UDC004.056.5:004.9:004.89 **doi:** https://doi.org/10.20998/3083-6298.2025.02.08

Serhii Pohasii[1], Ruslan Vegiiev[1], Vadym Stetsenko[1], Ruslan Trofymenko[1], Dmytro Rykov[2], Vitalii Pokalitsyn[3]

[1]National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
[2]Kharkiv National University of Radioelectronics, Kharkiv, Ukraine
[3]CS Ltd, Kharkiv, Ukraine

EXPERT-BASED ASSESSMENT OF CRITICAL SECURITY THREATS IN SMART HOME CYBER-PHYSICAL SYSTEMS

Abstract. Topicality. Smart home systems are becoming increasingly popular as they offer homeowners many benefits, such as increased convenience, energy efficiency, and improved security. However, these systems can also pose potential security risks if not properly secured. Detecting threats in a smart home system is crucial for protecting personal data, preventing physical security breaches and cyberattacks, and ensuring the proper functioning of the system. The article examines the assessment of the most dangerous threats to the cyber-physical system of a smart home. The process was carried out by conducting an in-depth examination based on a wide list of threats, taking into account their impact on security services. All threats were identified according to their source according to the concept of double-circuit security. The **subject of the article** is the methods of expert assessment of critical security threats in cyber-physical systems of a smart home. **The purpose of the study** is to identify and classify the most dangerous security threats to cyber-physical systems of a smart home based on expert assessment. As a **results**, the most critical threats to cyber-physical systems of a smart home were identified and the basis for developing algorithms for their effective prevention was formed. **Conclusions.** As a result of the expert assessment, the most critical threats to cyber-physical systems of a smart home were identified, which creates the basis for developing effective methods for their prevention and risk minimization.

Keywords: Internet of Things, cyber-physical systems, smart home, security threat, expertise.

Introduction

The relevance of the problem. The Internet of Things, like any other technology, can be vulnerable to cyber-attacks and hacking. Attackers can exploit various areas of the Internet of Things to gain unauthorized access to devices, steal data, or weaponize cyberattacks.

Cyber-physical smart home systems consist of three main components:

Physical components that include various IoT devices such as smart thermostats, smart locks, security cameras, motion sensors, and other devices.

Software components that provide the user with the ability to control and monitor smart home devices. These components can be installed on user devices such as smartphones and tablets, as well as computers and cloud servers.

Network components that provide communication between physical and software components, as well as provide access to the Internet.

One of the challenges in IoT security is that many devices are built with old or weak components with limited security capabilities. Some manufacturers may also not pay enough attention to the software security of their devices, so there are risks of using outdated versions of applications or those that contain vulnerabilities [1].

Ensuring the security of cyber-physical systems of a smart home is an important aspect that requires efforts from both device manufacturers and users. The main problems are: insufficient data encryption, weak password protection, lack of authentication and authorization mechanisms [10-12].

1. Main part

The problem with insufficient data encryption in the Internet of Things is that data transmitted between devices can be intercepted and read by third parties. This can lead to the theft of confidential information or violation of user privacy [2].

Insufficient encryption can be caused by the use of weak encryption algorithms or improper configuration of IoT devices.

To avoid problems with insufficient data encryption, it is important to use strong encryption methods.

The solution to this problem is the use of cryptographically stable encryption algorithms in the post-quantum period. The use of McEliece (Niederreiter) crypto-code constructions (CCC) on algebra-geometric codes (codes using an additional session key – the equation of a geometric curve) allows to ensure confidentiality (security of data transmission) in "Smart Home" systems. Ensuring integrity can be formed by additional encryption of data (forming a safe), as well as forming multi-contour security systems (forming internal and external contours) [3].

Each measurement subsystem is a device that can work completely autonomously, independently of the general smart home system, controlling a certain part of it with the possibility of direct protected control via a smartphone or computer.

