним, що високочастотні сигнали рухаються у прямій лінії, зазвичай без огибання. Тому вони мають меншу здатність проникнення через перешкоди та меншу зону покриття. Геометрія Землі також грає важливу роль. На пласких поверхнях сигнали можуть огинати на менших відстанях, ніж у гірських районах, де земля може бути більш кривою. Отже, розуміння впливу частоти сигналу на огибання навколо Землі важливе для планування та оптимізації телекомунікаційних систем передачі інформації.

У ході даної роботи було виявлено, що частота сигналу має значний вплив на його фізичні властивості, зокрема, на здатність сигналу огинати поверхню Землі. Високочастотні сигнали рухаються у прямій лінії та мають обмежену здатність проникнення через перешкоди, тоді як низькочастотні сигнали мають кращу здатність огибати Землю та подолати перешкоди.

Врахування цього фактору має ключове значення при проектуванні та оптимізації телекомунікаційних систем. Розуміння впливу частоти сигналу на його розповсюдження дозволяє розробникам ефективно вирішувати проблеми зв'язку, забезпечуючи стабільний та надійний зв'язок навіть у складних географічних умовах. Такий підхід допомагає підвищити ефективність телекомунікаційних систем бездротової передачі інформаціх та забезпечити їх найкращу працездатність у різних умовах експлуатації.

1. Shchepak A., Parkhomenko V., Parkhomenko V. Developing solution for using artificial intelligence to obtain more accurate results of the basic parameters of radiosignal propagation // Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie S′rodowiska. 2021 11(1). P. 36–39. URL: https://doi.org/10.35784/iapgos.2577

Антена протидії роботі радіомережі в діапазоні 2,4 ГГц

УДК 004.3.01(043.2)

Юрій Пепа[1], Володимир Бичков[2]

Державний університет інформаційно-комунікаційних технологій,
[1]yurka14@gmail.com, [2]5954440@gmail.com

Досить часто виникає необхідність заблокувати роботу бездротових систем зв'язку та передачі даних, щоб зменшити або унеможливити витік інформації через радіоканал. Повсякденне застосування мобільних гаджетів та бездротових систем відеоспостереження стандарту 802.11 [1] створює саме таку небезпеку. Для оперативного блокування цього каналу витоку інформації досить часто використовують пасивні та активні засоби протидії [2]. Перші – не завжди бувають ефективними, а другі – виконують свою задачу досить добре.

Пропонується розглянути ефективну мікросмужкову однокільцеву антену (рис. 1), яку можна застосувати для протидії роботі радіомереж в діапазоні 2,4 ГГц.

Рис. 1. Однокільцева антена та схема її підключення

При роботі кільцевого елементу такої антени необхідно утворити в її плечах режим біжучої хвилі струму. Для цього застосуємо узгоджувальні фазообертальні пристрої (рис. 1). Антена живиться несиметричною смужковою лінією від генератора радіозавад.

Для дослідження роботи такої антени та її характеристик необхідно змоделювати кільцеву антену з біжучою хвилею. Для цього застосуємо програмний пакет FEKO [3].

Модель друкованої антени, радіусом 1,7 см, була досліджена для частот 2,2-2,7 ГГц. В якості підкладки вибрано діелектрик з товщиною 0,25 см і з відносною діелектричною проникністю 4,4. Тангенс кута діелектричних втрат склав 0,017.

На рис. 2 та рис. 3 представлені основні характеристики роботи кільцевої антени: залежність коефіцієнту підсилення мікросмужкової кільцевої антени від частоти та залежність коефіцієнту стоячої хвилі за напругою мікросмужкової кільцевої антени від частоти .

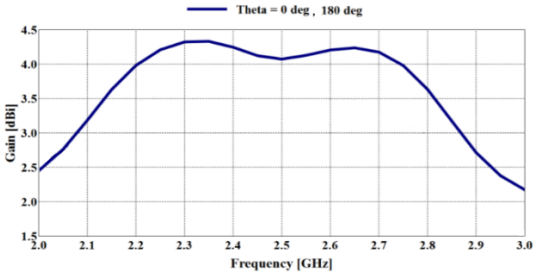


Рис. 2. Залежність коефіцієнту підсилення мікросмужкової кільцевої антени від частоти

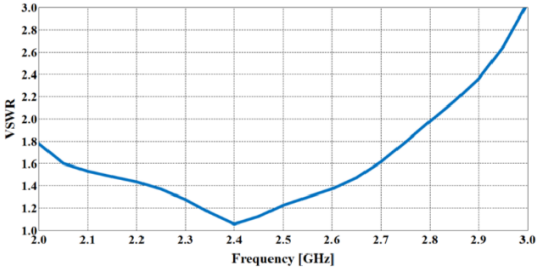


Рис. 3. Залежність коефіцієнту стоячої хвилі за напругою мікросмужкової кільцевої антени від частоти

Моделювання показало досить гарне узгодження такої антени з фідерною лінією живлення в 50 Ом, коефіцієнт стоячої хвилі в смузі робочих частот не перевищує значення 1,1 (рис. 3). Ширина діаграми спрямованості за половинною потужністю випромінювання складає 81 град. З рис. 2 видно, що антена досить добре працює в діапазоні 2,2-2,7 ГГц з коефіцієнтом підсилення близько 4,5 дБі.

Таким чином, можна зробити висновки, що така антена буде ефективно виконувати свої функції перекриваючі діапазон 2,4 ГГц в обидві сторони з запасом, а коефіцієнт підсилення антени дасть додатковий приріст за ефективною потужністю в процесі протидії роботі радіопристроям стандарту 802.11.

1. Михалевський Д.В. Дослідження розподілу потужності сигналу в умовах багатопроменевого поширення хвиль для стандарту 802.11 // Збірник наукових праць Sword, 2017. – Вип. 47. – Т.1. – С.30-34.
2. Богдан В.П. Блокування засобів стільникового зв’язку та бездротового доступу // Сучасна спеціальна техніка, 2013. – №1(32). – С.100-107.
3. FECO Suite 7.0. – Режим доступу до ресурсу: https://www.rfglobalnet.com/doc/feko-suite-0001 (дата звернення: 11.03.2024).

Аналіз кібератак на елементи інфраструктури об’єктів смарт технологій

УДК 004.056.5

Дмитро Печериця

Національний Технічний Університет “Харківський Політехнічний Інститут”, dmytro.pecherytsia@cs.khpi.edu.ua

Анотація. Розглядається інфрастуктура підприємства з різноманітними мережевим технологіями та кібератаки на таку інфрастуруктуру. Виділені найбільш поширені види атак та відповідні вектори атак. Об'єктом дослідження є аналіз існуючих типів атак на об’єкти смарт технологій, об’єкти внутрішньої та зовнішньої інфраструктури. Метою дослідження є виявлення найбільш вразливих місць, та формування деяких загальних рекомендацій та підходів що до безпеки інфраструктури.

Зростання важливості захисту в кіберпросторі відбувається паралельно із швидким прогресом у галузі інформаційних технологій та злиттям інформаційних систем у різних областях діяльності. Водночас, існує високий інтерес з боку третіх осіб порушити захист периметру інфраструктури корпоративних смарт мереж, що містять цінну та конфіденційну інформацію, складні технологічні процеси, мотивований політичними або економічними причинами.

Для оцінки кібератак розглянемо інфраструктуру невеликого підприємства з різноманітними мережевим технологіями, а саме інфраструктуру з підключенням до мережі Internet з доступом працівників до внутрішніх сервісів завдяки VPN. Допустимо, що на підприємстві використовуються наступні смарт технології з підключенням до локальної мережі: система відео спостереження, система доступу до приміщень завдяки безконтактним перепусткам та система «розумний дім», яка керує вентиляцією, освітленням, опалюванням, та ліфтами. На підприємстві існує багато приладів IoT, таких як датчики чистоти повітря, температури, електронні замки, камери спостереження, блоки управління вентиляцією, освітленням, опалюванням, ліфтами то що. Усі пристрої IoT під’єднані до своїх контролерів завдяки дротовому та бездротовому з’єднанню (WiFi).

Атаки на будь яку інфраструктуру можливо поділити на 2 типи: зовнішні та внутрішні атаки. 90% успішних атак проводиться із середини, коли зловмисники отримують управління пристроєм який знаходиться у середині, а підприємство не приділяє достатньо уваги внутрішній безпеці[1].

Отримати (перемкнути) управління пристроями усереднені можливо завдяки наступним видам атак:

1. Використання шкідливих застосунків (Malware). Використання шкідливих застосунків для зараження комп’ютерів користувачів та смарт пристроїв для отримання керування пристроєм та здійснення подальших атак на інші вузли інфраструктури підприємства.
2. Між мережеві атаки (Interception) Цей вид атаки здійснюється завдяки перехопленню мережевого трафіку та його аналізу. Завдяки таким атакам можливо отримати облікові данні користувачів і подальший контроль над пристроями, до яких ці данні відносяться. Найуразливішими для цієї атаки є бездротові з’єднання.

3. Fishing

Ці атаки використовують підробні сайти, роблять електронні розсилки з посиланнями на ці сайти для отримання облікових та персональних даних та відомостей користувачів для подальшого використання в отриманні доступу до різноманітних систем.

Після отримання управління над пристроєм всередині мережі можливі наступні вектори атаки[2]:

1. Атаки на системи управління пристроями, використовуючи вже заздалегідь відомі вразливості, чи атаки з пошуком вразливості в Web застосунку системи управління (це SQL Injection, XSS, підробка CSRF).
2. Атака на мережеві пристрої з метою отримати контроль над пристроями та змінити його конфігурацію, а також отримати прямий доступ до необхідного ресурсу мережі.

Якщо мета це вивести з ладу пристрої на деякий час, можливо використання DDoS атак. Також цей тип атаки зловмисники можуть використовувати як прикриття інших атак. Наприклад, при масованій зовнішній DDoS атаці можна не звертати увагу на камери спостереження. Таким чином прикривають основні атаки.

Можна побачити, що мета більшості атак є отримання контролю над пристроями в середні інфраструктури підприємства.

Таким чином, моєна зробити висновки, що захищати необхідно не тільки зовнішній контур, а і всю внутрішню мережу, а також кожен пристрій окремо. Що стосується каналів передачі даних, то найбільш вразливішими є бездротові канали. Для гарного захисту підприємства потрібно аналізувати весь наявний трафік на сигнатури атак, так як атака може бути спрямована на будь який пристрій інфраструктури.

1. Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O., Korol, O., Milevskyi, S. et. al.; Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O. (Eds.) (2023). Models of socio-cyber-physical systems security. Kharkiv: PC TECHNOLOGY CENTER, 184. doi: http://doi.org/10.15587/978-617-7319-72-5.
2. Yevseiev, S., Tolkachov, M., Shetty, D., Khvostenko, V., Strelnikova, A., Milevskyi, S., & Golovashych, S. (2023). The concept of building security of the network with elements of the semiotic approach. ScienceRise, (1), 24-34. https://doi.org/10.21303/2313-8416.2023.002828.

Кібербезпека системи "Connected Car"

УДК 004.4:056.57

Підлісний Ю.І.

Національний університет «Чернігівська політехніка», ypodlesny@ukr.net

Сучасні електромобілі, згідно концепції "Підключений автомобіль" (Connected Car), стали частиною всесвіту "Інтернету речей" (Internet of Things, IoT), що відкриває нові можливості для покращення безпеки, комфорту, ефективності та розваг пасажирів. Більш того, з року в рік вони стають все більш автоматизованими і здатними приймати самостійні рішення в процесі їх експлуатації.

Виробники не приховують, що розумні датчики вже зараз збирають і передають інформацію про поточне GPS положення автомобіля, про стиль водіння власника, діагностичну інформацію тощо. Крім того, у виробника є можливість для віддаленого підключення авто з метою повної діагностики та оновлення програмного забезпечення, тобто, по суті, є доступ практично до всіх функцій електромобіля. Власник також має віддалений доступ до свого авто через спеціальне програмне мобільне забезпечення.

Недостатня захищеність подібних даних може призвести до потенційних ризиків. Наприклад, отримання можливості несанкційно дистанційно керувати системами автомобіля, що може привести, у залежності від цілей зловмисника, до загроз життю і здоров'ю водія та оточуючих його людей.

У зв’язку з цим існує актуальна проблема забезпечення відповідного рівня кібербезпеки сучасних електромобілів (як окремої одиниці, так й їх сукупності, що незалежно переміщуються по дорогах), тому що ще немає єдиного стандарту безпеки передавання даних від розумних датчиків електромобіля, їх шифрування та забезпечення захисту від вірогідного втручення у систему злочинців.

Основною метою дослідження був аналіз потенційних загроз та вразливостей "Connected Car" та оцінка їх впливу на стан кібербезпеки усієї системи та її складових. Це дозволило нам дослідити різноманітні потенційні загрози, зокрема атаки з використанням вразливостей пристроїв IoT, зловживання з боку користувачів і виробників, витік конфіденційної інформації тощо та у подальшому розробити та впровадити механізми контролю передачі і захисту данних, з якими оперує система.

При проведені дослідження аналізувалися наступні потенційні загрози кібербезпеці системи "Connected Car":

1) *Можливості злому систем керування автомобілем (CAN-шиною)*. CAN-шина (Controller Area Network) використовується для зв'язку між різними компонентами електромобіля, такими як двигун, гальмівні системи, системи безпеки та розваг. Злом цих систем може призвести до віддаленого контролю над автомобілем, включно з управлінням його рухом і безпекою.

2) *Виявлення вразливостей у мобільних додатках*. Багато виробників електромобілів надають мобільні додатки для управління та моніторингу автомобілем. Уразливості в цих додатках можуть дозволити зловмисникам отримати доступ до особистої інформації власників, керувати функціями автомобіля та відстежувати його місце розташування.

3) *Аналіз можливих атак на системи навігації та розваг*. Сучасні електромобілі зазвичай оснащені системами розваг і навігації, які можуть бути схильні до атак. Зловмисники можуть використовувати вразливості в цих системах для злому і отримання доступу до інших компонентів автомобіля.

4) *Забезпечення неможливості підробки оновлень ПЗ.* Виробники електромобілів регулярно випускають оновлення програмного забезпечення (ПЗ), щоб усувати вразливості та покращувати функціональність. Однак зловмисники можуть підробляти ці оновлення, щоб впровадити шкідливе ПЗ на електромобіль або зламати його системи.

5) *Захист та безпека даних, що знаходиться у системі*. Електромобілі збирають велику кількість даних про водіння, маршрути, звички користувачів тощо. Ці дані можуть бути вкрадені або скомпрометовані, якщо системи зберігання та передачі даних не захищені належним чином.

6) *Можлива наявність спеціальних закладних функцій від виробника*, які дозволяють їм здійснювати незадекларований прихований контроль через системи IoT, що може становити певну проблему з точки зору приватності та безпеки користувачів. Наприклад, виробники можуть включити в автомобілі функції, які дозволяють збирати та передавати різноманітні дані про автомобіль, його водія та пасажирів на центральний сервер без повідомлення або згоди власника автомобіля.

Проведені дослідження дозволили розробити превентивні стратегії забезпечення безпеки у системі "Connected Car".

Для вирішення виявлених потенційних загроз запропоновано застосувати такі заходи захисту, як шифрування даних, аутентифікація, мережеві фільтри та системи виявлення вторгнень для захисту пристроїв IoT та мереж, що їх обслуговують, тощо. Також представляє інтерес у застосуванні штучного інтелекту для аналізу відео і аудіо інформації, яка передається з камер відеоспостереження та інших пристроїв електромобілю без дозволу власника.

1. Songqing Chen, Chen Song, Jin-Hee Cho, Kewei Sha "Cybersecurity for Electric Vehicles: Vulnerabilities, Threats, Intrusions, and Mitigations" – 17th International Conference, WASA 2022, Dalian, China (November 24–26, 2022), Proceedings, Part II. – pp. 4-10.
2. Houbing Song, Glenn A. Fink, Sabina Jeschke "Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications" – NY: Wiley-IEEE Press, 2017 – 472 p.
3. Craig Smith "The car hacker's handbook: a guide for the penetration tester" (1st edition, March 1, 2016) – NY: No Starch Press, 2016 – 304 p.

Виявлення безпекових аномалій інформаційно-комунікаційних мереж за допомогою моніторингових систем

УДК 004.77

Василь Пограничний[1], Сергій Заблоцький [2], Мар'ян Кирик[3]

Національний університет "Львівська політехніка",
[1]vasyl.y.pohranychnyi@lpnu.ua, [2]serhii.o.zablotskyi@lpnu.ua,
[3]marian.i.kyryk@lpnu.ua

У наш час безпека інформаційно-комунікаційних мереж є одним з найбільш критичних аспектів функціонування організацій та установ, для яких важлива безвідмовна робота сервісів для забезпечення їхніх потреб. Відповідно, з кожним днем з'являються новітні загрози та збільшується кількість атак, з підвищенням продуктивності обладнання, які ставлять під ризик успішну роботу мережевих систем. Таким чином моніторинг мережі стає невід'ємною складовою стратегії безпеки.

Різноманітність кіберзагроз та їх постійні модифікації і вдосконалення не завжди дають змогу вчасно відрізнити корисне навантаження від шкідливого та в короткі терміни ліквідувати загрозу.

Аномальна поведінка в інформаційно-комунікаційних мережах часто може слугувати ознакою шкідливої діяльності, що відбувається в мережі або може вказувати на проблеми з її функціонуванням. Як приклад це може бути різке відхилення значень моніторингових метрик від типових значень за минулий період часу [1].

Метою даної роботи є покращення безпеки інформаційно-комунікаційних мереж за рахунок використання моніторингових систем шляхом виявлення безпекових аномалій, розгляд методів їх виявлення та прикладів застосування.

Для виявлення аномалій застосовується такий метод, який найбільш гнучко підходить для певного сегменту мережі і вирішується для застосування системним адміністратором. Серед основних методів можна відмітити:

- Розпізнавання вторгнень (IDS) – це метод активного моніторингу та пошуку зразків, що вказують на можливі атаки або підозрілу поведінку.
- Аналіз поведінки мережі (NBA) – це метод аналізу нормальної поведінки мережі, який виявляє аномалії шляхом порівняння відхилень від звичайних патернів.
- Аналіз вимірювань (MA) – метод аналізу метрик мережі таких як пропускна здатність, кількість пакетів, затримка, використання ресурсів та інші параметри котрі можуть показувати не звичні значення.
- Інтелектуальна аналітика безпеки (SIEM) – метод об'єднання даних з різних джерел, для прикладу системи логування, мережевих пристроїв та інших безпекових інструментів щоб виявити кіберзагрози або інші аномалії [2].

Дослідження було проведено методами аналізу поведінки мережі та аналізом вимірювання оскільки, як показує практика, вони найбільш гнучко підходять для застосування у моніторингових системах інформаційно-комунікаційних мереж.

На зображеннях нижче продемонстровано виявлення аномальної поведінки в мережі методами аналізу поведінки та аналізу вимірювань застосованих в системі

моніторингу Prometheus з інструментом відображення Grafana та системи детектування шкідливого трафіку Maltrail [3].

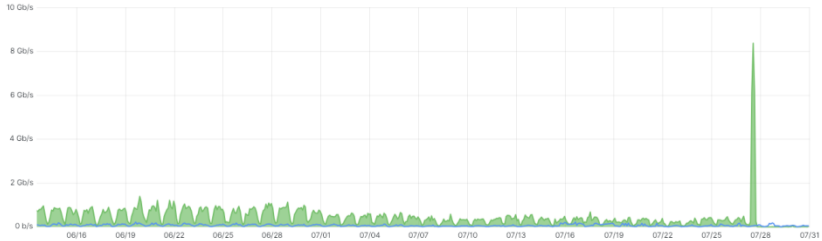


Рис.1. Аналіз вимірювань (MA)

На рисунку 1 можна спостерігати виявлення аномальної поведінки в мережі – різке підвищення величини трафіку, яке значною мірою відрізняється від типового навантаження мережі за попередній період.

dst_ip	dst_port	proto	type	trail	info
51.83.171.208	5655	TCP	IPORT	51.83.171.208:5655 ovh	rmsrat (malware)
51.83.171.223	5655	TCP	IPORT	51.83.171.223:5655 ovh	rmsrat (malware)
51.83.171.223	5655	TCP	IPORT	51.83.171.223:5655 ovh	rmsrat (malware)
51.83.171.223	5655	TCP	IPORT	51.83.171.223:5655 ovh	rmsrat (malware)
51.83.171.223	5655	TCP	IPORT	51.83.171.223:5655 ovh	rmsrat (malware)
51.83.171.223	5655	TCP	IPORT	51.83.171.223:5655 ovh	rmsrat (malware)
51.83.171.208	5655	TCP	IPORT	51.83.171.208:5655 ovh	rmsrat (malware)
51.83.171.223	5655	TCP	IPORT	51.83.171.223:5655 ovh	rmsrat (malware)

Рис.2. Аналіз поведінки мережі (NBA)

На рисунку 2 зображено аномальну поведінку з’єднання яка зафіксована системою Maltrail на реагування по патернам. IP адреса, на яку спрацювала система, належить до переліку не надійних і додана в списки заборонених адрес, на основі яких працюють патерни.

Таким чином, в результаті проведених досліджень, встановлена можливість покращення безпеки інформаційно-комунікаційних мереж шляхом використання методів аналізу вимірювань та аналізу поведінки мережі в системах моніторингу. Варто зауважити недоліки методу NBA - для більш ефективного виявлення аномальної поведінки важлива постійна актуалізація патернів. Оскільки застарілі значення патернів можуть давати хибні результати та ідентифікувати помилки мережі як шкідливий трафік.

1. C. Sanders, J. Smith, “Applied Network Security Monitoring: Collection, Detection, and Analysis”, Waltham, MA, USA 2014.
2. S. Neupane, J. Ables, W. Anderson, S. Mittal, “Explainable Intrusion Detection Systems (X-IDS): A Survey of Current Methods, Challenges, and Opportunities”, IEEE Access 10(7):112392-112415 October 2022.
3. ”Stamparm/maltrail” URL: https://github.com/stamparm/maltrail (дата звернення 14.03.2024)

Актуальні клептографічні загрози та потенційні методи протидії

УДК 004.4:056.57

Олександр Полевод

Національний університет «Чернігівська політехніка»,
oleksandr.polevod23@gmail.com

Клептографія – це наука про безпечне та приховане викрадення інформації. Термін був введений Адамом Янгом і Моті Юнгом у 1996 році. На відміну від традиційних методів крадіжки інформації, які можуть залишити сліди або попередити жертву, клептографія прагне викрасти дані непомітно, не порушуючи цілісність системи та не розкриваючи себе. Досягається це за допомогою складних математичних алгоритмів та хитрих прийомів, які впроваджуються в програмне забезпечення або апаратне забезпечення.

Метою цього дослідження є розкриття клептографії у аспектах, ширших за криптографічні алгоритми, де вона була визначена початково. Актуальність обраної теми дослідження визначається все частішими новинами зі сфери захисту інформації про скомпрометоване різноманітними закладками програмне та апаратне забезпечення. Наукова новизна полягає у відході від криптографічної основи при розгляді клептографії.

Клептографія знаходить застосування у різноманітних сферах інформаційної діяльності, де необхідно отримати доступ до конфіденційних даних без відома власників. Ось декілька прикладів:

1. Промислове шпигунство: Вбудовування прихованих каналів у програмне забезпечення промислових систем для викрадення винаходів, комерційних таємниць або даних про дослідження та розробки. Також використання стеганографії для приховування викраденої інформації в зображеннях, аудіо- або відеофайлах і впровадження апаратних закладок у мережеве обладнання для перехоплення даних, що передаються між компаніями; 2. Кіберзлочинність: Крадіжка фінансової інформації з платіжних систем або онлайн-банків шляхом імплементації бекдорів у програмне та апаратне забезпечення. Викрадення особистих даних з веб-сайтів або баз даних та використання компрометуючої інформації, отриманої через приховані канали, у зловмисних цілях; 3. Безпека держави: Впровадження програмного забезпечення для моніторингу на комп'ютери або мобільні пристрої для збору необхідних даних, розшифровка зашифрованих комунікацій за допомогою потужних комп'ютерних систем і використання вразливостей у криптографічних протоколах для отримання доступу до секретної інформації; 4. Інформаційна війна: Впровадження шкідливого програмного забезпечення в критичну інфраструктуру для її саботажу або виведення з ладу, перехоплення та маніпулювання даними для сіяння розбрату або дезінформації, відключення або порушення роботи мереж для створення хаосу або перешкоджання військовим діям.

Як проміжний висновок, можемо сказати, що клептографія дійсно має широке коло застосування та великий потенціал у сучасну інформаційну епоху. Іншим висновком з вищеописаного є те, що абослютна більшість клептографічних атак зав’язана на використанні бекдорів у програмно-апаратному забезпеченні.

Існує ряд базових методів інформаційної безпеки, які також є ефективними для захисту від клептографічних атак:

- Шифрування даних: Шифрування даних робить їх нечитабельними для несанкціонованих осіб, навіть якщо вони викрадені.
- Контроль доступу: Застосування строгих заходів контролю доступу для обмеження доступу до даних лише авторизованим користувачам.
- Регулярний аудит безпеки: Проведення регулярних аудитів безпеки для виявлення та виправлення потенційних вразливостей у системах.
- Використання надійних криптографічних протоколів та алгоритмів: Використання перевірених та стійких до атак криптографічних протоколів для захисту даних під час передачі та зберігання.
- Оновлення програмного забезпечення: Застосування останніх оновлень програмного забезпечення для усунення відомих вразливостей.
- Навчання персоналу: Навчання персоналу основам кібербезпеки та методам розпізнавання та запобігання фішинговим атакам та соціальній інженерії.

Такі вразливості можуть бути імплементовані у програму або апаратне забезпечення на різних етапах їх розробки як без відома виробника так і *навмисно та свідомо* самим виробником, що викликає обгрунтоване занепокоєння чи дійсно пристрої виконують те і тільки те, що заявлене у специфікації.

Якщо для несанкціонованих модифікацій ПЗ та пристроїв існують методи виявлення та нейтралізації, то які дії можна вчинити у разі навмисного впровадження масовими виробниками смартфонів та іншої електроніки?

Останні новини від урядів західних країн про заборону використання пристроїв, вироблених китайськими компаніями свідчать про небезпідставні страхи щодо наявності бекдорів, які можуть збирати конфіденційні дані користувачів. Питання про те «чи існує зараз справжня приватність» залишається відкритим.

Отже, у даному дослідженні клептографію було розглянуто у більш широкому сенсі, не обмеженому тільки криптографією, викладено сфери застосування та потенційні методи протидії. У процесі дослідження також було сформовано проблему використання та впровадження клептографічних закладок виробниками електроніки та контроль держави за інформаційною діяльністю населення. Це питання потребує подальшого розгляду.

1. CNET. URL: https://www.cnet.com/tech/mobile/us-finds-huawei-has-backdoor-access-to-mobile-networks-globally-report-says (дата звернення 14.04.2024)
2. Cryptologie. URL: https://www.cryptologie.net/article/210/kleptography-hidding-a-private-key-in-plain-sight (дата звернення 14.04.2024)

Дослідження загроз інформаційної безпеки Wi-Fi мереж

УДК 004.056.5

Орест Полотай[1], Наталія Федінець[2]

Львівський державний університет безпеки життєдіяльності,
[1]orest.polotaj@gmail.com, [2]nataliafedynets@gmail.com

Останнім часом спостерігається зростання використання бездротових комп'ютерних мереж, які працюють по стандарту Wi-Fi. До них відносяться смартфони, ноутбуки та пристрої "розумного дому". Це збільшило ризики інформаційної безпеки таких технологій.

Бездротовий зв'язок, як відомо, працює шляхом передачі сигналів по повітрю. Бездротові сигнали можуть проникати крізь тверді об'єкти, такі як стеля, підлога і стіни, і виходити за межі будинку або офісу. Без належних заходів безпеки встановлення бездротової локальної мережі може бути синонімом встановлення портів Ethernet скрізь, навіть на вулиці.

Бездротові мережі доступні будь-кому, хто перебуває в радіусі дії точки доступу і має відповідні облікові дані для приєднання до точки доступу. За допомогою бездротового мережевого адаптера та хакерських технологій зловмиснику не потрібно бути фізично присутнім, щоб отримати доступ до таких мереж. Атаки можуть бути ненавмисно згенеровані сторонніми особами, незадоволеними співробітниками або навіть самими працівниками.

Розглянемо основні загрози інформаційної безпеки бездротових Wi-Fi мереж. Бездротові мережі особливо вразливі до кількох типів загроз:

Підслуховування даних – бездротові дані повинні бути зашифровані, щоб запобігти їх прослуховуванню.

Бездротові зловмисники – несанкціоновані користувачі, які намагаються отримати доступ до мережевих ресурсів, можуть бути зупинені за допомогою ефективних методів автентифікації.

Атаки типу "відмова в обслуговуванні" (DoS) – доступ до послуг бездротової локальної мережі може бути порушений випадково або зі зловмисними намірами.

Несанкціоновані точки доступу – несанкціоновані точки доступу, встановлені добросовісним користувачем або зловмисниками, можуть бути виявлені за допомогою програмного забезпечення для управління.

Атака "людина посередині" – хакер розташовується між двома легітимними об'єктами для зчитування або зміни даних, які передаються між двома сторонами.

Бездротові атаки на відмову в обслуговуванні (DoS) можуть бути спричинені такими факторами:

Неправильна конфігурація пристрою – помилки конфігурації можуть вимкнути бездротову мережу. Наприклад, адміністратор може випадково змінити конфігурацію і вимкнути мережу, або зловмисник з адміністративними привілеями може навмисно вимкнути її.

Навмисне втручання в бездротовий зв'язок – мета полягає в тому, щоб повністю вимкнути бездротову мережу або зробити носій даних недоступним для легальних пристроїв.

Випадкові перешкоди – бездротові мережі чутливі до перешкод від інших бездротових пристроїв, таких як мікрохвильові печі, бездротові телефони та

радіоняні Варто зазначити, що діапазон 2.4 ГГц більш чутливий до перешкод, ніж діапазон 5 ГГц.

Несанкціонована точка доступу – це точка доступу або бездротовий маршрутизатор, підключений до корпоративної мережі без явного дозволу та всупереч корпоративній політиці. Будь-хто, хто має доступ до приміщення, може встановити дешевий бездротовий маршрутизатор, який може мати доступ до захищених мережевих ресурсів.

Поширеною бездротовою атакою "людина посередині" є атака "зловмисного двійника точки доступу", коли зловмисник розгортає несанкціоновану точку доступу і налаштовує її на той самий SSID, що і легітимну точку доступу. Через відкриту автентифікацію місця, що пропонують безкоштовний Wi-Fi, такі як аеропорти, кафе і ресторани, є особливо популярними цілями для цього типу атак.

Бездротовий клієнт, який намагається підключитися до бездротової мережі, побачить дві точки доступу, що пропонують бездротовий доступ з однаковим SSID. Та, що знаходиться ближче до несанкціонованої точки доступу, з більшою ймовірністю виявить і підключиться до сильнішого сигналу. Трафік користувача надсилається на несанкціоновану точку доступу, яка перехоплює дані і перенаправляє їх на легальну точку доступу. Зворотний трафік з легітимної точки доступу надсилається на зловмисну точку доступу, перехоплюється і перенаправляється користувачеві, який нічого не підозрює. Зловмисники можуть викрасти паролі та особисті дані користувачів, отримати доступ до пристроїв і скомпрометувати системи.

Щоб запобігти втручанню зловмисників у бездротову мережу і захистити дані, більшість маршрутизаторів і точок доступу все ще мають дві традиційні функції безпеки: маскування SSID і фільтрацію MAC-адрес.

1. Belej O., Nestor N., Sadeckii J., Polotai O. Features of Application of Data Transmission Protocols in Wireless Networks of Sensors. 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019. Proceedings. 2019. Article ID 8847878. P. 317–322.
2. Kukharska N.P., Lagun A.E., Polotai O.I. The steganographic approach to data protection using arnold algorithm and the pixel-value differencing method. Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP 2020. 2020. Article ID 9204108. P. 174–177.
3. Полотай О.І., Кичма А. Загрози безпеки Wi-Fi мереж та основні протоколи захисту. Зб. тез доп. V Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів “Інформаційна безпека та інформаційні технології”. (м. Львів, 26 листопада 2021 р.). Львів : ЛДУБЖД, 2021. С. 49–51.

