DEVELOPMENT OF SECURITY MECHANISMS FOR SCADA SYSTEMS IN THE POSTQUANTUM PERIOD

The formation of new systems based on the synthesis of mobile Internet technologies with cyberspace significantly expands the possibilities of creating smart technologies based on mesh and sensor networks. This allows to significantly increase the speed of information transmission using modern wireless communication channels based on technology standards IEEE802.16, IEEE802.16e, IEEE802.15.4, IEEE802.11, Bluetooth 5, 6. It is possible to use SCADA automation and scheduling systems with new functions of managing information flows of various technological processes, to create new principles for building hyperphysical social systems (CPSS) – a set of subjects and objects of cybernetic, physical and social worlds that allow to form “smart” communities, on the one hand, and intellectual space on the other. However, the development of modern computer systems, the advent of full-scale quantum computers significantly impairs the security of modern security systems. According to NIST experts, a full-scale quantum computer breaks both symmetric and asymmetric cryptosystems in polynomial time, which significantly reduces their stability. The goal of the work is to develop mechanisms for providing security services based on post-quantum algorithms - crypto-code constructions. To ensure security in the post-quantum period – the emergence of a full-scale quantum computer, NIST specialists suggest the use of post-quantum algorithms. Structural schemes of crypto-code constructions of McEliece and Niederreiter on algebrogeometric codes are used in the work. The paper proposes mechanisms of post-quantum cryptography, which allow to ensure the stability of not only communication channels, but also elements of the structure of the management system of SCADA systems, not only in critical infrastructure, but also in modern wireless communication channels. The basis of post-quantum encryption algorithms is the combination of algorithms (schemes) of crypto-code structures with cryptosystems on unprofitable codes (multi-channel cryptography), as well as the possibility of combining them with digital steganography methods. The developed approach provides the ability to hide elements of management commands, and the use of different channels provides the ability to hide individual elements of cryptograms. The use of post-quantum encryption algorithms provides a significant increase in the cryptographic stability of security mechanisms SCADA-systems.

Keywords: SCADA-systems, sociocyberphysical systems, post-quantum algorithms, cryptocode constructions, algebro-geometric codes

Introduction

General Problem Statement. The development of computing resources and “G” technologies has determined the rapid growth of smart technologies based on mesh and sensor networks based on the synthesis of physical systems and Internet technologies.

SCADA systems (SCADA – supervisory control and data acquisition) – a system of dispatch control and data collection, real-time processing of information received through communication channels from the sensors of the control object (as a control objects are not only objects of critical infrastructure based on the synthesis of information and communication systems (ICS) and cyber-physical systems (CPS), which are the core of modern information-critical cybernetic systems information-critical cybernetic systems, CCIS), as well as the formation of sociocyberphysical systems – systems of complexing SPS with elements of the infrastructure of social networks and technologies (cyberphysical social system, CPSS). It can reach several tens of thousands, which allows to significantly expand the possibilities of SCADA dispatching not only critical infrastructure facilities, but also sociocyberphysical systems [1–4].

The development of smart technologies based on the combination of CPS with Internet mobile technologies can significantly increase the speed not only of information transmission and processing of information flows, but also to ensure the development of new functionalities of scheduling systems, their integration with cloud technologies and networks. networks using wireless channel standards: mobile technologies LTE (Long-Term Evolution - long-term evolution), IEEE802.16, IEEE802.16e, IEEE802.15.4, IEEE802.11, Bluetooth [5–9].

However, their development determines a new direction in the development and/or modification of old threats, which is manifested not only in the possibility...
of hacking and unauthorized access to confidential (personal) information of users, but also the possibility of “energy apocalypse”. This approach allows cybercriminals to use CPSS to obtain a synergistic effect from the implementation of threats in cyberspace as a whole. Thus, to prevent or maintain a security contour in CPSS processes for the analysis of deviations from normal operation and/or hacking of the system requires a unified approach to building a classification of threats, taking into account their synergy and hybridity to all components of security: information security (IS), cybersecurity (CS) and security of information (SI), in terms of their presentation with the methods of social engineering and lack of funds to ensure the required level of security [5–8].