Each measurement subsystem sends a data packet to a local server, which allows to control the house without the Internet, being in the same local network (being connected to a WI-FI router). To ensure the protection of wireless channels, it is proposed to use post-quantum algorithms based on asymmetric cryptosystems,

which are built on the basis of the crypto-code structures of McEliece and Niederreiter. The use of crypto-code structures provides basic security services: confidentiality, integrity and authenticity. In addition, crypto-code structures integratedly provide the necessary level of stability (also in the conditions of the appearance of a full-scale quantum computer), efficiency (encryption speed is comparable to the speed of cryptographic transformations in modern block ciphers) and reliability (due to the use of interference-resistant codes when building asymmetric cryptosystems). Taking into account the level (degree) of secrecy in the proposed crypto-code structures, it is possible to use various codes: elliptical codes, modified elliptical codes, LDPC and lossy codes. The use of two symmetrical systems allows to increase the level of the protection system as min by 2 times [4].

Information in the network of the internal circuit of the "Smart House" cyber-physical system (CPS) is transmitted via open wireless channels with encryption based on Niederreiter's crypto-code constructions (CCC) on jamming-resistant codes.

When managing the modified "Smart House" CPS from the external environment (Internet), an external circuit of interaction with other systems is added to the system. In this case, the information received from the sensors and processed in the local server (which is physically located in the house) is transmitted over the Internet connection to the end user using encryption algorithms based on McEliece's CCC on LDPC codes [5].

LDPC codes (Low-Density Parity-Check codes) are one of the types of codes used in digital communication systems to detect and correct errors in data transmission. In recent years, these codes have become widely used in the Internet of Things (IoT) due to their high characteristics of error correction and data transmission efficiency [6].

The modified "Smart House" CPS manages a complex of autonomous systems, each of which controls certain devices in the house, connecting them into a common system, which allows you to conveniently control each one separately, apply various automation protocols, and also has the possibility of fully autonomous operation. In fig. 1 in the modified CFS "Smart House" two contours of information processing and transmission and possible cyber-attacks are given.

The internal contour contains two main subsystems:

the measurement subsystem collects information from all sensors about the physical condition of the building;

the management subsystem sends protection commands to the device itself, which is controlled by the local server system.

Each measurement subsystem is a device that can work completely autonomously, independently of the overall smart home system, controlling a certain part of it with the possibility of direct protected control via a smartphone or computer [7].

Each measurement subsystem sends a data packet to a local server, which allows you to control the house without the Internet, being in the same local network (being connected to a WI-FI router). To ensure the protection of wireless channels, it is proposed to use post-quantum algorithms based on asymmetric cryptosystems, which are built on the basis of the crypto-code structures of McEliece and Niederreiter.

According to the diagram in Fig. 1, three directions of cyber-attacks are defined: external, internal, and attacks on communication channels that provide data transmission between contours.

The most comprehensive, open industry standard used for vulnerability assessment is The Common Vulnerability Scoring System (CVSS). When building a security threat model, it is often difficult to identify and indicate risk factors that can be implemented in CPS [9].

The consequences of the implementation of the threat are categorized according to the three main properties of information from the point of view of information security – confidentiality, availability and integrity.

Compilation of a list of relevant risk factors for CPS involves the use of a database of 220 CVSS threats. Based on the relevance of the attack area, the type of intruder was classified as: an internal intruder with low, medium and high potential, similarly an external intruder with the same potentials, the consequences of the threat implementation: violation of confidentiality, violation of integrity, violation of availability [9].

An analysis of cyberattacks for additional expert assessment can be relevant for the identification of inconsistencies in the system, and the assessment of the level of threat, like a stink. Below is a general algorithm for analyzing cyberattacks based on expert evaluation. The general scheme of expert assessment of threats at the CPS is shown in Fig. 2.

