DOI: https://doi.org/10.53052/9788367652001.15

Serhii YEVSEIEV[1], Serhii POHASII[2], Anna STRELNIKOVA[3], Stanislav MILEVSKYI[4]

Opiekun naukowy: Serhii YEVSEIEV[5]

METODY OCHRONY INFORMACJI W SYSTEMACH CYBER-FIZYCZNYCH

Sreszczenie: W artykule przedstawiono nowe ujęcie problemu zapewnienia bezpieczeństwa zasobów informacji w systemach cyber-fizycznych. Obecnie, takie systemy, z zasady należą do obiektów infrastruktury krytycznej. Rozważane systemy powstają w konsekwencji integracji różnych elementów systemów komunikacji mobilnej, klasycznych sieci komputerowych oraz systemów typu Internet of Things (IoT), a także innych współczesnych technologii Internetowych. W niniejszej pracy zaproponowano rozważenie formowania/budowy system bezpieczeństwa w oparciu o multi-kontury, w którym rozważa się dwa kontury systemu bezpieczeństwa - wewnętrzny (infrastruktura fizyczna systemu cyber-fizycznego) and zewnętrzną (tj. system kontroli obiektów infrastruktury krytycznej zbudowany w oparciu o technologie chmurowe). Za pomocą zaawansowanego klasyfikatora zagrożeń obiektów infrastruktury krytycznej, tworzy się klasyfikator atakujących (hackerów, ataków). Określa się zasoby/wymagania obliczeniowe. System, na podstawie analizy zagrożeń, umożliwia określenie w terminowy/nadążny sposób poziomu możliwości atakujących, a także ich intencje. System generuje środki/akcje prewencyjne zabezpieczające zasoby. Działanie zaproponowanego modelu ochrony zasobów oparte jest na słynnym modelu Lotka-Volterry, który umożliwia uwzględnianie trendów rozwoju nowoczesnych technologii, a także wektora cyber-zagrożeń skierowanego na obiekty infrastruktury krytycznej, które zawierają nowoczesne systemy cyber-fizyczne.

Dla zapewnienia bezpieczeństwa przesyłu informacji przez kanały otwarte w sieci systemów cyber-fizycznych, zaproponowano metody ochrony z zastosowaniem algorytmów post-kwantowych, zastosowano krypto-kody McEliece'a z wykorzystaniem kodów LDPC (liniowych kodów korekcyjnych, low density parity check code), które umożliwiają "domknięcie" kanałów transmisji danych w infrastrukturze systemów cyber-fizycznych.

Praca zawiera linki do źródeł, gdzie zamieszczono dalsze wyjaśnienia do zaprezentowanych rozważań.

Keywords: systemy cyberfizyczne, bezpieczeństwo informacji, cyberbezpieczeństwo, bezpieczeństwo informacji, modele bezpieczeństwa Lotka-Volterra, klasyfikator zagrożeń informacyjnych systemów cyberfizycznych, system ochrony informacji

[1] National Technical University "Kharkiv Polytechnic Institute", Serhii.Yevseiev@gmail.com

[2] National Technical University "Kharkiv Polytechnic Institute", SPogasiy1978@gmail.com

[3] Assistant, National Technical University "Kharkiv Polytechnic Institute", Anna.Strelnikova@khpi.edu.ua

[4] Assoc. Professor PhD., National Technical University "Kharkiv Polytechnic Institute", MilevskiySV@gmail.com

[5] Professor Doct. of Techn. Sc., National Technical University "Kharkiv Polytechnic Institute", Serhii.Yevseiev@gmail.com

INFORMATION PROTECTING METHODS IN CYBERPHYSICAL SYSTEMS

Summary: The article presents a new approach to ensuring the security of information resources in cyber-physical systems. Today, such systems, as a rule, belong to objects of critical infrastructure. These systems are formed as a result of the integration of various elements of mobile communication technologies, classic computer networks and systems, as well as Internet of Things and Internet technologies. The work proposes consideration of the formation of the security system based on multi-contours, which allows considering two contours of the security system - internal (physical infrastructure of cyberphysical systems) and external (infrastructure of the control system based on cloud technologies). With the help of the developed classifier of threats to critical infrastructure objects, the formation of a classifier of attackers is ensured, in which its financial and computing capabilities are determined, which allows, based on the analysis of threats, to determine in a timely manner the degree of capabilities of attackers, as well as their intentions, and to form preventive protection measures. The use of the proposed protection models based on the Lotka-Volterra model allows taking into account the trends in the development of modern technologies, as well as the vector of cyber threats directed at critical infrastructure objects, which include modern cyberphysical systems. To ensure the security of information transmission through open channels of the cyber-physical systems network, information protection methods are proposed based on post-quantum algorithms – McEliece crypto-code constructions on LDPC codes, which allows to "close" the data transmission channels of the cyberphysical systems infrastructure.

The work contains links to sources that clarify the presented material.