Критерії виявлення повільних DDoS-атак

УДК 004.21.1(043.2)

Петро Поночовний[1], Ігор Аверічев[2]

Державний університет інформаційно-комунікаційних технологій,
[1]petja91@ukr.net, [2]iaverichev19@gmail.com

В TCP/IP-мережах при передачі даних можуть виникати шкідливі повільні DDoS-атаки [1], які призводять до перевантажень і відмови в обслуговуванні, при яких передача даних унеможливлюється.

На сьогодні не має чітких правил, які дозволяють виявити такі види атак. Деякими вченими запропоновані нечіткі алгоритми [2], ефективність яких варіюється від виду переданої інформації та від кількості фактичних запитів до серверу, однак і вони не дають чітку відповідь, як можна виявити повільну DDoS-атаку і як їй протидіяти.

Сформулюємо вимоги для аналізу повільних DDoS-атак.

1. Аналіз тривалості з'єднання.

Під час нормальної роботи мережі ці значення коливаються від дуже малих до великих. Необхідно знайти середнє арифметичне значення цієї множини.

2. Аналіз кількості байтів і потоків в секунду.

Під час повільної DDoS-атаки цей показник повинен бути дуже малий, тому що пакети між атакуючим хостом та сервером майже не відправляються, а сервер знаходиться в режимі очікування, не розриваючи з'єднання. Необхідно знайти медіану кожної з двох вибірок.

3. Аналіз кількості пакетів, відправлених з хоста.

Визначається кількість переданих даних відправником за одну секунду. Знаходимо медіану вибірки для всіх сеансів і визначаємо яку саме кількість даних клієнт може відправити в середньому на сервер.

4. Аналіз кількості пакетів, відправлених на сервер.

Це кількість переданих даних назад з сервера до відправника за одну секунду. Знаходимо медіану вибірки, враховуючи дані всіх сеансів.

5. Аналіз мінімального значення підключень з однієї IP-адреси, створених за одну хвилину.

Потрібно розбити вибірку на класи, групуючи значення по IP-адресам джерела і визначати кількість підключень протягом кожної хвилини. З даної вибірки обираємо середнє значення. Мінімальним значення з якого почнеться спостереження – одне підключення на секунду, тобто шістдесят підключень на хвилину. Менша кількість підключень у вибірку входити не буде.

6. Аналіз мінімального коефіцієнту варіації для вибірки із кількості переданих байтів в потоці з кожної IP-адреси.

Необхідно розбити всю вибірку відправлених байтів на класи по IP-адресам джерел. Фіксуються значення кількості байт для кожного підключення з конкретної IP-адреси, потім для кожного класу розраховується дисперсія та середнє значення. Далі знаходяться коефіцієнти варіації для кожної IP-адреси, серед яких обираються два мінімальних значення і знаходиться серед них середнє. Це значення і буде складовою критерія.

Сформулюємо основні критерії для визначення шкідливих з'єднань.

Критерій 1 – залежність тривалості сеансу від кількості переданої інформації.

Під час повільної DDoS-атаки на відмову в обслуговуванні, тобто при великій тривалості з'єднання маємо дуже малу кількість переданих пакетів. Таке з'єднання вважається підозрілим по першому критерію, якщо відповідає наступним умовам: 1) тривалість TCP сеансу більша за граничну; 2) кількість переданої інформації менша за граничну;

Критерій 2 – однорідність множин переданої інформації та тривалості.

При нормальній роботі мережі множини значень кількості байт в секунду можуть суттєво відрізнятися від сеанса до сеансу, створених з однієї IP-адреси, тому вони вважаються неоднорідними, як і значення тривалості сеансу.

Тривалість з'єднання буде вважатися однорідною, тому що під час атаки зловмисник намагається якомога довше зайняти сервер. Тобто єдине, що може скинути з'єднання – це часовий ліміт сервера, тому тривалість буде варіюватися навколо конкретного значення. Підключення вважається підозрілим, якщо з'єднання з однієї IP-адреси будуть відповідати таким вимогам: 1) коефіцієнт варіації кількості переданих байтів даних з даної IP-адреси менший, ніж значення, що визнані граничними у даній мережі; 2) значення тривалості підключень з даної IP-адреси є однорідною множиною, тобто її коефіцієнт варіації приймає значення менше на 30%.

Критерій 3 – велика кількість підключень за хвилину.

При атаці на відмову в обслуговуванні спостерігається велика кількість з'єднань з IP-адреси атакуючого. Після того, як кількість підключень за хвилину прийме значення більше, ніж зазначено у файлі з границями, підключення буде вважатися підозрілим по другому критерію.

Приведені критерії були сформовані виходячи із практичних спостережень, якими можна оперувати при аналізі мережевого трафіку представленого у вигляді двонаправлених TCP потоків.

На основі кожного з критеріїв не можна робити висновки щодо шкідливості програм, тому що їм можуть відповідати і легітимним з'єднанням, що викличе хибні спрацювання. Однак співпадіння по комбінації двох критеріїв підвищує ймовірність того, що сеанс виявиться шкідливим і з даної IP-адреси відбувається повільна DDoS-атака. Якщо TCP потік відповідає трьом критеріям одночасно, то висновок однозначний, що саме з цієї IP-адреси відбувається атака, а з'єднання є шкідливим і його необхідно перервати чи заблокувати.

1. Collection and Analysis of Slow Denial of Service Attacks Using Machine Learning Algorithms. – Режим доступу до ресурсу: https://www.proquest.com/openview/c5edb8073f8b9e10eb12c9c6e588d92e/1?pqorigsite=gscholar&cbl=18750&diss=y (дата звернення: 10.04.2024).
2. Лаптєв О.А., Бучик С.С., Савченко В.А., Наконечний В.С., Михальчук І.І., Шестак Я.В. Виявлення та блокування повільних DDOS-атак за допомогою прогнозування поведінки користувача // Наукоємні технології, 2022. – № 3(55). – С.184-192.

Оцінювання та оптимізація ризику для консервативних систем захисту інформації

УДК 004.681

Іван Прокопишин[1,2]

[1]*Львівський національний університет імені Івана Франка,*
[2]*Національний університет "Львівська політехніка", lviv.pi@gmail.com*

Розглядається система захисту незмінної структури, яка включає об'єкт захисту, вразливості, загрози та засоби захисту. Для опису втрат протягом деякого періоду часу використовується стохастична модель [1].

Припустимо, що об'єкт захисту має вразливості з множини $V = \{V^1, V^2, ..., V^K\}$, засоби захисту можна вибрати з множини $S = \{S^1, S^2, ..., S^M\}$, всі атаки та пристрої захисту є незалежними, кількість атак за рік для кожної вразливості n_k – відома.

Введемо вектор $\mathbf{x} = (x_1, x_2, ..., x_M)$ з бінарними компонентами $x_m \in \{0,1\}$, $m = 1,2,...,M$. Змінна $x_m = 1$, коли пристрій S^m задіяно у захисті, і $x_m = 0$, коли цей пристрій не використовують.

Вразливості є каналами для атак. Позначимо a_{mk}, $m = 1, 2, ..., M$ ймовірності злому захисту S^m при захисті каналу V^k $k = 1, 2, ..., K$. Коли захист S^m не захищає цей канал, тоді $a_{mk} = 1$. Для врахування можливого невикористання пристрою S^m для захисту введемо узагальнену ймовірність його злому:

$$s_{mk}(x_m) = 1 - (1 - a_{mk})\, x_m . \quad (1)$$

Ймовірність злому захисту по каналу V^k дорівнює добутку ймовірностей злому усіх засобів захисту, які захищають цей канал:

$$r_k(\mathbf{x}) = \prod_{m=1}^{M} s_{mk}(x_m) . \quad (2)$$

За ряду припущень про незалежність пристроїв захисту та атак сумарна кількість первинних ушкоджень системи буде сумою біноміально розподілених випадкових величин [1]:

$$\xi : \sum_{k=1}^{K} Bin(n_k, r_k(\mathbf{x})) . \quad (3)$$

Зазначимо у випадку коли кількість атак n_k по каналу *k* менша за одиницю, але відома ймовірність атаки – p_k, у формулі (3) потрібно покласти:

$$n_k = 1, \;\; r_k(\mathbf{x}) = p_k \prod_{m=1}^{M} s_{mk}(x_m). \quad (4)$$

Нехай величина економічних збитків від вдалої атаки по каналу V^k дорівнює w_k, а загальні капітальних та поточні витрати на захист S^m за період дорівнюють

C_m. Також припустимо, що втрати від можливого ушкодження засобів захисту – незначні. Тоді випадкова величина сумарних втрат, зумовлених атаками та витратами на захист, з урахуванням формули (3), буде дорівнювати:

$$\tilde{L}(\mathbf{x}) = \sum_{k=1}^{K} w_k Bin(n_k, r_k(\mathbf{x})) + \sum_{m=1}^{M} x_m C_m \qquad (5)$$

Аналогічно [1] знаходимо математичне сподівання та стандартне відхилення цієї величини:

$$L_E(\mathbf{x}) = E(\tilde{L}) = \sum_{k=1}^{K} w_k r_k(\mathbf{x}) n_k + \sum_{m=1}^{M} x_m C_m , \qquad (6)$$

$$L_\sigma(\mathbf{x}) = \left(L_D(\mathbf{x})\right)^{1/2}, \; L_D(\mathbf{x}) = D(\tilde{L}) = \sum_{k=1}^{K} y_k w_k^2 r_k(\mathbf{x})(1 - r_k(\mathbf{x})) n_k \; . \qquad (7)$$

За припущень $L_E < +\infty$, $L_D < +\infty$, як випливає з нерівності Кантеллі [2], сумарні втрати $\tilde{L}$ не перевищать величини

$$L_R(\mathbf{x}) = L_E(\mathbf{x}) + \lambda L_\sigma(\mathbf{x}) , \qquad (8)$$

з надійністю $\alpha = \lambda^2 / (1 + \lambda^2)$, зокрема $\alpha = 90\,\%$ при $\lambda = 3$.

Величина $L_R(\mathbf{x})$ є мірою ризику для системи захисту, а також мірою її ефективності.

На основі викладеної моделі ризику для систем захисту інформації:

– отримано інтервальну оцінку показника ризику (8) в аналітичній формі при малих приростах параметрів;

– запропоновано спрощену агреговану модель оцінки ризику та відповідну методику побудови дискретних шкал ризику;

– дано формулювання задачі оптимізації систем захисту у формі задачі нелінійної бінарної оптимізації.

1. Dudykevych V. , Prokopyshyn I., Chekurin V., Opirskyy I., Lakh Yu., Kret T., Ivanchenko Ye., Ivanchenko I. A multicriterial analysis of the efficiency of conservative information security systems. *Eastern-European Journal of Enterprise Technologies.* – 2019. – Vol. 3, Issue 9 (99). – P. 6–13.
2. Ross S. M. Probability models for computer science. Harcourt/Academic Press, 2002. 288 p.

Динамічне емулювання як засіб виявлення поліморфних вірусів із маскувальними техніками

УДК 004.49

Павло Регіда[1], Марія Капустян[2], Лигун Олексій[3]

Хмельницький національний університет, [1]pavlo.rehida@gmail.com, [2]kapustian.mariia@gmail.com, [3]oleksii.lyhun@gmail.com

Мета роботи: розробка методу виявлення поліморфних вірусів, що використовують маскувальні техніки.

Широке залучення ІТ у повсякденному житті вимагає користувачів застосовувати різноманітні програмні, мобільні додатки та веб-сервіси. Усі ці засоби, в тій чи іншій мірі використовують персональні або корпоративні дані. Розробники вірусних засобів інфікуючи ці додатки, ставлять на меті отримати ці дані. Тому, дослідження сучасних методів виявлення таких загроз, є актуальною та важливою задачею сьогодення.

Зловмисники часто використовують поліморфні віруси, що демонструють здатність змінювати структуру власного коду і при цьому зберігають зловмисні функції. Це досягається за допомогою використання технік маскування, що враховують основні методи їх виявлення. Основним сучасним методом виявлення вірусів є технологія емуляції та відтворення програм та файлів у ізольованому середовищі. Тому, розробники вірусів використовують анти-емуляційні техніки, як один із основних видів захисту від виявлення. Дослідження таких методів, є важливим в контексті виявлення поліморфних вірусів, розглянемо основні їх види: атаки на основі часових характеристик – t_{tsc}; пошук артефактів [1] – t_{arf}; аналіз інструкцій SIDT, SLDT, STR [2] – t_{ima}; перевірка доступності набору інструкцій [3] – t_{isa}, аналіз API викликів – t_{apia}. Особливістю поліморфних вірусів є також, те що вони можуть змінювати свою поведінку під час виконання. Тому, якщо такий вірус визначив присутність емуляції, він може припинити свої зловмисні дії.

Застосування усіх відомих технік захисту одночасно не притаманне для інфікованої програми або файлу. Це спричинено тим, що в такому разі для користувача може бути помітна різниця із оригінальним файлом чи програмою, і він буде виглядати підозрілим для нього, і може ним не скористатись.

Тому, якщо представити описаний вище набір анти-емуляційних технік у вигляді $T_{ae} = \{t_{tsc}, t_{arf}, t_{ima}, t_{isa}, t_{apia}\}$, то поліморфні віруси, які використовують частину таких технік – $V_1 = \langle t_{tsc}, t_{ima} \rangle$, або $V_2 = \langle t_{apia}, t_{arf} \rangle$.

Враховуючи це, описані приклади поліморфних вірусів будуть приховувати свою зловмисну дію тільки у випадку, якщо його наявні техніки маскування виявлять в середовищі виконання емуляцію. І тут постає проблема, антивірусні засоби не можуть наперед знати які саме техніки будуть застосовані, що теоретично дозволить уникнути виявлення самих вірусів.

Щоб вирішити поставлену проблему, пропонується застосувати концепцію динамічного емулювання у пісочниці. Основною ідеєю цього підходу є формування декількох об’єктів емуляції, що будуть використовуватись для відтворення одного і того самого файлу чи програми, але в різних умовах. Пісочниця буде

використовуватись в якості засобу, який аналізує процес роботи емулятора та слідкує як змінюється його стан використовуючи системне переривання.

На рис. 1 зображена узагальнена модель процесу динамічного емулювання для виявлення зловмисного дії.

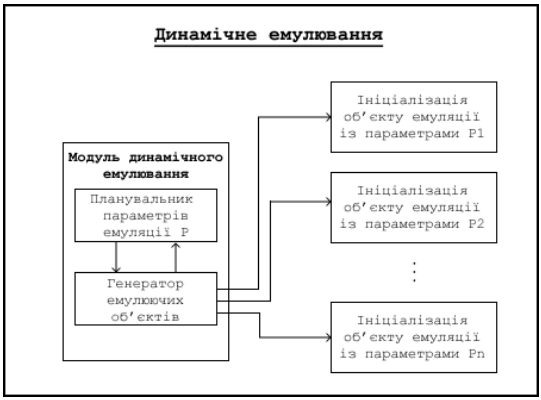


Рис. 1 – Модель виявлення поліморфних вірусів із динамічним емулюванням

В запропонованому підході, система буде формувати набір різних параметрів, що будуть слугувати налаштуваннями набору пісочниць. На виході система отримає набір пісочниць (об'єкти емуляції) в яких інфіковані програми будуть поводити себе по різному враховуючи застосовані в них анти-емуляційні техніки. Після виконання програми у кожній пісочниці вона генерує стан емулятора, та відправляє результат на керуючий динамічний емулятор. Він в свою чергу приймає рішення про наявність зловмисного дії: якщо усі стани однакові – зловмисний дія відсутня, в іншому випадку – присутня.

1. Liu S., Feng P., Wang S., Sun K. Cao J., Enhancing malware analysis sandboxes with emulated user behavior. *Computers & Security*. – 2022. – V. 115. – p. 102613.
2. Olaimat M.N, Maarof, M.A, Al-rimy, B.A.S., Ransomware anti-analysis and evasion techniques: A survey and research directions. *Cyber Resilience Conference*. – 2021. – P.1-6.
3. Zhang Z., Cheng Y., Gao Y., Nepal S., Liu D., Zou Y., Detecting hardware-assisted virtualization with inconspicuous features. *IEEE Transactions on Information Forensics and Security*. – 2020. – V. 16 – P.16-27.

Удосконалення методу малоресурсного гешування HDG

УДК 621.395.7 (043.2)

Віталій Селезньов[1], Володимир Лужецький[2]

Вінницький національний технічний університет,
1seleznov.vitalii@gmail.com, 2v.luzhetskyi@vntu.edu.ua

У сучасному цифровому світі використання малоресурсних пристроїв Інтернету речей (IoT), таких як розумні годинники, браслети, сенсорні вузли, смарт-карти, модулі, що використовують RFID-мітки або NFC технологію (Near Field Communication), тощо стає все більш поширеним. Однак обмежені обчислювальні та енергетичні можливості цих пристроїв створюють нові виклики для забезпечення безпеки та конфіденційності даних, зокрема, у контексті процесу гешування.

Проблема гешування на малоресурсних пристроях полягає в обмеженості їхніх ресурсів, які не завжди дозволяють ефективно виконувати складні алгоритми гешування. Це може призвести до повільної роботи пристроїв, високого споживання енергії та низької продуктивності. Крім того, існує ризик зниження безпеки даних через використання слабких або недостатньо надійних алгоритмів гешування на цих пристроях. У зв'язку з цим виникає потреба в розробці та оптимізації методів гешування, спеціально адаптованих до можливостей малоресурсних пристроїв. Метод малоресурсного гешування HDG (Hash Data Generator) є одним з потенційних рішень для вирішення цієї проблеми, однак він містить суттєвий недолік, а саме обмеження для застосування на даних, мінімальна довжина яких сягає 64 байти.

Метою даної роботи є удосконалення методу малоресурсного гешування HDG для усунення або максимального зменшення обмеження на довжину цільових даних для його застосування.

Метод малоресурсного гешування HDG передбачає використання підходу до гешування «дані – генератор» відповідно до якого проміжні та остаточні значення геш-функції обчислюється шляхом додавання байтів даних у позиціях, що відповідають бітам, які генерується псевдовипадковим чином.

Вхідне повідомлення m подається у вигляді послідовності байт :

$$m = \{m_1, m_2, \ldots, m_L\} \tag{1}$$

Початкове геш-значення h_0 є сукупністю псевдовипадкових байтів та представлено у вигляді послідовності:

$$h_0 = \{h_{0,0}, h_{0,1}, \ldots, h_{0,k-1}\}, \tag{2}$$

де $k = l/8$, l – довжина геш-значення в бітах.

Проміжні геш-значення $h_i = \{h_{i,0}, h_{i,1}, \ldots, h_{i,k-1}\}$ обчислюються на основі попереднього геш-значення h_{i-1} і поточного значення m_i шляхом виконання функції ущільнення f. В якості модифікації оригінального методу HDG пропонується використання $\overline{m_i}$, що є оберненим до оригінального значення даних при обчисленні проміжних геш-значень.

Кроки виконання функції ущільнення для *i*-го байту даних:

1. Для j від 0 до $k-1$ виконувати:

2. Згенерувати псевдовипадковий біт $g_{i,j}$.

3. Виконати обчислення:

$$h_{i,j} = \begin{cases} (h_{i-1,j} + m_i) \bmod 256, & \text{якщо } g_{i,(k-1-j)} = 1 \\ (h_{i-1,j} + \overline{m}_i) \bmod 256, & \text{якщо } g_{i,(k-1-j)} = 0 \end{cases} \quad (3)$$

Схему обрахунку модифікованої функції ущільнення за методом гешування наведено на рис. 1.

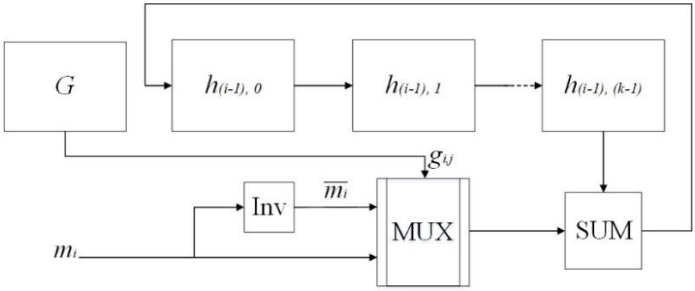


Рис.1. Схема обчислень геш-значень

Виконано статистичне тестування у пакеті NIST STS 800-22 модифікованого методу HDG на основі 200000 геш-значень, що обчисленні на основі повідомлень довжиною L = 8, 10, 11, 12, 16, 64 байт.

Таблиця 1

Результати статистичного тестування модифкованого HDG

L	Номер тесту NIST STS 800-22													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
8	+	-	+	+	+	-	+	+	+	+	-	+	+	+
9	+	-	+	+	+	+	-	+	+	+	+	+	+	+
10	+	-	+	+	+	+	-	+	+	+	-	+	+	+
11	+	+	+	+	+	+	-	+	+	+	+	+	+	+
12	+	+	+	+	+	+	+	+	+	+	-	+	+	+
13	+	+	+	+	+	+	+	+	+	+	+	+	+	+
14	+	+	+	+	+	+	+	+	+	+	+	+	+	+
15	+	+	+	+	+	+	+	+	+	+	+	+	+	+
16	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Відповідно до таблиці 1 для довжини повідомлення L=8 реалізація модифікованої функції ущільнення забезпечує усі успішні тести, окрім № 2, 6 та 11. Для довжини повідомлень L=12 успішними є усі тести, окрім №11. Починаючи з довжини повідомлень L=13 модифікований метод HDG забезпечує усі успішні тести, що є кращим у порівнянні з оригінальним HDG, який у свою чергу забезпечує усі успішні тести NIST при значеннях L=64 та більше.

1. Encryption and hash based security in Internet of Things / B. Vinayaga Sundaram та ін. 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), м. Chennai, India, 26–28 берез. 2015 р. 2015. URL: https://doi.org/10.1109/icscn.2015.7219926 (дата звернення: 16.04.2024).
2. DeeR-Hash: A lightweight hash construction for Industry 4.0 / IoT. Journal of Scientific & Industrial Research. 2023. Т. 82, № 01. URL: https://doi.org/10.56042/jsir.v82i1.69938 (дата звернення: 16.04.2024).
3. Селезньов В. І., Лужецький В. А. Метод малоресурсного гешування типу «дані – генератор». Кібербезпека: освіта, наука, техніка. 2023. 2(22). С. 84-95.
4. Селезньов В. І. Програмний засіб для віддаленого статистичного тестування методів малоресурсного гешування за допомогою пакету NIST STS 822 / LIII Науково-технічна конференція факультету інформаційних технологій та комп`ютерної інженерії, ВНТУ, м. Вінниця, 20-22 березня 2024 р.
5. A statistical test suite for random and pseudorandom number generators for cryptographic applications / L. E. Bassham та ін. Gaithersburg, MD : National Institute of Standards and Technology, 2010. URL: https://doi.org/10.6028/nist.sp.800-22r1a (дата звернення: 16.04.2024).
6. NIST 800-22 українською мовою URL: http://www.itsway.kiev.ua/pdf/Articles180106.pdf (дата звернення 13.04.2024).

Дослідження log-файлів засобами платформи Elastic Stack

УДК 004.4:004.896

Ольга Смотр[1], Микита Купріков[2]

Львівський державний університет безпеки життєдіяльності,
[1]olgasmotr@gmail.com, [2]nkuprikov@ldubgd.edu.ua

Однією з найбільш поширених загроз для даних є несанкціонований доступ, що може призвести до втрати конфіденційності, цілісності та доступності інформації. Адже у сучасному світі, де взаємозв'язки набувають все більшого значення, конфіденційність інформації про продукти, процеси, клієнтів та постачальників є критично важливою для будь-якої компанії. Особливо відчутною ця необхідність стає в контексті спалаху інформаційної війни, що супроводжує повномасштабне вторгнення російських військ на територію України у 2022 році. Відповідно до прогнозів спеціалістів Cybersecurity Ventures на 2024 рік витрати світової спільноти на кіберзлочинність становитимуть близько 9,5 трильйонів доларів США. [1]. В свою чергу, кількість кібератак з метою заволодіння даними зросте більш ніж на 18%, середня вартість збитків від витоку даних становитиме понад 4,5 млн доларів США. [2].

Для розв'язання цих проблем на передньому краї технологічного розвитку стоїть аналіз log-файлів. Log-файли представляють собою записи подій, які відбуваються в системі або програмі, і є важливим інструментом для виявлення аномальних або підозрілих активностей. Аналіз log-файлів допомагає розуміти, як функціонує система та виявляти аномальну поведінку, що може свідчити про зловживання доступом або зловмисну діяльність. Це може бути корисно при розслідуванні інцидентів безпеки та при виявленні вразливостей, які можуть бути використані для атак на систему. Однак, аналіз log-файлів є трудомістким завданням, що, як правило, є складним для ручного аналізу. зважаючи на їх значний розмір та різні формати, залежно від того, яка система їх генерує. Адже log-файли можуть бути текстовими, бінарними або ж представленими у інших спеціальних форматах для зберігання даних. Для ефективного аналізу log-файлів доречно використовувати методику структурного аналізу даних, з метою відокремити корисну інформацію від зайвої та виявити можливі загрози безпеці даних та алгоритми машинного навчання для виявлення аномальної активності в системі.

На сьогодні на ринку існує ряд платформ з інструментарієм аналізу log-файлів. Це такі як Elastic Stack, Splunk, Graylog, Fluentd тощо. Для подальшої роботи з log-файлами використовуватимемо Elastic Stack. Elastic Stack (ELK) складається з таких компонентів як: Elasticsearch, Logstash, Kibana та Beats, і забезпечує комплексне рішення для збору, аналізу та візуалізації даних. Вона має ряд переваг: висока швидкість, масштабованість, а також розширені можливості візуалізації та аналізу даних [3-6]. Однак, слід зазначити, що вона також має свої недоліки, зокрема, складність налаштування та використання для не досвідчених користувачів. Зокрема продемонструємо процес розробки фільтрів для Logstash .

Розробка фільтрів для Logstash є одним із вирішальних етапів у створенні системи аналізу log-файлів. Фільтри дозволяють трансформувати та розбирати вхідні дані на більш деталізовані складові, що спрощує подальший аналіз. Одним з

основних типів фільтрів, які будуть розроблені в рамках даної роботи, є фільтр "grok". Фільтр grok дозволяє структурувати неструктуровані log-файли, шляхом використання шаблонів. Цей інструмент ідеально підходить для обробки логів syslog, Apache та інших веб-серверів, MySQL та, загалом, будь-якого формату логів, який зазвичай пишуть для людей, а не для обробки комп'ютерами.

Основа роботи з Grok полягає в комбінуванні текстових шаблонів у такий, що відповідає вашим логам. Синтаксис для шаблону grok виглядає так:

```
%{SYNTAX:SEMANTIC}
```

де SYNTAX - це назва шаблону, який буде збігатися з вашим текстом. Наприклад, число 3.44 буде збігатися з шаблоном NUMBER, а IP-адреса 55.3.244.1 - з шаблоном IP. SEMANTIC - це ідентифікатор, який ви задаєте частині тексту, яка збігається. Наприклад, число 3.44 може бути тривалістю події, тому ви можете іменувати його просто "duration". Рядок "55.3.244.1" може ідентифікувати клієнта, який робить запит. У цьому випадку наш фільтр grok міг би виглядати так:

```
%{NUMBER:duration} %{IP:client}
```

Також можемо додати до свого шаблону grok перетворення типів даних. За замовчуванням, всі семантичні складові зберігаються як рядки. Якщо ви хочете змінити тип даних семантичної складової, наприклад, змінити рядок на ціле число, додайте до нього цільовий тип даних. Наприклад, %{NUMBER:num:int}, який конвертує семантичну складову "num" з рядка в ціле число. На даний момент підтримуються тільки перетворення в int і float.

Розглянемо, як за допомогою синтаксису і семантики можна витягти корисні поля, для прикладу, з такого логу HTTP-запиту:

```
55.3.244.1 GET /index.html 15824 0.043
```

Шаблон для цього логу може бути наступним:

```
%{IP:client} %{WORD:method}
%{URIPATHPARAM:request}
%{NUMBER:bytes} %{NUMBER:duration}
```

У кінцевому результаті наш файл конфігурації виглядатиме так (рис. 1).

```
input {
  stdin { } # Вхідний логік для отримання даних з консолиfile {
    path => "/var/log/http.log" # Шлях до файлу журналу, який потрібно обробити
  }
}
filter {
  grok {
    match => { "message" => "%{IP:client} %{WORD:xethod}
%{URIPATHPARAM:request} %{NUMBER:bytes} %{NUMBER:duration}" }
  }
}
output { stdout {
    codec => rubydebug # Вивід даних у форматі Ruby-відладки
  }
  elasticsearch {
    hosts => ["http://localhost:9200"] # Адреси серверівElasticsearch
    index => "test.logstash" # Індекс, у який будуть зберігатись
дані
    user => "elastic" # Користувач Elasticsearch
    password => "3guzVh6WIwXCb*qVFQfp" # Пароль користувача
Elasticsearch
```

Рис.1. Лістинг - Конфігурація Logstash-файлу «learn.conf» для обробки журналу HTTP

Наш запит можемо здійснити через командний рядок або ж у Kibana. Результат запиту з командного рядка та Kibana відображено на рисунках 2 та 3 відповідно.

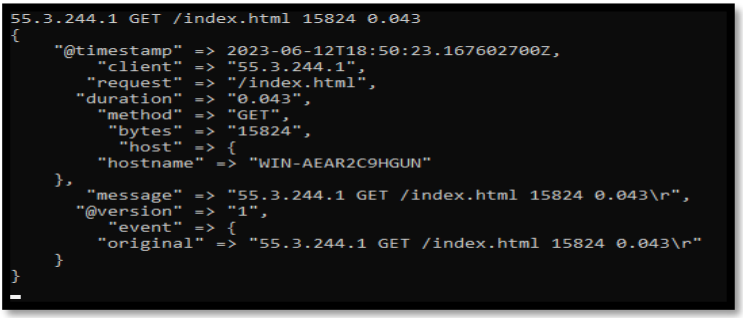


Рисунок 2 - Результат зчитування log-файлу у командному рядку

Запит "55.3.244.1 GET /index.html 15824 0.043" був оброблений Logstash і вивід результату показує, що дані були успішно розпізнані і відформатовані за допомогою grok-виразу. Кожен елемент запиту відображений відповідним полем, наприклад, IP-адреса ("client"), HTTP-метод ("method"), URL-шлях ("request"), обсяг байтів ("bytes") та тривалість ("duration"). Додаткові поля, такі як "@timestamp" та "host.hostname", також відображаються. Загальний результат містить ключі та значення для кожного поля, яке було оброблено. Ці дані можна використовувати для подальшої аналітики, візуалізації та зберігання у Elasticsearch для подальшого використання.

У Kibana, в розділі "Expanded document" ми також можемо побачити розширені дані документу, які були збережені у Elasticsearch після обробки Logstash (див. рис. 3).

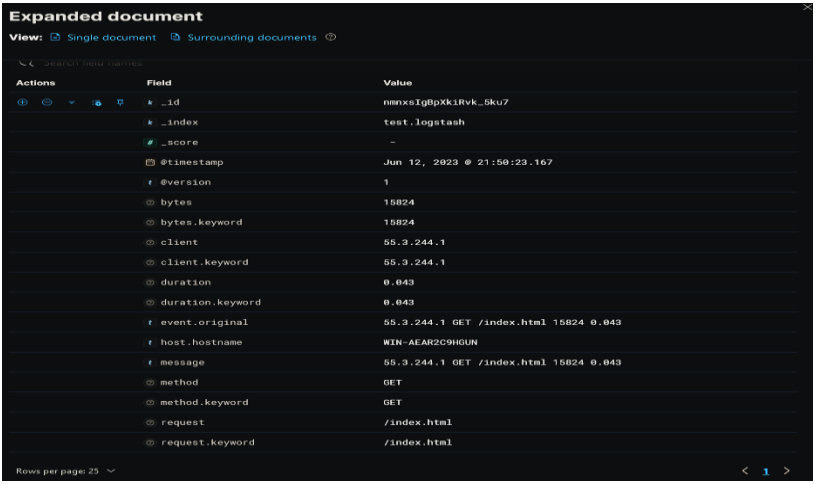


Рисунок 3 - Результати нашого запиту у Kibana

Тепер за допомогою Kibana можна встановлювати фільтри за різними полями, такими як "client", "method" або "request", і швидко отримувати підсумкові дані для конкретних сегментів інформації. Окрім того, Kibana пропонує нам розширені можливості фільтрування та пошуку. Ми можемо виконувати розширені пошукові запити, використовуючи синтаксис Elasticsearch Query DSL, щоб знайти конкретні документи або аналізувати дані за певними умовами. Як наслідок, ми можемо точно налаштувати свої запити та отримувати результати, які відповідають конкретним потребам користувача. Наприклад, можна налаштувати систему моніторингу трафіку на мережевому рівні, щоб виявляти незвичайну активність, таку як велика кількість запитів від одного IP-адреси або незвичайні шаблони поведінки.