In the race for speed, such channels do not provide confidentiality and integrity services, and the KNX standard (ISO / IEC 14543 standard) provides separate security services for smart House technologies using symmetric encryption systems, which in the conditions of full-scale quantum computer reduce the level of stability [10–17]. The Diameter protocol provides interaction between clients in order to authenticate, authorize and account for various security services, but has significant shortcomings in terms of modern cyberattacks [17–19]. In such conditions, post-quantum cryptoalgorithms based on the synthesis of theories of noise-tolerant coding and information protection – crypto-code constructs (CCC – crypto code constructions) – can be considered as an alternative mechanism for security [5; 20–23]. Such designs are hybrids, because The formation of an asymmetric cryptosystem (crypto-resistance is based on a theoretically complex task – decoding a random code) is provided through the use of algebraic codes. According to US NIST experts, Galois field (GF 210–213) is needed to ensure crypto-stability of noise code generation, which is a rather difficult question even with modern computing resources. Use in wireless cyberphysical systems requires a significant reduction in the field, which will allow on the one hand to reduce energy consumption, and on the other hand requires the required level of cryptocurrency. Thus, CCIS/CPSS (SCADA) based on wireless mobile technologies requires cryptosystems that will provide the required level of crypto-resilience in the post-quantum period, energy consumption that will allow the use of smart technologies, as well as provide a full range of security services.

**Analysis of the Recent Research and Publications.** The analysis of works [5–8] determines the need to create conditions for ensuring the security of the business process contour in CPSS. Thus, the NIST of the United States has conducted research that calls into question the stability of modern symmetric and asymmetric cryptosystems with the advent of a full-scale quantum computer. In addition, the Shore algorithm allows to factorize the number N over time $O(\lg N)$, using $O(\lg N)$ bits register, which is significantly faster than any classical method of factorization. The advantages of using quantum registers are significant memory savings (N quantum bits can contain $2^n$ bits of information), the interaction between qubits makes it possible to influence the entire register in one operation (quantum parallelism) [2–5]. Table 1 shows the results of a comparative analysis of the complexity of factorization for classical and quantum algorithms [2–5; 20].

**Table 1**

<table>
<thead>
<tr>
<th>Module size N, bit</th>
<th>The number of required qubits $2n$</th>
<th>The complexity of the quantum algorithm $4n^3$</th>
<th>The complexity of the classical algorithm $f(n)=7n+4\log_2 n+1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>512</td>
<td>1024</td>
<td>0.54·10$^9$</td>
<td>1.6·10$^{19}$</td>
</tr>
<tr>
<td>3072</td>
<td>6144</td>
<td>12·10$^{10}$</td>
<td>5·10$^{41}$</td>
</tr>
<tr>
<td>15360</td>
<td>30720</td>
<td>1.5·10$^{13}$</td>
<td>9.2·10$^{40}$</td>
</tr>
</tbody>
</table>

Source: developed by the authors.

Table 2 shows the results of the analysis of the complexity of the implementation of the Shore method of discrete logarithmization of a group of EC points [2–5; 20].

**Table 2**

| Algorithm for calculating the discrete logarithmic equation $f(n)=7n+4\log_2 n+1$ |
|-----------------|---------------------------------|---------------------------------|---------------------------------|
| The size of the order of the base point, bits | Number of required qubits $360n^3$ | Complexity of the quantum algorithm $360n^3$ | Complexity of the classical algorithm $f(n)$ |
| 163             | 1210                           | 1.6·10$^9$                     | 3.4·10$^{24}$                   |
| 256             | 1834                           | 6·10$^9$                      | 3.4·10$^{38}$                   |
| 571             | 4016                           | 6.7·10$^{10}$                 | 8.8·10$^{35}$                   |
| 1024            | 7218                           | 3.8·10$^{11}$                 | 1.3·10$^{154}$                 |

Source: developed by the authors.