Keywords: cyberphysical systems, information security, cyber security, security of information, Lotka-Volterra security models, classifier of cyber-physical systems information threats, information protection system

1. Introduction

The creation of large systems of critical infrastructure, the intensification of research into the dynamics of cyber-physical systems require constant improvement and updating of the current apparatus of modeling and control of dynamic systems [1–5]. The development of cyber-physical systems in recent years has significantly changed the infrastructures of modern information and cybernetic systems (ICS), as well as critical infrastructures (CI), and even Internet of Things (IoT) systems. The synthesis of these infrastructures allows to significantly expand the digital range of services, on the one hand, but also increases the level of cyber threats [6–9]. The use of security models is required for timely changes in the structure of protective resources, assessment of the necessary and current situation of the security system. It makes possible to significantly reduce the costs of restoring the network infrastructure, to take preventive measures in a timely manner with the necessary costs for security mechanisms. In addition, the creation based on the integration of threats to elements of the physical infrastructure of cyber-physical systems and elements of the management system, which is created on the basis of cloud technologies, requires the creation of a multi-loop security system. And the emergence of a full-scale quantum computer requires the use of post-quantum algorithms to provide security services and maintain an appropriate level of security to ensure the security of information resources, both in the internal and external contours of the security system.

2. Analysis of recent research and publications

Analysis of the global trends in cyber threats showed that today there is no way to ensure security in its entirety. For example, works [3, 4] provide an analysis of cyber threats for the years 2017–2019. The presented analysis shows that the vector of cyber threats is changing with the development trends of digital services, Internet of Things and cryptocurrencies based on blockchain technology. The work [5] presents 10 main trends in the field of cyber security in 2021, which confirms the trends of cyber attacks in the context of a pandemic, primarily on cryptocurrency exchanges, and secondly, on private VPN channels (in connection with remote work), and in the third - on the basis of social engineering methods - phishing letters in pdf format within the framework of corporate mail. Methodological aspects of building a security system based on crypto-code structures, their application in various objects of critical infrastructure, as well as the ability to resist modern threats are considered in the paper [6].

In work [8], it is proposed to use dynamic models based on the methods of the theory of differential games and differential transformations, while providing an assessment of the current state of the system in offline mode. However, such methods require significant computing resources, which significantly reduces the possibility of their practical implementation. In the work [9], the authors consider the use of dynamic models in various systems of the information space. However, the models do not take into account the possibility of increasing the computing capabilities of attackers, their grouping in order to achieve the goals of the attack. In [10], the authors consider economic aspects that can affect the construction of not only the security model, but also its practical implementation in the information protection system of the transport system. However, the authors do not take into account the complexation of threats, their synergism and hybridity, which makes it possible to form targeted (complex) threats with social engineering methods.

3. Information resources security system building concept

The conducted threat analysis [11–17] showed that cyber-physical systems intersect with critical infrastructure objects. At the same time, cyber-physical systems (Cyber-Physical System, CPS) are systems consisting of various natural objects, artificial subsystems and controllers that manage and allow to imagine such education as a single whole. In CPS, close communication and coordination between computational and physical resources is ensured. Computers monitor and control physical processes using such a feedback loop, where what happens in physical systems affects calculations and vice versa [11, 13, 14]. In addition, the emergence of a full-scale quantum computer calls into question the stability of almost all symmetric and asymmetric cryptography algorithms, and the rapid growth of IT computing resources and "G" technologies contributes to the increase in the growth of targeted attacks on information and communication (ICS) and cyber-physical systems (CPS), which are the core of modern information-critical cybernetic systems. As a rule, the direction of smart technology and "Smart Home" technologies use security mechanisms without a preliminary comprehensive approach to the provision of security services. Basically, the mechanisms of computer systems and technologies are integrated with wireless network technologies, which does not allow forming information protection systems with the required level of security. The works [18–25] consider the main approaches to ensuring security in cyber-physical systems and smart technologies. As a rule, the KNX standard (ISO/IEC 14543) is used, which is not so secure, it is possible to monitor the network, record the sent packets and easily repeat them, because there is no line connector with the "Security Proxy" function. In addition, the use of the AES-128 algorithm for tunneling in the post-quantum period will not provide the necessary level of protection of the internal circuit.

However, a significant drawback of this approach is the lack of an objective assessment of the current state of system security. As a rule, such systems are built from two main subsystems - a cyber-physical one, which directly performs service functions, and a control system, which is deployed in the cloud. The use of security mechanisms of the second subsystem is usually not taken into account when assessing the current state of security. It is formally considered that cloud technologies provide the required level of security. The main security threats in the cloud: data theft, data loss, account hacking, breaches in interfaces and Application Programming Interface (API), DDos attacks, insider actions, the possibility of hacker penetration, as well as downtime due to the fault of the provider [25].

The proposed new authentication approach in CPS and smart technologies is also based on symmetric encryption, which calls into question its effectiveness in the conditions of the post-quantum period (the emergence of a full-scale edge computer) [26, 27].

Thus, there is a need to develop an approach to CPS security based on the integration of threats and the formation of the concept of two-loop security, which will allow to ensure the objectivity of assessing not only the current state of information security of such systems, but also to identify signs of synergy and hybridity of targeted attacks on such systems.

The article based on research [11–17] proposes a fundamentally new concept of building a security system of information resources based on methods and models of building multi-circuit security systems, as well as mechanisms for providing basic security services based on post-quantum algorithms - crypto-code structures on LDPC codes, which differ in speed and are used in mobile Internet technologies. It includes five stages: 1) determination of the probability of the impact of threats on cyber-physical systems, 2) formation of models of preventive measures based on the Lotka-Voltera model, 3) evaluation of effectiveness based on models of the game-theoretic approach, 4) construction of integrated mechanisms for ensuring confidentiality, integrity, authenticity and reliability of information resources of cyber-physical systems, 5) determination of the state and formation of strategies for the construction of multi-circuit protection systems.