Висновок. Застосування системи Elastic Stack для аналізу log-файлів є доволі ефективним засобом виявлення потенційних загроз безпеці інформації. Даний підхід дозволяє підвищити рівень захисту інформації та забезпечити вчасне виявлення можливих загроз. Під час аналізу загроз безпеці інформації в системі ELK, можливо виявити різноманітні типи атак, такі як діяльність шпигунів, спам-атаки, фішингові атаки, вторгнення в систему, DDOS-атаки та інші. Для виявлення таких атак можна використовувати різноманітні техніки та методи, такі як: машинне навчання, статистичний аналіз, розробка правил або комбінування цих підходів.

Аналіз log-файлів надає можливість виявляти та вирішувати проблеми безпеки, що виникають в системі, а також розгортати проактивні заходи безпеки, щоб запобігти майбутнім інцидентам. Розробка шаблонів та фільтрів для аналізу log-файлів є ключовою складовою налаштуванню Elasticsearch. Вона передбачає створення шаблонів для Elasticsearch, які визначають структуру даних та надають змогу ефективно зберігати та швидко отримувати доступ до них. Розробка фільтрів для Logstash допомагає приймати, обробляти та передавати дані в Elasticsearch для подальшого аналізу. Налаштування та впровадження системи ELK для аналізу log-файлів вимагає ретельного планування і налаштування, але при цьому дозволяє здійснювати ефективний моніторинг та виявлення потенційних загроз безпеки.

1. eSentire. Офіційний звіт про кіберзлочинність за 2023 рік. URL: https://www.esentire.com/resources/library/2023-official-cybercrime-report (дата звернення: 12.04.2024).
2. H-X Technologies. Прогнози на 2024 рік. URL: https://www.h-x.technology/ua/blog-ua/cyber-threats-forecast-2024-ua (дата звернення: 12.04.2024).
3. Elastic N.V., "Elastic Stack Documentation." - [Електронний ресурс]. - Режим доступу : https://www.elastic.co/guide/index.html (дата звернення: 01.04.2024)
4. Kuprikov M, Smotr O. Monitoring and analysis of large amounts of data using the elastic stack platform. Information security and information technologies IBIT-2023: collection of abstracts of the VI All-Ukrainian scientific and practical conference, November 30, 2023. - Lviv, LSU of Life Safety, 2023. - P.341-343.

Модифікація методу вибору контейнера для зменшення чутливості стеганоповідомлення до збурних дій

УДК 004.056.5

Сокальський Сергій

Національний університет «Одеська Політехніка»,
sokalskiyserhiy1@gmail.com

На сьогоднішній день питання захисту інформації є одним із найважливіших у сфері інформаційних технологій. Оскільки поширення інформаційних технологій у всі сфери людського життя не припиняється, то і не припиняється як розвиток методів захисту цієї інформації від несанкціонованого доступу, так і розвиток методів отримання нелегального доступу до даних. Тому необхідно постійно покращувати системи та методи захисту інформації, перешкоджаючи зловмисникам.

Однією із ключових складових комплексної системи захисту інформації є стеганосистема [1], яка забезпечує безпечну передачу даних по прихованому каналу зв'язку, приховуючи сам факт наявності даних, які потрібно вберегти від зловмисників.

При побудові стеганосистеми до неї висувається ряд вимог, і деякі із них можна забезпечити вибравши відповідний стеганоконтейнер. Однією із ключових вимог є забезпечення стійкості стеганосистеми до атак проти вбудованого повідомлення, адже простота використання таких атак робить їх надзвичайно популярними і розповсюдженими.

Процес стеганографії можна розділити на три основні етапи:

- Вибір контейнера.
- Попереднє кодування інформації.
- Вбудовування інформації у контейнер для створення стеганоповідомлення.

При організації прихованого каналу зв'язку можна використовувати різні типи контейнерів, такі як випадкові, нав'язані або обрані. Однак саме вибір контейнера, який дозволяє підвищити якість забезпечення певних характеристик отриманого стеганоповідомлення, і, як результат, підвищити ефективність стеганосистеми в цілому, є важливою актуальною задачею [2].

Метою робити є підвищення ефективності стеганосистеми шляхом модифікації методу вибору контейнера з поданої сукупності, розробленого автором раніше, що забезпечить максимально можливу для аналізованих зображень, або близьку до максимальної, стійкість стеганоповідомлення до атак проти вбудованого повідомлення.

Вибір відповідного стеганографічного контейнера може допомогти виконати певні вимоги, які поставлені перед стеганосистемою при її розробці. Однією з ключових вимог є забезпечення стійкості стеганоповідомлення проти атак, спрямованих на вбудоване повідомлення. Атака на вбудоване повідомлення означає активну атаку на стеганоповідомлення з подальшим зміненням його, наприклад, через стиск з втратами, накладання шуму, фільтрацію та інші методи.

Такі атаки відзначаються тим, що для їх здійснення не потрібні високі технічні навички або спеціальні технічні засоби, тому вони є досить поширеними. Це робить

завдання захисту вбудованого повідомлення від таких атак дуже важливим та актуальним.

Над вирішенням цієї задачі працює багато вчених-стеганографів, так, наприклад, у роботі [3] представлено метод вибору стеганографічного контейнера із деякої виборки цифрових зображень, що забезпечить максимальну, або близьку до максимальної, стійкість стеганоповідомлення до атак проти вбудованого повідомлення. Цей метод базується на введеній у роботі кількісній характеристиці об'єму інформації, що буде правильно декодована після атаки на стеганоповідомлення. Ця характеристика обчислюється виходячи з розподілу вбудованої інформації по власним векторам матриці контейнера та їх чутливістю до збурних дій.

Але недоліком даного методу є використання спектру матриці та власних векторів як набору параметрів, визначаючих матрицю контейнера, тоді як на практиці вони визначають не саму матрицю контейнера, а її деяку модифікацію, оскільки для отримання цих параметрів спочатку потрібно симетризувати матрицю.

Так у роботі [4] цей набір параметрів був змінений на набір сингулярних чисел матриці та її сингулярних векторів. Метод, запропонований у цій роботі, базується на формальному представлені стеганоперетворення, як деякої адитивної операції над матрицею контейнера:

$$F = \overline{F} + \Delta F \tag{1}$$

де $\overline{F}$ - $n \times n$-матриця контейнера, F - матриця стеганоповідомлення (СП), ΔF - $n \times n$-матриця збурення, яке виникло в результаті вбудовування додаткової інформації (ДІ), яка представляє цифрову послідовність і є результатом роботи прекодера в стеганографічній системі, у контейнер. Співвідношення (1) залишається в силі незалежно від конкретного стеганографічного алгоритму, що використовувався, а також від того, в якій області контейнера (просторовій, частотній або іншій області перетворення) безпосередньо відбувалася вбудова прихованої інформації. Для повного набору формальних параметрів, що однозначно визначають контейнер або стеганоповідомлення, було вибрано комплекс сингулярних векторів та сингулярних чисел, які можна отримати за допомогою стандартного сингулярного розкладу:

$$F = U \Sigma V^T \tag{2}$$

де U, V - ортогональні $n \times n$-матриці, стовпці яких u_i, v_i, $i = \overline{1,n}$ є лівими та правими сингулярними векторами відповідно, $\Sigma = diag(\sigma_1, ..., \sigma_n), \sigma_1 \geq ... \geq \sigma_n \geq 0$ - сингулярні числа F. Нормальне сингулярне розкладання, на відміну від звичайного, визначається однозначно для будь-якої матриці, що не має кратних сингулярних чисел [5] Сингулярні числа є добре обумовленими через співвідношення:

$$\max_i \left| \sigma_i(F) - \sigma_i(F+E) \right| \leq \left\| E \right\|_2 \tag{3}$$

де $\left\| \bullet \right\|_2$ - спектральна матрична норма, E - $n \times n$-матриця збурення.

Для формування методу вибору стеганографічного контейнера було запропоновано у цій роботі нову кількісну характеристику, що буде характеризувати стійкість стеганоповідомлення, сформованого за вибраним контейнером, до атак проти вбудованого повідомлення, що буде визначатись за формулою:

$$S = \left\| \sum_{k=1}^{m} \overline{\sigma_k} \overline{u_k} \overline{v_k}^T - \sum_{k=1}^{m} \sigma_k u_k v_k^T \right\| \tag{4}$$

де m - максимальний індекс серед сингулярних чисел F, які мають достатню по відношенню до E відокремленість [2], $(\overline{\sigma_i}, \overline{u_i}, \overline{v_i})$ - сингулярні трійки матриці стеганоповідомлення. Формула (4) являє собою інформацію, 190 обула вбудована у захищене поле контейнера і визначається як різниця малорангових апроксимацій матриці контейнера та стеганоповідомлення.

Запропонований у [4] метод є ефективнішим за його аналоги, але все ще не гарантує систематичний вибір контейнера, що забезпечить максимально можливу для стеганоповідомлення стійкість до атак проти вбудованого повідомлення. Тому було вирішено його модифікувати.

Згідно відношенню (1) будь-яку вбудовану інформацію можна представити як деяке збурення матриці контейнера, та обчислити за допомогою формули:

$$\Delta F = \overline{F} - F \tag{5}$$

Але в такому випадку, при вбудовувані однієї і тієї ж інформації у різні контейнери, та обчисленю її за формулою (5) ми будем отримувати різне її формальне представлення.

У роботі [4] обсяг захищеної інформації визначався як різниця малорангових апроксимацій матриць контейнера та стеганоповідомлення. Це означає, що обсяг впливає не лише на кількість сингулярних чисел, які мають достатню відокремленість від збурення, але й на саме збурення, яке отримує матриця при стеганоперетворенні.

Крім того, поняття достатньої відокремленості сингулярних чисел вводиться з урахуванням збурення E, яке оцінюється матричною нормою, що залежить від розміру матриці збурення. Хоча характеристики збурення, нападу на вбудоване повідомлення визначаються параметрами збурення, а не розмірами контенту, на який вони спрямовані.

З урахуванням цього, правильне використання формули (4) для порівняння властивостей контейнерів в однакових умовах їх використання вимагає, серед іншого, однакових розмірів всіх цифрових зображень, які використовуються як контейнери. Проте на практиці це, як правило, не виконується.

Для зменшення впливу негативних факторів, які були вказані вище, пропонується модифікувати формулу обчислення обсягу захищеної інформації згідно з наступним:

$$S = \frac{\left\| \sum_{k=1}^{m} \overline{\sigma_k} \overline{u_k} \overline{v_k}^T - \sum_{k=1}^{m} \sigma_k u_k v_k^T \right\|}{\left\| \overline{F} - F \right\|} \tag{6}$$

Ця формула розраховує відношення об’єму захищеної інформації до загального об’єму вбудованої інформації. Таким чином, вирішено проблему негативного впливу розміру контейнера на об’єктивну оцінку його здатності забезпечити стійкість стеганоповідомлення до атак проти вбудованого повідомлення.

З урахуванням формули (6) було створено відповідний метод вибору контейнера, що забезпечить максимальну, або близьку до максимально можливої, стійкість стеганоповідомлення до атак проти вбудованого повідомлення, серед усіх наявних можливих контейнерів.

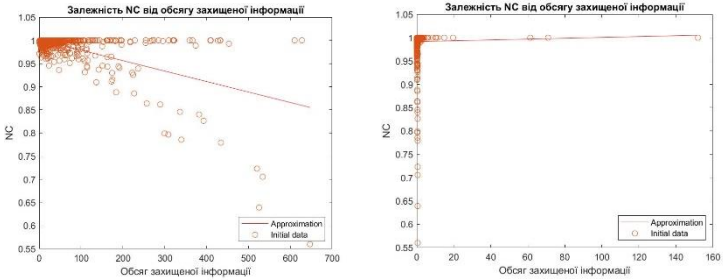


Рисунок 3. – Залежність NC від об'єму захищеної інформації вирахованої за допомогою: а – методу, запропонованого у роботі [4], б – методу описаного в даній роботі, з використанням стеганометоду Жао і Коха та накладанням мультиплікативного шуму з математичним очікуванням 0,001 як імовірної атаки проти вбудованого повідомлення

У роботі було вирішено важливу науково-практичну задачу: підвищення ефективності стеганосистеми за допомогою модифікації методу вибору контейнера з певної групи цифрових зображень, який був запропонований у [4]. Під час модифікації було вдосконалено кількісну оцінку об’єму, захищеного від збурної дії E, шляхом введення нормування об’єму за формулою (6). Також проведено оцінку ефективності, включаючи порівняльний аналіз з модифікованим методом. Отримані результати свідчать про підвищення ефективності запропонованого методу на 12,695% в порівнянні з методом-аналогом.

1. Mandal P.C., Mukherjee I., Goutam P., Chatterji B.N. Digital image steganography: A literature survey. Information Sciences. 2022. Vol. 609, P.1451-1488
2. Abed S., Al-Roomi S. A., Al-Shayeji M. Efficient cover image selection based on spatial block analysis and DCT embedding. Journal on Image and Video Processing. 2019. No. 1. https://doi.org/10.1186/s13640-019-0486-8
3. Надвоцький О.Ю., Кобозєва А.А.. Метод розв’язку задачі про вибір контейнера, що забезпечує малу чутливість стеганоповідомлення до збурних дій. URL: http://immm.op.edu.ua/files/archive/n3_v11_2021/immm_n3_v11 _2021.pdf
4. Bobok I., Kobozieva A., Sokalsky S. The Problem of Choosing a Steganographic Container in Conditions of Attacks against an Embedded Message. URL: https://journal.ie.asm.md/assets/files/07_04_56_2022.pdf

Аналіз проблем кібербезпеки при використанні програмного забезпечення з відкритим кодом

УДК 004.052.2

Андрій Тарасенко[1], Мар'ян Кирик[2]

Національний університет "Львівська політехніка",
[1]andrii.d.tarasenko@lpnu.ua, [2]marian.i.kyryk@lpnu.ua

Програмне забезпечення (ПЗ) з відкритим кодом набуло широкого використання за рахунок надійності, гнучкості і невеликих фінансових вкладень. Операційні системи (ОС) на основі відкритого ядра Linux займають вагому частку серверної інфраструктури та досить часто є основним вибором для розгортання веб-серверів, баз даних, хмарних платформ та інших важливих систем. Однак ці ОС несуть певні архітектурні та безпекові ризики, оскільки супроводом розробки займається не конкретна компанія, а публічна спільнота розробників.

Метою даної роботи є аналіз проблем та методів покращення захисту критичної IT інфраструктури при використанні програм з відкритим кодом.

Тільки за перші три місяці 2024 було виявлено декілька критичних вразливостей:

- CVE-2024-23897 Вразливість дозволяє зловмиснику, який не пройшов перевірку автентичності, виконувати віддалене виконання коду в системі Jenkins. [1]

- CVE-2024-0402 Вразливість дозволяє віддаленому зловмиснику, який пройшов перевірку автентичності, виконувати запис довільних файлів на сервері GitLab при створенні робочого простору. [2]

- CVE-2024-3094 у пакеті XZ, виявлено бекдор який може бути використаний для віддаленого доступу до системи де встановлений SSH сервіс без авторизації. [3]

Ці та інші випадки які час від часу виявляються в програмах з відкритою кодовою базою стають серйозним прецедентом для перегляду забезпечення кібербезпеки при використанні таких програм у критичній інфраструктурі. Проблематика навколо цих вразливостей піднімає більш глибокі питання щодо безпеки у проектах відкритого програмного забезпечення.

Аналізуючи проблему з нещодавно виявленою вразливістю у пакеті XZ можна відмітити що зловмисникам необов'язково використовувати складні методи компрометації. В даному випадку було достатньо отримати статус довіреної особи проекту шляхом внесення незначних правок в кодову базу. Після чого зловмисники замаскували бекдор під типову зміну в коді і розробник, що займається супроводом проекту не запідозривши нічого додав його до основної гілки програми. Разом з тим було сформовано пакети інсталяції програм для більшість дистрибутивів на основі ядра Linux, які в подальшому були встановлення вже в операційних системах по всьому світу.

Універсальний метод для захисти ПЗ від такого виду атак, нажаль, відсутній. Проте, пропонується сформувати основні підходи для мінімізація ризиків та стратегій протидії у випадку їх виявлення:

1) Ретельний вибір проектів з відкритим кодом. Рекомендується використовувати операційні системи з відкритим кодом, підтримкою яких займаються великі компанії такі як: RedHat, SUSE, Ubuntu Enterprice. Вони

проводять аудит кодової бази та несуть відповідальність та випускають оновлення безпеки за їх необхідності.

2) Підтримка балансу між функціональністю та надійністю. Більшість програм, як правило, мають декілька редакцій: одну з довготривалою підтримкою (Long Time Support – LTS) і одну з останнім оновленням (Latest). В критичній інфраструктурі рекомендується використовувати саме програми з LTS, оскільки вони призначенні для гарантованої роботи та містять перевірені та протестовані оновлення [4].

3) Оскільки ніхто не застрахований від помилок, потрібно постійно відслідковувати виявлення критичних вразливостей та вчасно проводити оновлення ПЗ.

4) Рекомендується залучення штучного інтелекту для перевірки кодової бази проектів[5].

5) Використовувати заходи по обмеженню прав доступу не лише користувачів, а також сервісів та ПЗ.

6) Використовувати інструменти моніторингу трафіку та завантаженості системи; централізованого збору і аналізу журналів подій для відслідковування небажаної активності та вчасної реакції на нетипові інциденти.

Таким чином, провівши аналіз проблем та методів покращення захисту критичної IT інфраструктури при використанні програм з відкритим кодом, рекомендується застосовувати комплексний підхід для покращення кібербезпеки, надавати перевагу тільки перевіреному ПЗ, безперервно відслідковувати виявлені критичні вразливості та обмежувати доступ не тільки на рівні користувача, але й на рівні програм та сервісів, що в свою чергу дозволить мінімізувати внутрішні та зовнішні кіберзагрози в інфраструктурі.

1. “Jenkins Security Advisory 2024-01-24" URL: https://www.jenkins.io/security/advisory/2024-01-24/ (дата звернення 15.03.2024).
2. “GitLab Critical Security Release: 16.8.1, 16.7.4, 16.6.6, 16.5.8” URL: https://about.gitlab.com/releases/2024/01/25/critical-security-release-gitlab-16-8-1-released/ (дата звернення 15.03.2024).
3. “CVE-2024-3094" URL: https://ubuntu.com/security/CVE-2024-3094 (дата звереннння 02.04.2024).
4. Calles M., Serverless Security: Understand, Assess, and Implement Secure and Reliable Applications in AWS, Microsoft Azure, and Google Cloud, 1st ed., NY, USA, Apress, 2020 pp 39-64.
5. A. Rodrigo, B. Paulo, “Privacy and security constraints for code contributions”, Software - Practice and Experience, vol. 50, issue 10, pp 1905 – 1929, October 2020.

Оптимізація повного суматора у квантовій моделі обчислень

УДК 519.6

Андрій Терещенко[1], Валерій Задірака[2]

Інститут кібернетики ім. В.М. Глушкова, [1]teramidi@ukr.net, [2]zvk140@ukr.net

Публікація алгоритму Шора [1] для розв'язання задачі факторизації великих чисел була одним з найбільших поштовхів для прискорення розробки квантових комп'ютерів. Архітектура комп'ютера, у складі якого є двох-рівневі квантово-механічні системи (кубути), визначила квантову арифметику у вигляді елементарних операцій, які виконуються вентилями, послідовне та паралельне виконання яких формує квантову схему. На жаль, квантовий комп'ютер не підтримує класичні операції такі, як додавання, віднімання, множення, тощо. Теоретично доведено, що будь-який класичний алгоритм може бути перенесено у квантову модель обчислень. Існує потреба оптимального переносу реалізації арифметичних операцій [2] у квантову модель обчислень.

У даній роботі розглядається оптимізація повного суматора для двох однобітних значень у квантовій моделі обчислень. Зручними інструментами для переносу класичних обчислень у квантову модель є універсальні вентилі такі, як вентиль Тоффолі, Переса, і т.д., які є реверсивними вентилями [3]. Відома реалізація повного суматора, яка використовує два вентилі Тоффолі (CCNOT) та три вентилі CNOT, як показано на рис. 1. Вентиль CNOT, виділений точками у вигляді прямокутника, потрібен для відновлення стану $|B\rangle$ і його можна не використовувати, якщо відновлення непотрібне. Цей вентиль у подальшому не будемо брати до уваги для спрощення аналізу складності.

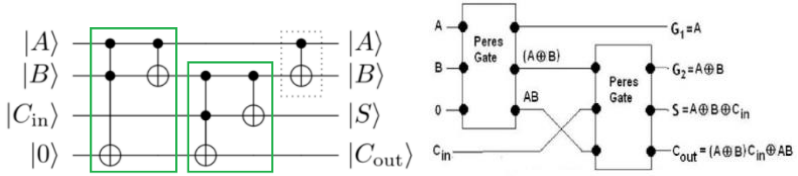


Рис.1. Реалізація Фейнманом повного суматора на основі вентилів Тоффолі (зліва), реалізація повного суматора на основі вентилів Переса (справа)

На рис. 1 прямокутниками зеленого кольору виділені вентиль Тоффолі та вентиль CNOT, які у такій комбінації утворюють вентиль Переса. Різниця в схемі зліва і справа на рис. 1 полягає у тому, що входи 0 та C_{in} (знак переносу) поміняні місцями. Квантовим числом вентиля Тоффолі є 5, а Переса – 4, тому складність схеми зліва дорівнює 12, а справа – 8. Для реалізації схеми зліва необхідно 12 двохкубітних вентилів.

Покажемо, що можна побудувати ефективну схему повного суматора на основі шести двохкубтних вентилів. За основу візьмемо схему зліва на рис. 1, в якій вентилі Тоффолі замінимо їхніми реалізаціями на основі двохкубітних вентилів. На рис. 2 реалізація вентилів Тоффолі показана прямокутниками з прикладом обчислення, коли кубіти A, B, C_{in} (вхідний знак переносу) у стані $|1\rangle$. Існують інші реалізації вентиля Тоффолі, але вибрана така реалізація, яка дозволяє ефективну

подальшу оптимізацію. Вентилі T та T‘ необхідні для корегування повороту фаз результатів обчислення.

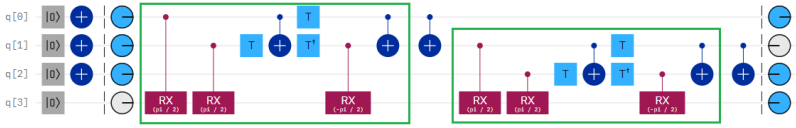


Рис.2. Реалізація повного суматора з розкриттям реалізації вентиля Тоффолі з прикладом обчислення максимального значення

На рис. 3 виділені вентилі, які у послідовному виконанні компенсують один одного, тобто їх попарна відсутність не змінює результату обчислення.

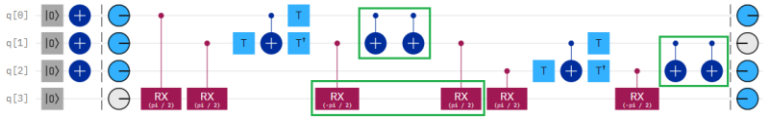


Рис.3. Реалізація повного суматора з позначенням елементів для оптимізації

Після попарного видалення вентилів CNOT вентилі CRX($\pi/2$) та CRX($-\pi/2$), позначені прямокутником, будуть послідовно повертати фазу на $\pi/2$ і потім на $-\pi/2$, що не буде змінювати результат. Ці вентилі можуть бути також видалені. На рис. 4 надано результат оптимізації реалізації повного суматора, який був перевірений за допомогою IBM Quantum Composer [4].

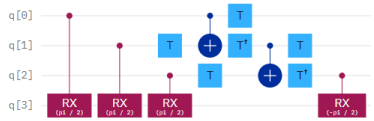


Рис.4. Оптимізація реалізації повного суматора

Для реалізації квантового повного суматора достатньо шести двохкубітних вентилів: чотирьох вентилів CRX та двох CNOT. Враховуючи, що реалізація повного суматора на основі вентилів Переса потребує восьми двохкубітних вентилів, запропонована оптимізація зменшує на 25% кількість двохкубітних вентилів, що значно зменшує реалізацію операції додавання і таких операцій, як віднімання, множення і т.д., реалізація яких залежить від реалізації додавання.

1. P. W. Shor, “Algorithms for quantum computation: discrete log and factoring”, Proc. 35th Ann. Symp. on the Foundations of Computer Science (IEEE Computer Society Press, Los Alamitos, CA, 1994), p. 124.
2. A. Tereshchenko, V. Zadiraka, “Algorithm for calculation the carry and borrow signs in multi-digit operations in the parallel computational model”, International Journal of Computing, 22(1), 21-28. (2023).
3. D. Deutsch, A. Barenco, and A. Ekert, “Universality in quantum computation”, submitted to Proc. R. Soc. Lond. (1995).
4. IBM Quantum Composer URL: https://quantum.ibm.com/composer (дата звернення: 15.04.2024).

Розробка програмного забезпечення для симуляції акустичних хвиль за допомогою трасування променів

УДК 621.395.7 (043.2)

Олександр Терлецький[1], Валерій Трушевський[2]

Львівський національний університет ім. І. Франка,
[1]oleksandr.terletskyi@lnu.edu.ua, [2]valeriy.trushevsky@lnu.edu.ua

Трасування променів - це метод моделювання розповсюдження звуку, що базується на ідеї, що звук може бути розглянутий як потік енергії, який поширюється через середовище у вигляді променів. Цей метод поділяє середовище на невеликі області, відомі як промені, і визначає взаємодію звуку з об'єктами в кожній з них. Це дозволяє моделювати відбиття, розсіювання та поглинання звуку, а також імітувати ефекти різних акустичних середовищ за допомогою матеріалів геометрії[1].

Для реалізації програмного забезпечення використовується ігровий двигун Unity[2], де створюється сцена з геометрією. Промені запускаються у випадковому напрямку від джерела звуку, після чого вони відбиваються в залежності від кута (під яким попадають на геометрію) та матеріалу (в який вони потрапили). Після кожного відбиття відбувається збір променів, де вираховується прямий шлях до слухача за допомогою бінарного пошуку. У випадку, якщо шлях знайдений, обчислюється втрата енергії, яка виникає внаслідок дифракції, що є зображено на рис. 1.

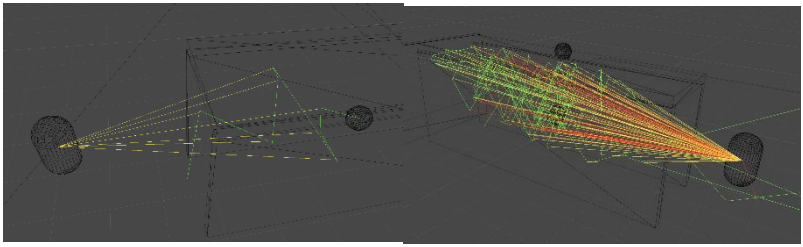


Рис.1. Трасування променів та визначення дифракції (жовті лінії - дифракції, яка доходить до слухача з позитивною енергією, червоні лінії - дифракції, які доходять до слухача з нульовою енергією) для 1 і 20 променів відповідно (8 відбиттів на промінь в обох випадках).

Кожен промінь під час відбиттів зберігає інформацію про те, яку він пройшов відстань, скільки втратив енергії під час взаємодії з матеріалами, а також свій шлях у вигляді послідовності елементів, від яких було здійснене відбиття. Відстань і втрата енергії від взаємодії з матеріалами необхідні для того, щоб визначити зміну в коливаннях тиску при проходженні звуку через повітря в децибелах. Отриманий результат зберігається для конкретно пройденого шляху. Під час трасування наступних променів, можна натрапити на промінь, який відбиватиметься по такому ж шляху, як і попередній промінь. В такому випадку відбирається промінь, який має більшу енергію. Отримавши інформацію про тиск на різних шляхах променів

результати додаються, щоб отримати фінальне значення тиску на відповідній частоті.

Оскільки промені випускаються в випадковому напрямку, то велика кількість променів не доходять до слухача. Для оптимізації використовується трасування центрального променя напряму від джерела до слухача. За допомогою цього отримується результат про тиск на відповідній частоті і використовувати при цьому меншу кількість променів.

В подальшому звук розбивається на 10 проміжків частот за допомогою Csound[3] використовуючи buterbp opcode [4]. На кожній частоті трасування променів відбувається окремо, що є зображено на рис. 2. Після збору інформації про коливання тиску на різних частотах інформація в реальному часі відправляється в Csound для того, щоб приглушити чи навпаки підсилити відповідні звук на відповідних частотах.

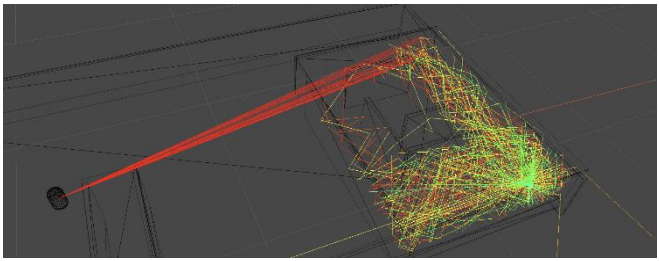


Рис.2. Трасування променів одночасно на різних частотах (колір променів відповідають частоті звуку)

Оскільки в кожному промені є збережена інформація про те, яку він пройшов відстань, можна порахувати час за який він дійшов до слухача. Це дає змогу обчислити ревербації на різних частотах. Ця інформація також передається в Csound в реальному часі.

Отримані результати свідчать про ефективність використання даного підходу для симуляції поширення хвиль в реальному часі. Важливо відмітити, при тестуванні програми використовувалось 20 променів, які випускались за 1 кадр для кожного частотного проміжку. За рахунок усереднення значень протягом послідовних кадрів можна досягнути достатньо реалістичних результатів звучання.

1. Ouellet-Delorme, Émile & Venkatesan, Harish & Durand, Emmanuel & Bouillot, Nicolas. Live Ray Tracing and Auralization of 3D Audio Scenes with vaRays. 18th Sound and Music Computing Conference – 2023. – p.1-3.
2. Unity Game Engine. URL: https://unity.com/
3. CSound - Audio Programming Language. URL: https://csound.com/
4. Bilkent Samsurya. Realtime Audio Raytracing and Occlusion in Csound and Unity. ICSC– 2022. – p.2-3.

Побудова нелінійних криптосистем та криптографічних протоколів

УДК 004.056.55

Вєра Тітова[1], Володимир Анікін[2], Наталія Петляк[3]

Хмельницький національний університет, [1]titovav@khmnu.edu.ua, [2]anikin_volodymyr@khmnu.edu.ua, [3]npetlyak@khmnu.edu.ua

Криптографічний захист є одним з найбільш поширених на сьогоднішній день напрямків кібербезпеки та інформаційної безпеки, що має широкий спектр практичного застосування. Дослідження, спрямовані на підвищення стійкості криптосистем та криптографічних протоколів є особливо актуальними в умовах зростаючої кіберзлочинності, активної розвідувальної та диверсійно-підривної діяльності різноманітних організацій, угруповань, спецслужб та навіть військових спецпідрозділів. Одним із способів підвищення стійкості криптографічних систем є використання нелінійних перетворень у процесі шифрування [1].

Запропонована концепція нелінійних криптографічних систем передбачає введення додаткових параметрів в процес шифрування [2].