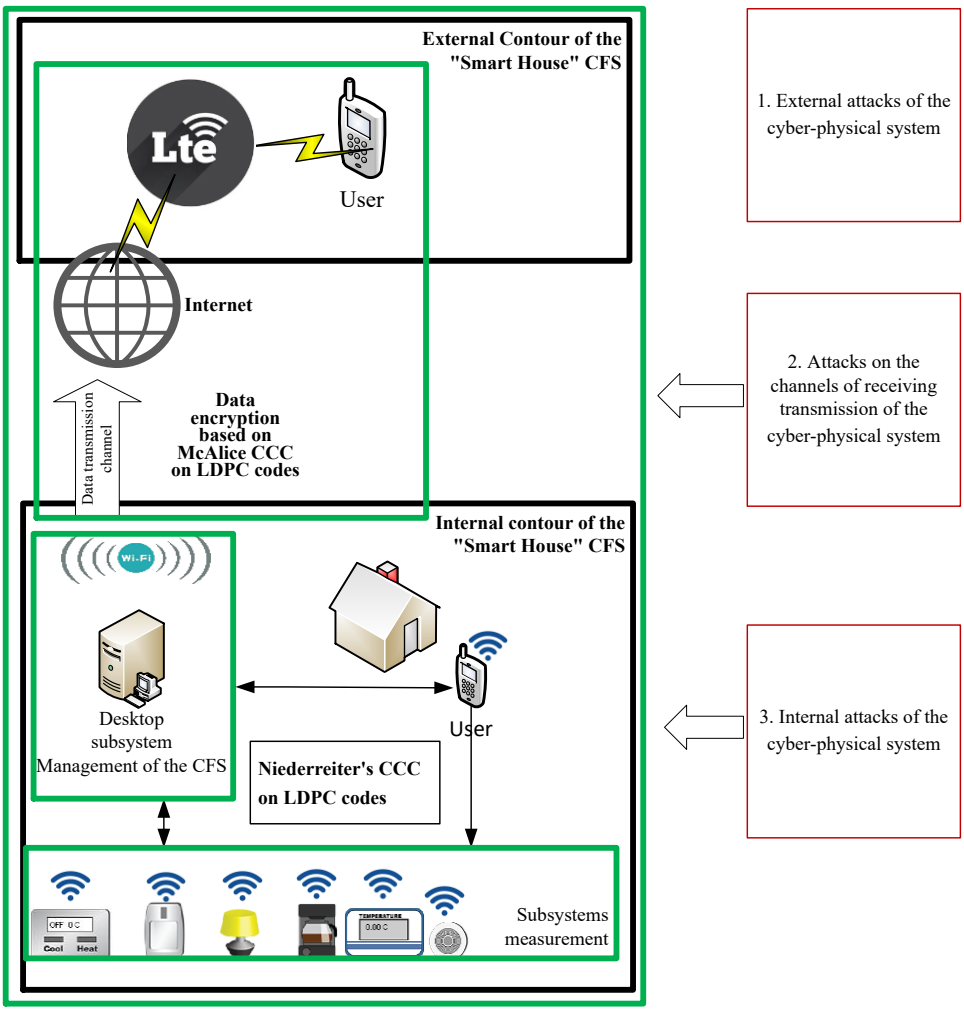

Fig. 1. Modified "Smart House" CPS with directions of possible cyber-attacks [8]