1) Determining the probability of threats impact on cyber-physical systems

To determine the probability of the impact of threats on cyber-physical systems, we use the approach proposed in [11], the main difference is the expert assessment of the distribution of threats taking into account their hybridity and synergism based on the synergistic threat model. To form an expert assessment, we use a modification of the threat classifier proposed in works [11, 13, 14]. To assess the objectivity of experts' judgments, we use weighting coefficients of experts' competence.

To determine the economic costs of preventing an attack, we will use an algorithm taking into account the cost indicators of threats. This approach makes it possible to estimate the economic costs of intentional protection mechanisms, taking into account the ranking of potential threats and the importance of information resources to be protected [11, 13, 14, 16]. Both sides of the attack are determined by the importance (rating) of attacks that are economically feasible to carry out.

2) Forming models of preventive measures based on the Lotka-Volterra model

The works [14,18] propose a method for assessing the security of cyber-physical systems, which is based on the basis of the developed classifier of threats and allows to assess the current level of security, as well as dynamically form recommendations for the distribution of limited protection resources based on an expert assessment of known threats. This approach allows for dynamic modeling in off-line mode, which allows timely identification of the capabilities of attackers and the formation of preventive protection measures based on threat analysis.

Security models of cyber-physical systems are proposed: "predator-victim" taking into account the computing capabilities and targeting of targeted cyber attacks, "predator-victim" taking into account the possible competition of attackers in relation to the "victim", "predator-victim" taking into account the relationships between "species" victims" and "species of predators", "predator-victim" taking into account the interrelationships between "species of victims" and "species of predators". Based on the proposed approach, the coefficients of the Lotka-Voltery model α=0.39, β=0.32, γ=0.29, φ=0.27 were obtained, which take into account the synergy and hybridity of modern threats, funding for the formation and improvement of the defense system, and also allows you to determine the financial and computing capabilities of the attacker based on the identified threats.

A method for assessing the security of cyber-physical systems based on the Lotka-Volterra "predator-prey" model is proposed, which consists of the following steps:

At the first stage. Formed and/or calculated:

- metric coefficients of threats;
- weighting coefficients of manifestation of threats;
- determination of the implementation of each threat;
- determination of the implementation of threats to the security service;
- determination of total threats to the security component;
- determining the economic costs of preventing an attack.

At the second stage. Based on the analysis of stage 1, the Lotka-Voltera model is selected, and the corresponding coefficients and components of the expressions are calculated.

At the third stage, the current state of security of the cyber-physical system is determined.

3) Performance evaluation based on models of the game-theoretic approach

In [16], models of the main problems of the security systems antagonistic agents interaction are proposed. The models made it possible to obtain a solution to two of the most common problems in the field of cyber security, namely, the interaction between a system administrator and an attacker when organizing the protection of information resources. The tasks are solved for two different conditions - the game matrix contains the cost estimates of resources and the matrix reflects the probabilities of the threat's realization. Pure and mixed strategies are defined for different initial conditions, which allows to exclude from consideration the strategies that are not part of the solution.

Conducted research into the use of game-theoretic modeling in the tasks of ensuring cyber security made it possible to identify the most common game-theoretic models used in the field of security. These include Stackelberg, Nash games, and signaling games. The selected game models do not exhaust the entire variety of game-theoretic models used, but are only examples of the most common applications.

4) Construction of integrated mechanisms for ensuring confidentiality, integrity, authenticity and reliability of information resources of cyber-physical systems

In the conditions of the rapid growth of mobile technologies computing capabilities and the creation of wireless Mesh, sensor networks, Internet of Things technologies, and smart technologies based on them, ensuring information security is becoming an urgent problem. At the same time, there is a need to consider security in two circuits, internal (directly inside the network infrastructure) and external (cloud technologies). In such conditions, it is necessary to integrate threats to both the internal security circuit and the external circuit. This allows not only to take into account the hybridity and synergy of modern target threats, but also to take into account the level of significance (level of secrecy) of information flows and information circulating both in the internal and external security circuit. The concept of building security based on two contours is proposed. To ensure the security of wireless mobile channels, it is proposed to use crypto-code structures of McEliece and Niederreiter on LDPC codes, which allows integration into the technologies for ensuring the reliability of the IEEE 802.15.4, IEEE 802.16 standards. This approach makes it possible to provide the necessary level of security services (confidentiality, integrity of authenticity) in the conditions of a full-scale quantum computer.

To provide basic services, it is suggested to use McEliece and Niederreiter crypto-code constructions, which are discussed in detail in works [12–14].

Fig. 1 presents a structural diagram of the decoding of the received sequence based on soft decoding.