In the conditions of post-quantum cryptography, NIST experts suggest considering special attacks (SIDE-CHANNEl ATTACKS). The implementation of these attacks is aimed at finding vulnerabilities in the practical implementation of the cryptosystem, especially in the means of cryptographic protection [2–5; 20].

The possibility of using quantum technologies by the enemy and/or cybercriminals to hack the command and control system of troops and weapons is questionable to ensure cryptographic stability of cryptograms, which are based on modern algorithms of symmetric and asymmetric cryptography. This requires in the post-quantum period to significantly increase the length of
Purpose and problem statement

The aim of the work is to develop mechanisms for providing security services based on post-quantum algorithms – crypto-code constructions.

To achieve this goal it is necessary to solve the following tasks:

– to analyze current threats to CCIS / CPSS (SCADA) and protection mechanisms;
– to analyze the mechanisms of construction of crypto-code constructions of McEliece and Niederreiter;
– to develop CCIS / CPSS (SCADA) protection mechanisms based on CCC.

Current threats to CCIS/CPSS (SCADA) and protection mechanisms

CCIS / CPSS (SCADA) are formed by combining information and communication technologies of computer systems with elements of cyberspace based on wireless networking technologies and mobile Internet technologies.

It is this combination that suggests that such systems belong to the objects of critical infrastructure – a set of interconnected elements combined into a single whole, the correct functioning and interaction of which significantly affects the cyber security of the state during a certain interval time. Fig. 1 shows the relationship of the structure with CCIS, on the example of organizations in the transport sector.

![Diagram](image_url)

Fig. 1. The scheme of interconnection of the structure with CCIS, on the example of organizations in the transport sector

Source: developed by the authors.

Given the openness of the CCIS/CPSS (SCADA) elements, the use of cyberspace as the main “channel” of relationships between structural elements in the post-quantum period, such systems are prone to targeted attacks based on threats to individual security components based on hybridity and synergism. Fig. 2 shows a block diagram of the threat model.

Analysis of fig. 1-2 suggests that CCIS/CPSS (SCADA) systems form new structures of critical infrastructure, which on the one hand improve the capabilities of such systems, the quality of customer service, speed of transmission and processing of information flows, digitalization of services, reducing the energy intensity of operation), on the other - the creation of APT-attacks (Advanced Persistent Threat, a complex constant threat or target cyberattack), on the one hand, a complex constant threat (APT) is a high-precision cyber attack. On the other hand, APT can be called a hacker group that is sponsored by the state, organization or people who pay for a targeted attack. Which significantly reduces the level of security of such systems. To protect CCIS / CPSS (SCADA) elements, ISO / IEC 14543 protocols are used to ensure confidentiality and integrity, and Diameter protocol, which provides 3A (AAA, authentication, authorization, accounting) services. security services.
The analysis of the mechanisms of security services shows that in the presence of mobile wireless technologies only this protocol does not solve the problem of confidentiality and integrity. The use of KNX mechanisms provides these services only within the infrastructure of cyberphysical systems, and does not provide protection in the external security contour – a platform based on cloud technology. In the table, 3 shows the main characteristics of wireless mobile and computer networks and security services based on the KNX standard and the Diameter protocol [23]. Analysis of table 3 shows that in the conditions of the appearance of a full-scale quantum computer, services in the internal security circuit are questioned due to quantum algorithms for breaking symmetric and asymmetric algorithms. In addition, only AAA services are

Fig. 2. Block diagram of the synergetic model of synthesis threats on CCIS/CPSS (SCADA)

Source: developed by the authors.
provided in Diameter-based mobile technologies. In today’s conditions of hybridity and synergy of cyberattacks, this allows unimpeded access to both internal and external security contours and the practical implementation of targeted attacks on cyberphysical systems.