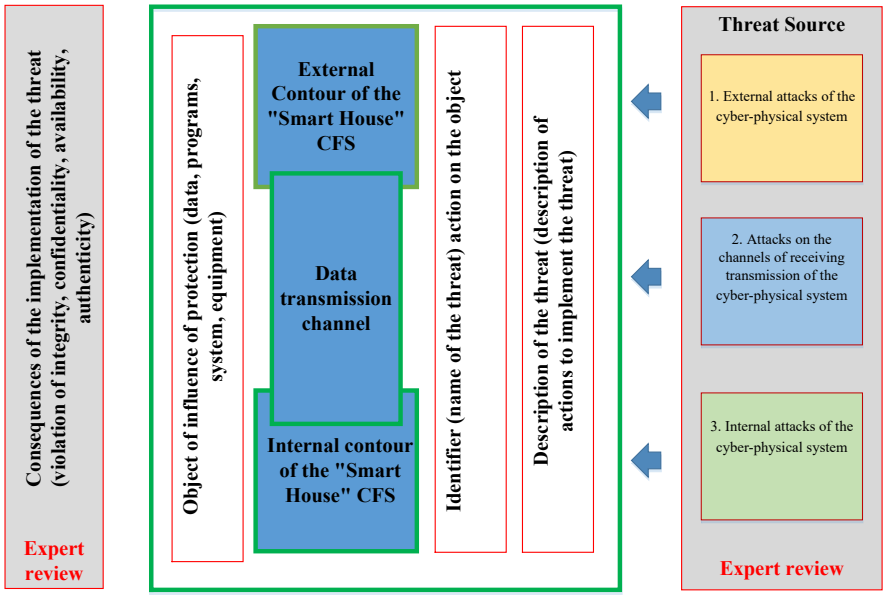

Fig. 2. General scheme of expert assessment of threats at the CPS

The severity level of a detected vulnerability in the database, depending on the value of the base vulnerability score V, uses the following severity levels:

- low level, if 0,0 < V < 3,9;
- average level, if 4,0 < V < 6,9;
- high level, if 7,0 < V < 9,9;
- critical level, if V = 10,0.

At the same time, for the objectivity of expert judgments, we use the weight coefficients of expert competence (k_k) [13] presented in Table. 1.

Table 1 **– Expert competence weight coefficient**

No	*Expert qualification*	*The value of the weighting factor (k_k)*
1	international expert in the field of IS, CS	1,00
2	national expert in the field of IS, CS	0,95
3	certified international specialist in the field of IS, CS	0,90
4	full doctor of science in IS, CS	0,90
5	security chief	0,85
6	Doctor of Philosophy in IS, CS	0,80
7	security officer	0,70
8	system administrator	0,60
9	security engineer	0,50
10	postgraduate student in the field of IS, CS	0,40

The total assessment of the i_{th} threat is determined by the number of experts according to the expression:

$$x_i = \frac{\sum_{k=1}^{K} x_k \times k_k}{K}, \quad (1)$$

where x_k– assessment of the *k-th* expert in the *i-th* threat; k_k – expert competence level; K – number of experts.

A measure of the consistency of expert assessments is the dispersion, which is determined by the expression:

$$\sigma_x^2 = \frac{1}{K}\sum_{k=1}^{K} k_k \left(x_k - x_i\right)^2. \quad (2)$$

Statistical probability of the received results $1 - \alpha_i$, will amount to: $\left[x_i - \Delta, x_i + \Delta\right]$, where the value x_i distributed according to the normal law with the center in x_i and dispersion σ_x^2. Then Δ is determined by the expression:

$$\Delta = t\sqrt{\sigma_x^2 / N}, \quad (3)$$

where t – value according to the Student's distribution for $K - 1$ freedom degree.

After an expert evaluation by twenty experts, 220 possible attacks were previously divided by threat sources into: external, internal, and attacks on communication channels that provide data transmission between circuits. An expert scale from 0 to 1 could be used to assess the threat level of a cyberattack, the value 0 on this scale corresponds to zero threat, and the value 1 - the maximum threat of violation: confidentiality, integrity, availability, authenticity. The assessment of the level of the threat of a cyber-attack based on an expert scale may include factors: the level of access to the target system, the complexity of the attack, the presence of vulnerabilities in the target system, the level of motivation of the attacker, the presence of defensive measures in the target system.

As a result of the analysis of expert opinions based on the sum of expert evaluations for security services, and the average expert evaluation for the source of the threat within the group, the most influential threats to the contours of the CPS smart building were selected (Table 2).