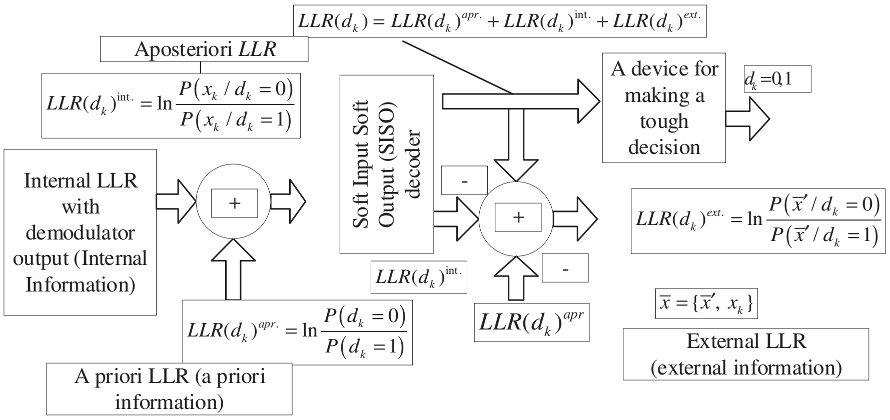
$LLR(d_k) = LLR(d_k)^{apr.} + LLR(d_k)^{\text{int.}} + LLR(d_k)^{ext.}$
Aposteriori *LLR*
$LLR(d_k)^{\text{int.}} = \ln\frac{P(x_k / d_k = 0)}{P(x_k / d_k = 1)}$
Soft Input Soft Output (SISO) decoder
A device for making a tough decision
$d_k = 0,1$
Internal LLR with demodulator output (Internal Information)
+
-
+
-
$LLR(d_k)^{ext.} = \ln\frac{P(\bar{x}' / d_k = 0)}{P(\bar{x}' / d_k = 1)}$
$LLR(d_k)^{\text{int.}}$
$\bar{x} = \{\bar{x}', x_k\}$
$LLR(d_k)^{apr.} = \ln\frac{P(d_k = 0)}{P(d_k = 1)}$
$LLR(d_k)^{apr}$
External LLR (external information)
A priori LLR (a priori information)

Figure 1. Decoding scheme taking into account the soft decision

This approach provides security services, and by using a local management server, it reduces the likelihood of targeted attacks to gain unauthorized access to the Smart Home management system. Also, the approach provides the necessary level of security when using mobile management programs, based on the use of the McEliece and Niederreiter CCC on LDPC codes. To ensure the security of the database, the McEliece and Niederreiter SSS on the EC (MEC) can be used, which will greatly complicate the possibility of R2L (Remote to Local (user) Attack) cyber attacks.

5) Determination of the state and formation of strategies for the construction of multi-contour protection systems

To ensure the security of socio-cyberphysical systems and systems based on their infrastructure, it is necessary to take into account not only the rapid development of computing capabilities of mobile technologies (wireless communication channels) with their ability to provide information transmission from 1 Tb/s and above, the growth of service capabilities and functionality of cloud technologies, as well as the integration of modern threats based on the synthesis of social engineering mechanisms, cyber threats (with signs of hybridity and synergism), as well as the ability of special services to control a significant part of cloud technology resources. To implement such an approach, it is proposed to divide the CPS into two subsystems of security and infrastructure - the internal circuit, the cyber-physical system (CPS), which provides the necessary set of services and functionality, and the external circuit - the managerial system (MS) based on the synthesis of wireless networks and systems cloud technologies.

This approach provides a synthesis of internal and external circuits, takes into account operational efficiency, energy consumption and relative safety (each circuit builds safety on its own mechanisms and principles), on the one hand. On the other hand, it allows you to objectively assess the threats of each of the contours, taking into account the computing resources and financial capabilities of the attackers. Fig. 2 presents a structural diagram of the CPS two-contour security concept.