Table 3

<table>
<thead>
<tr>
<th>Technology</th>
<th>Range of reception of transfer, m</th>
<th>V, G/c</th>
<th>topology</th>
<th>Transmission spectrum</th>
<th>Modulation</th>
<th>security services before PQ</th>
<th>security services in PQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>LTE (4G)</td>
<td>up to 13400</td>
<td>up to 100 Mbps</td>
<td>AIPN</td>
<td>600 MHz to 2.5 GHz</td>
<td>64QAM</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>LTE (5G)</td>
<td>500</td>
<td>20 Gbps</td>
<td>Heterogeneous backbone network</td>
<td>from 30 GHz to 300 GHz</td>
<td>256-QAM</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>IEEE 802.11ac (WiFi 5)</td>
<td>500</td>
<td>up to 7 Gbps</td>
<td>P2MP</td>
<td>5 GHz</td>
<td>256-QAM</td>
<td>+</td>
<td>–</td>
</tr>
<tr>
<td>IEEE 802.11ax, WiFi 6</td>
<td>9607 Mbps</td>
<td>32 Mbps</td>
<td>mesh</td>
<td>10–66 GHz</td>
<td>64QAM O-QPSK</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>IEEE 802.16</td>
<td>5000</td>
<td>32 Mbps</td>
<td>mesh</td>
<td>10–66 GHz</td>
<td>64QAM O-QPSK</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>IEEE 802.16m (WiMAX2)</td>
<td>6000</td>
<td>90 Mbps</td>
<td>mesh</td>
<td>11 GHz</td>
<td>64QAM O-QPSK</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>IEEE 802.15.1 Bluetooth 5</td>
<td>200</td>
<td>2–6 Mbps</td>
<td>mesh</td>
<td>2.4–2.485 GHz</td>
<td>64QAM O-QPSK</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>IEEE 802.15.4</td>
<td>1000</td>
<td>250 kbps</td>
<td>P2P Cluster tree</td>
<td>2.4–2.483 GHz</td>
<td>BPSK O-QPSK</td>
<td>+</td>
<td>–</td>
</tr>
</tbody>
</table>

Note: C – confidentiality; I – integrity; A – accessibility; Au – authenticity, B – involvement

Source: developed by the authors.

Mechanisms for constructing crypto-code constructions of McEliece and Niederreiter

To ensure security in the post-quantum period - the emergence of a full-scale quantum computer, NIST specialists propose to use post-quantum algorithms.

Such algorithms require symmetric cryptosystems to increase to 512 bits of key sequences (providing a secure time of about 60 years) or the use of post-quantum asymmetric cryptosystems (PQAS). Among the contestants of the third round of the contest there are algorithms based on the combination of the theory of interference coding and cryptography.

Figure 3 shows the block diagrams of McEliece and Niederreiter crypto-code constructions on algebraic geometric codes (elliptical codes (EC) above the GF field (2^28)), which provide protection against Sidelnikov attacks. This allows unimpeded access to both internal and external security contours and the practical implementation of targeted attacks on cyberphysical systems.

Fig. 3. Structural schemes of the McEliece and the Niederreiter CCC on EC

Source: developed by the authors.
$G$ is a generating matrix of dimension $k \times n$ with elements $GF(q)$ (McEliece CCC); $H$ is a test matrix of dimension $r \times n$ with elements $GF(q)$.

In addition, a distinctive feature of Niederreiter CCC is the prior use of equilibrium coding, which allows to provide almost a relative coding rate equal to one.

McEliece CCC provides integrated (single mechanism) error correction $0 \leq w(e) \leq \lfloor \frac{d-1}{2} \rfloor$. The use of modified elliptical codes (MEC) in the CCC provides the required level of crypto-resistance by using initialization vectors ($IV_i$, where $i$ – numbers of symbols of shortening or lengthening), and also allows to provide their construction over $GF(2^s)$. In works [5, 21] mathematical models and practical algorithms of their realization, and also results of researches of their cryptostability are resulted. The use of hybrid crypto-code constructions (HCCC) on the basis of unprofitable codes allows to reduce the level of energy consumption (built over the field $GF(2^s)$), and ensure the required level of cryptocurrency by using two-channel cryptography [5; 22]. However, their use in smart technologies and standards of wireless mobile networks is difficult, due to the need for additional conversion of $m$-nary code sequences into binary and vice versa, which requires additional energy consumption. To solve this problem, it is proposed to use LDPC codes to build crypto-code structures. In [23], a mathematical model and algorithms for the use of CCC/HCCC on LDPC codes are proposed. Table 4 shows the comparative characteristics of the use of crypto-code structures in the post-quantum period, taking into account the integration with different standards of wireless and mobile Internet technologies, as well as taking into account the criticality (degree of confidentiality) of data.