Table 2 **– Summary table of the most influential threats to the contours of the smart house CPS**

Threat group	*The name of the smart house CPS threat*	*The source of the threat (the second characteristic of grouping)*	*The sum of expert assessments by the security services*	*Average expert assessment by source of threat within the group*
External threats	The threat of bypassing multi-factor authentication	An external attack with a high potential for implementation	17,4з	14,2
	The threat of overcoming physical protection	An external attack with medium implementation potential	18,6	13,4
	Code or data injection threat	External attack with low implementation potential	13,7	10,4
Internal threats	The threat of introducing malicious code into the BIOS	Internal violator with high realization potential	17,3	14,8
	The threat of spreading unauthorized elevated rights to the entire grid system	Internal violator with average realization potential	15,9	12,8
	The threat of inconsistency in the rules of access to big data	Internal violator with low realization potential	13,2	10,2

Threat group	*The name of the smart house CPS threat*	*The source of the threat (the second characteristic of grouping)*	*The sum of expert assessments by the security services*	*Average expert assessment by source of threat within the group*
Attacks on communication channels that provide data transmission between circuits	The threat of violation of information processing technology by unauthorized changes to the images of virtual machines	External attack with medium potential; An internal attack with medium implementation potential	16,7	13,1
	The threat of interception of control of the automated control system of technological processes	External attack with high potential; An internal attack with medium implementation potential	15,7	13,8
	The threat of distortion of information entered and output on peripheral information devices	External attack with high potential; An insider attack with low implementation potential	15,6	15,1
	The threat of bypassing incorrectly configured authentication mechanisms	External attack with low potential; An insider attack with low implementation potential	15,4	11,2
	The threat of using a compromised trusted software update source	Internal attack with medium potential; An external attack with medium implementation potential	13,8	13,8
	Threat of using default identification/authentication information	Internal attack with low potential; An external attack with medium implementation potential	12,9	10,5

External threats to the CPS that have priority monitoring consist of:

Threats of bypassing multi-factor authentication, which consists in the possibility of bypassing multi-factor authentication by introducing malicious code into the discredited system and components participating in the multi-factor authentication procedure. in the case of a discredited user working with files from untrusted sources, if he has software installation privileges.

The threat of overcoming physical protection – opens the possibility for the violator to carry out almost any destructive actions against the discredited information system when he obtains physical access to the computer hardware of the system by overcoming the physical access control system organized in the enterprise building. locks in the room, staff mistakes, etc.).

The threat of introduction of code or data is based on the possibility of introduction by an offender into a discredited information system or an IoT device of malicious code, which can be later launched "manually" by users, automatically upon fulfillment of a certain condition (onset of a certain date, user login, etc.) or with the use of authentication data set "by default", as well as the possibility of unauthorized introduction by the violator of some of his own data for processing into a discredited information system, actually making illegal use of other people's computing resources, and blocking the operation of the device when executing certain commands.

Implementation of this threat is possible: in the case of a discredited user working with files coming from untrusted sources; if he has privileges to install programs_0 in the case that the owner has not changed the credentials of the IoT device

Regarding the internal threats of the CPS from the entire volume presented to the study, according to the experts, primary attention should be given to the following.

The threat of introducing malicious code into the BIOS is to force the BIOS/UEFI to execute the malicious code every time the server is started by injecting it into the BIOS/UEFI by updating the BIOS/UEFI software to a version that already contains the malicious code. by updating the BIOS/UEFI software and replacing the BIOS/UEFI chipset.

The threat of the spread of unauthorized elevated rights to the entire KFS grid system is the possibility of automatic distribution of privileges illegally obtained by the violator on one node to the entire grid system. possible if the violator successfully increases his rights on one node of the grid system.

The threat of inconsistency in the rules of access to big data can be realized by providing erroneous unauthorized access to protected information or, conversely, the possibility of denying access to protected information to legal users due to mistakes made by them when delegating privileges by other legal users of the big data storage, access to information of different users in the big data repository.

Attacks on communication channels that provide data transmission between circuits.

The threat of violation of information processing technology through unauthorized changes to images of virtual machines, destructive software influence on a discredited system or indirect destructive software influence through it on other systems by unauthorized access to images of virtual machines. Implementation of this threat may result in:

to violation of the confidentiality of protected information processed using virtual machines created on the basis of unauthorized modified images;

to violation of the integrity of programs installed on virtual machines;

to violation of the availability of virtual resources;

to create a botnet by injecting malware into virtual machine images used as templates (reference images).