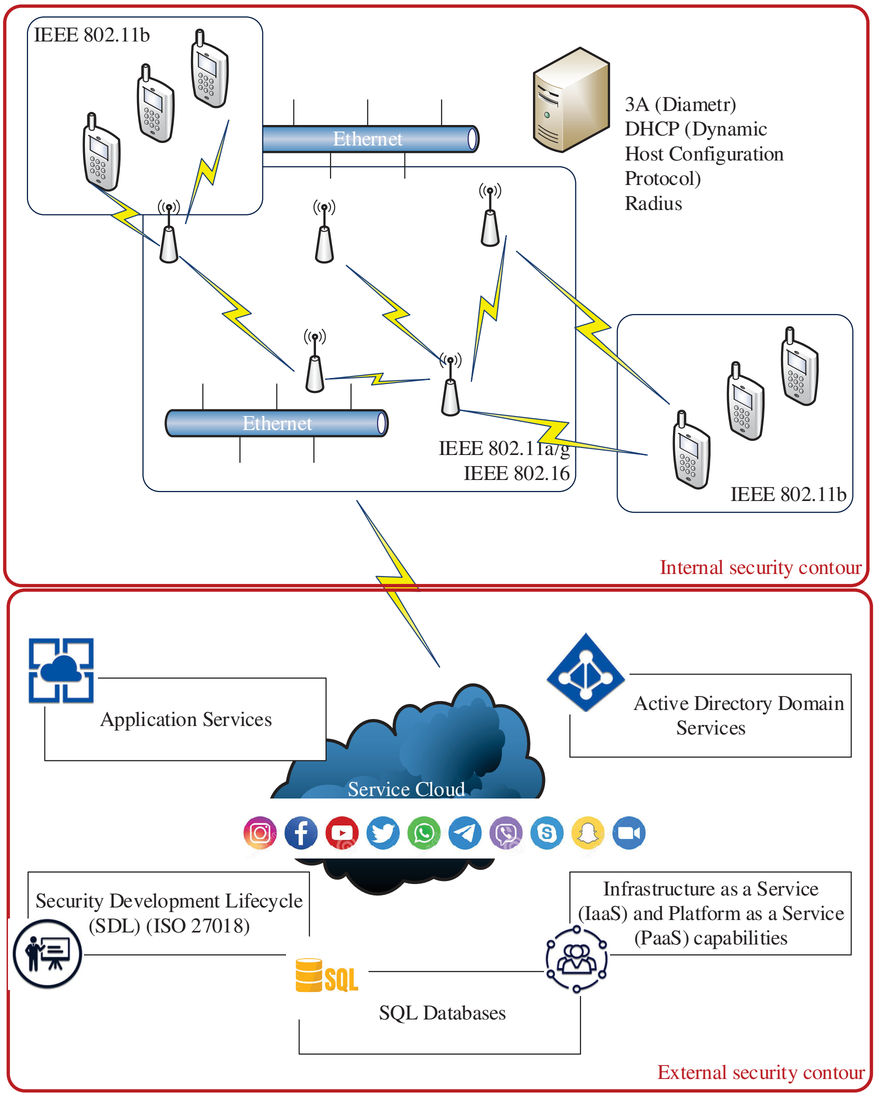

Figure 2. Structural diagram of the concept of two-contour security of cyber-physical systems

To determine the current state of security of the internal circuit, we use the approach proposed in [9], the main difference is the expert assessment of the distribution of threats taking into account their hybridity and synergism based on the synergistic threat model. The main stages are given in [11].

The proposed Concept of two security contours provides integration and takes into account the possibilities of targeted cyber attacks, their synergy, hybridity and the possibility of integration in the conditions of the growth of computing resources and the expansion of the spectrum of smart technologies.

4. Practical implementation of McEliece and Niederreiter's crypto-code structures

Examples of the practical implementation of such systems is the protocol for ensuring the security of voice messages in online mode, proposed in [60], based on McEliece and Niederreiter's *CCC* on *EC* (*MEC*), which is shown in Fig. 3.

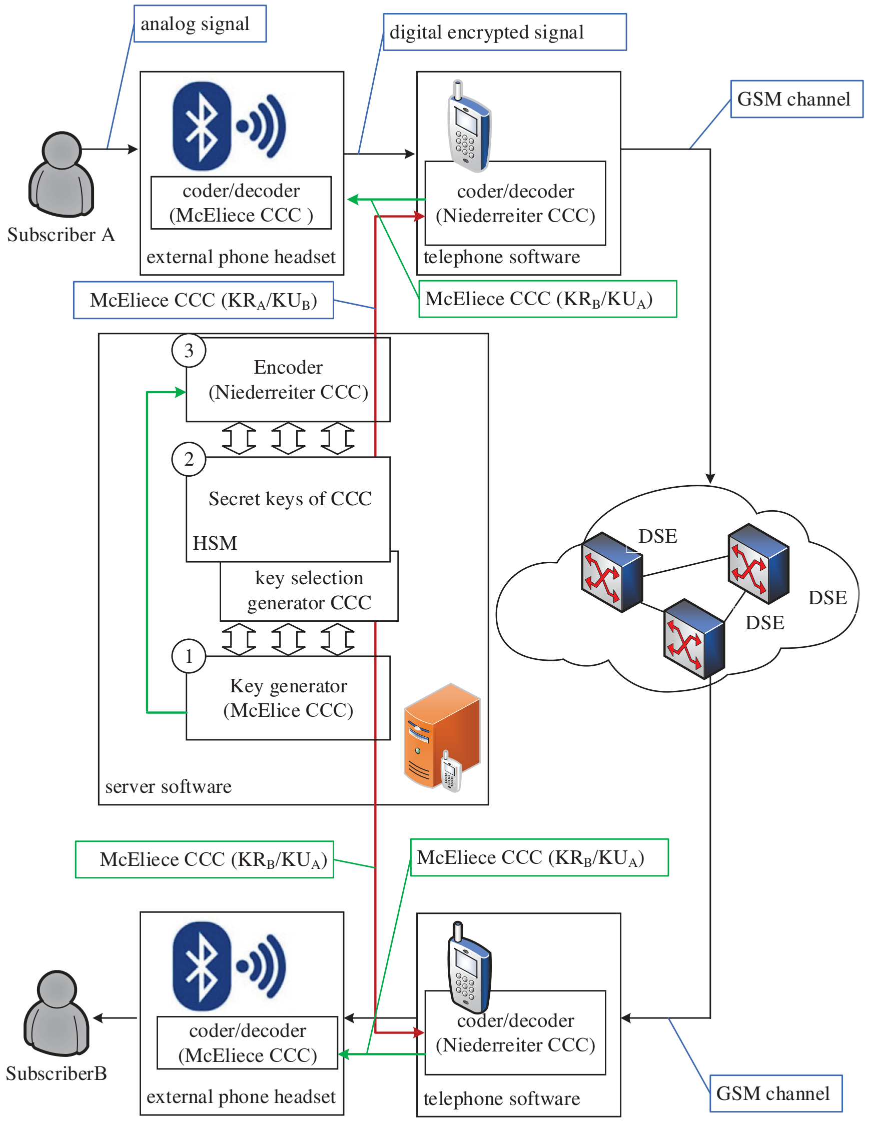
analog signal
digital encrypted signal
GSM channel
Subscriber A
coder/decoder (McEliece CCC)
external phone headset
coder/decoder (Niederreiter CCC)
telephone software
McEliece CCC (KR$_A$/KU$_B$)
McEliece CCC (KR$_B$/KU$_A$)
3
Encoder (Niederreiter CCC)
2
Secret keys of CCC
HSM
key selection generator CCC
1
Key generator (McElice CCC)
server software
DSE
DSE
DSE
McEliece CCC (KR$_B$/KU$_A$)
McEliece CCC (KR$_B$/KU$_A$)
SubscriberB
coder/decoder (McEliece CCC)
external phone headset
coder/decoder (Niederreiter CCC)
telephone software
GSM channel