Нелінійна криптосистема, створена за даною концепцією може містити в собі деяку кількість типових криптоперетворень f, із множини можливих перетворень F. Усі криптоперетворення із множини F повинні приймати однакові за розміром ключі та блоки відкритих даних на вході та повертати однакові за розміром шифровані блоки даних, чим повинна забезпечуватись їх повна взаємозамінність. Кожен із них повинен зберігати рівномірність розподілу при шифруванні та відповідати звичайним критеріям стійкості. Шифрування вхідного блоку даних C використовуватиме додатковий параметр M – модифікатор, окрім криптографічного ключа K. Даний модифікатор буде відігравати роль перемикача, який обиратиме яке криптоперетворення із множини F буде застосоване. У результаті шифрування дана криптосистема утворюватиме множину шифрованих блоків $\overline{C}$, що включатиме варіанти шифротексту для різних модифікаторів шифрування:

$$F = \{f_1, f_2, \dots, f_n\} \quad n \in \mathbb{N} \tag{1}$$

$$\hat{C_M} = f_M(C, K) \quad f \in F \tag{2}$$

$$\overline{C} = \{\hat{C_1}, \hat{C_2}, \dots, \hat{C_n}\} \quad n \in \mathbb{N} \tag{3}$$

Важливу роль в цій схемі також відіграє модифікатор. Теоретично, він може бути публічним, проте найкращих результатів можливо досягнути якщо модифікатори будуть не доступні для аналітика. Найбільш оптимальним способом отримання модифікаторів у нелінійних криптосистемах є генерація на основі деякого алгоритму розгортання гами, сідом якого виступає ключ, або окремий його параметр. Для цього можна застосувати практично будь-який алгоритм розгортання гами, такий як RC4, Salsa20 тощо. Однак для використання генератора для утворення модифікаторів, він повинен відповідати переліку вимог, серед яких: розгортання повинне бути одностороннім, без можливості зворотної дії; повторні розгортання повинні давати ідентичний результати; розгортання повинно бути

криптографічно стійким; розподіл модифікаторів повинен бути рівномірним по всій їх множині.

Перевагою запропонованого підходу є те, що він легко масштабується під будь-які рівні та може бути застосований на рівні протоколу шифрування, без необхідності змінювати конструкцію існуючих криптосистем. У якості криптоперетворень можуть використовуватись вже існуючі криптографічні системи, за умови що у них однакового розміру вхідні та шифровані блоки, ключі, приблизно рівна криптографічна стійкість та їх шифротекст не містить ознак, що вказують на криптосистему, якою він був створений.

Схема побудови нелінійного протоколу шифрування буде повністю подібною до схеми нелінійної криптосистеми, за вийнятком того, що криптоперетворення в ній представлені окремими криптосистемами (Рис. 1).

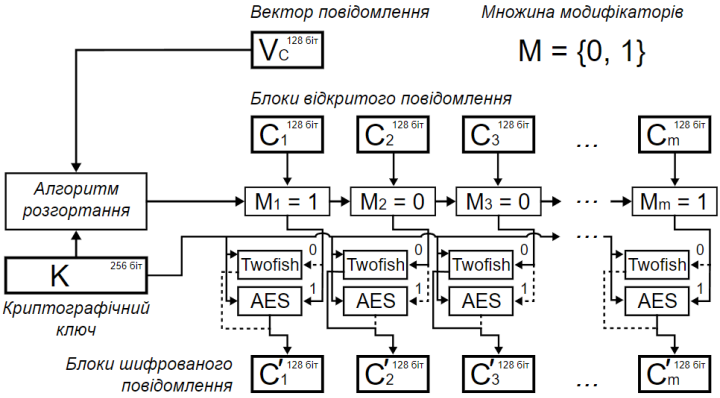


Рис.1. Схема нелінійного полікриптосистемного криптографічного протоколу на прикладі криптосистем Twofish та AES

Загалом, наведена схема нелінійного полікриптосистемного криптографічного протоколу є проста в реалізації, зокрема й через наявність вже готових серійних рішень, із високою швидкістю роботи, для конкретних криптосистем.

Перевагами запропонованої схеми є підвищення криптографічної стійкості, гнучкість та масштабованість запропонованої схеми, використання в своїй структурі готових рішень, без жодної модифікації їх конструкції.

1. Bellare, Mihir, and Phillip Rogaway. "Introduction to modern cryptography." Ucsd Cse 207 (2005): 207.
2. Анікін В.А. Симетрична криптосистема з нелінійним шифруванням та можливістю контролю шифротексту з метою маскування / В. А. Анікін, В. М. Джулій, І.В. Муляр, В.С. Орленко, В.Ю. Тітова // Вісник Хмельницького національного університету. Технічні науки. – 2020. – № 6. – С. 12-19

Розроблення та застосування експлойтів з подальшою інтеграцією в ботнет

УДК 004.738.5

Ростислав Ткачук, Артур Ткаченко, Роман Андріїв

Львівський державний університет безпеки життєдіяльності, rlvtk@ukr.net, tkachenko9720@ukr.net, roman.andriiv@icloud.com

Веб-браузери завжди будуть пріоритетною ціллю для пошуку вразливостей, оскільки ними користується кожна людина. Це означає, що якщо буде знайдена нова вразливість у веб-браузері – це стане ключем доступу до акаунтів дуже багатьох людей та великих потужностей обчислювальних ресурсів. Це дозволить у свою чергу проводити надзвичайно великі та складні кібероперації на зразок розвиненої сталої загрози [1].

Розроблення експлойта для використання ресурсів будь-якого веб-браузера

Наше дослідження зосереджено на пошуку нетипової поведінки та обходу різного роду обмежень в елементі, що міститься в кожному веб-браузері, а саме – JavaScript [2]. Цей експлойт в даній роботі фундаментальний, оскільки без нього всі решта не будуть працювати. Він працює на межі можливостей JavaScript виконуючи функціонал, який не передбачений навіть у відомих бібліотеках, при тому в коді якого не міститься жодної додаткової бібліотеки та використовує такі особливості JavaScript, як спільні змінні між скриптами, у дуже нестандартний спосіб, а саме використовує їх для отримання команд та скриптів із командного сервера, які в подальшому він динамічно розгортає на веб-сторінці. Тобто достатньо запустити один невеликий скрипт, а він може динамічно розгорнутись умовно у 20-30 та більше скриптів.

Це свого роду завантажувальна програма, тіло якої потрібно будь-яким способом запустити на веб-сторінці і яку добре використовувати в атаках типу XSS.

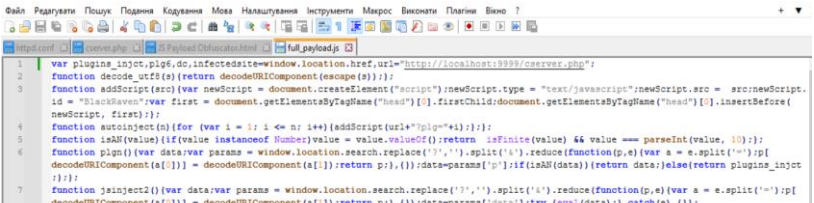


Рис. 1. Експлойт 1

Експлойт для записування всіх натиснутих клавіш на веб-сторінці з відправкою на віддалений сервер

Даний експлойт буде завантажуватися за допомогою попереднього. Він очікує коли нажата будь-яка клавіша і надсилає дані на командний сервер. Для цього було використано нетипове використання функції addEventListener, яка реєструє будь-яке натискання на клавішу, та повертає її код, який потім передається у функцію keylogger. Ця функція в залежності від числа повертає натиснуту клавішу та відправляє її на командний сервер. В ній здійснюється обхід безпеки веб-браузера,

так як у JavaScript закрита функціональність надсилати http/https get запити на сторонні веб-ресурсів, то для обходу цього обмеження було використано нетипове застосування html тега img, який призначений для завантажування зображень, а командний сервер зчитує ці дані і записує їх у файл [3].

Експлойт для проведення DDOS-атак за допомогою веб-браузер та IP-адреси відвідувача веб-сторінки

Цей експлойт аналогічно попереднім використовує спільні змінні між скриптами та спосіб обходу обмежень безпеки веб-браузера на заборону відправки http/https get запитів за допомогою HTML-тега img та iframe.

Після завантаження на веб-сторінці експлойт виконує запуск веб-браузера за допомогою експлойта-завантажувача, після чого він зчитує змінну ціль, яка вказана на командному сервері, зчитує обраний режим для атаки (звичайна http/https get атака, або вдосконалена http/https get атака що викликає помилку 404) та починає атакувати обрану ціль.

Експлойт має функцію створення контейнера із вигаданим HTML-тегом «zlo», в якому знаходиться тег img, або iframe в залежності від обраного типу атаки. Також має функцію самовидалення. Це зроблено для того, щоб у користувача не переповнювалась пам'ять через велику кількість створених тегів та не зависав веб-браузер. Далі ці функції за допомогою SetInterval постійно виконуються у веб-браузері з інтервалом у 0,5 секунди.

Командний сервер та інтеграція корисних навантажень і експлойтів

Для командного сервера потрібен сервер із підтримкою PHP. Тому було обрано Apache 2.4 сервер та PHP 8 версії із стандартними налаштуваннями. Їх потрібно завантажити та встановити на сервер. В нашому випадку це сервер під управлінням Windows Sever 2019 Base у хмарі Amazon (рис. 2).

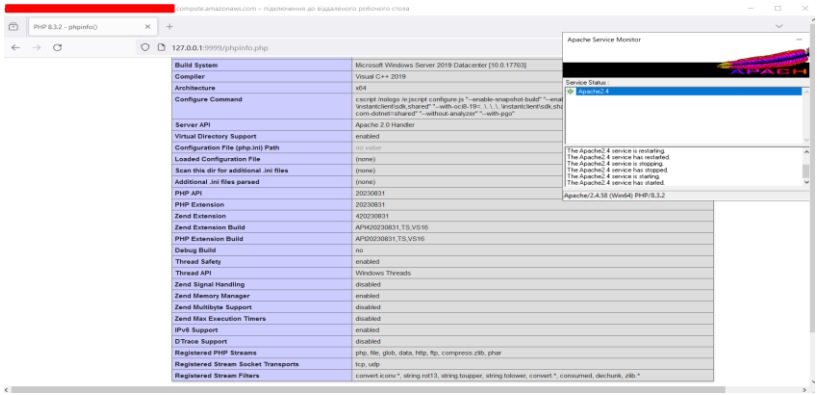


Рис. 2. Встановлений Apache2.4+PHP8

Тепер у папці htdocs необхідно створити конфігураційний файл командного сервера під назвою inject.js. Цей файл є файлом командного сервера, де відбувається управління ботнетом. За допомогою цього файлу можна увімкнути/вимкнути будь-який експлойт, вказати час обновлення команд, створити власний вміст веб-сторінки та зробити дефейс, вказати метод для ddos-атаки, додати власні скрипти.

Далі створюємо php-файл під назвою call.php, який записує дані з кейлогера, інформацію про відвідувача веб-сайту, вести логи, повертає код корисного навантаження та експлойтів завантажувачу, що запускається у веб-браузері, які відвідавши заражену веб-сторінку самі того не знаючи тимчасово стають учасниками ботнету. Цей файл є основою командного сервера.

Далі потрібно встановити проксі-ретранслятор командного сервера, який можна завантажувати на будь-який скомпроментований php-сайт.

Цей файл працює посередником між сервером та клієнтом, через який проходять всі дані і він є невід'ємною частиною командного сервера. Тепер, щоб інтегрувати багатоплатформне корисне навантаження на python достатньо просто створити файл code.txt у папці командного сервера [4] (рис. 3).

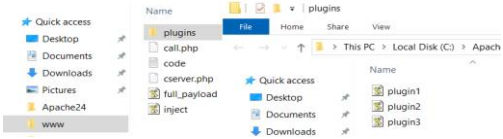


Рис. 3. Вигляд готового командного сервера

Далі необхідно перемістити експлойти у папку plugins під іменами plugin1,2,3 і код із файлу full_payload.js потрібно обробити обфускатором, щоб заплутати код. На цьому інтеграцію експлойтів та багатоплатформного корисного навантаження в ботнет є завершеною.

В роботі розглянута можливість написання простих експлойтів, їхній принцип роботи з подальшим їхнім об'єднанням в ботнет, а саме – створення простого командного сервера ботнета, який керує написаними експлойтами. Це необхідно для того, щоб розуміти як відбувається процес створення вище зазначених речей та як їм протидіяти, оскільки в процесі розробки завжди допускаються помилки, які потім можуть бути використані для проведення атак.

1. Беспалько О., Ткачук Р.Л., Андріїв Р.Р. Дослідження методів захисту інформації веб-сайтів на основі моделей розподілення доступу та моніторингу ідентифікаторів користувача Зб. тез доп. VI Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів "Інформаційна безпека та інформаційні технології". Львів : ЛДУБЖД, 2023.
2. Експлойт [Електронний ресурс] – Режим доступу до ресурсу:https://ukeywaf.com/baza/eksplojt-shho-cze-take/
3. Metasploit Framework [Електронний ресурс] – Режим доступу до ресурсу: https://www.varonis.com/blog/what-is-metasploit
4. Відкритий вихідний код корисного навантаження на python [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/Xehos/Python-Socket-shell/tree/main

Анонімізація користувача в мережі інтернет за допомогою WHONIX

УДК 004.738.5

Ростислав Ткачук, Богдан Філіпчук, Богдана Федина

Львівський державний університет безпеки життєдіяльності, rlvtk@ukr.net, bohdanfil2015@gmail.com, fedynabogdana@gmail.com

Зі зростанням рівня розвитку інформаційних технологій, безпека комп'ютерних систем викликає щораз більше занепокоєння. Розвиток інформаційно-комунікаційних технологій та мережі Інтернет характеризується експоненціальним створенням інформаційних баз і реєстрів з персональними даними користувачів та їх численним дублюванням. Вимоги до ідентифікації суб'єктів є скрізь і стрімко зростають. Фактично ідентифікаційні дані стали стратегічним ресурсом будь-якої держави і потребують відповідного фізичного, технічного та правового регулювання, а також обов'язкового захисту. Для уникнення витоку персональних даних потрібно анонімізовуватися (приховувати свою особистість — використовувати псевдоніми та захищені, прозорі мережі) [1, 2, 9].

Анонімні мережі створені для досягнення анонімності в Інтернеті працюють поверх глобальної мережі. Специфіка таких мереж полягає в тому, що розробники змушені йти на компроміс між ступенем захисту та легкістю використання системи, її «прозорістю» для кінцевого користувача. Багаторівневе шифрування та розподілений характер анонімних мереж, усуваючи єдину точку відмови і єдиний вектор атак, дозволяють зробити перехоплення трафіку або навіть злом частини вузлів мережі не фатальною подією [3-5].

Для відкрито розробленого безкоштовного програмного забезпечення з відкритим вихідним кодом (FOSS), ліцензованого GPL гіпервізора, який може запускати Whonix, рекомендується використовувати віртуальну машину ядра (KVM), яка постачається з ОС GNU/Linux. KVM у поєднанні з Virtual Machine Manager має надавати знайомий, інтуїтивно зрозумілий і простий у використанні графічний інтерфейс. Вона використовує libvirt. Тому виконана на персональному комп'ютері зі засобом віртуалізації та гіпервізором QEMU/KVM [7, 8].

Завантаження образів операційних систем Whonix необхідно робити в захищеному середовищі та завжди перевіряти цілісність файлів. Це необхідно для того, щоб система з самого початку була цілісною і Whonix не був скомпроментований. Скачувати бажано через спеціальне дзеркало в мережі Tor. Для цього необхідно порівняти контрольну суму файлу та хеш суму на сайті [6].

Після перевірки файлів встановлюється гіпервізор з депозитаріїв, якщо він не встановлений, тоді добавляємо користувача до груп, щоб встановити політику безпеки.

Далі необхідно відредагувати конфігураційні файли під потреби користувача, а саме прописати шляхи до машин (рис. 1). Цю операцію необхідно зробити для двох файлів налаштувань.

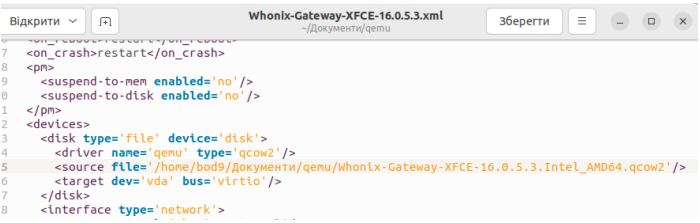


Рис. 1. Конфігураційний файли машини Gateway

Наступним кроком буде добавляння віртуальних мереж, та їх запуск. Також необхідно перевірити, чи утворилися необхідні мости. Після цього добавляємо системи в гіпервізор.

На певних операційних системах необхідно буде виконати додаткові налаштування конфігураційного файлу для коректної роботи систем (рис 2).

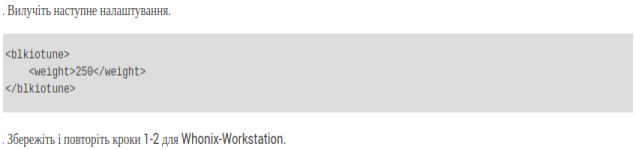


Рис. 2. Зміна конфігурації

Після виконання основних налаштувань (налаштування користувача, політики доступу та зміни паролів), далі налаштовується система під можливості персонального комп'ютера. Після цього можна запускати системи та починати активне їх використання. Дається дозвіл на мережу Tor (без цього дозволу Інтернет не появиться і спосіб не буде працювати). Далі виконуються запити на сайт, їх основна мета це показати IP-адресу (виконується на усіх системах та на персональному комп'ютері).

Після порівняння IP-адреси на системах (Whonix-Workstation [185.14.97.176], Whonix-Gateway [185.241.208.206], Host [93.178.254.150]), практично видно, що схема загортання трафіку в мережу Tor працює відмінно на всіх етапах, тобто анонімізація мережі виконана (рис. 3).

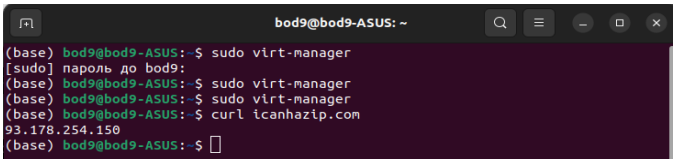


Рис. 3. IP-адрес Host

Таким чином зловмисникам буде дуже складно скомпрометувати систему Whonix-Workstation, тому що сама вона теж загортає трафік в мережу Tor і також шлюз операційної системи Whonix-Gateway теж загортає все в Tor і тому відслідкувати весь шлях інформації надзвичайно складно, отже таким чином ми добилися надійної анонімізації.

У роботі здійснювалося дослідження методу анонімізації за допомогою операційної системи Whonix. У результаті отримано систему, яка забезпечує анонімність власної IP-адреси та DNS (якщо ми його використовуємо), при чому анонімність складається з кількох обгортань в мережу Tor, що дає велику ефективність анонімізації трафіку. Також отримано змогу налаштування дозволів DNS через DNSCrypt та тунелювання UDP, що ще більше покращує анонімність користувача та забезпечує відповідний захист конфіденційних даних та унеможливлює контроль та цензуру свободи слова. Досягнутий результат роботи забезпечує прозоре користування інтернет ресурсами та високий рівень анонімності персонального комп'ютера, що є надійним методом захисту від компрометація локальної комп'ютерної мережі.

1. Anonymity on the Internet Must be Protected Karina Rigby [Електронний ресурс] — Режим доступу до ресурсу: http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall95-papers/rigby-anonymity.html
2. Костенко О. В. Проблеми правового регулювання анонімізації та псевдонімізації [Електронний ресурс] — Режим доступу до ресурсу: https://t1p.de/9b21b
3. Анонімна мережа [Електронний ресурс] — Режим доступу до ресурсу: https://www.wiki.uk-ua.nina.az/%D0%90%D0%BD%D0%BE%D0%BD%D1%96%D0%BC%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0.html
4. Анонімність в Інтернеті [Електронний ресурс] — Режим доступу до ресурсу: https://repair.lviv.ua/anonimnist-v-interneti/
5. Філіпчук Б., Ткачук Р.Л., Репетило Т.Б. Потенційні вразливості брандмауера. Зб. тез доп. IV Міжнародної науково-практичної конференції “Інформаційна безпека та інформаційні технології”. (м. Львів, 30 листопада 2022 р.). Львів : ЛДУБЖД, 2022. С. 111-114.
6. How Does Whonix Make Kali Linux Anonymous & How to Prevent It? [Електронний ресурс] — Режим доступу до ресурсу: https://cybersecurity.att.com/blogs/security-essentials/how-does-whonix-make-kali-linux-anonymous-how-to-prevent-it
7. Whonix [Електронний ресурс] Режим доступу до ресурсу: https://cybersecurity.att.com/blogs/security-essentials/how-does-whonix-make-kali-linux-anonymous-how-to-prevent-it
8. Who uses Whonix ™ [Електронний ресурс] — Режим доступу до ресурсу: https://www.whonix.org/wiki/Users_of_Whonix
9. Мельцов В. В., Ткачук Р. Л. Організація захисту сайту створеного за технологіями: MONGODB, ANGULAR 12, HTML5, CSS3, JAVASCRIPT, NESTJS. Збірник тез доповідей VIII Всеукраїнської заочної науково – практичної конференції “Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України” (м. Київ, 28 квітня 2022 р.). Київ, НПУ імені М.П. Драгоманова, 2022. С. 84–85.

Маркери компетентності персоналу критичної інфраструктури.

УДК 004.9:621.39

Ірина Трегубенко

ДержНДІ технологій кібербезпеки, wr.irttri@gmail.com

Основною складовою забезпечення кібербезпеки та захисту критичної інформаційної інфраструктури України є рівень професійної підготовки відповідних фахівців. Держспецзв'язку України формує ефективну систему професіональної кваліфікації в галузі кібербезпеки та захисту інформації, що в першу чергу необхідно для забезпечення захисту критичної інформаційної інфраструктури держави. Вже зафіксовано 27 професій галузі кібербезпеки та захисту інформації в Україні які гармонізовано зокрема із рівнями National Initiative for Cybersecurity Education Cybersecurity Workforce Framework NIST 800-181_1r [1]. Розроблено відповідно 21 професійний стандарт [2]. Виникає потреба побудови незалежної та об'єктивної системи контролю професійної компетенції фахівців в галузі кібербезпеки та захисту інформації які задіяні на об'єктах критичної інформаційної інфраструктури держави.

Необхідно щоб така система діяла постійно, оцінювання компетенцій конкретного персоналу для конкретних об'єктів проводилось безперервно у відповідності із швидко змінюваними технологіями та потрібними практичними навичками галузі. Система контролю компетенції повинна бути гнучкою, бути налаштовуванню до потреб конкретного об'єкту та конкретних трудових функцій. Одним із результатів системи має бути визначення персоніфікованого плану навчання певного фахівця.

При оцінці рівня компетентності персоналу необхідно орієнтуватись в першу чергу на практичні навички та на те фундаментальне підґрунтя, на якому вони базуються зараз та на якому можуть розвіватись у майбутньому. Тому не потрібно роботи перекоси типу «тільки практика» або «спочатку уся теорія». Потрібен баланс. Для побудови збалансованого діючого процесу оцінки компетентності, потрібно сформувати систему ознак, яка зможе достовірно описати та виявити певну професійну компетенцію. Такі ознаки, які є значущими та визначальними для рівня професіональної компетенції спеціалістів, будемо називати маркерами компетенції. При умові своєчасного оновлення професійних стандартів із залученням реальних діючих, а не тільки академічних професійних фахівців, цілком можливо за основу побудови маркерів компетенції взяти складові діючих професійних стандартів та посадових інструкції на конкретних об'єктах критичної інфраструктури.

1. Вільям Ньюхаус, Стефані Кіт, Бенджамін Скрібнер, Грег Вітте. Національна освітня ініціатива у сфері кібербезпеки (NICE). Загальні принципи управління персоналом у сфері кібербезпеки. *NIST* : веб-сайт. URL: https://doi.org/10.6028/NIST.SP.800-181r1 (дата звернення 19.04.2024)
2. Ставка на освіту: Україна посилює стійкість у кіберпросторі через професійну підготовку. *Держспецзв'язку* : веб-сайт. URL: https://cip.gov.ua/ua/news/stavka-na-osvitu-ukrayina-posilyuye-stiikist-u-kiberprostori-cherez-profesiinu-pidgotovku (дата звернення 19.04.2024)

Можливості використання структур на основі бактеріородопсину для високошвидкісної комутації оптичних сигналів та захисту інформації в оптоволоконних лініях

УДК 539.23, 538.958, 004.056.53

Іван Трикур[1], Михайло Січка [2], Олександр Чобаль[3], Галина Різак[4], Василь Різак[5]

ДВНЗ «Ужгородський національний університет» [1]ivan.trikur@uzhnu.edu.ua, [2]mykhaylo.sichka@uzhnu.edu.ua, [3]oleksandr.chobal@uzhnu.edu.ua, [4]galyna.rizak@uzhnu.edu.ua, [5]vrizak@uzhnu.edu.ua

Широке використання оптичних ліній передачі та обробки інформаційних потоків актуалізує питання розробки швидкісних оптичних комутаторів. Крім того використання таких ліній потребує розробки нових методів захисту інформації в них. Один з таких методів, наприклад, передбачає формування спеціальних лінійних кодів, при передачі інформації по оптоволоконним лініям, що значно підвищує захищеність інформації при несанкціонованому доступі до лінійних споруд. Проте, при використанні постійного типу коду, виникає небезпека його перехоплення. Вирішенням проблеми може бути регулярна зміна таких лінійних кодів за псевдовипадковим законом, що потребує, знову ж таки, використання активних пристроїв - оптичних комутаторів. Для забезпечення ефективності роботи, такі комутатори повинні бути надійними, недорогими, мати високу швидкодію, можливість виконання пасивних та активних оптичних елементів в інтегрально-оптичному виді. Розробка механізмів та дослідження нових матеріалів, що можуть бути використані для комутації оптичних сигналів, становить надзвичайно цікаву та актуальну задачу. Одним з елементів, який може бути успішно використаний для комутації оптичних потоків, як у класичних оптичних волокнах так і у планарних хвилеводах, можуть стати плівкові структури на основі бактеріородопсину (БР).

Метою даної роботи є систематизація, аналіз та узагальнення даних про можливості використання матеріалів на основі БР для комутації оптичних сигналів і розробки надійних високошвидкісних оптичних комутаторів.

Бактеріородопсин – фотохромний білок, який за рахунок структурної організації молекул у двомірну гексагональну кристалічну ґратку, демонструє набагато більшу, порівняно з іншими білками, фізичну та хімічну стабільність. Поглинання кванту світла з діапазону 550-630 нм приводить до збудження молекули БР, після чого, через ряд проміжних станів - інтермедіатів, вона повертається у вихідний стан. Для оптичної комутації цікаві інтермедіати J_{610} ($\lambda_{мах}$=610 нм, час переходу $БР_{570}\rightarrow J_{610}$ 0,4-1 пс), K_{590} ($\lambda_{мах}$=590 нм, час переходу $J_{610}\rightarrow K_{590}$ 3-5 пс), L_{550} ($\lambda_{мах}$=550 нм, час переходу $K_{590}\rightarrow L_{550}$ - 1мкс). Для запуску фотоциклу БР достатньо імпульсу світла тривалістю 0,6 пс (λ=615 нм, енергія 0,5 мДж). Описані інтермедіати є фотоактивними, тобто при дії світла, довжина хвилі якого відповідає максимуму поглинання даного інтермедіату, БР повертається у вихідну форму, минаючи наступні стадії фотохімічного циклу. Поряд з фотохімічними перетвореннями БР володіє: циклічністю більше 10^6; високою стійкістю до лазерного випромінювання; не має періоду відновлення; відсутній

період прихованого зображення, яке вимагає додаткової хімічної обробки, що спрощує процес запису дифракційної решітки. Плівки на основі БР характеризуються світловою чутливістю 0.1 - 20 мДж/см^2, фотоіндукованими змінами оптичної густини при 570 нм до 95%, показника заломлення – 0,001 - 0,01. На плівках БР можливий запис голографічної решітки. При просторовій частоті 10^3 мм (теоретично можлива просторова частота 10^4 мм), дифракційна ефективність варіюється від 0.4% до 2% (η_{max}=7%), що забезпечує можливість розробки комутаторів, в яких перемикання реалізується за рахунок запису динамічної голограми на плівці БР, яка розташована між комутованими каналами.

С. Корпош з колективом дослідників із університету Нотінгему, продемонстрував можливість повністю-оптичного перемикання з використанням волоконно-оптичних довгоперіодних ґраток (ВОДПҐ) на класичних оптичних волокнах (перехід $БР_{570} \rightarrow М_{412}$), модифікованих БР отриманим в лабораторії УжНУ. Довжина хвилі перемикання в таких структурах визначається періодом ВОДПҐ і, таким чином, може бути адаптована шляхом вибору відповідного періоду ґратки. Ефективність перемикання становила 16±1 і 32±2% для ВОДПҐ і інтерферометра Маха-Цендера, занурених у розчин БР (12 мг/мл), відповідно.

Л. Фабіан з колегами із Сегедського університету продемонстрували можливість надшвидкого повністю оптичного перемикання частоти й амплітуди у планарних хвилеводах з використанням двох фотореакцій (пікосекундного переходу $БР_{570} \rightarrow K_{590}$ і субпікосекундного переходу $БР_{570} \rightarrow J_{610}$) фотоциклу БР. Ефективність перемикання може бути підвищена за рахунок модифікації плівкових структур на основі БР (шляхом хімічної модифікації хромофора або охолодження). Перемикання частоти може бути використане для частотного демультиплексування, найважливішої операції широкосмугових оптичних інформаційних технологій, де широкосмуговий імпульс може бути розділений на кілька вузьких частотних діапазонів, що дозволяє їх незалежне кодування або декодування шляхом переключення амплітуди.

Проведені авторами даної роботи вимірювання фотоіндукованих змін показника заломлення плівок БР вказують на можливість досягнення достатнього динамічного діапазону для здійснення переключень у хвилеводах на основі БР. Математичні розрахунки та аналіз інтегрально-оптичних структур, до складу яких входять плівки БР, дозволили визначити оптимальний тип структури планарного хвилеводу для створення повністю оптичного перемикача з високим динамічним діапазоном: найкраще підходить конструкція у якої при зовнішній засвітці зникає нульова мода і вся енергія з хвилеводу випромінюється через підкладку. Для створення фотоіндукованої зміни показника заломлення плівок бактеріородопсину у волоконно- та інтегрально-оптичних системах можуть бути використані компактні світлодіоди з максимумом випромінювання у видимому діапазоні спектру, де зміни показника заломлення матеріалу є найбільшими. З використанням таких пристроїв технологія повністю оптичної комутації може пересунути нинішню максимальну частоту в кілька десятків ГГц далеко за межі ТГц бар'єру.

Застосування штучних нейронних мереж з радіально-базисними функціями до розв'язування початково-крайових задач

УДК 681.324

Валерій Трушевський

Львівський національний університет імені Івана Франка,
valeriy.trushevsky@lnu.edu.ua

Штучна нейронна мережа (ШНМ) побудована на основі радіально-базисних функцій (РБФ) є універсальним апроксиматором функцій та її можна ефективно застосовувати до розв'язування початково-крайових задач математичної фізики [2]. У загальному випадку початково-крайову задачу можна записати у такому вигляді:

$$\begin{aligned} &L(u) = f,\ u = u(x,t), (t,x) \in \Omega \subset R^n; \\ &B_i(u)\big|_{\Gamma_i} = b_i, u\big|_{t=0} = u_0(x), \partial\Omega = \Gamma = \bigcup_i \Gamma_i, \end{aligned} \tag{1}$$

де n – розмірність простору задачі; , L, B_i – диференційні оператори.

Розв'язок задачі (3) шукається у вигляді

$$u(t,x) = \sum_{i=1}^{m} w_i \varphi_i(t,x), \tag{2}$$

де φ_i – радіальні базисні функції, w_i – вагові коефіцієнти мережі.

Схематично структуру нейронної мережі на основі РБФ зображено на рис.1

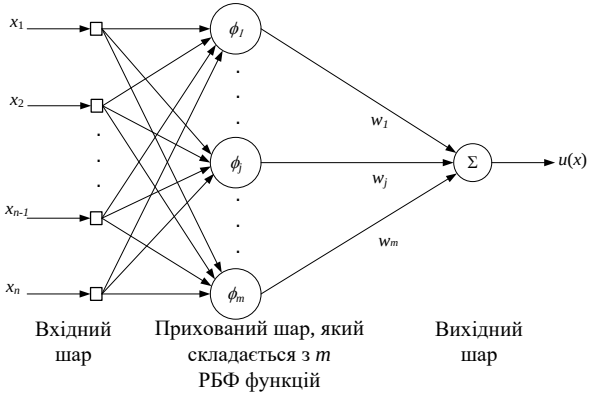


Рис.1. Структура нейронної мережі на основі РБФ

Кожен i-й нейрон РБФ-мережі виконує нелінійне перетворення, яке характеризують такі параметри: $c_i = (c_{1i}, c_{2i})$ – центр та a_i – ширина. Для побудови мережі будемо використовувати РБФ типу Гауса (Gaussian).

$$\varphi_i(t,x) = exp\left(-\frac{(t-c_{1i})^2+(x-c_{2i})^2}{a_i^2}\right), \tag{3}$$

Навчання мережі зводиться до знаходження невідомих параметрів w_i, c_i, та a_i. за рахунок мінімізації функціоналу похибки:

$$E(u) = \int_{\Omega} |L(u) - f|^2 d\Omega + \sum_i \int_{\Gamma_i} \delta_i |B_i(u) - b_i|^2 d\Gamma \quad (4)$$

де $\delta_i > 0$ – штрафні множники, які відповідають за виконання крайових умов на відповідних частинах границі.