### Table 4

<table>
<thead>
<tr>
<th>Technology</th>
<th>Provision of security services</th>
<th>The degree of information secrecy ($\beta_i$)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$C$</td>
<td>$I$</td>
</tr>
<tr>
<td>LTE (4G), LTE (5G)</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>IEEE 802.11 ac (Wi-Fi 5)</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>IEEE 802.11ax, Wi-Fi 6+KNX</td>
<td>–/+/–</td>
<td>–/+/–</td>
</tr>
<tr>
<td>IEEE 802.16+KNX</td>
<td>–/+/–</td>
<td>–/+/–</td>
</tr>
<tr>
<td>IEEE 802.16m (WiMAX2)</td>
<td>–/+/–</td>
<td>–/+/–</td>
</tr>
<tr>
<td>IEEE 802.15.1 Bluetooth 5+KNX</td>
<td>–/+/–</td>
<td>–/+/–</td>
</tr>
<tr>
<td>IEEE 802.15.4+KNX</td>
<td>–/+/–</td>
<td>–/+/–</td>
</tr>
<tr>
<td>Мобільні технології + CCC EC(MEC)</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Мобільні технології + HCCC EC(MEC)</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Мобільні технології + CCC на LDPC</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

Source: developed by the authors.

Analysis of table 4 shows that the use of classical (symmetric) cryptosystems based on block and stream ciphers (used in the KNX standard) does not provide full integrity and confidentiality services.

Application to ensure the distribution of key data for symmetric cryptosystems, as well as authenticity and involvement services.

In addition, the use of cryptosystems based on elliptic curves also does not provide the required level of resistance to hacking algorithms based on quantum calculations.

### Table 5

<table>
<thead>
<tr>
<th>Degree of secrecy</th>
<th>Security time</th>
<th>Suggested codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>critical</td>
<td>up to 1 year</td>
<td>$MEC$, unprofitable</td>
</tr>
<tr>
<td>high</td>
<td>up to 1 month</td>
<td>$MEC$</td>
</tr>
<tr>
<td>medium</td>
<td>up to 1 time</td>
<td>$EC$</td>
</tr>
<tr>
<td>low</td>
<td>up to 10 minutes</td>
<td>$EC$</td>
</tr>
<tr>
<td>very low</td>
<td>up to 1 minute</td>
<td>LDPC</td>
</tr>
</tbody>
</table>

Source: developed by the authors.

Table 5 shows the ratio of time and degree of secrecy of information [23].

This approach will provide the necessary level of security in a timely manner, taking into account the degree of confidentiality of information and/or secure time required to ensure confidentiality services.

**CCC-based CCIS/CPSS (SCADA) protection mechanisms**

New approaches to security services are needed to ensure the development of mesh and sensor networking technologies using wireless channel standards: mobile technologies LTE, IEEE802.16, IEEE802.16e, IEEE802.15.4, IEEE802.11, Bluetooth. With the advent of the quantum computer (possible reduction of “trust” in modern cryptosystems based on symmetric and asymmetric cryptography (including cryptography on elliptical curves), it is necessary not only to use postquantum cryptographic algorithms, but also a new approach to security based on synthesis CPSS, which is rapidly evolving on the basis of smart and Internet
To provide CCIS/CPSS (SCADA) security services, [23] proposes the concept of dual-contour security based on post-quantum algorithms – crypto-code constructions of McEliece and Niederreiter. It is proposed to use complex solutions for the use of certain codes in crypto-code systems based on the gradation of the degree of secrecy of information in CPSS.