The threat of interception of the control of the automated system of technological process control by the violator of unauthorized access to the information infrastructure at the expense of the violator obtaining the right to control the automated system of technological process control, which is part of it, by exploiting the vulnerabilities of its software or the weaknesses of technological data transmission protocols. This is due to the presence of a smart house, software network interfaces of interaction and, as a result, the possibility of unauthorized access to this system, as well as the insufficiency of network traffic filtering and anti-virus protection measures. The implementation of this threat is possible provided that the violator has the rights to interact with the automated process control system. The implementation of this threat can lead to: blocking or distortion (incorrect execution) of algorithms for working out the tasks of managing technological processes, direct management of the company's equipment; violation of the normal flow of technological processes; partial or complete stoppage of technological processes without) equipment failure; emergency situation in the critical information infrastructure system.

The threat of distortion of information entered and output on peripheral information devices is based on misinforming users of the CPS, by replacing or distorting output data coming from sensors, keyboards or other information input devices, as well as replacing or distorting information output on peripheral devices.

The threat of bypassing incorrectly configured authentication mechanisms is the possibility of an offender obtaining privileges in the system without going through the authentication procedure by performing actions that violate the conditions for the correct operation of authentication tools (for example, entering data in an unsupported format). input data.

The implementation of this threat is possible if there are errors in the specified values of the settings of the authentication mechanisms.

The threat of using a compromised trusted source of software updates is the possibility of introducing malicious code into the information system due to the use of compromised trusted sources of software updates.

The threat of using identification/ authentication information set by default when the offender passes the authorization procedure on the basis of identification and authentication information received from open sources or from an information service, corresponding to the "default" account of the discredited protection object. The "default" accounts are intended for the initial login to the system or because the automatic password generation mechanism issues the same or similar passwords to users with similar logins when going through the registration procedure on the information service.

In this way, the first and partly the second tasks in the system of classification, identification and recognition of threats in the cyber-physical system of a smart house was solved. Solving the following tasks is the object of further research.

2. Discussion of results

The conducted research allowed to systematize and assess the range of threats to cyber-physical systems of the "smart home", which is an important step in ensuring their security. The application of the expert assessment method turned out to be an effective tool for identifying and ranking threats in complex, multi-component systems, where statistical data on real incidents may be limited. The results confirmed that the risks to the "smart home" are not limited only to external cyberattacks; internal threats and vulnerabilities in communication channels also pose a significant danger. In particular, the identification of attacks on communication channels as a separate group emphasizes the critical role of data transmission security between physical and cyberspace, which is often ignored in traditional protection models.

The obtained quantitative and qualitative threat indicators have direct practical significance. They allow not only to identify the most likely and dangerous attack vectors, but also to prioritize security measures. For example, by identifying a specific type of insider threat with a higher expert rating, developers can focus resources on building user authentication mechanisms or network segmentation, rather than just hardening external firewalls. This highlights that targeted application of research findings allows for more effective and cost-effective cybersecurity strategies.

3. Conclusions

According to the results of the study, it was found that the smart house CPS has three directions of possible cyber-attacks: external, internal threats, and attacks on communication channels that provide data transmission between circuits.

In order to determine the most probable threats to the contours of the smart house CPS, it is proposed to use an expert analysis consisting of an assessment of 220 threats by 20 experts with varying degrees of professionalism. Based on the results of the analysis, violations were determined: confidentiality, integrity, availability, authenticity, calculated The calculated sum of expert evaluations for security services, the average expert evaluation for the source of the threat within the

groups that make up the arrays: external, internal threats, and attacks on communication channels.

Based on the results of calculations, the most likely most dangerous threats in groups of threats were determined based on the values of the sums of expert evaluations for security services and the average expert evaluation for the source of the threat within the group, which made it possible to form arrays of the most likely threats along all contours of the smart house CPS. Qualitative threat indicators for security services for CPS make it possible to further develop an algorithm to prevent cyberattacks, giving priority to testing CPS for identified threats.