Figure 3. Structural diagram of building a two-loop information protection system on the CCC to ensure the confidentiality of voice messages

In figure 3 shows the practical implementation of the proposed Concept and crypto-code structures on LDPC codes. The proposed protocol for ensuring security in cyber-physical systems (“Smart Home”) is based on the use of a two-loop security concept and post-quantum algorithms.

So, to ensure the security of voice messages, it is proposed to use a hardware-software encoder that is built into the headset headset (it is proposed to use Bluetooth headphones) and provides encryption of a digital message based on the McEliece CCC (Fig. 3). After that, the encrypted message is transmitted via a Bluetooth channel to a mobile gadget. In this case, standard protocols of the GSM mobile Internet channel are used. This allows you to ensure the confidentiality of the conversation without taking into account the requirements of the communication channel, the requirements of manufacturers of headsets and mobile gadgets, and does not take into account modifications of both the Bluetooth channel and mobile Internet technology. In addition, the use of a hardware-software implementation of the encoder in the form of a chipset can significantly reduce the cost of production and implementation of this approach. To ensure security, only the session password is recorded in the headphones, depending on the role (sender, recipient), which are recorded from the mobile application.

After the end of the conversation, they are deleted. In this case, the chipset implements an encoder based on the McEliece *CCC*. Ensuring the security of the transfer of key data between the mobile application and the server is provided by Niederreiter's *CCC*. To ensure the security of the server part, after generating the keys for conducting a conversation and transferring them to the sender and recipient, the server RAM is reset, which ensures channel tunneling between users. The secret keys of the McEliece and Niederreiter crypto-code structures change at different time intervals and are OTP keys (session keys).
Next we consider a voice message security protocol based on post-quantum algorithms:

SUBSCRIBER A (call initiator)

1. Opens the phone software and in the list of subscribers find the corresponding subscriber (Subscriber B)
2. Sends a request to subscriber B through the server.
3. Receives on the phone software through a private channel (using encryption based on Niederreiter's CCC on the *EC*) a private key, and a public key of subscriber B.
4. Confirms readiness for a conversation. At the same time, a private key KR_A and a public key KU_B are transmitted from the phone software via a Bluetooth channel.
5. In the Bluetooth headphones in the encoder (coder/decoder), the key is recorded.
6. After the key is written, a ready signal is generated.
7. After confirmation of the readiness of subscriber B, a conversation is carried out.

SERVER SOFTWARE

1. At the request of subscriber A in Secret keys of CCC (block 2), the *CCC* Key Selection Generator randomly selects the key parameters and sends it to key generator (block 1).
2. In key generator, secret keys are received from GSM (masking matrices – X, P, D, and generating matrix G^{EC}).
3. In key generator, KR_A (McEliece *CCC* private key of subscriber A) and KU_A (public key of subscriber A) are formed.
4. Based on the response of subscriber B, a public key KU_B is formed and transmitted to subscriber A.
5. In encoder (block 3) from key generator (bock 1), the generated KR_A and KU_A are received, after the transfer of the keys in key generator, the data is erased.
6. In encoder KR_A, KU_A, KU_B are encrypted.
7. From encoder, respectively, KR_A, KU_B are sent to subscriber A (the subscriber who initiates the call), KU_A – to subscriber B (the subscriber who is being called), after the transfer of the keys in encoder, the data is erased.

SUBSCRIBER B (recipient of the call)

1. Receives a request from the server in the phone software to transfer the public key (KU_A).
2. Confirms the request to the server, sends KR_B.
3. Receives the public key KU_A on the phone software via a private channel (using encryption based on Niederreiter CCC in the EC).
4. Confirms readiness for a conversation. At the same time, a public key (KU_A) is transmitted from the phone software via a Bluetooth channel.
5. In the Bluetooth headphones in the decoder (coder/decoder), the key is written.
6. After the key is written, a ready signal is generated.
7. After confirmation of readiness, subscriber B sends a signal to the server that he is ready to talk.

Thus, the proposed protocol ensures the closure of the mobile Internet channel using a set of software and hardware. Using a hardware solution for closing (encrypting) a voice message in a headset will counteract almost all threats, and using a key server provides a tunnel mode, which eliminates the possibility of "eavesdropping" of voice messages.

To ensure security in cyber-physical systems, it is proposed to use the McEliece and Niederreiter CCCs on LDPC codes (fig. 4).