The use of post-quantum asymmetric cryptosystems will provide the necessary level of security in the provision of security services. In addition, the CCC on LDPC codes will allow the use of mobile wireless technologies based on IEEE802.11ac, IEEE802.11ax, IEEE802.16m, IEEE802.15.1, IEEE802.15.4 standards without significant changes.

The smart home system controls a set of autonomous systems, each of which controls certain devices in the house, combining them into a common cyberphysical system. However, to ensure the safety of the external contour (control and storage systems), it is proposed to use a developed server, which is located physically in the house.

Each system sends a data packet to a local server, which allows to manage home without the Internet, being in the same local network (being connected to a Wi-Fi router). Information in the network of the cyberphysical system is transmitted by open wireless channels with encryption based on McEliece and Niederreiter CCC on LDPC codes.

This approach provides security services and, by using a local management server, reduces the likelihood of targeted attacks to gain unauthorized access to the Smart Home management system. The approach also provides the required level of security when using mo-

---

**Fig. 4. CCC-based CCIS / CPSS (SCADA) security services framework**
Source: developed by the authors.
bile management applications, based on the use of McEliece and Niederreiter CCC on LDPC codes. To ensure the security of the database, the McEliece and Niederreiter CCC on the EC (MEC) can be used, which will significantly complicate the possibility of R2L (Remote to Local (user) Attack) cyberattacks. Fig. 4 shows a block diagram of security services in CCIS/CPSS (SCADA) based on CCC.

The basis for providing main security services: confidentiality, integrity and authenticity of data is the closure of CCIS/CPSS communication channels (SCADA) software (software and hardware) applications based on post-quantum cryptosystems – McEliece and Niederreiter CCC, taking into account the degree of confidentiality) information and/or information flows. In addition to providing security services based on McEliece and Niederreiter CCC, the required level of efficiency (speed of crypto-transformations in CCC is comparable to the transformation of modern symmetric encryption algorithms), probability due to the use of noise-tolerant coding methods.

This approach will allow to consider the possibility of scaling and creating integrated with cloud technology networks.

Using the concept of a dual-contour security system proposed in [23], an objective assessment of the CCIS/CPSS flow state (SCADA) is formed. The main part of the proposed security services is a key sequence generation server, which generates OTP-keys for use in software and/or hardware-software applications CCIS/CPSS (SCADA).

In order to ensure the required level of security for the transmission of key sequences (OTP-keys) is used Niederreiter CCC, in software and/or hardware-software applications CCIS/CPSS (SCADA) is proposed to use McEliece CCC. This approach will significantly increase the level of security in mesh networks based on smart technologies and mobile wireless Internet channels.

Conclusions

The development of computing resources, quantum computers and the rapid growth of wireless and mobile technologies allows the formation and development of smart technologies, new network formats based on their synthesis with classical networks of computer networks with cyberphysical and sociocyberphysical systems. However, in the pursuit of super-speed and digitalization, developers do not pay due attention to the security of such systems. The formation of CPSS based on the integration and synthesis of wireless and mobile Internet technologies, with Internet languages, on the one hand, provide further development of digital services. On the other hand, they form unprotected critical points that are used by cybercriminals to target and enable targeted (ART) attacks.

The use of post-quantum cryptosystems to ensure the security of crypto-code constructs provides a timely transition to the algorithms of the post-quantum period. This approach provides the necessary level of security of security services, and the use of different codes allows, taking into account the value (degree of secrecy) of information to ensure its security when using modern standards of wireless communication channels. At the same time, the cost of security is proposed to be assessed not by several estimates of losses in case of its compromise, but sometimes by its relevance, which allows to vary the use of noise codes in the CCC.

The proposed structural scheme of security services in CCIS/CPSS (SCADA) on the basis of CCC provides the use of a new approach to ensuring the required level of security of systems in a new direction of smart technology development. This approach will significantly reduce the possibility of creating “chaos” with the advent of a full-scale quantum computer and the possibility of CCIS/CPSS (SCADA) hacking based on Grover and Shore’s post-quantum algorithms.