Для навчання мережі використовується градієнтний алгоритм [2] мінімізації функціонала E шляхом налаштування ваг w_i, центрів c_i та ширин a_i.

У даній роботі розглянуто ефективність застосування нейронної мережі на основі РБФ до розв'язування одновимірної задачі стоку мілкої води у кінематичному наближенні [1]. Застосовано різні методики навчання мережі: 1) навчальна вибірка не змінюється протягом навчання; 2) протягом процесу навчання відбувається додавання нових нейронів у вузли де функціонал похибки досягає максимального значення; 3) через задану кількість кроків проводиться зміна навчальної вибірки з метою забезпечення незалежності нейронної мережі від вхідних даних.

Отримані числові результати свідчать про ефективність застосування РБФ мереж до розв'язування нелінійних задач стоку мілкої води. Важливо відмітити, що при великих значеннях чисел Рейнольдса потоки та їх градієнти різко змінюються, в результаті чого отриманий розв'язок задачі за методом скінченних елементів втрачає свою стійкість та з'являються "паразитичні" осциляції [2]. Для їх усунення багатьма авторами запропоновані різні протипотокові схеми МСЕ. На противагу цьому нейронна мережа здатна врахувати тонкі прошарки області де розв'язки різко змінюються та результати не потребують згладжування.

Важливим моментом для реалізації алгоритмів навчання ШНМ є розпаралелення процесів обчислень. Розроблено програмне забезпечення на мові C++ з використанням відкритого стандарту OpenMP. Розпаралелення процесів відбувається на етапах обчислення часткових похідних функціоналу E (4) для кожного нейрона. Загальна кількість потоків обчислення дорівнює кількості ядер процесора. Обчислення похідних для кожної групи нейронів відбувається незалежно в окремому потоці. Такий підхід дає змогу значно зменшити час навчання мережі.

1. Венгерський П., Трушевський В. Застосування нейронної мережі до розв'язування задачі стоку мілкої води у кінематичному наближенні. Міжнародна наукова конференція "Сучасні проблеми прикладної математики та інформатики" (APAMCS-2019) 24 - 27 вересня 2019 року, Львів.– С. 206-208.
2. Трушевський В., Шинкаренко Г., Щербина Н. Метод скінченних елементів і штучні нейронні мережі: теоретичні аспекти та застосування: монографія. – Львів: ЛНУ ім. І. Франка.–2014. – 396 с
3. Трушевський В., Шинкарнко Г. Розпаралелена апроксимація еліптичних крайових задач штучною нейромережею з радіально-базисними функціями. Вісник Університету.– 2014. – Вип. 22.– С. 108-117

Використання штучного інтелекту для виявлення та запобігання атакам соціальної інженерії

УДК 004.056

Ірина Удовик[1], Володимир Гнатушенко[2]

Національний технічний університет «Дніпровська політехніка»,
[1] udovyk.i.m@nmu.one, [2] vvgnat@ukr.net

Сучасне інформаційне середовище надзвичайно вразливе перед соціально-інженерними атаками, що стають все більш вдосконаленими та складними. Ці атаки включають в себе маніпулювання людським фактором, здебільшого через психологічні та соціальні методи, з метою отримання несанкціонованого доступу до інформації або систем. Діяльність зі сторони зловмисників може варіюватися від підманювання персоналу до надання конфіденційної інформації або навіть крадіжки ідентифікаторів доступу. Рівень ризику значно зріс через стійкий тренд до дистанційної зайнятості та складну геополітичну обстановку, де кібератаки стають інструментом економічного та політичного тиску. Зокрема, мають місце масові DDoS-атаки на критичну інфраструктуру. З розвитком штучного інтелекту зростає його здатність створювати обманливий та індивідуально налаштований контент за допомогою соціальної інженерії. Тому важливо підкреслити необхідність кібербезпеки у соціальних медіа та покращити інструментарій, яким автоматизовані програми виявляють атаки соціальної інженерії. У зв'язку з цим, розробка ефективних методів захисту від соціально-інженерних атак є надзвичайно важливою.

Метою дослідження є розробка концептуальної моделі з використанням штучного інтелекту, яка забезпечить ефективну синергетичну перспективу для опису соціально-інженерної атаки.

Соціально-інженерні атаки представляють серйозну загрозу безпеці інформаційних систем, оскільки вони використовують людський фактор як вразливість [1, 2]. Зловмисники можуть використовувати різноманітні техніки, такі як фішинг, техніки маніпулювання та ін. (в тому числі Baiting, Honey Trap, Scareware, Water Holing, Quid pro Quo). Багато з таких атак є досить субтельними та складними для виявлення, оскільки вони не використовують технічні методи, а замість цього вдаються до маніпулювання людьми [1]. Найпоширеніший приклад соціальної інженерії – це фішинг. Атаки фішингу, як правило, полягають у тому, що зловмисник надсилає електронний лист або повідомлення, яке здається відомим джерелом, таким як банк або відома компанія, і просить отримувача натиснути на посилання або завантажити вкладення. Посилання або вкладення можуть вести на фальшивий веб-сайт або завантажити шкідливе програмне забезпечення на пристрій потерпілого. Після цього зловмисник використовує цю інформацію, щоб викрасти інформацію, таку як дані для входу, або інфікувати пристрій потерпілого шкідливим програмним забезпеченням.

Технології, такі як машинне навчання та штучний інтелект, ймовірно, зроблять атаки соціальної інженерії ще більш ефективними та агресивними [3]. Соціальна інженерія розвивається в серйозну, універсальну та постійну загрозу безпеці. Кіберзлочинці використовують генеративний штучний інтелект для зламування паролів, витоку конфіденційної інформації та обману на різних платформах. Хоча

чат-боти та інші автоматизовані системи зробили великі кроки в ідентифікації та зменшенні різних типів зловмисних дій, завжди є місце для покращень. Адресація джерела атак соціальної інженерії може забезпечити більш комплексну стратегію захисту.

На сьогодні існують різноманітні підходи та методи для захисту від соціально-інженерних атак. Їх виявлення та запобігання вимагають комплексного підходу, який включає в себе навчання персоналу, використання технологічних засобів захисту та постійний моніторинг та аналіз середовища. Вирішення цієї проблеми вимагає спільних зусиль соціальних, технічних та організаційних аспектів інформаційної безпеки. Особливо складно аналізувати веб-додатки через їхню різноманітність та широке поширення використання власних практик програмування. Тому вважаємо ефективним використання машинного навчання в веб-середовищі, оскільки воно може викрити людське розуміння семантики веб-додатків для автоматизованих засобів аналізу.

Нами запропоновано модель на основі штучного інтелекту, що спрямована на виявлення та запобігання атакам соціальної інженерії, особливо фішингу. Дослідження детально розглядає людські наслідки та заходи по протидії атакам соціальної інженерії та дозволяє виявити та оцінити вплив таких атак, спричинених штучним інтелектом, шляхом імітації людських взаємодій та використання алгоритмів глибокого навчання. Побудовану модель було протестовано на практиці за декількома сценаріями. Було оброблено дані, зібрані з взаємодій учасників з чат-ботом, що дало змогу оцінити ефективність та наслідки цих атак. Крім того, створення та застосування чат-бота, підтриманого алгоритмом глибокого навчання, дозволило визначити, як кіберзлочинці можуть використовувати штучно створені інструменти для соціально-інженерних атак. Взаємодія чат-бота з соціальними мережами, такими як Facebook, WhatsApp та Telegram, дозволила провести дослідження потенційних шляхів атаки, що використовують зловмисники. Таким чином використання штучного інтелекту підвищує можливості реального часу для аналізу, виявлення загроз та реагування, сприяючи більш надійніому захисту проти атак соціального інженерії.

1. Basha G., Mahitha Thakur Sai, Priya T., Patnaik S., 2023. Social engineering in cyber security: effect mechanisms, human vulnerabilities and attack methods. Turkish Journal of Computer and Mathematics Education. 14, 2 (May 2023), 561–570. DOI:10.17762/turcomat.v14i2.13686.
2. Syafitri W., Shukur Z., Mokhtar U.A., Sulaiman R. and Ibrahim M.A., Social Engineering Attacks Prevention: A Systematic Literature Review, in IEEE Access, vol. 10, pp. 39325-39343, 2022, doi: 10.1109/ACCESS.2022.3162594.
3. Falade, Polra. (2023). Decoding the Threat Landscape: ChatGPT, FraudGPT, and WormGPT in Social Engineering Attacks. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 185-198. DOI:10.32628/CSEIT2390533.

Використання стеганографії для забезпечення безперервності бізнес-процесів у банківських системах: аналіз ризиків і стратегій захисту

УДК 004.056.5

Олександр Уманський[1], Олександр Мілов[2]

Національний Технічний Університет «Харківський політехнічний інститут»
[1]oleksandr.umanskyi@cs.khpi.edu.ua, [2]oleksandr.milov@khpi.edu.ua

У сучасному цифровому світі значення безперервності бізнес-процесів у банківському секторі важко переоцінити, особливо для України, яка зіткнулася з викликами воєнного часу. Регулярні кібератаки, які веде країна-агресор, ставлять під загрозу стабільність не лише окремих фінансових установ, а й усієї економічної системи країни. В таких умовах, кібербезпека перетворюється з одного з аспектів банківської діяльності на основу її стійкості та надійності. Стеганографія, як метод приховування інформації у цифрових зображеннях, пропонує витончений і ефективний спосіб захисту даних. Ця техніка не лише дозволяє зберігати конфіденційність інформації, але й виступає як додатковий бар'єр на шляху несанкціонованого доступу до неї. У цьому контексті, застосування стеганографії у банківській сфері України відкриває нові можливості для забезпечення неперервності бізнес-процесів, підвищуючи захист від кіберзагроз, які постійно еволюціонують і стають все більш складними.

Мета роботи – продемонструвати потенціал стеганографії як інструменту кіберзахисту, з огляду на її здатність приховувати важливу інформацію від потенційних загроз. Необхідно у теоретичному плані оцінити ефективність стеганографії та на практиці перевірити її можливості через розробку моделей і методів, які можуть бути впроваджені у банківські системи для посилення їх безпеки. З огляду на постійно зростаючі кіберзагрози, особливо в контексті військових дій, такий підхід не просто покращує захист інформації, але й створює стратегічну основу для забезпечення довгострокової стійкості та надійності фінансової системи України. Важливість стеганографії в контексті забезпечення кібербезпеки банківських систем України є незаперечною. Вивчення та впровадження стеганографії не тільки відповідає на потребу в захисті від нинішніх кіберзагроз, але й відкриває нові шляхи для зміцнення національної безпеки в умовах цифрової ери.

В контексті забезпечення безперервності банківських процесів значну увагу приділяється аналізу вразливості інформаційних систем і ефективності механізмів захисту перед обличчям постійно еволюціонуючих кіберзагроз. Серед таких загроз виділяються розширені постійні загрози (APT), які вимагають від системи інформаційної безпеки не лише реактивних, але й прогностичних здібностей. Дослідження, як от робота Islam та ін. (2022), демонструють, що DDoS-атаки є значною загрозою для інформаційної безпеки в банках, акцентуючи на важливості розробки машинного навчання моделей для їх виявлення в моніторингових системах банківського сектору [1].

З іншого боку, Zimba (2022) вказує на шкідливе програмне забезпечення (malware) як на один із найбільш пріоритетних способів кібератак проти банків та

інших фінансових інституцій, зазначаючи, що malware досягло нових рівнів еволюції, включно з використанням шифрованих вантажів та технік обфускації, що ускладнює його виявлення [2].

Надзвичайно популярні кібератаки в банківській сфері – це фішинг, кіберсталкінг, хакінг, XSS та DDoS. Hasan та Al-Ramadan (2021) підкреслюють розмаїття методів, якими користуються кіберзлочинці для порушення безпеки фінансових установ [3]. Водночас, Revenkov та ін. (2021) та Tariq (2018) підтверджують, що фішинг залишається одним із найпоширеніших методів вчинення шахрайських дій, оскільки він дозволяє красти паролі та інші конфіденційні дані, обманом виманюючи їх у жертв [4, 5].

Зазначені дослідження наголошують на важливості не лише реагування на вже відомі загрози, але й на необхідності розвитку новітніх технологій для прогнозування та запобігання майбутнім атакам, підкреслюючи складність та динамічність кіберзагроз, з якими зіштовхуються банківські системи.

Для аналізу можливостей застосування стеганографії у забезпеченні безперервності банківських бізнес-процесів необхідно, перш за все, використовувати релевантний теоретичний підхід. Основою методології є критичний огляд існуючих досліджень у галузі кібербезпеки та стеганографії, з метою ідентифікації найефективніших стеганографічних методів, які можуть бути адаптовані для захисту інформаційних ресурсів в банківській сфері.

Аналіз літератури необхідно поєднати з математичним моделюванням, що дозволиять визначити потенційні сценарії використання стеганографії в рамках банківських систем. Такий підхід включає оцінку сумісності стеганографічних методів з існуючими технологіями та їх потенціал для зниження ризику втрати даних або несанкціонованого доступу.

Для підтвердження теоретичних припущень слід розглянути використання сценарного аналізу, що допомагає моделювати реакцію банківської системи на введення стеганографічних елементів захисту. Сценарний аналіз спрямований на ідентифікацію можливих викликів та переваг використання стеганографії, з урахуванням різних рівнів загроз та атак.

Важливою частиною методології є також розробка рекомендацій щодо інтеграції стеганографії у комплексні системи захисту інформації банківських інституцій. Ці рекомендації базуватимуться на аналізі отриманих теоретичних та модельних даних, з метою надання практичних напрямків для ефективної реалізації стеганографії як частини загальної стратегії кіберзахисту [6,7].

Таким чином, методологія передбачає використання інтегрованого підходу, що поєднує теоретичне дослідження та аналітичне моделювання, з метою визначення найбільш перспективних шляхів використання стеганографії у банківській сфері. Цей підхід дозволяє не лише виявити потенційні переваги та обмеження стеганографії, але й розробити конкретні рекомендації щодо її ефективного впровадження та використання як інструменту підвищення безпеки банківських інформаційних систем.

Такий підхід вимагає ретельного вибору джерел, а також критичного аналізу існуючих досліджень у цій області, щоб забезпечити актуальність і об'єктивність рекомендацій. Врахування широкого спектру думок і досліджень сприятиме глибшому розумінню теми та забезпеченню високої якості кінцевих висновків.

Попередні дослідження показують, що впровадження стеганографічних механізмів може значно ускладнити виявлення конфіденційної інформації з боку неавторизованих осіб. Використання вейвлет-перетворень для застосування цифрових водяних знаків прогнозується ефективним в запобіганні несанкціонованого доступу до даних без істотного впливу на продуктивність системи. Однак, важливим є додатковий аналіз можливості адаптації таких методів до масштабних реальних банківських систем і визначення оптимального балансу між ступенем приховування інформації та легкістю її регулярного використання системами банку. Необхідно враховувати, що збільшення складності процедур захисту не має заважати ефективності та швидкості банківських операцій.

В подальшому дослідження покликані зосередитися на ретельному аналізі стеганографічних технік з точки зору стійкості до сучасних методів криптоаналізу. Зокрема, необхідно проаналізувати вплив квантових обчислень та машинного навчання на здатність стеганографії приховувати дані, а також розробляти стратегії адаптації та вдосконалення відповідно до нових викликів. Окрім того, слід розглянути імплементацію стеганографії у багатошарову модель безпеки, де вона виступає як один із елементів комплексного захисту інформаційних активів.

При інтеграції стеганографії в системи банківської безпеки необхідно враховувати не тільки технічні, але й соціальні та організаційні аспекти. Стеганографія може вимагати значних змін у корпоративних стандартах та навчанні персоналу для ефективного впровадження. Правові аспекти, такі як дотримання GDPR та інших нормативно-правових актів, також відіграють ключову роль у процесі адаптації стеганографії.

Необхідно прийняти до уваги потенційні ризики, такі як використання стеганографії для неетичних цілей, і необхідність розробки ефективних засобів виявлення таких зловживань. Важливо обговорити стратегії забезпечення прозорості та підзвітності при використанні стеганографії у фінансових системах, щоб гарантувати, що ці технології використовуються на користь організації та її клієнтів.

Загальний висновок щодо запропонованого підходу полягає у наступному. Стеганографія пропонує обнадійливий підхід до забезпечення безпеки банківських бізнес-процесів, вносячи новий вимір у захист конфіденційної інформації. Її здатність приховувати існування даних може стати вирішальним фактором у протидії розширеним кіберзагрозам, що цілеспрямовано шукають цінну інформацію. Дослідження підтверджують, що, незважаючи на певні виклики в імплементації та потенційні ризики, інтеграція стеганографічних методів у систему загальної кібербезпеки може значно посилити захист інформації.

Враховуючи швидкий розвиток кіберзагроз, робота над вдосконаленням і адаптацією стеганографічних технік повинна тривати. Важливо проводити подальші дослідження щодо стійкості цих методів перед лицем квантових обчислень та розвинутих методів криптоаналізу. Разом із тим, необхідно забезпечити баланс між секретністю і відкритістю, належно розглядаючи етичні, правові та організаційні аспекти стеганографії. Можна константувати, що міцна база наукових знань та добре обґрунтовані стратегії впровадження можуть дозволити стеганографії зайняти міцне місце у відповідях на сучасні та майбутні кіберзагрози в банківській сфері.

1. Islam, U., Muhammad, A., Mansoor, R., Hossain Md, S., Ahmad, I., Eldin, E.T., Khan, J.A., Rehman, A.U., Shafiq, M. Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models. Sustainability, 2022, 14(14): 8374.
2. Zimba, A. A Bayesian attack-network modeling approach to mitigating malware-based banking cyberattacks. International Journal of Computer Network & Information Security, 2022, 14(1): 25-39.
3. Hasan, M.F., Al-Ramadan, N.S. Cyber-attacks and cyber security readiness: iraqi private banks case. Social Science and Humanities Journal, 2021, 5(8): 2312-2323.
4. Revenkov, P.V., Oshmankevich, K.R., Berdyugin, A.A. Phishing schemes in the banking sector: Recommendations to internet users on protection and development of regulatory tasks. Finance: Theory and Practice, 2021, 25(6): 212-226.
5. Tariq, N. Impact of cyberattacks on financial institutions. Journal of Internet Banking and Commerce, 2018, 23(2): 317.
6. Hryshchuk, R., Yevseiev, S. The synergetic approach for providing bank information security: the problem formulation. Ukrainian Scientific Journal of Information Security, 2016, 22(1): 64-74.
7. Yevseiev, S., Milov, O., Aleksiyev, V., Berdnik, P., Voitko, O., Dyptan, V., Ivanchenko, Y., Pavlenko, M., Salii, A., Yarovyy, S. Development of the interacting agents behavior scenario in the cyber security system. Eastern-European Journal of Enterprise Technologies, 2019, 5/9(101): 46–57.
8. Construction methodology of information security system of banking information in automated banking systems : monograph – Vienna.: Premier Publishing s.r.o., 2018. – 284 p.

Методи та моделі оцінки уразливості інформації в мережах зв'язку

УДК 004. 056

Володимир Хорошко, Олександр Лаптєв, Наталія Вишневська, Абдуллах Аль-Далваш

Національний авіаційний університет professor_va@ukr.net, nataliia.vyshnevska@npp.nau.edu.ua

Уразливість інформації є подія, що виникає як результат такого збігу обставин, коли в силу якихось причин використовувані в автоматизованих системах обробки даних засоби захисту не в змозі надати достатньої протидії прояву факторів, що дестабілізують, і небажаного їх впливу на інформацію, що захищається. Модель уразливості інформації у мережах зв'язку у загальному вигляді показано на рис. 1.

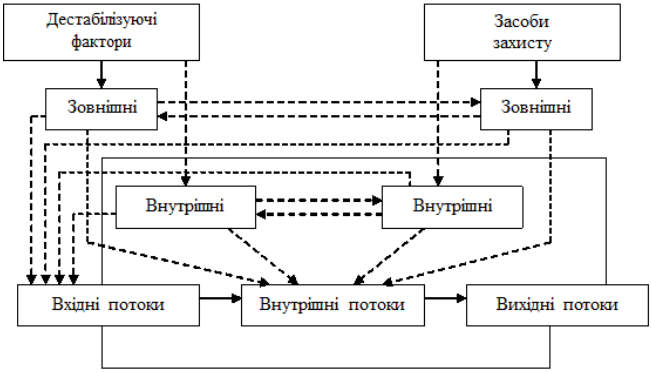


Рис. 1. Загальна модель впливу на інформацію

Ця модель деталізується щодо конкретних видів уразливості інформації: порушення фізичної чи логічної цілісності, несанкціонованої модифікації, несанкціонованого отримання, несанкціонованого розмноження.

При деталізації загальної моделі основна увага акцентується на тому, що переважна більшість порушень фізичної цілісності інформації має місце у процесі її обробки на різних ділянках технологічних маршрутів. У цьому цілісність інформації залежить тільки від процесів, які відбуваються об'єкті, а й від цілісності інформації, що надходить з його вхід. Основну небезпеку становлять випадкові дестабілізуючі фактори (відмови, збої та помилки компонентів автоматизованих систем обробки даних), які потенційно можуть проявитися у будь-який час, і щодо цього можна говорити про регулярний потік цих факторів. Зі стихійних лих найбільшу небезпеку становлять пожежі, небезпека яких більшою чи меншою мірою також є постійною. Небезпека побічних явищ практично може бути зведена нанівець шляхом належного вибору місця для приміщень автоматизованої системи обробки даних та їх обладнання. Щодо зловмисних дій, то вони пов'язані головним чином з несанкціонованим доступом до ресурсів автоматизованої системи обробки даних. При цьому найбільшою небезпекою є занесення вірусів.

Відповідно до викладеного, загальна модель процесу порушення фізичної цілісності інформації на об'єкті автоматизованої системи обробки даних представлена на рис. 2.

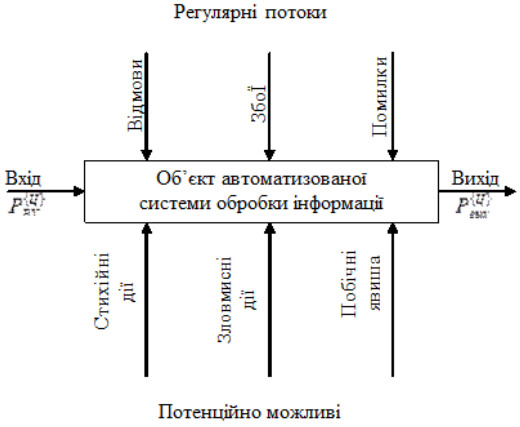


Рис. 2. Загальна модель процесу порушення фізичної цілісності інформації

З точки зору несанкціонованого отримання інформації принципово важливою є та обставина, що в сучасних автоматизованих системах обробки даних воно можливе не лише шляхом безпосереднього доступу до баз даних, а й багатьма шляхами, які не потребують такого доступу. При цьому основну небезпеку становлять зловмисні дії людей. Вплив випадкових факторів безпосередньо не веде до несанкціонованого одержання інформації, воно лише сприяє появі каналів несанкціонованого одержання інформації, якими може скористатися зловмисник.

Розглянемо трансформацію загальної моделі вразливості з погляду несанкціонованого розмноження інформації. Принциповими особливостями цього процесу є:

• будь-яке несанкціоноване розмноження є зловмисною дією;

• несанкціоноване розмноження може здійснюватися в організаціях-розробниках компонентів автоматизованої системи обробки даних, безпосередньо в автоматизованій системі обробки даних та сторонніх організаціях, причому останні можуть отримувати носій, з якого робиться спроба зняти копію як законним, так і незаконним шляхом.

У процесі розвитку теорії та практики захисту інформації сформувався методологічний підхід до оцінки вразливості інформації: емпіричний, теоретичний і теоретико-емпіричний.

Емпіричний підхід до оцінки уразливості інформації в мережах зв'язку

Сутність емпіричного підходу полягає в тому, що на основі тривалого збору та обробки даних про реальні прояви загроз інформації та про розміри того збитку, який при цьому мав місце, суто емпіричним шляхом встановлюються залежності

між потенційно можливим збитком та коефіцієнтами, що характеризують частоту прояву відповідної загрози. і значення розміру шкоди, що мав при її прояві.

Найбільш характерним прикладом моделей розглянутого різновиду є моделі, розроблені фахівцям американської фірми IBM. Розглянемо підходи, що розвиваються на цих моделях.

Вихідним посилом розробки моделей є майже очевидне припущення: з одного боку, у разі порушення захищеності інформації завдається певні збитки, з іншого – забезпечення захисту інформації пов'язані з витрачанням коштів. Повна очікувана вартість захисту може бути виражена сумою витрат на захист та втрат від її порушення. Цілком очевидно, що оптимальним рішенням було б виділення на захист інформації засобів, що мінімізують загальну вартість робіт із захисту інформації.

Для того, щоб скористатися цим підходом до вирішення проблеми, необхідно знати (або вміти визначати), по-перше, очікувані втрати при порушенні захищеності інформації, а по-друге, залежність між рівнем захищеності та засобами, що витрачаються на захист інформації.

Вирішення першого питання, тобто оцінки очікуваних втрат при порушенні захищеності інформації, принципово може бути отримано лише тоді, коли йдеться про захист промислової, комерційної та подібної до них таємниці, хоча і тут зустрічаються дуже серйозні труднощі. Щодо оцінки рівня втрат при порушенні статусу захищеності інформації, що містить державну, військову та їм подібну таємницю, то тут досі суворих підходів до їх отримання не знайдено. Ця обставина істотно звужує можливу область використання моделей, заснованих на підходах, що розглядаються.

Для визначення рівня витрат, що забезпечують необхідний рівень захищеності інформації, необхідно принаймні знати, по-перше, повний перелік загроз інформації, по-друге, потенційну небезпеку для інформації для кожної загрози і, по-третє, розміри витрат, необхідних для нейтралізації. кожній із загроз.

Оскільки оптимальне вирішення питання про доцільний рівень витрат на захист полягає в тому, що цей рівень повинен дорівнювати рівню очікуваних втрат при порушенні захищеності, достатньо визначити лише рівень втрат. Фахівцями фірми IBM запропоновано наступну емпіричну залежність очікуваних втрат від *i*-ї загрози інформації:

$$R_i = 10^{(S_i + V_i - 4)}, \quad (1)$$

де S_i – коефіцієнт, що характеризує можливу частоту виникнення відповідної *i*-ої загрози; V_i – коефіцієнт, що характеризує значення можливої шкоди при її виникненні.

Сумарна вартість втрат визначається формулою:

$$R = \sum_{V_i} R_i \cdot \quad (2)$$

Таким чином, якби вдалося зібрати достатню кількість фактичних даних про прояви загроз та їх наслідки, то розглянуту модель можна було б використовувати для вирішення широкого кола завдань захисту інформації, причому неважко бачити, що модель дозволяє не тільки знаходити потрібні рішення, а й оцінювати

їхня точність. Щодо України така статистика нині практично відсутня. У США ж, наприклад, збору та обробці зазначених даних велику увагу приділяє ціла низка установ (Стенфордський дослідницький інститут та ін.). В результаті вже отримано досить представницькі дані щодо цілої низки загроз, які можуть бути покладені в основу орієнтовних розрахунків і для інших країн.

Розробка алгоритму оптимізації захищених мереж зв'язку

Велика кількість технічних та економічних параметрів, що впливають на ефективність ТСЗІ, потребує вибору узагальненого техніко-економічного критерію *К* для оптимізації. Відомі способи поєднання технічних та економічних характеристик ТСЗІ (парних критеріїв) не завжди обґрунтовані. Так, найпоширенішим є уявлення узагальненого критерію як деякої функції приватних показників нормованих «ваговими» коефіцієнтами, чи побудова ієрархії приватних критеріїв. Суб'єктивізм у виборі «ваг» і призначення порядку переваги чесних критеріїв істотно обмежує сферу застосування таких методів об'єднання, а використання обмежень не завжди можливе через невизначеність у величині обмеження, що накладається.

Створення будь-якої ТСЗІ має бути виправдане економічно та ефект від її застосування Е повинен перевищувати включення коштів на створення системи *С*. При цьому ТСЗІ слід розглядати як частину складної комплексної системи захисту, яка спільно з рештою складових елементів призначена для досягнення певної мети, яка збігається з метою забезпечення відповідного рівня захищеності інформації в цілому за час її використання. Дійсно, результат будь-якого захисного заходу в кінцевому рахунку виходить для того, щоб використовувати с;о для вирішення поставлених завдань [1]. Тому:

$$K=Э-C, \tag{3}$$

витрати реалізацію системи С визначаються безліччю економічних $\{X_g\}$, $g=\overline{1,Q}$ параметрів (заборони проектування. виготовлення C_i, експлуатацію $Cэ= EcCэгод$ ТСЗІ і каналів зв'язку системи $Cкс= CoZкс$):

$$C=C(X_g)=C_u+T_cC_{эгод}+C_{КС}. \tag{4}$$

Ефективність використання ТСЗІ Е є різницею між величиною ефекту Е*, що визначається при заданих технічних вимогах до захисту об'єкта $Xd \le Xd^*$, та втратами ефективності від неідеальності технічних характеристик ТСЗІ:

$$Э=Э^*-\sum_{f}^{F}\Delta Э_f \cdot \tag{5}$$

Очевидно, що $f \ne d, Д \le F$ і задача оптимізації ТСЗІ з врахуванням (4) і (5) буде мати вигляд:

$$\max K=\max\left\{Э(X^*d)-\sum_{\substack{j=1\\f=2}}^{F,Q}\left[C(X_g)+\Delta(X_f)\right]\right\}. \tag{6}$$

$d=1,\ldots,Д \le F$

$f \ne d$

$$X_d \le X_d^*$$

Узагальнений техніко-економічний критерій (6) є критерієм повних витрат $K^1 = \left(C + \sum_{\Delta} Э\right)$ [2] з обмеженнями на технічні характеристики X_d^*. Параметри X_d^* визначають величину Е* при проведеному передпроектному дослідженні з урахуванням доцільності проектування ТСЗІ взагалі та є обмеженнями при виборі набору технічних засобів ТСЗІ

$$H_\varphi^n = \left\{\{h_i\}\alpha_\varphi^n\right\}; \quad \alpha_\varphi^n = 1,\ldots,\beta_\varphi^n.$$

Безліч технічних засобів H_φ^n відповідає певним параметрам $n = \overline{1,N}$ при заданому законі функціонування системи $\{З\}\varphi,\ \varphi = \overline{1,\phi}$. Для визначення оптимальної ТСЗІ найбільш ефективний шлях перебору набору технічних засобів з розрахунком для кожного з них *max K* або min K^1 відповідно до виразів (4) - (6) згідно з алгоритмом (рис.3).

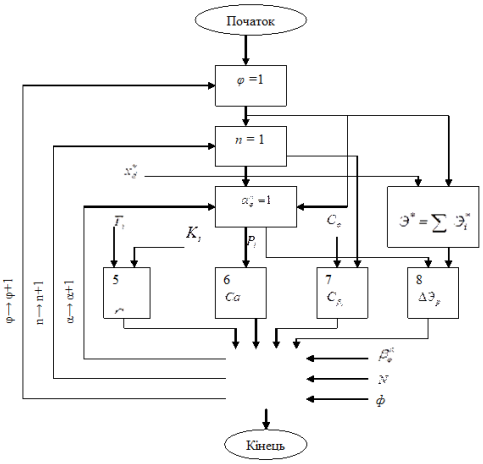


Рис. 3. Алгоритм оптимізації ТСЗІ за узагальненим критерієм ефективності

Алгоритм синтезу оптимальної ТСЗІ є послідовним перебором варіантів за координатами $\alpha_\varphi^n \to n \to \varphi$, причому підцикли оптимізації допускають автономне рішення, що спрощує процес проектування ТСЗІ.