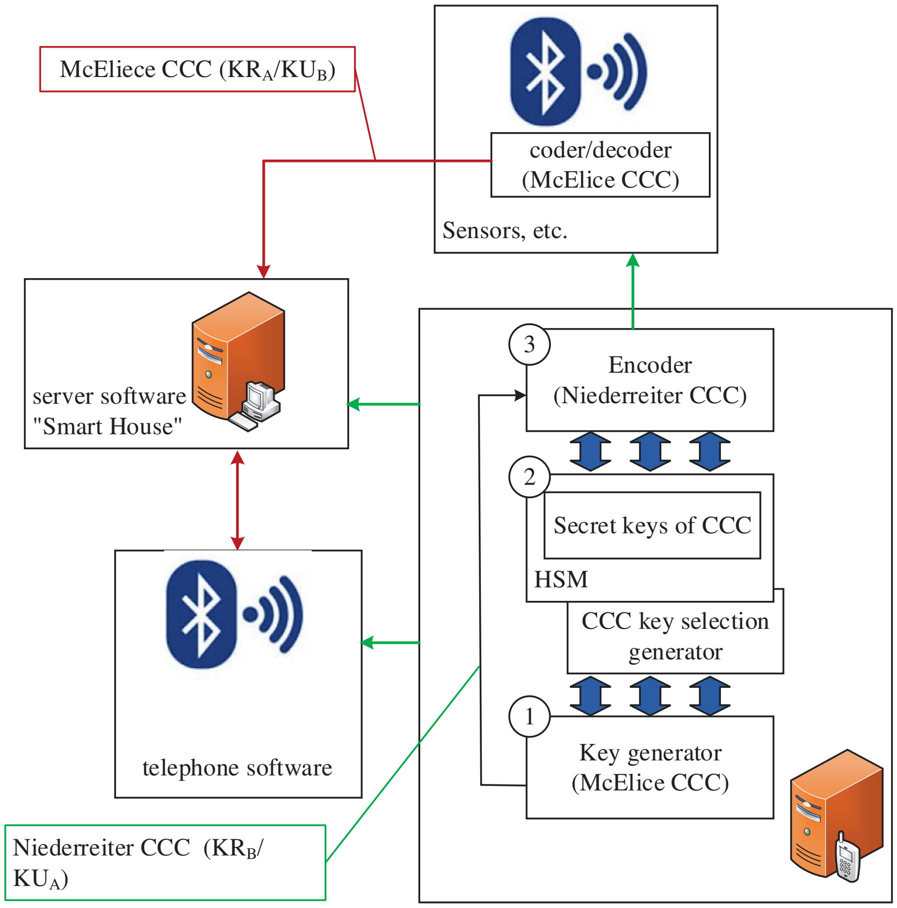

Figure 4. Structural diagram for constructing a two-circuit protection system of the "Smart House" system based on CCC

The use of these post-quantum asymmetric cryptosystems will provide the required level of security when providing security services. The use of LDPC codes allows using 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 complex of autonomous systems, each of which controls certain devices in the house, connecting their common cyber-physical system. However, to ensure the security of the external circuit (control and information storage systems), it is proposed to use the developed server, which is physically located in the house.

Each system sends a data packet to a local server, which allows you to manage your home in the absence of the Internet, being on the same local network (being connected to a WI-FI router). Information in the network of the cyber-physical system is transmitted over open wireless channels with encryption based on the McEliece and Niederreiter *CCC* using LDPC codes.

This approach provides security services, and through the use of a local control server, it reduces the likelihood of targeted attacks to gain unauthorized access to the Smart Home control system. Also, the approach provides the required level of security when using mobile control applications, based on the use of *CCC* McEliece and Niederreiter on LDPC codes. To ensure the security of the database, McEliece and Niederreiter's *CCC* on the *EC* (*MEC*) can be used, which will greatly complicate the possibility of implementing cyber attacks of the R2L class (Remote to Local (user) Attack).

5. Conclusion

The development of computing resources, quantum computers and the rapid growth in the use of wireless and mobile technologies allows the formation and development of smart technologies, new formats of networks based on their synthesis with classical networks. However, in the pursuit of ultra-speed and digitization, developers do not pay due attention to the security of such systems. The formation of cyber-physical systems based on the integration and synthesis of wireless technologies and mobile Internet technologies, with Internet languages, on the one hand, ensure the further development of digital services. On the other hand, they form unprotected critical points that cybercriminals use for their purpose. The appearance of a full-scale quantum computer only increases the possibility of providing the necessary level of security. In addition, the use of cloud technologies requires a reassessment of approaches to the formation of a security system. In such conditions, the proposed approach of using a two-circuit security system is relevant and timely. The proposed concept allows not only to take into account the signs of synergism and hybridity of modern threats, but also provides an objective approach to assessing the current level of security in cyber-physical systems.

The use of crypto-code structures to ensure the security of post-quantum cryptosystems ensures a timely transition to the algorithms of the post-quantum period. This approach ensures the necessary level of security of security services, and the use of various 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, it is proposed to assess the value of security not by the quantitative assessment of losses in case of its compromise, but by the time of its relevance, which allows to vary the use of tamper-resistant codes in the CCC.

Security models of cyber-physical systems are proposed, taking into account computing capabilities and targeting of targeted cyber-attacks, as well as the possible competition of attackers with respect to the "victim". The models also reflect the possibilities of grouping in order to achieve the goals of a cyber attack, the relationships between "species of victims" and "species of predators". Based on the proposed approach, the coefficients of the Lotka-Volterra model α=0.39, β=0.32, γ=0.29, φ=0.27 were obtained, which take into account the synergism and hybridity of modern threats, funding for the formation and improvement of the defense system, and also allows you to determine the financial and computing capabilities of the attacker in relation to the detected threats. A method for assessing the security of cyber-physical systems based on the Lotka-Volterra "predator-prey" model has been developed. The method is based on the basis of the classifier of threats, taking into account their hybridity and synergism. The proposed method, in contrast to the existing ones, allows to give assessments of the level of security of cyber-physical systems and developing security systems, that is, to produce a dynamic assessment, and not a static one, as proposed in previous studies.