References

8. The official site of CREATIVECOMMONS. Last Line of Defense: Reliability through Inducing Cyber Threat Hunting with Deception in SCADA Networks. This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see, available at: https://creativecommons.org/licenses/by/4.0/.
Список літератури

8. Last Line of Defense: Reliability through Inducing Cyber Threat Hunting with Deception in SCADA Networks. This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see : Creativecommons : web-site. URL: https://creativecommons.org/licenses/by/4.0/ (доступ 01 березня 2022 р.
23. Sidelnikov, V.M. (2022), "Криптографія та теорія кодування" [Cryptography and coding theory], Moscow University and the Development of Cryptography in Russia, Collection of abstracts, Moscow State University, pp. 1-22.
Відомості про авторів:

Воропай Олексій Валерійович
dоктор технічних наук
професор кафедри
Харківського національного автомобільно-дорожнього університету,
Харків, Україна
https://orcid.org/0000-0003-3396-8803

Погасій Сергій Сергійович
cандидат економічних наук
doцент кафедри
Національного технічного університету “Харківський політехнічний інститут”,
Харків, Україна
https://orcid.org/0000-0002-4540-3693

Король Ольга Григорівна
cандидат технічних наук
доцент кафедри
Національного технічного університету “Харківський політехнічний інститут”,
Харків, Україна
https://orcid.org/0000-0002-8733-9984

Мілевський Станіслав Валерійович
cандидат економічних наук
doцент кафедри
Національного технічного університету “Харківський політехнічний інститут”,
Харків, Україна
https://orcid.org/0000-0001-5087-7036

Information about the authors:

Alexey Voropay
Doctor of Engineering Science
Associate Professor
of National Technical University
“Kharkiv polytechnical institute”,
Kharkiv, Ukraine
https://orcid.org/0000-0003-3396-8803

Serhiy Pohasii
PhD in Economics
Associate Professor
of National Technical University
“Kharkiv polytechnic institute”,
Kharkiv, Ukraine
https://orcid.org/0000-0002-4540-3693

Olya Korol
PhD in Engineering
Associate Professor
of National Technical University
“Kharkiv polytechnic institute”,
Kharkiv, Ukraine
https://orcid.org/0000-0002-8733-9984

Stanislav Milevsky
PhD in Economics
Associate Professor
of National Technical University
“Kharkiv polytechnic institute”,
Kharkiv, Ukraine
https://orcid.org/0000-0001-5087-7036

РОЗРОБКА МЕХАНІЗМІВ БЕЗПЕКИ SCADA-СИСТЕМ В ПОСТКВАНТОВІЙ ПЕРИОД

О.В. Воропай, С.С. Погасій, О.Г. Король, С.В. Мілевський

Формування нових систем на основі синтезу технологій мобільного інтернету з кіберпростором значно розширює можливості створення інтелектуальних технологій на основі пористих та сенсорних мереж. Це дозволяє значно збільшити швидкість передачі інформації та забезпечує значний ріст ефективності комп'ютерних систем.

При цьому, для забезпечення безпеки в постквантовий період, має бути розроблено нові механізми, що забезпечують високу стійкість інформаційних систем перед угрозами, що виникають з усіх напрямків.

Інформаційні технології, що базуються на квантових комп'ютерах, мають значно більші швидкості виконання операцій за рахунок використання квантових шифрувальних алгоритмів, що змушує до розробки нових методів захисту інформації.

У роботі розглядається питання розробки нових механізмів забезпечення безпеки SCADA-систем в постквантовий період. Розглядаються можливості використання квантових комп'ютерів для забезпечення безпеки інформаційних систем, а також існуючі можливості використання квантових алгоритмів для розв’язання задач криптографії.

Ключові слова: SCADA-системи, соціокібербезпечні системи, постквантові алгоритми, криптокоодові конструкції, алгебро-геометричні коди.