При технічному вдосконаленні ТСЗІ необхідний попередній аналіз залежності $Э\left(X_d^*\right)$, яка може бути отримана в результаті об'єкта захисту. Найбільший вплив на величину Е* надає точність та надійність функціонування ТСЗІ, що характеризується хибними спрацьовуваннями

або перепустками атак на об'єкт. Втрати ефективності визначаються переважно ненадійністю технічних засобів ТСЗІ.

Якщо $Э^* = Э_o \gamma^{-\gamma}$, $C = C_o \delta^{-g}$, $\Delta Э_p = Э^* P$, де γ, g - показники ступеня, що визначаються експериментальним шляхом (цілі, дробові, позитивні), то відповідно до (6) можна знайти оптимальне - доцільне - значення похибки δ_{opt}, виправдане економічно. Так, при γ=1,g=2:

$$\delta_{opt} = \frac{^2 C_o}{Э_{o(1-p)}}.$$

Передбачуваний підхід до вибору критерію ефективності дозволяє обґрунтовано проектувати ТСЗІ та визначати ефективність технічного вдосконалення та модернізації технічних засобів, елементів та вузлів системи.

1. Брайловський М.М., Хорошко О.В. Хорошко В.О., Чирков Д.В. Взаємозв'язок між інформативністю та ефективністю в системах технічного захисту // Захист інформації. 2000. № 1. С. 15-18.
2. Козлова К.В., Хорошко В.О. Кількісна оцінка захисту радіоелектронних об'єктів // Захист інформації, № 1, 2007. С. 30-33.
3. Кудінов В.О., Хорошко В.О. Методика системного проектування корпоративної мережі ОВС України // Захист інформації, № 2, 2005. С. 4-13.
4. Кудінов В.О., Плус Д.В., Хорошко В.О., Чирков Д.В. Методика синтезу оптимальної топології структури корпоративної мережі // Захист інформації, № 1, 2005. С. 12-21.
5. Ланде Д.В. Основи інтеграції інформаційних потоків. К.: Інжиніринг, 2006. 240с.

Моделі векторів атак на кіберполігон кафедри ТЕІБ

УДК 004.256:378.16 (043.2)

Олександр Черепов[1], Юрій Матьовка[2]

Ужгородський національний університет,
[1]oleksandr.cherepov@uzhnu.edu.ua, [2]yurii.matovka@uzhnu.edu.ua

Реалії сучасного світу показують стрімке зростання використання автоматизованих систем, що збільшує ризики спрямованих кібератак атак. Зростаюча складність і інтенсивність кібератак веде до актуальності покращення підготовки спеціалістів у даній сфері з зосередженням у набутті практичних навичок.

Метою роботи є дослідження створення векторів кібератак,а також у моделюванні цих векторів атак,та взаємодії червоної і синьої команди під час проведення тренінгів на базі полігону.

Вектори кібератак на даний полігон базуються на моделі “Cyber Kill Chain”, що запропонований компанією Lockheed Martin. Дана модель є зручною для опису дій кожної команди, що у свою чергу покращує взаємодію членів команд, що беруть участь у тренінгах на кіберполігоні.Її головною перевагою є вербальний опис етапів APT атаки, що є вагомим аргументом при організації тренінгів.

Досить велика кількість є інтерпертацій цієї моделі,що відрізняються ступенем деталізації,межами,а також відмінностями етапів.

Для налагодження початкової стадії роботи з даним полігоном,а саме з вибором програмного забезпечення було проаналізовано декілька варіантів з його отриманням.Найбільш зручним для роботи з даним полігоном є використання віртуальної машини з налаштованим Kali Linux дистрибутивом. Обрання даного варіанту зумовлено тим, що це зменшує час для підготовки симуляцій атак на даний кіберполігон учасниками,а також надає змогу швидко розширюватись при потребах.

Головною проблематикою використання даного полігону є можливості членам команд блокувати роботу іншим, що у свою чергу знижує ефективність тренінгів для учасників команд.Використання даної моделі надає змогу знайти проблематичні місця під час проведення тренінгів.

Результатом роботи є деталізовані інструкції векторів атак на кіберполігон кафедри ТЕІБ,що базуються на моделі “Cyber Kill Chain”. Показано,що дана модель є ефективною для використання у рамках організації роботи взаємодії команд під час проведення тренінгів.

1. E. M. Hutchins, M. J. Clopperty, and R. M. Amin. “Intelligence-Driven Computer Network Defense. Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”, Lockheed Martin Corporation, 2009 URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf. (дата звернення: 12.04.2024)
2. B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, MITRE ATT&CK: Design and Philosophy, McLean, VA, USA: The MITRE Corporation. 2020. URL: https://www.mitre.org/news-

insights/publication/mitre-attck-design-and-philosophy. (дата звернення: 12.04.2024)
3. Best Practices for MITRE ATT&CK. Mapping, Cybersecurity and Infrastructure Security Agency (CISA), 2023.URL: https://www.cisa.gov/sites/default/files/publications/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf (дата звернення: 17.04.2024)

Дослідження застосування JWT (JSON Web Tokens) для забезпечення безпеки у ASP.NET CORE WEB API

УДК 621.395.7 (043.2)

Ждан Чернявський

Державний університет інформаційно-комунікаційних технологій,
zhdancherniavskyi@gmail.com

JWT (JSON Web Token) — це компактний, безпечний спосіб для представлення даних, які можуть бути перевірені та довірені завдяки цифровому підпису. JWT зазвичай використовується для аутентифікації користувачів та передачі інформації про авторизацію між клієнтом та сервером через HTTP у вигляді об'єкта JSON.

Мета дослідження — аналіз ефективності JWT як інструменту для забезпечення безпеки API, розроблених на платформі ASP.NET Core.

Огляд технології JWT — JWT складається з трьох частин: Header: Тип токена (зазвичай JWT) та алгоритм підпису (наприклад, HMAC SHA256). Payload: Містить претензії (claims), які включають інформацію про користувача та інші метадані. Signature: Цифровий підпис, що забезпечує інтеграцію та аутентичність даних.

Використання JWT у ASP.NET Core — В ASP.NET Core JWT використовується через механізми аутентифікації, які вбудовані у фреймворк. Для активації JWT аутентифікації необхідно налаштувати middleware, який декодує та валідує токени на основі секретного ключа та встановлених параметрів безпеки.

Потенційні ризики та вразливості JWT — Хоча JWT забезпечує зручний спосіб для передачі безпечних креденціалів, ця технологія має декілька потенційних ризиків та вразливостей:

- Викрадення токенів: Якщо атакуючий вдасться вкрасти JWT, він може використовувати його для доступу до ресурсів сервера, представляючись користувачем.
- Перехресне сайтове скриптування (XSS): Якщо сайт вразливий до XSS, JWT можуть бути вкрадені через клієнтські скрипти.
- Неналежне зберігання: Небезпечне зберігання JWT на клієнтській стороні може призвести до їх витоку.
- Відсутність поворотної зв'язності (Revocation): JWT не можуть бути відкликані динамічно, що може створити проблеми, якщо потреба в доступі змінюється.

Заходи безпеки:

- Використання HTTPS для захисту передачі токенів.
- Реалізація короткочасних токенів з автоматичним оновленням.

- Забезпечення безпеки за допомогою сучасних заголовків безпеки HTTP, наприклад, **Content-Security-Policy** для боротьби з **XSS.**

Безпека на рівні коду — Програмування безпеки на рівні коду в ASP.NET Core з використанням JWT вимагає дотримання певних практик:

- **Валідація вхідних даних:** Переконатися, що вхідні дані не можуть використовуватися для ін'єкції шкідливих скриптів.
- **Обмеження доступу до HTTP токенів:** Використання HttpOnly cookies для зберігання JWT на клієнтській стороні, щоб запобігти їх доступу через JavaScript.
- **Шифрування токенів:** Додавання додаткового шару захисту шляхом шифрування JWT.

JWT є могутнім інструментом для реалізації безпечної передачі даних і авторизації у веб-додатках, зокрема на платформі ASP.NET Core. Правильне використання JWT може значно підвищити безпеку додатків, але важливо враховувати потенційні ризики і застосовувати комплексні заходи безпеки для запобігання атакам.

1. Parisi A. JSON Web Tokens (JWT) Essentials: Practical Guide for Developers. Birmingham: Packt Publishing, 2021. 176 p.
2. Meyerovich L.A., Rabkin A. Secure and Scalable Web Programming. In: Security and Programming Languages. MIT Press, 2020. pp. 103-128.
3. Atkinson J. Mastering JSON Web Tokens. San Francisco: Apress, 2020. 158 p.
4. Венгерський П.С., Вишневська Н.С., Хохлачова Ю.Є., Хорошко В.О., Чобаль О.І. Кількісна оцінка кіберзахищеності інформації. Захист інформації. – 2023. – Т. 25, №2. – С. 53-61.

Блокчейн для безпеки ідентифікації та автентифікації

УДК 004.056.5:004.738
Віктор Чешун[1], Євген Майор[2], Наталія Купчик[3]

Хмельницький національний університет, [1]cheshunvn@khmnu.edu.ua, [2]evmaior@khmnu.edu.ua, [3]nataliiakupchyk@khmnu.edu.ua

У традиційних системах ідентифікації дані користувачів зберігаються централізовано, що робить ці системи вразливими до кібератак. Замість цього, блокчейн може використовуватися для зберігання ідентифікаційних даних у розподіленій мережі, де кожен блок містить криптографічно захищену інформацію про користувача. Це забезпечує більшу безпеку, оскільки немає одного центрального пункту вразливості.

Технологія блокчейн не зберігає цифрові дані, замість цього у хронологічній послідовності фіксуються всі перевірені транзакції. Ці транзакції об'єднуються в блоки, які в свою чергу утворюють ланцюжки. Спроби змінити або видалити будь-які записи призведе до порушення цілісності ланцюжка блоків.

Основним призначенням цієї технології є захист персональних даних за допомогою криптографії. Після формування транзакційних даних в блоки вони проходять криптографічну перевірку та записуються в базу даних. Усі дані, пов'язані з блокчейном, зберігаються у децентралізованій мережі з високим рівнем захисту. Доступ до цієї мережі здійснюється за допомогою спеціальних криптографічних ключів, що робить неможливим підроблення інформації, яка знаходиться в мережі [1].

Смарт-контракти, подібно до звичайних контрактів, визначають угоду між двома або більше сторонами. Однак смарт-контракти використовують код для використання переваг технології блокчейн, таких як ефективність, прозорість та безпека. Вони можуть автоматизувати процеси завдяки своїй цифровій природі [2].

Покроковий опис роботи смарт-контракту: 1) Перший крок передбачає створення та узгодження між сторонами угоди, що буде закріплена у смарт-контракті; 2) Смарт-контракт встановлює умови його виклику або виконання. Це може бути здійснено автоматично, якщо виконуються певні попередньо визначені умови; 3) На цьому етапі визначається логіка смарт-контракту через програмування. Смарт-контракт складається з комп'ютерного коду, який містить логіку виконання угоди та управління даними; 4) Для забезпечення безпеки та конфіденційності використовується шифрування. Дані передаються та зберігаються у безпечному форматі. Крім того, використовується технологія блокчейну для зберігання даних та підтвердження їх унікальності; 5) Коли виконуються умови, визначені в смарт-контракті, він автоматично виконується. Після виконання смарт-контракту дані обробляються та результати записуються у блокчейн; 6) Після виконання смарт-контракту всі вузли мережі оновлюють свої дані, щоб відобразити новий стан. Зміни в мережі реєструються у блокчейні, і після підтвердження їх не можна змінити або вилучити.

Для поліпшення рівня захисту та перевірки ідентичності задіяне використання унікальних біометричних даних. Ці дані можуть бути використані для надійної аутентифікації особи та її ідентичності. Пропонується інтегрувати біометричні дані

в систему блокчейну з метою забезпечення ще вищого рівня безпеки та конфіденційності.

Дослідження підкреслює важливість використання біометричних даних у контексті блокчейну для покращення систем ідентифікації. Шляхом використання смарт-контрактів у приватній блокчейн-інфраструктурі, дослідники розробили механізм, що спрощує систему біометричної автентифікації обличчя та забезпечує її безпеку. Цей метод демонструє високу продуктивність та ефективність на різних наборах даних, що свідчить про його потенціал для застосування в різних галузях, включаючи IoT [3].

Зберігання біометричних даних тягне за собою правові аспекти, тому використання технології нульового знання (Zero-knowledge proof) може вирішити цю проблему. ZKP - це криптографічний протокол, що дозволяє переконати одну сторону у правильності певного факту, не розголошуючи конкретні дані. У контексті зберігання біометричних даних в блокчейні ZKP використовується для підтвердження достовірності даних без їх розкриття. Користувач генерує докази, що його біометричні дані відповідають певним параметрам, але сторона перевірки не отримує доступ до самого зображення чи даних. Такий підхід забезпечує високий рівень конфіденційності та безпеки при зберіганні чутливих даних в блокчейні.

За допомогою смарт-контрактів на блокчейні можна розробити систему ідентифікації та автентифікації, яка забезпечить користувачам контроль над їхніми особистими даними та приватністю. Ця система дозволить користувачам керувати доступом до своїх ідентифікаційних даних та надавати їх іншим сторонам тільки за власною згодою, що підвищить рівень довіри та безпеки. Використання блокчейну для реалізації цієї системи дозволить забезпечити надійність, унікальність та безпеку даних, а також забезпечить стійкість до зловживань та атак. Такий підхід може бути корисним для різноманітних сфер, включаючи фінанси, медицину, торгівлю та інші галузі, де важливо забезпечити високий рівень захисту особистих даних та конфіденційності.

Інтеграція біометричних даних у систему блокчейну відкриває шлях до надійної та безпечної ідентифікації. Це поєднання забезпечує не лише високий рівень захисту особистих даних, але й відкриває нові можливості для автентифікації та авторизації користувачів. Впровадження цього підходу в системи ідентифікації може мати значний вплив на різні сфери, від фінансів до медицини, сприяючи підвищенню безпеки та конфіденційності особистих даних.

1. Blockchain технології та захист даних. URL: https://newline.tech/blockchain-technology-and-protecting-data-uk/ (дата звернення: 11.04.2024).
2. How smart contracts work with blockchain: A step-by-step guide. URL: https://www.britannica.com/money/how-smart-contracts-work (дата звернення: 11.04.2024).
3. Salem, S.H.G., Hassan, A.Y., Moustafa, M.S. et al. Blockchain-based biometric identity management. Cluster Comput (2023). https://doi.org/10.1007/s10586-023-04180-x

Інтеграція гнучкого управління інформаційною безпекою та ризиками під час розробки програмного забезпечення

УДК 004.056.53

Чура Тарас[1], Чура Назар[2]

Національний університет «Львівська Політехніка»
[1]taraschura@gmail.com, [2]nazar.r.chura@lpnu.ua

Що становить собою Гнучке Управління Безпекою та Ризиками?

Зазвичай управління безпекою передбачає ідентифікацію активів компанії та встановлення політик для їх захисту. Розширюючи це, гнучке управління безпекою втілює постійний, всепроникаючий та просунутий підхід до захисту активів на дрібний рівень. Цей метод включає всіх членів команди на всіх етапах життєвого циклу розробки.

Згідно з ISO 31000, управління ризиками визначається як "вплив невизначеності на цілі". Так само, гнучке управління ризиками - це метод, який постійно ідентифікує, оцінює, вирішує, перевіряє, звітує та контролює вразливості на всіх етапах життєвого циклу. [1]

Три Основні Принципи ГУБР

Хоча ці визначення можуть здатися простими, перехід від традиційного управління ризиками до гнучкої структури вимагає значних змін і спільних зусиль з боку різних відділів та зацікавлених сторін. Фахівцям з безпеки слід прийняти наступні принципи ГУБР для успішної реалізації цих стратегій у всій організації.

ГУБР - Справа Всіх

Хоча фахівці з безпеки та ризиків і надалі гратимуть ключову роль, ГУБР повинен постійно викладатися, використовуватися та перевірятися всіма доступними корпоративними ресурсами, включаючи як людський персонал, так і обчислювальні пристрої на основі штучного інтелекту. Компанії повинні надавати навчання, канали для непокараних звітів та комплексні процеси для підготовки всіх ресурсів до реагування на надходження хвилі кіберзлочинності на основі штучного інтелекту.

Від повноцінних корпоративних керівників до підрядників, постачальників, партнерів, клієнтів та обчислювальних систем, всі ресурси повинні активно брати участь у проактивному захисті корпоративних активів. Використання ресурсів, таких як Центр Команди IBM X-Force, може допомогти командам вдосконалити свої навички реагування на інциденти та кіберзахист.

Постійне, Ітеративне та Інкрементне Впровадження ГУБР

Сучасні практики огляду часто передбачають найм групи експертів для оцінки відповідності різних розгортань вимогам загальних регуляцій, стандартів та

принципів, що може пропустити важливі прогалини в безпеці. Ефективніше для організацій залучати всі свої ресурси для впровадження практик безпеки та ризиків на всіх етапах життєвого циклу, починаючи з фаз планування та початкового стадії до видалення.

Постійне навчання за методологією ГУБР має проводитися для впровадження заходів безпеки та ризиків ітеративним та інкрементним чином. Постійне та всепроникаюче впровадження є ключовим для успіху підходу ГУБР.

Прийняття Рішень ГУБР Зверху Вниз та Знизу Вгору

Ієрархічні організації та суспільства можуть зростати та підтримувати порядок, але вони не можуть адаптуватися до сьогодення, коли децентралізовані, всепроникаючі та розмножуються нові світи все більш руйнівних кібератак - вони просто недостатньо гнучкі.

Фактично, через страх перед покаранням працівники часто уникають повідомлення про потенційні загрози і ризики. Компанії повинні розробляти програми для пошуку помилок, щоб підтримувати та відзначати обговорення гнучкої безпеки та ризиків. Як частина щоденних стендапів ГУБР, команди з безпеки мають тестувати свій код, переглядати архітектуру та оцінювати свою політику патчів в контексті ГУБР. Шляхом забезпечення постійного зворотного зв'язку щодо всіх гнучких дій команди можуть випускати функції вищої якості та вищої цінності за швидшим темпом.

1. Keramati, H., & Mirian-Hosseinabadi, S.-H. (2008). Integrating Software Development Security Activities with Agile Methodologies. 2008 IEEE/ACS International Conference on Computer Systems and Applications (pp. 749 - 754). IEEE.
2. Mougouei, D., Sani, N. F., & Almasi, M. M. (2013). S-Scrum: a Secure Methodology for Agile Development of Web Services. World of Computer Science and Information Technology Journal (WCSIT), 3(1), 15-19.
3. Bob Bruns, (2019). Cybersecurity In An Agile World, https://www.forbes.com/sites/forbestechcouncil/2019/01/02/cybersecurity-in-an-agile-world/?sh=2ad67e091be9

Ітераційні методи типу Ньютона без обчислення оберненого оператора для розв'язування нелінійних рівнянь

УДК 519.6

Степан Шахно[1], Богдан Голуб[2], Юрій Шунькін[3], Михайло Гавдяк[4]

Львівський національний університет імені Івана Франка,
[1]stepan.shakhno@lnu.edu.ua, [2]bohdan.holub@lnu.edu.ua,
[3]yuriy.shunkin@lnu.edu.ua, [4]mykhailo.havdiak@lnu.edu.ua

Нехай задано нелінійне операторне рівняння

$$F(x) = 0, \tag{1}$$

де оператор F визначений на опуклій множині D банахового простору X зі значеннями у просторі Y. Для цього рівняння необхідно знайти $x_* \in D$, для якого $F(x_*) = 0$. Задачі такого типу виникають при моделюванні систем та процесів у різних галузях науки та інженерії. Базовим методом для розв'язування (1) є метод Ньютона

$$x_{n+1} = x_n - F'(x_n)^{-1}F(x_n), \quad n = 0,1,2,\dots, \tag{2}$$

де $F'(x)^{-1}$ позначає обернений оператор до похідної Фреше $F'(x)$ оператора $F(x)$, x_0 – початкове наближення до розв'язку x_*.

Пошук оберненого оператора може бути важким завданням залежно від конкретної ситуації і властивостей. Його знаходження може потребувати значних обчислювальних затрат, особливо якщо розмірність простору велика або якщо оператор має складну структуру. Нелінійність також вводить додаткову складність у розв'язання рівнянь. Нами проведено дослідження ітераційного методу ньютонівського типу, який використовує суму операторів, що містять похідну Фреше $F'(x)$.

Нехай $\mathcal{L}(X,Y)$ – простір лінійних обмежених операторів. Нехай $M \in \mathcal{L}(X,Y)$ та існує обернений оператор для M та $(I - M^{-1}(M - F'(x)))$. Тоді із (2) отримуємо метод вигляду [1]:

$$x_{n+1} = x_n - \left[I - M^{-1}(M - F'(x_n))\right]^{-1} M^{-1}F(x_n), \quad n = 0,1,2,\dots \tag{3}$$

Далі замінимо $\left[I - M^{-1}(M - F'(x_n))\right]^{-1}$ на суму операторів $I + A(x_n) + A^2(x_n) + \cdots + A^k(x_n)$, де k – натуральне число, $A = A(x_n) = M^{-1}(M - F'(x_n))$. Отримаємо метод вигляду:

$$\begin{aligned} x_{n+1} &= x_n - BM^{-1}F(x_n), \\ B &= I + A + A^2 + \cdots + A^k, \end{aligned} \tag{4}$$

де x_0 – початкове наближення до розв'язку задачі (1), M- фіксований лінійний оператор. Метод (4) потребує лише одного обертання лінійного оператора M. У випадку, коли $M = F'(x_0)$, $k = 2$, отримуємо

$$\begin{aligned} x_{n+1} &= x_n - BM^{-1}F(x_n), \\ A &= M^{-1}(M - F'(x_n)), \\ B &= I + A + A^2. \end{aligned}$$

Для чисельного порівняння розглянемо також метод із послідовною апроксимацією оберненого оператора [2]

$$x_{n+1} = x_n - A_n F(x_n),$$
$$A_{n+1} = A_n[2I - F'(x_{n+1})A_n], \quad (5)$$

де A_0 – деяке початкове наближення до оператора A^{-1}, I – одиничний оператор. Проведемо порівняння запропонованого методу (4) із методами (2) та (5) на кількох тестових задачах. Обчислення проводилися, використовуючи 2.4 GHz 8-Core Intel i9.

Приклад 1. Broyden tridiagonal function

$$f_i(x) = (3 - 2x_i) - x_{i-1} - 2x_{i+1} + 1,$$
$$x_0 = x_{n+1} = 0.$$

Таблиця 1.

CPU- час та кількість ітерацій для досягнення розв'язку за заданої точності 10^{-13}

n	x_0	Метод (2)		Метод (4)		
		Час	Ітерацій	Час	Ітерацій	k
6	$(-1,\ldots,-1$	0,03313	6	0,032342	6	8
6	$(-2,\ldots,-2$	0,03971	7	0,052662	7	14
12	$(-2,\ldots,-2$	0,068651	7	0,081608	7	22
30	(-7,…-7)	0,422025	9	0.529229	12	38
30	(-10,…-10)	0.249424	9	0,706828	16	36
100	$(-2,\ldots,-2$	1,223344	7	1,855618	7	14

Час визначено як середнє значення зі 100 повторних виконань у секундах $\times 10^{-3}$. Метод (5) для даного прикладу розв'язку не знайшов.

Приклад 2. Brown almost-linear function

$$f_i(x) = x_i + \sum_{j=1}^{n} x_j - (n+1), \quad 1 \le i < n,$$
$$f_n(x) = \left(\prod_{j=1}^{n} x_j\right) - 1\,.$$

Таблиця 2

Кількість ітерацій для досягнення розв'язку за заданої точності 10^{-13}

x_0	Метод (2)	Метод (4)	$t_2 \ / \ t_4$
$(3,-3,3,-3,3)$	9	11	1,317
$(-3{,}1,-3,-3,-3{,}0)$	10	43	1,117
$(1{,}1,-3,-3{,}1{,}0)$	9	11	1,178
$(1{,}1,-3,-3{,}1)$	7	8	0,832
$(1{,}1,-3,-3{,}1,-3)$	13	18	1,178
$(-3,-3{,}1{,}0)$	9	9	1.211

В табл. 2 t_2 – середній час виконання однієї ітерації за методом (2), t_4 –середній час виконання однієї ітерації за методом (4).

Метод (5) для цієї задачі розв'язку не знайшов. Час визначено як середнє значення зі 100 повторних виконань у секундах $\times 10^{-3}$. Із таблиці 2 видно, що метод (4) потребує менше часу для обчислення нового наближення до розв'язку, проте в залежності від задачі та обраного k може використовувати більшу кількість ітерацій у порівнянні з методом Ньютона.

Приклад 3.

$$f_1(x) = x - 0.1\sin x - 0.3\cos y + 0.4,$$
$$f_2(x) = y - 0.2\cos x + 0.1\sin y + 0.3.$$

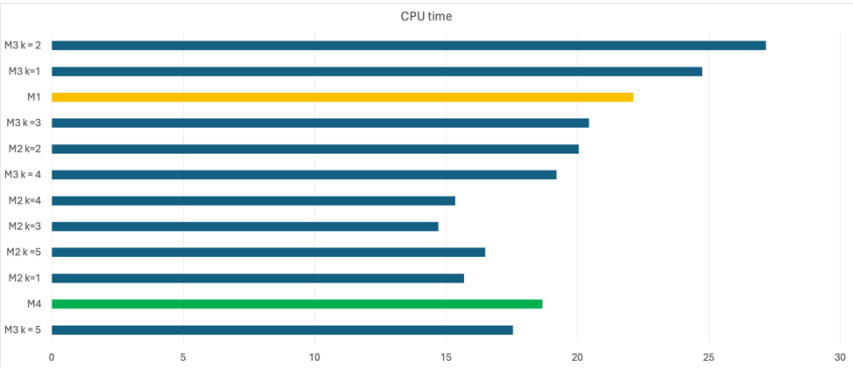


Рис. 1. CPU-час для отримання розв'язку з точністю 10^{-12} для прикладу 3

На рис.1 для методу Ньютона (2) використано жовтий колір, для методу (4) – синій колір та для методу (5) – зелений колір. Час визначено як середнє значення з 1000 повторних виконань у секундах $\times 10^{-6}$. М3 – метод (4) із використанням $M = I$, М2 – метод (4) із використанням $M = F'(x_0)$.

Для випадків із невеликим значенням k необхідно більше ітерацій для досягнення бажаної точності, що впливає на загальний час роботи методу.

Запропонована робота розв'язує проблему обчислення $F'(x_n)^{-1}$ на кожному кроці методу Ньютона. Обертання оператора замінено скінченною сумою лінійних операторів, які залежать від $F'(x)$. Також наведені обчислення показують, як зміни у запропонованому методі впливають на збіжність та швидкість обчислень для задач різної розмірності.

1. Argyros I.K., George S., Shakhno S., Regmi S., Havdiak M., Argyros M.I. Asymptotically Newton-Type Methods without Inverses for Solving Equations. -–*Mathematics* . – 2024. – 12, №. 7: 1069. https://doi.org/10.3390/math12071069
2. Ulm S.U. On iterative methods with successive approximation of the inverse operator. – *Izv. Acad. Nauk Est. SSR. Fiz. Mat*. – 1967. – 6, №. 4. – P. 403-411.

Вплив оптичних бездротових технологій на розвиток мереж 5G та 6G

УДК 004.7

Максим Шрам

Державний університет інформаційно-комунікаційних технологій, Київ, dut.maxim@gmail.com

Стільниковий зв'язок – це різновид радіозв'язку, при якій абоненти виходять на зв'язок один з одним з використанням мережі базових станцій. Ці станції приймають і ретранслюють сигнал від приймачів користувачів.

Радіозв'язок – це спосіб передачі повідомлень на відстань за допомогою радіохвиль.

В даний час радіозв'язок широко використовуються для різних бездротових з'єднань, але зв'язок на основі радіочастот стикається з рядом обмежень, таких як: обмежений спектр; залежність від погодних умов; великий ефект перешкод; суворе регулювання.

Бездротовий зв'язок на основі оптичного спектру активно розглядається в якості основного виду для майбутніх мереж зв'язку, включаючи мережі п'ятого і шостого поколінь (5G і 6G, відповідно).

Optical wireless communications (OWC) – це форма оптичного зв'язку, яка використовує видиме, ультрафіолетове та інфрачервоне випромінювання для передачі сигналу. OWC привернули великий інтерес дослідників завдяки своїм характеристикам. Мережі зв'язку п'ятого і шостого поколінь, штучний інтелект, Інтернет речей стануть основою сучасної цифрової економіки. Інтернет речей (Internet of Things, IoT) – це концепція мережі передачі даних між фізичними об'єктами («речами»), оснащеними вбудованими засобами і технологіями для взаємодії один з одним або з зовнішнім середовищем.

Перелік специфічних особливостей і вимог, що пред'являється до системи зв'язку 5g вже сформульований. П'яте покоління стільникового зв'язку пропонує нові послуги з дуже високою якістю обслуговування (Quality of Service, QoS). QoS включає в себе дві найбільш важливі характеристики мережі – продуктивність і надійність.

Послуги зв'язку 5g характеризуються: надвисокою пропускною спроможністю системи; наднизькою затримкою; надвисокою безпекою; масовим підключенням пристроїв; наднизьким енергоспоживанням.

Запуск системи зв'язку 6G очікується між 2027 і 2030 роками. Специфікація 6G ще точно не визначена, але вже сформульований перелік дослідницьких питань. Основними пунктами є: підвищення пропускної здатності; збільшення кількості підключень; зниження затримки; підвищення безпеки; підвищення енергоефективності; підвищення рівня QoS користувача; підвищення надійності.

Варто відзначити, що основні напрямки розвитку і поліпшення систем зв'язку схожі. Однак, очікується, що система зв'язку 6G стане глобальним засобом зв'язку, а рівень обслуговування буде в кілька разів краще в порівнянні з 5G.

Широкий оптичний діапазон вважається перспективним рішенням для розвитку мереж 5G, 6G і IoT.

Переваги технологія OWC в порівнянні з радіозв'язком:

– широкий спектр;
– висока швидкість передачі даних;
– низька затримка;
– висока безпека;
– низька вартість;
– низьке енергоспоживання.

Відстань між об'єктами зв'язку може варіюватися від декількох нанометрів до декількох тисяч кілометрів, що досягається завдяки розгортанню різних систем OWC.

Основні технології систем OWC:

– комунікація видимого світла (Visible Light Communication, VLC);
– Light Fidelity (Li-Fi);
– оптичний камерний зв'язок (Optical Camera Communication, OCC);
– оптичний зв'язок у вільному просторі (Free-Space Optics, FSO).

Перераховані вище технології мають відмінностями і подібностями, зокрема використовують різний вид випромінювання і приймально-передавальне обладнання, тому кожна з технологій має свої переваги, недоліки і обмеження щодо застосування.

Таким чином, технології OWC, через своїх актуальних характеристик, можуть зіграти важливу роль у розвитку і впровадженні мереж 5G, 6G і IoT.

Мережі 5G, 6G і IoT на базі технологій OWC

Під час організації каналу радіозв'язку використовуються частоти в діапазоні від 3 кГц до 3 000 ГГц. Частина діапазону радіочастот (3 кГц – 10 ГГц) повсюдно використовується існуючими бездротовими технологіями через сприятливих комунікаційних властивостей. Ця частина діапазону практично вичерпана, що залишилася не відповідає високим вимогам мереж 5G, 6G і IoT. Крім того, розподіл і використання частотного діапазону у всьому світі регулюється Міжнародним союзом електрозв'язку (International Telecommunication Union, ITU) та національними організаціями різних країн, які розподіляють частоти на основі правил ITU.

Технології OWC володіють відмінними характеристиками для створення каналів зв'язку в мережах 5G, 6G і IoT. OWC може використовуватися для широкого спектру додатків, реалізовувати різні типи комунікацій, такі як: міжмашинна взаємодія (machine-to-machine); взаємодія між пристроями (device-to-device); взаємодія між мікросхемами (chip-to-chip); взаємодія між транспортними засобами (vehicle-to-vehicle); взаємодія різних інфраструктур.