Practical ways to implement post-quantum algorithms provide a solution to a set of problems – ensuring the required level of security (when implementing security services), efficiency and reliability of information flows. The use of both software and hardware-software implementations of CCC McEliece and Niederreiter on various codes makes it possible to single them out as a separate direction of providing security and reliability services. This approach can significantly simplify security issues in the rapidly developing areas of SCPS, smart and mesh technologies.

REFERENCES

1. IoT Security Maturity Model: Description and Intended Use. URL: *http://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf.*
2. IoT Security Maturity Model: Practitioner's Guide. URL: IoT Security Maturity Model: Practitioner's Guide.
3. Key Findings of the 2017 Global Information Security Trends Survey. URL: *https://www.pwc.ru/ru/publications/gsiss-2017.html*
4. Antiphishing. Employee Protection Annual Report 2020. URL: *https://antiphish.ru/tpost/88km7s0a01-otchyot-antifishinga-o-zaschischennosti*
5. Gartner Names Top 10 Cybersecurity Trends in 2021. URL: *https://www.tadviser.ru/index.php/*.
6. YEVSEIEV S., PONOMARENKO V., LAPTIEV O., MILOV O.: Synergy of building cybersecurity systems: monograph, Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
7. HRYSHCHUK R.: The synergetic approach for providing bank information security: the problem formulation // R. Hryshchuk , S. Yevseiev/ Information security. 22(2016)1, 64 – 74. doi:10.18372/2225-5036.22.10456
8. HRYSHCHUK R.: Theoretical foundations of modeling processes attacking information by methods of the theory of differential games and differential transformations Monograph/R. V. Grischuk. - Zhytomyr: Ruta, 2010. 280 p.
9. HRYSHCHUK R.: Fundamentals of cybernetic security: Monograph. R.V. Grischuk, Yu.G. Danik; for zag. ed. SOUTH. Tributary. Zhytomyr: ZhNAEU, 2016. 636 p.
10. PETROV O.: Improving the information security of automated data processing systems in transport, Petrov O., Lakhno V. Information Technology in Selected Areas of Management. – Wydawnictwo AGH, Krakow 2016, 65 – 78.
11. POHASII S. and other: Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies 3/9 (2020)105,6-19.

12. POHASII S. and other. Development of a method for assessing forecast of social impact in regional communities. Eastern-European Journal of Enterprise Technologies. 6/2(2021)114, 30–47.
13. 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.
14. POHASII S. and other: Development of conception for building a critical infrastructure facilities security system. Eastern-European Journal of Enterprise Technologies. 3/9(2021)111, 63–83.
15. POHASII S.and other: Development and analysis of game the theoretical models of security systems agents interaction. Eastern-European Journal of Enterprise Technologies. 2/4(2020)104, 15–29.
16. POHASII S. and other: Development of a method for assessing the security of cyber-physical systems based on the Lotka–Volterra model. Eastern-European Journal of Enterprise Technologies 5/9(2021)113, 30–47.
17. KNX Technical Manual 2CKA001473B8668. KNX Technical Manual. Busch-Presence detector KNX / Busch-Watchdog Sky KNX. Busch-Jaeger Elektro GmbH, 2017. 198 p.
18. Technical documentation on KNX devices. ABB, 2006.
19. KNX Handbook Version 1.1 Revision 1. Konnex Association, 2004.
20. ABB i-bus KNX KNX Security Panel GM/A 8.1 Product Manual / Busch-Watchdog Sky KNX. Busch-Jaeger Elektro GmbH, 2016.
21. SCHILDER J., REIBEL T.: ABB GPG Building Automation Webinar ABB i-bus® KNX Basics and Products. March 3, 2016 / Busch-Watchdog Sky KNX. Busch-Jaeger Elektro GmbH, 2016. – 86 pp.
22. Manual for KNX Planning / Siemens Switzerland Ltd, 2017. – 100 pp.
23. Security Technology KNX-Intrusion Alarm System L240 Installation, Commissioning, Operation / Busch-Watchdog Sky KNX. Busch-Jaeger Elektro GmbH, 2010. – 116 pp.
24. Top Security Threats in the Cloud. URL: *https://tadviser.com/*
25. MUNILLA J., BURMESTER M., BARCO R.: An enhanced symmetric-key based 5G-AKA protocol. Computer Networks. URL: DOI:10.1016/j.comnet.2021.108373.
26. ABDULBASIT DAREM, ASMA A. ALHASHMI, JEMAL H.: A. Cybersecurity Threats and Countermeasures of the Smart Home Ecosystem. IJCSNS International Journal of Computer Science and Network Security, 22(2022)3, 303-311.
27. YEVSEIEV S., POHASII S., KHVOSTENKO V.: Development of a protocol for a closed mobile internet channel based on post-quantum algorithms. Information processing systems. 3(2021)166, 35–40. DOI: 10.30748/soi.2021.166.03.