However, it is important to note that the threat level assessment is only a forecast and does not guarantee that a cyber-attack will not occur, this data can be used to make decisions about what cyber security measures should be taken to prevent similar attacks in the future.

REFERENCES

1. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et. al. (2021), "Synergy of building cybersecurity systems", Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) *Kharkiv: PC Technology Center*, 188 p., doi: http://doi.org/10.15587/978-617-7319-31-2
2. Tondel, I. A., Cruzes, D. S., Jaatun, M. G., Sindre, Guttorm (2022), "Influencing the security prioritisation of an agile software development project", *Computers & Security,* Vol. 118, pp. 1–19., doi: https://doi.org/10.1016/j.cose.2022.102744
3. Șcheau, M. C., Leu, M. D., Udroiu, C. (2022), "At the Intersection of Interests and Objectives in Cybersecurity", *International Conference on Cybersecurity and Cybercrime,* Vol. 9, pp. 29–34., doi: https://doi.org/10.19107/CYBERCON.2022.03
4. Branco, P. de M. (2017), "A new LDPC-based McEliece cryptosystem", *Tecnico Lisboa,* 79 p., file:///C:/Users/Admin-EK/Downloads/Thesis.pdf
5. Engelbert, D., Overbeck, R., Schmidt, A. (2007), "A Summary of McEliece-Type Cryptosystems and their Security", *Journal of Mathematical Cryptology,* Vol. 1(2), pp. 151–199. doi: https://doi.org/10.1515/jmc.2007.009
6. Misoczki, R., Tillich, J.-P., Sendrier, N., Barreto, P. S. L. M. (2012), "MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes", https://eprint.iacr.org/2012/409.pdf
7. Pohasii, S. (2022), "Models and methods of information protection in cyber-physical systems", *Information security*, Vol. 28, No. 2, pp. 67–79.
8. Pohasii, S. (2022), "Assessment of the level of security in cyber-physical systems", *Protection of information,* Vol. 24, No. 2, pp. 81–94.
9. Mell, P., Scarfone, K. and Romanosky, S. (2007), "A Complete Guide to the Common Vulnerability Scoring System Version 2.0", *FIRST,* https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=51198
10. Laptiev, O., Lukova-Chuiko, N., Laptiev, S., Laptieva, T., Savchenko, V., Yevseiev, S. (2021), "Development of a method for detecting deviations in the nature of traffic from the elements of the communication network", International Scientific And Practical Conference "Information Security And Information Technologies", Kharkiv – Odesa, Ukraine (13-19 September 2021). pp.1–9.
11. Savchenko, V., Akhramovych, V., Dzyuba, T., Lukova-Chuiko, N., LaptievA, T. (2021), "Methodology for calculating information protection from parameters of its distribution in social networks", *IEEE 3rd International Conference on Advanced Trends in Information Theory,* ATIT, pp. 99–105.
12. Korchenko, A., Breslavskyi, V., Yevseiev, S., Zhumangalieva, N., Zvarych, A., Kazmirchuk, S., Kurchenko, O., Laptiev, O., Sievierinov, O., Tkachuk, S. (2021), "Development of a Method for Constructing Linguistic Standards for Multi-Criteria Assessment of Honeypot Efficiency", *Eastern-European Journal of Enterprise Technologies,* Vol. 1 (2(109)), pp. 14-23., doi: https://doi.org/10.15587/1729-4061.2021.225346
13. Milov, O., Yevseiev, S., Ivanchenko, Y., Milevskyi, S., Nesterov, O., Puchkov, O., Salii, A., Timochko, O., Tiurin, V., Yarovyi, A. (2019), "Development of the model of the antagonistic agents behavior under a cyber conflict", *Eastern-European Journal of Enterprise Technologies,* Vol. 4 (9–100), pp. 6–10., doi: https://doi.org/10.15587/1729-4061.2019.181047

Received (Надійшла) 18.07.2025
Accepted for publication (Прийнята до друку) 01.08.2025

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Погасій Сергій Сергійович – доктор технічних наук, доцент, професор кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Serhii Pohasii – Doctor of Technical Sciences, Docent, Professor of Cybersecurity Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: spogasiy1978@gmail.com; ORCID Author ID: https://orcid.org/0000-0002-4540-3693; Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57217487471.