Оптичний зв'язок дозволяє здійснювати комутацію пристроїв на відстанях від декількох нанометрів до більш ніж 10 000 км.

OWC забезпечує: високу швидкість передачі даних (до 100 Гбіт/сек); високу пропускну здатність; високий рівень безпеки; низьке енергоспоживання; низьку вартість інфраструктури та пристроїв; відсутність перешкод; простоту інтеграції в пристрої; відсутність необхідності ліцензування допустимої смуги частот.

Таким чином фізичні можливості технології OWC перекривають всі недоліки радіозв'язку, а також перевершують бездротовий зв'язок на основі радіочастот по ряду параметрів.

Зв'язок 6G, за прогнозами, буде запущена в період між 2027 і 2030 роками. Системи на основі радіочастот не здатні відповідати високим вимогам майбутніх мереж 5G/6G і IOT.

Таким чином, використання технологій OWC для побудови мереж стільникового зв'язку нового покоління дозволить вирішити проблеми, властиві системам зв'язку на основі радіочастот. OWC забезпечить ефективні канали зв'язку для мереж 5G, 6G та розгортання IOT.

1. Zaman M., Shahjalal M., Khalid M., Min Y. The Role of Optical Wireless Communication Technologies in 5G/6G and IoT Solutions: Prospects, Directions, and Challenges // Applied Sciences. 2019. Vol. 9, Iss. 20. 4367. URL: https://www.mdpi.com/2076-3417/9/20/4367 (дата звернення: 17.04.2024).
2. Arnon S., Barry J., Karagiannidis G., Schober R., Uysal M. Advanced Optical Wireless Communication Systems. URL: https://rizkia.staff.telkomuniversity.ac.id/files/2016/02/Advanced-OpticalWireless-Communication-Systems-.pdf (дата звернення: 17.04.2024).

Оцінювання стану кіберзахисту об'єктів критичної інфраструктури держави

УДК 004.946.5.056(477)(045)

Володимир Шульга [1], Олександр Корченко[2], Євгенія Іванченко[3]

Державний університет інформаційно-комунікаційних технологій
[1]volodymyr.shulha@nau.edu.ua,[2] agkorchenko@gmail.com,
[3]Національний авіаційний університет, evivancenko@gmail.com

На сьогодні процес реалізації кіберзагроз стає все більш вдосконаленим та складним. Розвиток технологій сприяє зростанню можливостей для кіберзлочинності, шпигунства та кібертероризму, що робить їх доступнішими та поширенішими. Критична інфраструктура, така як енергетика, транспорт та медичні заклади, стає все більш залежною від інформаційних технологій. Оцінка рівня кіберзахисту дозволяє оцінити ефективність витрачених ресурсів на безпеку. Оновлені методи оцінювання враховують кібервторгневі інновації та застосовують сучасні техніки та підходи до кіберзахисту.. Отже, методи оцінювання рівня підвищення стану кіберзахисту об'єктів критичної інфраструктури є актуальним питанням стратегії кібербезпеки держави та її важливою складовою для забезпечення стійкості суспільства у цифрову епоху.

Проблеми забезпечення кіберзахисту критичної інфраструктури в умовах зростаючих кіберзагроз [1] свідчать про потребу у розробці відповідних ефективних методів. Відомі методи оцінювання рівня кіберзахисту [2,3,4] не враховують специфіки критичної інфраструктури та не використовують сучасні техніки та інструменти. Розуміючи, що збільшення кількості кіберзагроз критичній інфраструктурі потребує нових інноваційних підходів до їхнього виявлення та управління, використання теорії нечітких множин стає ключовим інструментом для досягнення цієї мети. Це може суттєво підвищити ефективність кібербезпекових заходів організацій, як підтверджується низкою досліджень [5,6,7]. Однак сучасні публікації не містять методів оцінювання рівня підвищення стану кіберзахисту об'єктів критичної інфраструктури на основі експертного оцінювання, що ґрунтується на теорії нечітких множин. Проблема забезпечення кіберзахисту критичної інфраструктури в умовах зростаючих кіберзагроз [1] свідчить про необхідність розробки відповідних ефективних методів. Відомі методи оцінювання рівня кіберзахисту [2,3,4] не орієнтовані на врахування специфіки критичної інфраструктури та не використовують відповідні сучасні техніки та інструменти.

Тому *метою* даного дослідження є розробка методу оцінювання рівня підвищення стану кіберзахисту об'єкту критичної інфраструктури держави з метою підвищення її стійкості до кіберзагроз та забезпечення національної безпеки України. Запропонований метод включає процедури, що реалізуються шістьма етапами: формування лінгвістичних змінних (ЛЗ), фазифікацію інтервалів та побудову еталонів, формування множини характеристик об'єктів огляду, визначення поточних значень характеристик об'єктів огляду, процес первинного вимірювання, формування базових пар та евристичних правил і візуалізація результатів. Розглянемо кожен з них докладніше.

На етапі 1 сформуємо лінгвістичні змінні**,** де відповідно до [8] заходи кіберзахисту – «Ідентифікація ризиків кібербезпеки (ID)», «Кіберзахист» (PR), «Виявлення кіберінцидентів» (DE), «Реагування на кіберінциденти» (RS), «Відновлення стану кібербезпек» (RC), кожна з яких містить клас ЗКЗ «Ідентифікація ризиків кібербезпеки (ID)» - ID.AM, ID.BE, ID.GV, ID.RA, ID.RM, ID.SC, «Кіберзахист» (PR) – PR.AC, PR.AT, PR.DS, PR.IP, PR.MA, PR.PT, «Виявлення кіберінцидентів» (DE) – DE.AE, DE.CM, DE.DP, «Реагування на кіберінциденти» (RS) – RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, «Відновлення стану кібербезпеку» (RC) – RC.RP, RC.IM, RC.CO. Кожному класу притаманні відповідні ЗКЗ [4,8], так, наприклад, для ID – це ID.AM1÷6, ID.BE1÷5, ID.GV1÷4, ID.RA1÷6, ID.RM1÷3, ID.SC1÷5. Для формалізації процесу вимірювання системи заходів кіберзахисту (ЗКЗ) здійснюється формування лінгвістичної змінної (ЛЗ) на підставі кортежу [5] <***TL***, $\underset{\sim}{T}_{TL}$, X_{TL}> з певною областю визначення базової терм-множини ***TL*** за допомогою *f* термів.

Так, наприклад, для відображення результату оцінювання стану виконання класу ЗКЗ *q*-тим об'єктом огляду критичної інфраструктури ($q= \overline{1,m}$) введемо ЛЗ ***ACM*** – "*СТАН ЗАХОДІВ КІБЕРЗАХИСТУ*", яку на підставі (1) визначимо кортежем [4] <***ACM***, $\underset{\sim}{T}_{ACM}$, X_{ACM}>. Базова терм-множина ***ACM*** засновується на f термах і має вигляд:

$$\underset{\sim}{T}_{ACM_i} = \bigcup_{i=1}^{f} \underset{\sim}{T}_{ACM_i}, \qquad (1)$$

Наприклад, *для* ***ACM*** при $f = 4$ ($i = \overline{1,4}$)

$$\underset{\sim}{T}_{\text{ACM}} = \bigcup_{i=1}^{4} \underset{\sim}{T}_{\text{ACM}_i}, = \{\underset{\sim}{T}_{\text{ACM}_1}, \underset{\sim}{T}_{\text{ACM}_2}, \underset{\sim}{T}_{\text{ACM}_3}, \underset{\sim}{T}_{\text{ACM}_4}\}$$

$$= \{\text{"НЕ ПОТРЕБУЄТЬСЯ",}$$

"РОЗГЛЯДАЄТЬСЯ ДЛЯ РЕАЛІЗАЦІЇ", "У ПРОЦЕСІ", "РЕАЛІЗОВАНО"},

де $\underset{\sim}{T}_{ACM_i}$ ($i = \overline{1,f}$) – терми НЧ (значення ЛЗ), а $X_{ACM} = [x_{ACM}^{min}, x_{ACM}^{max}] = [x_{ACM}^{min} = X_{ACM1}; X_{ACM2}[, [X_{ACM2}; X_{ACM3}[,\ldots, [X_{ACMi}; X_{ACMi+1}[,\ldots, [X_{ACMf}; x_{ACM}^{max} = X_{ACMf+1}]$ – область визначення НЧ.

На другому етапі проведемо фазифікацію інтервалів та побудову еталону стан заходів кіберзахисту, де за допомогою метода [4] та табл. 1 реалізуємо фазифікацію інтервалів $[X_{ACM1}; X_{ACM2}[, \ldots, [X_{ACMi}; X_{ACMi+1}[,\ldots, [X_{ACMf}; X_{ACMf+1}]$, де з урахуванням досліджень в [5] визначимо коефіцієнт зближеності *CF=0,25*.

Таблиця 1

Значення інтервалів для *ACM* при *f*=4

Тип розподілу	$[X_{ACM_1}; X_{ACM_2}]$	$[X_{ACM_2}; X_{ACM_3}[$	$[X_{ACM_3}; X_{ACM_4}[$	$[X_{ACM_4}; X_{ACM_5}]$
Рівномірний	[0; 0]	]0; 50[	[50; 100[	[100; 100]

Результати фазифікації інтервалів для ***ACM*** при *f*=4 занесемо табл. 2.

Таблиця 2

Результати фазифікації інтервалів для *ACM* при *f*=4

Тип розподілу НЧ	‘НЧ $\underset{\sim}{T}_{ACM_i} = (a_i; b_{1i}; b_{2i}; c_i)_{LR}, (i = \overline{1,4})$			
	$\underset{\sim}{T}_{ACM_1}$	$\underset{\sim}{T}_{ACM_2}$	$\underset{\sim}{T}_{AM_{M3}}$	$\underset{\sim}{T}_{ACM_4}$
Різнорідний	$(0; 0; 0; 12{,}5)_{LR}$	$(0; 12{,}5; 37{,}5; 62{,}5)_{LR}$	$(37{,}5; 62{,}5; 87{,}5; 100)_{LR}$	$(87{,}5; 100; 100; 100)_{LR}$

Далі, здійснимо перетворення інтервалів ЛЗ ***ACM*** у еталонні НЧ.

За допомогою ЛЗ ***ACM*** можемо здійснювати оцінку системи заходів кіберзахисту, для чого визначимо відповідно категорії і заходи. Значення цих показників знаходиться в інтервалі від 0% до 100% (див. табл. 1) і відповідно визначаються як: не потребується; розглядається для реалізації; у процесі; реалізовано (див. табл. 2). Оцінювання показника [4,8] здійснюється за наступною шкалою: $[X_{ACM1}; X_{ACM2}] \in [0; 0]$ – «НЕ ПОТРЕБУЄТЬСЯ»; $]X_{ACM2}; X_{ACM3}[\in]0; 50[$; «У ПРОЦЕСІ» $[X_{ACM3}; X_{ACM4}[\in [50; 100[$ – «РОЗГЛЯДАЄТЬСЯ ДЛЯ РЕАЛІЗАЦІЇ»; $[X_{ACM4}; X_{ACM5}] \in [100; 100]$ – «РЕАЛІЗОВАНО». Виконаємо формування еталонів НЧ для ЛЗ ***ACM*** за допомогою [4] та табл.2. Графічна інтерпретація сформованих різнорідно розподілених НЧ $\underset{\sim}{T}^{(4)}_{\text{ACM}}$ наведена на рис. 1, де $\underset{\sim}{T}_{\text{ACM}_1}$, $\underset{\sim}{T}_{\text{ACM}_2}$, $\underset{\sim}{T}_{\text{ACM}_3}$ *та* $\underset{\sim}{T}_{\text{ACM}_4}$ відповідно відображають – «НЕ ПОТРЕБУЄТЬСЯ (НП)»; «РОЗГЛЯДАЄТЬСЯ ДЛЯ РЕАЛІЗАЦІЇ (РД)», «У ПРОЦЕСІ (ПР)» та «РЕАЛІЗОВАНО (РЛ)».

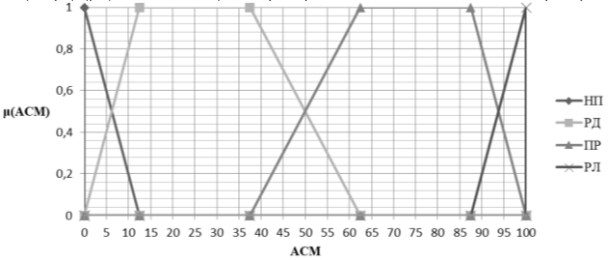


Рис. 1. Терми значень сформованих різнорідно розподілених НЧ для ЛЗ ***ACM*** $\underset{\sim}{T}^{(4)}_{\text{ACM}}$, де відповідно «НП» – «НЕ ПОТРЕБУЄТЬСЯ»; «РД» – «РОЗГЛЯДАЄТЬСЯ ДЛЯ РЕАЛІЗАЦІЇ», «ПР» – «У ПРОЦЕСІ», «РЛ» – «РЕАЛІЗОВАНО».

На третьому етапі сформуємо множину характеристик об’єктів огляду. Для цього введемо множину характеристик, що відображають стан заходів кіберзахисту (СЗКЗ) об’єктів огляду [4]

$$\widetilde{\boldsymbol{E}} = \left\{ \bigcup_{q=1}^{m} \tilde{E}^q \right\} = \{\tilde{E}^1, \tilde{E}^2, \dots \tilde{E}^m\}, \qquad (2)$$

де $\tilde{E}^q \subseteq \widetilde{\boldsymbol{E}}\left(q = \overline{1,m}\right)$ НЧ, що характеризує q-ий об’єкт огляду, а m – їх кількість.

Наприклад, при m=3, а $\tilde{E}^1 = \tilde{E}^{\text{АС}}$ = «СК АТОМНОЇ СТАНЦІЇ», $\tilde{E}^2 = \tilde{E}^{\text{АП}}$ = «СК АЕРОПОРТУ» та $\tilde{E}^3 = \tilde{E}^{\text{НПЗ}}$ = «СК НАФТОПЕРЕРОБНОГО ЗАВОДУ», де

$\tilde{E}^{\text{АС}}, \tilde{E}^{\text{АП}}$ та $\tilde{E}^{\text{НПЗ}}$ – НЧ, що характеризують відповідні об'єкти огляду критичної інфраструктури.

Множини системи характеристик q-го об'єкта огляду, яка охоплює класи ЗКЗ відобразимо як:

$$ACM^q = \left\{ \bigcup_{i=1}^{\eta} ACM_i^q \right\} = \{ACM, ACM_2^q, \dots, ACM_\eta^q\}, \quad (3)$$

де $ACM_i^q \subseteq ACM^q \left(i = \overline{1,\eta}\right)$ – ідентифікатор і-го класу ЗКЗ, η – їх кількість, а $q = \overline{1,m}$ (m – кількість об'єктів огляду (див. [4])).

Наприклад, при η =5 з урахуванням класів ЗКЗ [8] формулу (3) запишемо як:

$$ACM^q = \{\cup_{i=1}^{\eta} ACM_i^q\} = \{ACM_1^q, ACM_2^q, ACM_3^q, ACM_4^q, ACM_5^q\}$$

$$=\{ID, PR, DE, RS, RC\} = \{\text{"}\textit{ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ", "КІБЕРЗАХИСТ", "ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ", "РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ", "ВІДНОВЛЕННЯ СТАНУ КІБЕРБЕЗПЕКИ"}\text{ }\},$$

де ACM_1^q=*ID= "ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ",* ", ACM_2^q=*PR= "КІБЕРЗАХИСТ",* ACM_3^q=*DE= "ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ",* ACM_4^q=*RS= "РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ",* ACM_5^q=*RC="ВІДНОВЛЕННЯ СТАНУ КІБЕРБЕЗПЕКИ".*

Далі, надамо величину, що відображає стан виконання заходів кіберзахисту q-го об'єкту огляду критичної інфраструктури держави:

$$\tilde{E}^{\boldsymbol{q}} = (\sum_{i=1}^{\eta} \widetilde{ACM}_{ij}^q)/\eta = \quad (4)$$

$$(\widetilde{ACM}_1^q \oplus \widetilde{ACM}_2^q \oplus \dots \oplus \widetilde{ACM}_n^q)/\eta,$$

де $\widetilde{ACM}_i^{\boldsymbol{q}}\left(i = \overline{1,\eta}\right)$ *i*-й клас заходів кіберзахисту q-го об'єкту огляду (визначається НЧ), η – кількість категорій [5], а $\widetilde{\oplus}$ – нечітка сума [6].

На четвертому етапі визначимо поточні значення характеристик об'єктів огляду. Кожний *i*-й клас ЗКЗ q-го об'єкту огляду визначається за формулою:

$$\widetilde{ACM}_i^q = (\sum_{j=1}^{k_i} ACM_{ij}^q)/k_i = (\widetilde{ACM}_{i1}^q \oplus \widetilde{ACM}_{i2}^q \oplus \dots \oplus \widetilde{ACM}_{ik_i}^q)/k_i, \quad (5)$$

$$(j = \overline{1,k_i}).$$

На п'ятому етапі здійснюється процес первинного вимірювання, тобто вираховується рівень наближеності поточних значень характеристик об'єктів огляду до визначених на етапі 2 еталонних величин [5] із застосуванням відстані Хемінга (ВХ) [6].

Узагальнене значення для всіх $\widetilde{ACM}_{ij}^q$розрахуємо по формулі

$$h_{ij}^q(\widetilde{ACM}_{ij}^q, \tilde{T}_{scs_{ij}}^q) = \sum_{j=1}^{f} \left|\mu(\widetilde{ACM}_{ij}^q) - \mu(\tilde{T}_{scs_{ij}}^q)\right|, \quad (6)$$

де, наприклад, для $\widetilde{ACM}_1^{AC}$ "ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ" при $\mu(\widetilde{ACM}_{11}^1) = \mu(\widetilde{ACM}_{12}^1) = 0$, $\mu(\widetilde{ACM}_{13}^1) = 14{,}29, \mu(\widetilde{ACM}_{14}^1) = 28{,}57$, $\mu(\tilde{T}_{ACM_{11}}^1)$= 16,18, $\mu(\tilde{T}_{ACM_{12}}^1) = 29{,}97$, $\mu(\tilde{T}_{ACM_{13}}^1) = 48{,}78$, $\mu(\tilde{T}_{ACM_{14}}^1)$= 66,32 обрахуємо

$h_{11}^1(\widetilde{SD}_{11}^1, \tilde{T}_{scs_{11}}^1)$ = |(0-16,18)|+|(0-29,97)|+|(14,29-48,78)|+|(28,57-66,32)|= 118,39.

На етапі 6 здійснюється формування базових пар та евристичних правил, за якими, відповідно до оцінок експертів визначається рівень стану заходів кіберзахисту об'єкту огляду, для чого необхідно визначити базові пари мінімальних ВХ, що будуть виконувати роль аргументів у правилах. Відповідно до властивостей методу, використаному на Етапі 5, і враховуючи, що мінімальне із значень $h_{ij}^{q}(ACM_{ij}^{AC})$ буде свідчити про найбільшу наближеність НЧ до еталонного, знайдемо мінімальну ВХ із значень h_{ij} $(\widetilde{ACM}_{ij}^{q}, \tilde{T}_{scs_j}^{q})$, $(i = \overline{1,f})$ за формулою (7)

$$h_{i\,min}^{q} = \bigwedge_{i=1}^{f} h_{i\,j}^{q} \ (\widetilde{ACM}_{ij}^{q}, \tilde{T}_{scs_j}^{q}), \tag{7}$$

де $h_{imin}^{q} = h_{ij}^{q}$, при *min=j*.

Далі для формування базової пари (аргументів) для асоціативних правил визначимо значення

$$h_{i\,min'}^{q} = \begin{cases} h_{imin-1}^{q}(\widetilde{ACM}_{ij}^{q}, \tilde{T}_{scs_j}^{q}), \\ \text{при } h_{imin-1}^{q}(\widetilde{ACM}_{ij}^{q}, \tilde{T}_{scs_j}^{q}) \leq h_{imin+1}^{q}(\widetilde{ACM}_{ij}^{q}, \tilde{T}_{scs_j}^{q}) \\ h_{imin+1}^{q}(\widetilde{ACM}_{ij}^{q}, \tilde{T}_{scs_j}^{q}), \\ \text{при } h_{imin-1}^{q}(\widetilde{ACM}_{ij}^{q}, \tilde{T}_{scs_j}^{q}) > h_{imin+1}^{q}(\widetilde{ACM}_{ij}^{q}, \tilde{T}_{scs_j}^{q}) \end{cases}, \tag{8}$$

що є найближчим до $h_{i\,min}^{q}$.

Введемо нормуючий коефіцієнт щодо належності поточного значення до еталонного, який вираховується за виразом

$$k_i^q = \frac{1}{h_{i\,min}^{q} + h_{i\,min'}^{q}}. \tag{9}$$

Наступним сформуємо показники рівня впевненості експерта щодо належності поточних значень до оцінювання стану заходів кіберзахисту, що буде вираховуватися за виразом:

$$ECI_{ij} = 1 - k_i^q * h_{i\,min}^{q} \quad \text{та } ECI'_{ij} = 1 - k_i^q * h_{i\,min'}^{q}. \tag{10}$$

Наприклад, відповідно до (7) для $\widetilde{ACM}_1^{AC}$ "ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ":

$$h_{1\,min}^{q} = h_{11}^{1}(\widetilde{ACM}_{11}^{1}, \tilde{T}_{scs_{11}}^{1}) \wedge h_{12}^{1}(\widetilde{ACM}_{12}^{1}, \tilde{T}_{scs_{12}}^{1}) \wedge h_{13}^{1}(\widetilde{ACM}_{13}^{1}, \tilde{T}_{scs_{13}}^{1}) \wedge h_{14}^{1}(\widetilde{ACM}_{14}^{1}, \tilde{T}_{scs_{14}}^{1}) = 118{,}39 \wedge 18{,}39 \wedge 95{,}89 \wedge 195{,}89 = 18{,}39,$$

а відповідно до (8) $h_{1\,min'}^{q}$: $h_{1\,min'}^{q} = \begin{cases} 95{,}89 \text{ при } 95{,}89 \leq 18{,}39 \\ 18{,}39 \text{ при } 118{,}39 > 95{,}89, \end{cases}$

при цьому $h_{1\,min'}^{q}$ = 18,39.

Далі вирахуємо коефіцієнт належності поточного значення до еталонних за допомогою (9)

$$k_1^q = \frac{1}{18{,}39 + 95{,}89} \approx 0{,}009$$

та відповідно з (10) сформуємо показник

$ECI_{12} = 1 - 0{,}009 * 95{,}89 \approx 0{,}863$ та $ECI'_{13} = 1 - 0{,}009 * 18{,}39 \approx 0{,}166$.

Далі формуємо шаблон асоціативного правила $AR(\widetilde{ACM}^q$; $\underset{\sim}{T}_{SCS}/ECI$; $\underset{\sim}{T}'_{SCS}/ECI'$), де $\widetilde{ACM}_i^q$ – i-та характеристика об'єкту огляду, $j=\overline{1,f}$, $\underset{\sim}{T}_{SCSi}$ – рівні захисту. Для даної характеристики, при $\widetilde{ACM}^q = \widetilde{ACM}_1^{AC}$, $\underset{\sim}{T}_{SCS} = \underset{\sim}{T}_{SCS_2}$ = «ЗРЗ», $ECI = ECI_{12} \approx 0{,}863$, $\underset{\sim}{T}'_{SCS} = \underset{\sim}{T}_{SCS_3}$ = «ДРЗ», $ECI' = ECI_{12} \approx 0{,}166$, правило буде виглядати наступим чином:

$$AR(\widetilde{ACM}_1^{AC}\text{; "ЗРЗ"}/ECI'_{12}\text{,"ДРЗ"}/ECI_{13}\text{;)=}$$

AR ("ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ"; "ЗРЗ"/0,863; ДРЗ/0,166) .

Таким чином, відповідно до прикладу кінцевий варіант правила інтерпретується як: «Стан заходів кіберзахисту для класу заходів кіберзахисту «ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ» знаходиться в межах між «ЗАДОВІЛЬНИЙ РІВЕНЬ ЗАХИСТУ» з коефіцієнтом впевненості експерта 0,863 та «ДОСТАТНІЙ РІВЕНЬ ЗАХИСТУ» з коефіцієнтом впевненості експерта 0,166». Аналогічно, до виразів (7-10) визначаємо стан кіберзахисту для інших характеристик об'єкту огляду.

На наступному етапі проведемо візуалізацію результатів оцінювання стану кіберзахисту об'єктів огляду для $\widetilde{ACM}_j^q$, де $j=\overline{1,n}$, $q=\overline{1,m}$ та $\widetilde{SD}^q$. На рис. 2-8 представлена інтерпретація результатів оцінювання. Наприклад, для значення $\widetilde{ACM}_1^{AC}$ "ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ" (рис. 2) наведено графік отриманого результату, де візуально можна побачити, що зазначена характеристика знаходиться в межах між «ДРЗ» та «ЗРЗ», а на рис. 3, 4, 5, 6 та 7 продемонстровано результат візуалізації для $\widetilde{ACM}_2^{AC}$ "КІБЕРЗАХИСТ", $\widetilde{ACM}_3^{AC}$ "ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ", $\widetilde{ACM}_4^{AC}$ "РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ", $\widetilde{ACM}_5^{AC}$ "ВІДНОВЛЕННЯ СТАНУ КІБЕРБЕЗПЕКИ" та $\widetilde{ACM}^{AC}$ «СТАН ЗАХОДІВ КІБЕРЗАХИСТУ» де видно, що вони знаходяться в межах між «ДРЗ» і «ЗРЗ», «ДРЗ» і «ЗРЗ», «ДРЗ» і «ЗРЗ», «ДРЗ» і «ЗРЗ» та «ДРЗ» і «ЗРЗ» відповідно. На рис. 8 представлено значення $\widetilde{ACM}_{min}^{AC}$ коли всі поточні значення відповідають «НП» та $\widetilde{ACM}_{max}^{AC}$, коли всі значення відповідають «РЛ», що є очевидним з логіки причинно-наслідкових зв'язків.

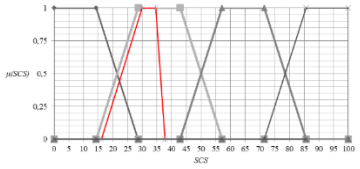


Рис. 2 Графічне подання отриманого результату $\widetilde{ACM}_1^{AC}$ "ІДЕНТИФІКАЦІЯ РИЗИКІВ КІБЕРБЕЗПЕКИ"»

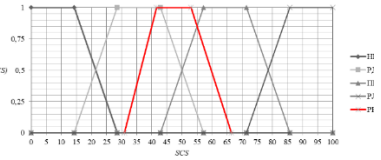


Рис. 3. Графічне подання отриманого результату $\widetilde{ACM}_2^{AC}$ "КІБЕРЗАХИСТ"»

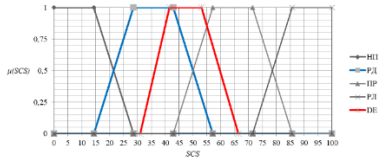


Рис. 4. Графічне подання отриманого результату $\widehat{ACM}_3^{AC}$ "ВИЯВЛЕННЯ КІБЕРІНЦИДЕНТІВ"

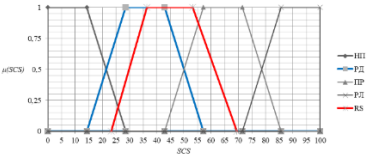


Рис. 5. Графічне подання отриманого результату $\widehat{ACM}_4^{AC}$ "РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ"

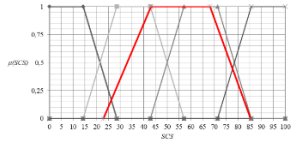


Рис. 6. Графічне подання отриманого результату $\widehat{ACM}_5^{AC}$ "ВІДНОВЛЕННЯ СТАНУ КІБЕРБЕЗПЕКИ"

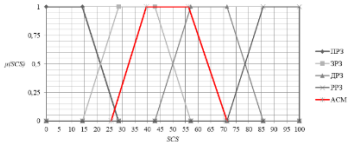


Рис. 7. Графічне подання отриманого результату $\widehat{ACM}^{AC}$ «СТАН ЗАХОДІВ КІБЕРЗАХИСТУ»

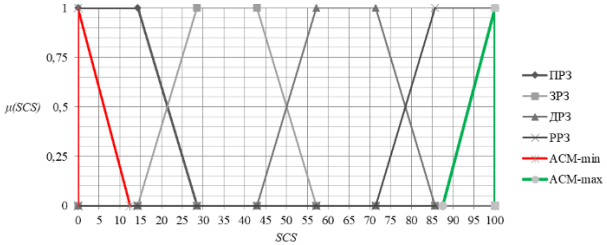


Рис. 8. Графічне подання отриманого результату $\widehat{ACM}_{min}^{AC}$ «СТАН ЗАХОДІВ КІБЕРЗАХИСТУ» та $\widehat{ACM}_{max}^{AC}$ «СТАН ЗАХОДІВ КІБЕРЗАХИСТУ»

Розроблений метод оцінювання, який за рахунок розробленої моделі системи характеристик, спрямованої на оцінку стану кіберзахисту в Україні, та процедур формування лінгвістичних змінних, фазифікації інтервалів та побудову еталонів, формування множини характеристик об'єктів огляду, процесу первинного вимірювання, формування базових пар і евристичних правил та візуалізації результатів, що формалізуються відповідними етапами, дозволяє реалізовувати процес оцінювання рівня підвищення стану кіберзахисту об'єктів огляду критичної інфраструктури держави. В подальшому необхідно побудувати систему, яка дозволить автоматизувати процес оцінювання підвищення зазначеного стану.

1. Потій О., Семенченко А., Бакалинський О., Мялковський Д. Публічне управління інституціональним розвитком у сфері кіберзахисту. Науковий вісник: Державне управління. 2021. № 3(9). С. 136-162.
2. П'ять методів досягнення кіберстійкості. URL https://www.megatrade.ua/news/ reviews /5- metodiv-dosyagnennya-kiberstiykosti/. (дата звернення 25.02.2024)

3. Належне врядування для забезпечення стійкості критичної інфраструктури, Огляди політики управління ризиками OECD, Публікація OECD, Париж. OECD. 2019.
4. Шульга В.П., Корченко О.Г. Іванченко Є.В., Бакалинський О.О., Мялковський Д.В., Зубков Д.А., Юдіна Д.О. Метод оцінювання стану кіберзахисту об’єкту огляду критичної інфраструктури держави. Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. 2023. Вип. 25 (ІІ). С. 40-57.
5. Корченко О.Г. Системи захисту інформації: Монографія. К.: НАУ, 2004. 264 с.
6. Корченко О.Г., Казмірчук С.В., Ахметов Б.Б. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія. Київ.: ЦП «Компринт», 2017. 435 с.
7. Корченко А. Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія. Київ.: ЦП «Компринт». 2019. 361 с.
8. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601. URL https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601. (дата звернення 25.02.2024).

Використання SDR-приймачів у навчальному процесі за спеціальністю «Кібербезпека»

УДК 378.162.33

Микола Щербина

Львівський національний університет імені Івана Франка,
Mykola.Shcherbyna@lnu.edu.ua

Аналізатори спектра радіосигналів (код 3.03.02 згідно класифікатора [1]) є ефективними засобами технічного захисту інформації (ТЗІ), що дозволяють детектувати та локалізовувати небезпечний сигнал (НС), який поширюється радіоканалом. Ці високотехнологічні пристрої працюють у широкому діапазоні частот і реалізують складні та ефективні алгоритми виділення НС у дуже завантаженому радіочастотному спектрі. Їх грамотне використання дозволяє вчасно виявити навмисно чи ненавмисно утворені радіоканали витоку інформації, в т.ч. закладні пристрої.

При викладанні дисциплін, пов'язаних з технічними каналами витоку інформації та її технічним захистом, студенти чи курсанти мають вивчати і цей клас пристроїв. Втім, професійні аналізатори спектра, доступні на українському ринку, характеризуються значною вартістю. Наприклад, визнаний прилад OSCOR Green виробництва американської Research Electronics International пропонується за 2,78 млн грн, топовий OSCOR Blue цього ж виробника — за майже 2,9 млн грн, а відносно дешевший MESA Basic зі значно скромнішим функціоналом все одно коштує понад 1 млн грн. Вочевидь, обладнання лабораторії навчального закладу цими чи подібними приладами виходить за всі розумні рамки бюджету, особливо в умовах воєнного часу.