Вегієв Руслан Станіславович – магістр психології, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Vegiiev Ruslan – Master Degree of Psychology, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: vegiev@gmail.com; ORCID Author ID: https://orcid.org/0009-0007-8636-8322.

Стеценко Вадим Олегович – аспірант кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Vadym Stetsenko – PhD student of Cyber Security Department, National Technical University "Kharkiv polytechnic institute", Kharkiv, Ukraine;
e-mail: 4all2dream@gmail.com; ORCID Author ID: https://orcid.org/0009-0008-5315-5539;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=59185285700.

Трофименко Руслан Валентинович – аспірант кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Ruslan Trofymenko – PhD student of Cybersecurity Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: Ruslan.Trofymenko@cs.khpi.edu.ua; ORCID Author ID: https://orcid.org/0009-0001-3114-2269;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=59951694400.
Риков Дмитро Миколайович – аспірант кафедри безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Харків, Україна;
Dmytro Rykov – PhD Student of Department of Information Technology Security, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine;
e-mail: dmytro.rykov@nure.ua; ORCID Author ID: https://orcid.org/0000-0002-3427-0290.
Покаліцин Віталій Вікторович – магістр з комп'ютерної механіки, керівник проекту–Головний статистичний програміст, CS Ltd, Харків, Україна;
Vitalii Pokalitsyn – Master's of computer mechanic; Project Lead–Principal, Statistical Programmer, CS Ltd, Kharkiv, Ukraine;
e-mail: v.pokaitsyn@gmail.com; ORCID Author ID: https://orcid.org/0009-0005-6348-3972.

ЕКСПЕРТНА ОЦІНКА КРИТИЧНИХ ЗАГРОЗ БЕЗПЕЦІ В КІБЕРФІЗИЧНИХ СИСТЕМАХ РОЗУМНОГО БУДИНКУ

С.С. Погасій, Р. С. Вегієв, В. О. Стеценко, Р. В. Трофименко, Д. М. Риков, В. В. Покаліцин

Анотація. Актуальність. Системи розумного будинку стають дедалі популярнішими, оскільки вони пропонують домовласникам багато переваг, таких як підвищена зручність, енергоефективність та покращена безпека. Однак ці системи також можуть становити потенційні ризики для безпеки, якщо вони не захищені належним чином. Виявлення загроз у системі розумного будинку має вирішальне значення для захисту персональних даних, запобігання порушенням фізичної безпеки та кібератак, а також забезпечення належного функціонування системи. У статті розглядається оцінка найнебезпечніших загроз для кіберфізичної системи розумного будинку. Процес було здійснено шляхом проведення поглибленої експертизи на основі широкого переліку загроз, враховуючи їхній вплив на служби безпеки. Усі загрози були ідентифіковані відповідно до їх джерела за концепцією подвійної контурної безпеки. **Предметом дослідження** у статті є методи експертної оцінки критичних загроз безпеці в кіберфізичних системах розумного будинку. **Метою статті** є визначення та класифікація найбільш небезпечних загроз безпеці для кіберфізичних систем розумного будинку на основі експертної оцінки. **Були отримані наступні результати.** Визначено найкритичніші загрози для кіберфізичних систем розумного будинку та сформовано основу для розробки алгоритмів їх ефективного попередження. **Висновки.** В результаті проведеної експертної оцінки було визначено найбільш критичні загрози для кіберфізичних систем розумного будинку, що створює основу для розробки ефективних методів їхнього попередження та мінімізації ризиків.

Ключові слова: Інтернет речей, кіберфізичні системи, розумний будинок, загроза безпеці, експертиза.