З іншого боку, суто теоретичний підхід до викладання дисциплін, пов'язаних з ТЗІ, аж ніяк не виглядає прийнятним. Ще давньоримський педагог Марк Фабій Квінтиліан зазначав: *«Практика без теорії цінніша, ніж теорія без практики»*, тож практичний досвід використання аналізаторів спектра є дуже бажаним. При цьому не слід фокусуватися на конкретному виробі, бо коли (і якщо) нинішнім студентам доведеться використовувати аналізатор спектра для практичної роботи з ТЗІ — це може виявитись зовсім інша модель.

Найдорожчі аналізатори спектра, такі як згадані OSCOR Green/Blue, мають вбудований масив антен, які автоматично перемикаються, і дозволяють за 1 секунду просканувати діапазон 24 ГГц з кроком 12,2 кГц. Але для розуміння принципу роботи аналізатора цілком можна обмежитися планкою 1,7 ГГц. Автором пропонується використати в якості аналізатора спектра відносно недорогий Software-defined radio (SDR) приймач, такий як Airspy Mini вартістю 5150 грн [3]. Програмний пакет SDR# від Airspy (поточна версія 1919 на середину квітня 2024 р.), на жаль, вже не містить програми SpectrumSpy. Втім, версія 1784 (остання з включеним SpectrumSpy) доступна для завантаження [4]. Функціонал згаданої програми великою мірою відповідає аналізатору спектра для ТЗІ. Студенти можуть на практиці спостерігати сканування доступного діапазону (відбувається за ≈4 сек), бачити особливості сигналів у частотному домені — у вигляді як спектрограми, так і «водоспаду» (рис. 1).

Рис.1. Візуалізація спектру програмою SpectrumSpy до увімкнення джерела НС

На рис. 2 активовано демонстраційне джерело НС частотою 224,9 МГц, реалізоване на базі радіомікрофона. У порівнянні з рис. 1 добре видно характерний пік навколо зазначеної частоти.

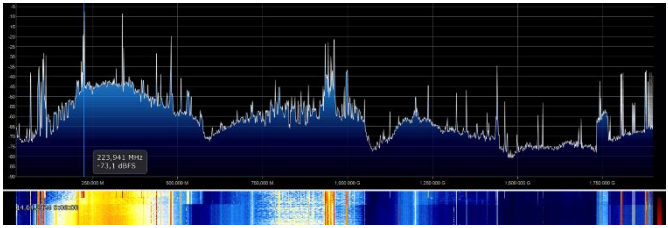


Рис.2. Візуалізація спектру програмою SpectrumSpy після увімкнення джерела НС

Таким чином, недорогий SDR-приймач з відповідним ПЗ дозволяє на практиці засвоїти основні прийоми роботи з аналізаторами спектра радіосигналів. Це підтверджується практичним досвідом лабораторних робіт зі студентами ЛНУ спеціальності «Кібербезека». Універсальність SDR-приймачів дозволяє застосувати їх і при викладанні інших дисциплін, таких як «Обробка сигналів в кібербезпеці», зокрема з використанням бібліотеки PySDR.

1. НД ТЗІ 1.5-002-2012. Класифікатор засобів технічного захисту інформації, наказ Адміністрації Держспецзв'язку від 29.08.2012 № 472. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=53451 (дата звернення: 13.04.2024).
2. Пошукові комплекси для виявлення закладних пристроїв і жучків. URL: https://lockers.com.ua/poiskovaja-tehnika/poiskovie-kompleksi/ (дата звернення: 13.04.2024).
3. SDR. Інтернет-магазин SDR (Software-Defined Radio). URL: https://sdr.in.ua/product-category/sdr/ (дата звернення: 13.04.2024).
4. SDR# (SDRSharp) revision 1784. https://airspy.com/downloads/sdrsharp-x86-dotnet4.zip (дата звернення: 25.03.2024).

Симетричний криптоалгоритм на основі поліноміальної системи залишкових класів

УДК 004.056.55

Ігор Якименко[1], Василь Яцків[2]

Західноукраїнський національний університет, [1]jiz@wunu.edu.ua, [2]vy@wunu.edu.ua

Альтернативою сучасних систем захисту інформації є поліноміальні симетричні криптоалгоритми. Основна ідея застосування поліномів у криптографії полягає в тому, що їх можна використовувати як ключі для шифрування та розшифрування повідомлень. У кільці Z[x], як і у будь-якому іншому кільці поліномів, ми можемо виконувати операції додавання, множення та ділення з остачею. Тому їх можна використовувати для шифрування та розшифрування повідомлень, побудови електронних підписів та інших криптографічних протоколів.

У статті розглядаються основні концепції поліноміальних симетричних криптоалгоритмів та систем залишкових класів (СЗК), а також їх використання у практичних застосуваннях.

Довільний поліном $N(x)$ в СЗК представляється у вигляді залишків $b_i(x)$ від ділення $N(x)$ на кожен із системи попарно взаємно простих модулів поліномів $p_i(x)$:

$$b_i(x) = N(x) \mod p_i(x). \quad (1)$$

Відновлення поліному $N(x)$ відбувається, як правило, на основі китайської теореми про залишки (КТЗ) в кільці поліномів $Z[x]$ [1]:

$$N(x) = \left(\sum_{i=1}^{s} b_i(x) M_i(x) m_i(x) \right) \bmod P(x), \quad (2)$$

де $P(x) = \prod_{i=1}^{s} p_i(x)$, $M_i(x) = \frac{P(x)}{p_i(x)}$, $m_i(x) = M_i^{-1}(x) \bmod p_i(x)$, $m_i(x)$ шукається з виразу, s – кількість модулів [2]. При цьому повинна виконуватися нерівність $N(x)<P(x)$.

Суть одного з методів поліноміального асиметричного шифрування в СЗК полягає в тому, що при відновленні полінома за його залишками у сумі (2) множення відбувається не на параметри $m_i(x) = M_i^{-1}(x) \bmod p_i(x)$, а на довільно вибрані поліноми $k_i(x)$.

Отже, для генерування ключів обидва абоненти повинні вибрати відомі тільки їм обом системи модулів $p_i(x)$ та відповідні поліноми $k_i(x)$, для яких виконуються такі умови: $1 < k_i(x) < p_i(x)$ та НСД ($k_i(x)$, $p_i(x)$)=1. Якщо $p_i(x)$ є незвідним поліномом, то друга умова виконується завжди. Відповідно, і відправнику, і отримувачу відомі параметри $M_i(x)$ та $m_i(x)$.

Для шифрування буквенну інформацію необхідно записати у числовій формі. Найпоширенішим класичним методом є заміна букви на її номер в алфавіті, причому нумерація починається з 0. Після цього її необхідно представити у вигляді поліному з коефіцієнтами, які відображають буквенну інформацію, тобто

$N(x)=a_n x^n+a_{n-1}x^{n-1}+\ldots+a_0 x^o \qquad a_i, i=\overline{0\ldots n}$

, де - послідовність цифрового представлення букв. Тоді на етапі шифрування спочатку вибирається блок відкритого тексту $N(x)<P(x)$, який потім записується в СЗК згідно виразу (1). Шифрування відбувається при відновленні числа в позиційну систему числення згідно такого виразу:

$$N(x)^{'}=\left(\sum_{i=1}^{s} b_i(x)M_i(x)k_i(x)\right)\bmod P(x) \quad . \qquad (3)$$

Знайдений поліном є шифртекстом, який передається по відкритому каналі зв'язку від одного абонента до іншого.

При розшифруванні спочатку обчислюються такі значення:

$$q_i(x)=\left(m_i(x)\left(k_i^{-1}(x)\bmod p_i(x)\right)\right)\bmod p_i(x)\ ;\ b_i^{'}(x)=N^{'}(x)\bmod p_i(x). \qquad (4)$$

Для отримання істинних залишків $b_i(x)$ необхідно виконати перетворення згідно співвідношення:

$$b_i(x)=\left(b_i^{'}(x)q_i(x)\right)\bmod p_i(x)=\left(b_i^{'}(x)m_i(x)k_i^{-1}(x)\right)\bmod p_i(x) \quad . \qquad (5)$$

Відповідно, відновлення полінома $N(x)$, який є відкритим текстом, здійснюється за формулою (2) або можна використати вираз, який з неї випливає:

$$N(x)=\left(\sum_{i=1}^{s} M_i(x)m_i(x)\left(\left(b_i^{'}(x)m_i(x)k_i^{-1}(x)\right)\bmod p_i(x)\right)\right)\bmod P(x)=$$

$$=\left(\sum_{i=1}^{s} M_i(x)m_i(x)\left(\left(b_i^{'}(x)q_i(x)\right)\bmod p_i(x)\right)\right)\bmod P(x). \qquad (6)$$

Коректність запропонованої криптосистеми встановлюється з властивостей конгруенцій, врахувавши, що $p_i(x)$ є дільником полінома $P(x)$, та рівність $m_i(x)=M_i^{-1}(x)\bmod p_i(x)$

Звідси отримуємо:

$$b_i(x)=\left(b_i^{'}(x)q_i(x)\right)\bmod p_i(x)=\left(N^{'}(x)\bmod p_i(x)\right)\cdot\left(m_i(x)k_i^{-1}(x)\right)\bmod p_i(x)\bmod p_i(x)=$$

$$=\left(\left(\left(\sum_{j=1}^{s} b_j(x)k_j(x)M_j(x)\right)\bmod P(x)\right)\bmod p_i(x)\cdot\left(m_i(x)k_i^{-1}(x)\right)\bmod p_i(x)\right)\bmod p_i(x)=$$

$$=\left(\left(b_i(x)k_i(x)M_i(x)\right)\bmod P(x)\cdot\left(m_i(x)k_i^{-1}(x)\right)\bmod p_i(x)\right)\bmod p_i(x)=$$

$$=\left(b_i(x)m_i(x)M_i(x)\right)\bmod p_i(x)=b_i(x). \qquad (7)$$

Отже, в даній статті вперше розроблено математичне забезпечення поліноміального симетричного криптографічного алгоритму, основаного на поліноміальній системі залишкових класів.

1. Roshanzadeh M., Saqaeeyan S. Error Detection & Correction in Wireless Sensor Networks By Using Residue Number Systems. International Journal of Computer Network and Information Security. 2012. №2. P. 29-35.
2. Sharoun A.O. Residue number system. Poznan university of technology academic journals. Electrical Engineering. 2013. №76. P. 265-270.

Координація діяльності організації при управлінні інцидентами інформаційної безпеки

УДК 004.056.5; 005.5

Юрій Якименко

Державний університет інформаційно-комунікаційних технологій, info@duikt.edu.ua

Управління інцидентами є однією з найважливіших процедур управління інформаційною безпекою, розвитку й удосконалювання системи управління інформаційною безпекою (СУІБ). Тому на практиці виконується побудова системи управління інцидентами інформаційною безпеки (СУІІБ), яка входить підсистемою в СУІБ [1], що дозволяє зрозуміти недоліки процесів і контролю забезпечення інформаційної безпеки (ІБ). Висвітлення основних процедур та процесів управління інцидентами завжди будуть пов'язані із організацією та супроводженням систем управління ІБ. Світовий досвід щодо управління ІТ-організаціями та їх взаємодією із замовниками детально описаний убібліотеці ITIL, де також міститься комплекс рекомендацій, необхідних для побудови процесів управління інцидентами.

Завжди завдання управління полягає в координації діяльності людей і підрозділів для ефективного вирішення стратегічних, тактичних і поточних завдань організації. Так до основних служб, які задіяні в організації при управлінні інцидентами відносяться: служба інформаційних технологій (ІТ), служба ІБ, служба внутрішнього контролю, служба економічної безпеки, служба управління ризиками (УР), служба юридична, служба управління персоналом , власники бізнес-процесів. У подібній ситуації, при відсутності чітких інструкцій і належного рівня навчання, процес управління інцидентами перетворюється в неорганізовані підходи до виявлення й усунення інцидентів. Найчастіше функції, дублюються між декількома співробітниками і лише втрачається час на їх своєчасне виконання.

Для злагодженої роботи підрозділів необхідно вибудовувати, формалізовувати й документовувати всі процеси відповідно до циклу управління інцидентами: виявлення, реагування, превентивні заходи, розслідування, усунення причин та наслідків.

При реалізації класичної системи управління процесами ІБ по використанню моделі PDCA [1] і відповідно до вимог стандартів ISO/IEC 27001 і 27035 [2,3], на її основних етапах управління можна визначати процеси, тісно пов'язені з виконанням одночасно – управлінських дій, насамперед, з інцидентами безпеки:

- корпоративна безпека і безпека системи / сервісу / мережі, оновлення попітик - зі створенням групи реагування на інциденти;
- виявлення подій ІБ (оповіщення, інформування про них), оцінка і прийняття рішення – з визначенням інцидента;
- аналіз вивчення засвоєних уроків і використання методів підвищення безпеки– з впливом результатів оцінки інцидента;
- поліпшення аналізу ризиків безпеки і результатів менеджменту – з поліпшенням системи управління інцидентами.

При підготовці до реалізації управління інцидентами необхідно визначити відповідальну особу, яка буде курирувати процес управління інцидентами. Як правило, ним може бути керівник служби ІБ (менеджер ІБ).

Після підтримки керівництвом організації необхідності і важливості управління інцидентами, визначаються ключові особи процесу управління та розподіл ролей між ними.

Такими типовими посадами в управлінських процесах ІБ будь-якої організації можуть бути:

- Комітет з інформаційної безпеки.
- Менеджер по інформаційній безпеці.
- Менеджер по реагуванню на інциденти.
- Член групи реагування на інциденти інформаційної безпеки (ГРІІБ).
- Фахівець із аналізу ризиків.
- Співробітник ІТ підрозділу.

Після того, як визначені всі ключові ролі, їх функції, порядок взаємодії, необхідно формалізувати і документувати процес управління інцидентами.

У подальшому процеси управління інцидентами повинні постійно удосконалюватися шляхом тестування і поліпшення процесів, пов'язаних з загальними процесами управління ІБ. Як показує практика проведення тренувань, поліпшення процесів управління інцидентами треба проводити в напрямках: змісту процедур реагування, часу реагування, скорочення часу відновлення, чіткості роботи персоналу, готовності і придатності інфраструктури до виконання процедур.

Для того, щоб приймати дійсно раціональні рішення по управлінню інцидентами ІБ, що будуть технічно, математично й економічно обґрунтованими, доцільно створювати інтелектуальну систему підтримки прийняття рішень (ІСППР), яка дозволить скординувати і автоматизувати діяльність організації при управлінні інцидентами інформаційної безпеки .

1. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с. URL: https://dut.edu.ua/uploads/l_2230_88161692.pdf (дата звернення: 15.04.2024).
2. ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT)
3. Методи захисту системи управління інформаційною безпекою. Вимоги.
4. ДСТУ ISO/IEC 27035-2:2018 (ISO/IEC 27035-2:2016, IDT). Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти.

Використання нейромереж для підвищення стійкості ідентифікації вторгнень у комп'ютерну систему

УДК 004:054

Юрій Яремчук[1], Кирило Безпалий[2], Вячеслав Гуменюк[3],

Вінницький національний технічний університет
[1]yurevyar@vntu.edu.ua, [2]kyrylo.bezpalyi@vntu.edu.ua, [3]hvv@vntu.edu.ua

Комп'ютерні системи, що знаходяться під загрозою вторгнення, представляють значний виклик у сфері кібербезпеки. У контексті даної проблематики, вторгнення визначається як несанкціонований доступ до системи з метою порушення її функціональності та безпеки, що може включати у себе крадіжку конфіденційних даних або порушення цілісності системи. Ефективне відмежування дій зловмисників від дій легітимних користувачів є ключовим для ідентифікації потенційних загроз [1].

Системи виявлення вторгнення (IDS) відіграють важливу роль у моніторингу та аналізі діяльності в мережах та у комп'ютерних системах для виявлення ознак кібератак у реальному часі. Вони характеризуються мінімальною необхідністю втручання людини та високою точністю виявлення незаконних дій. Сучасні дослідження в області IDS використовують різноманітні методології, включаючи статистичні підходи, машинне навчання та штучні нейронні мережі, що дозволяє проводити складний аналіз даних та виявляти відхилення, що можуть свідчити про загрози [2].

Подальші дослідження та розробка у цій сфері необхідні для підвищення ефективності систем виявлення вторгнення, що включає інтеграцію новітніх технологій у сучасні кібербезпечні системи. Такі зусилля мають на меті досягти вищого рівня захисту від кібератак у динамічному цифровому середовищі [2].

Експертні системи, такі як Snort, Tripwire, IBM ISS та McAfee, широко застосовуються у системах виявлення вторгнень для аналізу мережевого трафіку. Однак вони часто стикаються з проблемою невиявлення нових видів атак та є вразливими до методів обходження, як-то поліморфний код оболонки. Ці недоліки значно обмежують їхню ефективність у протистоянні сучасним кіберзагрозам.

З іншого боку, генетичні алгоритми (GA) та дерева рішень демонструють високу ефективність у виявленні вторгнень, завдяки їхній здатності до глобального пошуку та потужної класифікаційної моделі відповідно. На кожній гілці дерева рішень вказуються атрибути, що визначають цільову функцію, а у "листках" зберігаються значення цієї функції для класифікації об'єктів. Хоча GA вимагають значних обчислювальних ресурсів, їх гнучкість робить їх особливо корисними у виявленні складних загроз [3].

Моделі глибокого навчання, такі як багатошарові перцептрони та глибокі нейронні мережі, пропонують ще один перспективний підхід до виявлення вторгнень. Вони ефективно використовують багатошарову структуру для імітації біологічних нейронних мереж, що дозволяє кластеризувати та класифікувати великі обсяги даних з високою точністю. Використання таких моделей може значно підвищити здатність систем кібербезпеки до виявлення та реагування на непередбачені кібератаки, забезпечуючи більш ефективне виявлення та класифікацію мережевих загроз [3].

Штучна нейронна мережа (ART) перетворює вхідні дані на бажані вихідні, враховуючи характеристики елементів та їхні ваги. Основна ідея ART-2 полягає у розпізнаванні образів через виклик резонансу у відповідних нейронах, керованих керуючим прошарком мережі. Використання бібліотеки PCap сприяє швидкому отриманню та реєстрації мережевого трафіку, що дозволяє ART-2 ефективно аналізувати інформацію. Вхідний вектор містить 41 параметр мережевого з'єднання, які нормалізуються перед обробкою. Дані обробляються на прошарку P, після чого відбувається розрахунок значень нейронів прошарку Y за формулою

$$Y_j = P_i \cdot z_{ij}, \quad (1)$$

де z_{ij} - вага зв'язку між нейронами.

Далі, серед значень нейронів прошарку Y вибирається максимальне, що призводить до коригування нейронів прошарку P за формулою

$$P_i = U_i + d \cdot z_{mi}, \quad (2)$$

де d – константа, що становить 0.9.

Результати оцінюються шляхом обчислення вихідних значень нейронів керуючого прошарку за формулою

$$R_i = U_i + c \cdot P_i, \quad (3)$$

де $c = 0.1$.

Якщо норма RN вектора R не відповідає пороговому значенню, процедура розпізнавання повторюється з можливістю замороження активних нейронів або додавання нових для навчання. ART-2 має можливість створювати нові класи векторів без необхідності перенавчання для додавання нової інформації, що забезпечує високу адаптивність системи. В аналізі та класифікації трафіку також використовується нечіткий класифікатор, інтегруючи нейронні мережі та апарат нечіткої логіки [3].

Дослідження виявило, що наявні системи автоматизованого тестування не задовольняють потреби у виявленні загроз і вразливостей, тому була розроблена нова система на базі нейронної мережі Кохонена для підвищення інформаційної безпеки. Аналітичний огляд підтвердив важливість автоматизації тестування і виявив проблеми у захисті програмного коду, оцінивши існуючі системи.

1. Chaivat J., Naruemon W., Prasert K. Hybrid Neural Networks for Intrusion Detection System. 2002. URL: https://www.researchgate.net/publication/266608342 (дата звернення: 01.04.2024)
2. A Review on Application of Machine Learning and Deep Learning. URL: https://www.ijert.org/a-review-on-application-of-machine-learning-and-deep-learning-for-intrusion-detection (дата звернення: 01.04.2024)
3. Hindawi. Computer Network Intrusion Anomaly Detection with Recurrent Algorithms. URL: https://www.hindawi.com/journals/misy/2022/6576023/ (дата звернення: 01.04.2024).

Моніторинг процесів функціонування інформаційно-комунікаційних систем

УДК 004.73:658.5

[1]Валентина Ящук

[1]Львівський державний університет безпеки життєдіяльності,[1]valentina.lender@gmail.com

Повномасштабне вторгнення росії в Україну спричинило значне зростання кібератак. За даними Державної служби спеціального зв'язку та захисту інформації України, кількість кіберінцидентів у 2022 році збільшилась на 38% порівняно з 2021 роком. Найпоширенішими типами кібератак сьогодні є DDoS-атаки (розподілені атаки відмови в обслуговуванні), фішингові атаки, атаки на вебсайти, шкідливе програмне забезпечення. Ручне реагування на кіберінциденти стає все більш складним і трудомістким, тому виникає необхідність автоматизації цих процесів за допомогою, наприклад, SIEM-систем.

Сучасні організації використовують складні інформаційні системи та мережі, які включають в себе різноманітні пристрої, додатки та протоколи. Управління інформаційною безпекою є складним і трудомістким завданням, яке вимагає постійного моніторингу та аналізу великої кількості даних. SIEM системи дозволяють автоматизувати багато завдань безпеки, що звільняє персонал для виконання інших важливих завдань. Зважаючи на це актуальність використання SIEM систем в менеджменті інформаційної безпеки є незаперечною.

Питаннями, які торкаються найрізноманітніших аспектів менеджменту інформаційної безпеки, займались багато дослідників сучасності, зокрема: Гончар В. І., Сіренко В. В., Зайцев О. В., Шрамко О. В. тощо. Разом з тим,. продовжує залишатись актуальною необхідність у подальших дослідженнях низки питань щодо моніторингу процесів функціонування інформаційно-комунікаційних систем. Проблеми, перераховані вище, їхня актуальність обумовили вибір теми, визначили мету й завдання.

Метою є визначення методичних підходів до автоматизація процесів менеджменту інформаційної безпеки з використання SIEM-систем, що є основою оптимізації. SIEM-система – це система управління інформаційною безпекою та розслідуванням інцидентів (Security Information and Event Management). Вона призначена для збору, консолідації, зберігання, аналізу та візуалізації даних безпеки з різних джерел, таких як мережеві пристрої, сервери, робочі станції, програмне забезпечення безпеки тощо. SIEM-системи використовуються для виявлення, реагування та розслідування інцидентів безпеки, а також для забезпечення відповідності вимогам безпеки.

Роботу SIEM-системи можна розділити на чотири основних етапи: збір даних; консолідація та зберігання даних; аналіз даних; розробка звітів та сповіщень. Окрім цих основних етапів, SIEM-система може виконувати також інші функції, такі як: менеджмент відповідей на інциденти – допомога в реагуванні на виявлені інциденти; аналіз поведінки користувачів – виявлення аномалій у поведінці користувачів; відстеження відповідності вимогам – забезпечення відповідності вимогам безпеки.

SIEM-системи збирають дані з різних джерел, таких як: мережеві пристрої, такі як брандмауери, маршрутизатори, комутатори тощо; сервери, такі як веб-сервери, файлові сервери, бази даних тощо; робочі станції, такі як комп'ютери, ноутбуки, планшети тощо; програмне забезпечення безпеки, таке як антивірусні програми, системи виявлення вторгнень (IDS), системи управління вразливостями тощо. SIEM-системи можуть збирати дані в різних форматах, таких як текстові файли, XML, JSON, CSV тощо. SIEM-система повинна мати можливість обробляти та перетворювати дані в єдиний формат для подальшого аналізу.

SIEM-системи можуть збирати дані кількома способами, такими як: пряме підключення – SIEM-система може підключатися безпосередньо до джерела даних і отримувати дані в реальному час; сервер повідомлень – SIEM-система може отримувати дані з сервера повідомлень, який збирає дані з різних джерел; автоматичне завантаження – SIEM-система може автоматично завантажувати дані з локальних або віддалених файлів; вибір методу збору даних залежить від конкретного джерела даних і потреб організації.

Основними функціями SIEM-систем є збір даних, обробка даних, фільтрація, кореляція, аналіз, виявлення аномалій, виявлення вторгнень, виявлення загроз, генегація рішень, повідомлення про загрози, автоматичне реагування. Сьогодні на світовому ринку представлено широкий спектр SIEM-систем, які пропонують різні функції та можливості. Наведемо деякі з найпопулярніших сучасних SIEM-систем: IBM QRadar: Комплексна SIEM-система, яка пропонує широкий спектр функцій, включаючи виявлення вторгнень, аналіз загроз, управління інцидентами та реагування на них; Splunk Enterprise Security: SIEM-система, яка спеціалізується на аналізі великих обсягів даних; Microsoft Sentinel: SIEM-система, яка інтегрована з іншими продуктами Microsoft, такими як Azure Monitor та Azure Security Center; Siemplify: SIEM-система, яка пропонує простий і зручний інтерфейс; LogRhythm: SIEM-система, яка пропонує широкий спектр функцій та можливостей для великих організацій.

Серед переваг використання SIEM-систем можна виділити підвищення ефективності менеджменту інформаційної безпеки; зменшення часу на реагування на кіберінциденти; підвищення рівня захисту інформації; зниження ризиків кібератак.

При виборі SIEM-системи слід враховувати такі фактори, як: розмір організації, типи даних, які потрібно збирати, функції та можливості, які потрібні. SIEM системи є ефективним інструментом для підвищення рівня інформаційної безпеки організації. Вони допомагають організаціям виявити потенційні загрози на ранніх стадіях, забезпечити відповідність вимогам безпеки, зменшити час реагування на інциденти безпеки та покращити ефективність управління інформаційною безпекою.

1. Miller D. Security Information and Event Management (SIEM) - Implementation Guide / David R. Miller. CRC Press, 2020.
2. Pitis Andrei. SIEM: Trends and Best Practices for Operations and Development / Andrei Pitis, Apress: 2020.

Блокчейн технології при реалізації системи електронного голосування

УДК 004.73: 061.22

[1]Валентина Ящук, [2]Наталія Фединець

[1]Львівський державний університет безпеки життєдіяльності, [2]Львівський торговельно-економічний університет,[1]valentina.lender@gmail.com, [2]nataliafedynets@gmail.com

Процес цифрової трансформації відбувається швидко і докорінним чином змінює усталені системи та структури. Це в повній мірі відноситься до процесу організації волевиявлення громадян з використанням механізму електронного голосування. Між тим, невизначеність самого поняття "електронне голосування" породжує і нерозуміння шляхів практичного втілення електронного голосування, створює певні бар'єри подальшого просування у цьому напрямку.

Питаннями, які торкаються найрізноманітніших аспектів побудов та перспектив розвитку систем електронного голосування, присвячені праці багатьох дослідників сучасності. Разом з тим продовжує залишатись актуальною необхідність у подальших дослідженнях низки питань щодо прикладних проблем комп'ютерних технологій обробки та захисту даних в системах електронного голосування. Проблеми, перераховані вище, їхня актуальність обумовили вибір теми, визначили мету й завдання. Метою є визначення методичних підходів до реалізації системи електронного голосування з використанням блокчейн технології.

Під час регулювання питання електронного голосування необхідно враховувати інструменти захисту даних. Таємниця голосування вимагає, щоб ні орган адміністрування виборів, ні будь-які інші суб'єкти не знали, як проголосував виборець. Водночас орган влади має контролювати доступ до певного рішення, оскільки такий доступ обмежений лише тими, хто має на це право.

Систему електронного голосування доцільно впроваджувати тоді, коли 1) існуватиме чітке розуміння, що електронне голосування є найбільш прийнятним рішенням наявних проблем, 2) братиметься до уваги міжнародний досвід та перші кроки не здійснюватимуться у ізоляції, 3) існуватиме широка згода щодо її доцільності у ключових зацікавлених сторін, 4) буде виділено достатньо часу для технічної імплементації системи та її сприйняття суспільством, 5) у виборців буде довіра і впевненість у виборчій системі та виборчій адміністрації.

Технічно більшість систем е-голосувальних підпадають під один із таких чотирьох типів. Електронні апарати для голосування з прямим записом (direct recording electronic machines – DRE). DRE можуть поставлятися з паперовим слідом або без нього (voter-verified paper audit trail (VVPAT) або контрольний паперовий слід, що перевіряється виборцем). Системи оптичного розпізнавання міток (optical mark recognition – OMR), які використовують сканери, що можуть розпізнати вибір громадянина на спеціальних виборчих бюлетенях, що піддаються автоматичному зчитуванню. Системи OMR можуть бути центральними системами підрахунку (якщо виборчі бюлетені сканують і підраховують у спеціальних центрах підрахунку

голосів) або дільничними системами оптичного сканування й підрахунку (precinct count optical scanning – PCOS). Електронні принтери бюлетенів (electronic ballot printers – EBP), – пристрої, подібні до машин DRE, які видруковують папірці для машинного зчитування або електронні жетони, що містять вибір громадянина. Системи голосування в Інтернеті, коли голоси передаються через Інтернет до центрального серверу підрахунку.

Сьогодні технології – блокчейн підвищують якість життя, надають нові сервіси та послуги, зменшують ризики негативних подій та пом'якшують можливі наслідки. Децентралізація в блокчейні реалізується через складні та пов'язані між собою криптографічні механізми, які гарантують, що події, які вже відбулися та задокументовані, не можуть бути змінені чи скомпрометовані. Блокчейн-системи – це захищені сховища, в яких забезпечується історично стійке зберігання записів (реєстрів), і ці реєстри можуть містити будь-яку важливу інформацію.

Блокчейн представляє собою ланцюжок з блоків даних (що містять транзакції), який одночасно зберігається різними вузлами мережі. Нові блоки даних можуть бути додані до ланцюжка лише за згодою більшості вузлів в результаті досягнення консенсусу, а блоки, щодо яких вузли вже дійшли згоди, не можуть бути модифіковані у майбутньому. Технологія блокчейн базується на використанні надійної криптографії та дозволяє забезпечити: розподілене зберігання інформації на різних вузлах; функціонування системи у разі збою одного або декількох вузлів; надійність та безпеку операцій в режимі повної недовіри між вузлами.

Побудова системи електронного голосування на основі блокчейну дозволить забезпечити виконання таких властивостей як: прозорість: достовірність транзакції, що містить голос виборця, може бути перевірена учасниками протоколу голосування у будь-який момент; цілісність: транзакція, що містить голос виборця, не може бути модифікована або вилучена з блокчейну після того, як блок, в якому міститься ця транзакція, було прийнято у результаті консенсусу; анонімність голосування, що не дозволяє зв'язати транзакцію, що містить голос виборця, з його особою (ідентифікаційними даними); автоматичний підрахунок голосів та публікація результатів голосування. Впровадження технології блокчейн підвищує довіру до інформаційних ресурсів, надійність збереження інформації та якість наданих послуг. Відмітимо, що в Україні технологія блокчейн вже знайшла застосування при розробці електронних реєстрів.

Отже, розроблення системи електронного голосування, що базуватиметься на використанні технології блокчейн, є найперспективнішим напрямом розбудови національної системи електронного голосування.

1. Kateryna Isirova. Blockchain Technology as the Prospective Instrument for Ensuring Electronic Trust Services in Conditions of Cyberthreats // European Cybersecurity Journal. 2018. Issue 5 (1). P 34-43
2. Gorbenko I., Kuznetsov A., Gorbenko Y., Vdovenko S., Tymchenko V. Studies on Statistical Analysis and Performance Evaluation For Some Stream Ciphers // International Journal of Computing. 2019. 18(1). P. 82-88.

НАУКОВЕ ВИДАННЯ

МАТЕРІАЛИ
XIII Міжнародної науково-технічної конференції
«ITSec: Безпека інформаційних технологій»

9-11 травня 2024 року

м. Львів (Україна)

Організаційний комітет конференції та редакція можуть не поділяти думки авторів і не несуть відповідальність за достовірність викладеної інформації.

За науковий зміст і викладення матеріалу, достовірність та коректність фактичних даних (у тому числі класифікаційного індексу УДК) уся відповідальність покладається на авторів та їх наукових керівників.

Неінформативний текст матеріалів доповіді міг бути скорочений або вилучений на розсуд Оргкомітету конференції.

Оригінал-макет підготовлено на кафедрі кібербезпеки
Львівського національного університету імені Івана Франка