UDC 681.32:007.5 **doi:** https://doi.org/10.20998/2522-9052.2022.2.10

Serhii Pohasii[1], Stanislav Milevskyi[1], Bohdan Tomashevsky[2], Natalya Voropay[1]

[1] National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine
[2] Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine

DEVELOPMENT OF THE DOUBLE-CONTOUR PROTECTION CONCEPT IN SOCIO-CYBERPHYSICAL SYSTEMS

Abstract. The rapid development of mobile Internet technologies LTE (Long-Term Evolution) not only predetermined the further development of cyber-physical systems, which are based on the synthesis of technologies of classical computer systems and LTE technologies, as well as integration with Internet-of-Things technologies. As a result, the emergence of sociocyberphysical systems predetermines further development based on this integration. The creation of mesh- and sensor networks also allows the development of smart technologies and systems based on their conglomeration. The development and creation of a quantum computer, on the one hand, will make it possible to make a technical breakthrough in computing resources, use artificial intelligence, and on the other hand, it can lead to “chaos” in ensuring the security of modern technologies and systems. So, based on the algorithms of Shor and Grover quantum cryptography, symmetric cryptosystems based on traditional cryptography algorithms, as well as asymmetric cryptosystems, including systems based on elliptic curve cryptography, can be broken. The paper proposes to use a new approach to building security systems based on the concept of internal and external security contours. At the same time, security contours of continuous business processes are considered. This approach provides an objective assessment of the current state of security of the socio-cyber system as a whole.

Keywords: double-contour Security concept; post-quantum period; quantum computer; synergy; hybridity of cyberattacks.

Introduction

Problem statement. The development of modern LTE mobile Internet technologies makes it possible to use modern standards of wireless networks IEEE802.16, IEEE802.16e, IEEE802.15.4, IEEE802.11, Bluetooth 5, 6 to form not only mesh and sensor networks, but also integration with cyber-physical systems based on smart and Internet of things technologies. This approach allows the formation of sociocyberphysical systems (cyberphysical social system, CPSS) – a set of subjects and objects of the cybernetic, physical and social worlds that allow the formation of “smart” communities, on the one hand, and intellectual space, on the other. In CPSS, users are service consumers, and physical objects in the form of various devices are service providers. [1, 2].

Analysis of recent research and publications. In the context of the formation of a high-tech society, social networks based on Internet services have become one of the most effective and popular means of mass communication. One of the directions of development of CPSS is the impact on such communities, which are an effective mechanism of influence in the context of hybrid wars and color revolutions [1, 2]. Such a synthesis of social Internet services (SSIS) with cyber-physical systems makes it possible to form a sociocyberphysical system [2–7]. CPSS allows to form the social, political, economic "opinion" of the intellectual community (integration of the cybernetic, physical and social worlds), regulate and manage on the basis of SSIS, provide users with proactive services. The nature of CPSS data brings new requirements and challenges to the various stages of data processing, including the identification of data sources, the processing and aggregation of data of various types and scales. Another direction is the integration of cyberphysical systems with new technologies of wireless networks based on a mobile Internet resource. This approach forms not only the directions of high-performance sociocyberphysical systems based on smart technologies, but also makes it possible to significantly simplify the possibility of implementing targeted attacks based on the integration of cyber threats with social engineering methods [2, 8–10]. In addition, in the context of the emergence of a full-scale quantum computer, the stability of almost all algorithms of symmetric and asymmetric cryptography is called into question, and the rapid growth of IT computing resources and “G” technologies contributes to an increase in the growth of attacks on information and communication (ICS) and cyberphysical systems (CPS), which are the core of modern information-critical cybernetic systems (CCIS). Under such conditions, the primary task of maintaining the required level of security is the classification of modern threats that are combined with social engineering methods and acquire signs of synergy and hybridity [8–10]. The performed analysis [11–16] showed a change in the emphasis of CCIS (CPSS) from the development of an optimization problem for these computational components to the involved interaction between the physical environments and the computational elements with which they interact. In [11], a classification is proposed, consisting of four dimensions, which allows to combine the issues of building and modifying ICS with ensuring the required level of security. The first dimension of the classification covers the attack vector and the main attack scenario. The second dimension of classification identifies an attack by its primary target. Vulnerabilities are classified in the third dimension of the classification, and payloads in the fourth taxonomy. Paper [13] presents an information security risk analysis methodology that links assets, vulnerabilities, threats, and organizational controls. This approach allows to identify critical points in the network infrastructure, combine them with the appropriate elements of the control system. The approach uses a sequence of matrices that reflect the correlation of various elements in risk analysis [13].

In addition, [14] provides an example of how the organization of the process of collecting information about cyber incidents can be used by victims of cyber attacks. In addition, an attempt is made to assist in understanding the threat of cyber incidents for various purposes, which can be useful for increasing organizational focus in terms of a cyber incident. In [15–16], a classification is proposed, in which the following classes of entities are distinguished: an attacker, a vulnerability, a tool, a goal, an action, goals and an unauthorized result. Attackers use tools to perform actions that exploit a vulnerability in a target.

In addition, the direction of smart technologies and "Smart Home" technologies usually use security mechanisms without a preliminary integrated approach in the provision of security services. Basically, the mechanisms of computer systems and technologies are integrated with wireless network technologies, which does not allow the formation of information protection systems with the required level of security. The papers [17–24] 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 provides security services – confidentiality and data integrity. Fig. 1 presents the basic principles of security based on the use of the KNX standard.

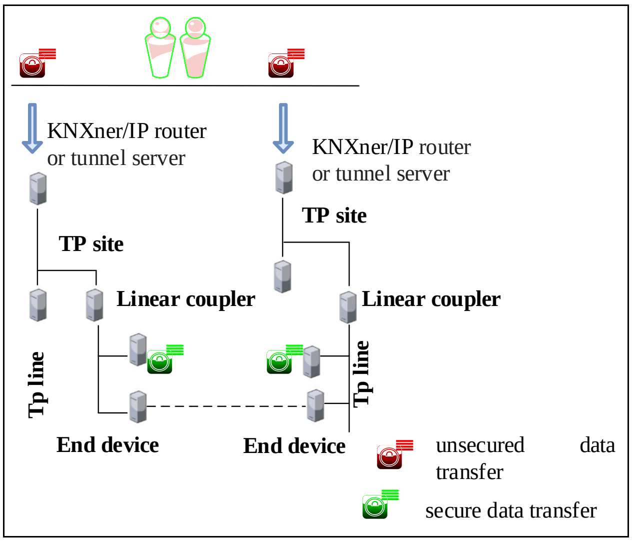


Fig. 1. Ensuring security in mobile wireless channels based on KNX

The KNX IP Secure standard allows to authenticate and encrypt KNX telegrams in IP networks. In this case, tunneling is usually formed, which ensures the confidentiality of information. KNX IP Secure mechanisms are an additional security shell (shell) that protects all KNXnet/IP data traffic.

However, KNX IP Secure is not so secure, it is possible to monitor the network, record sent packets and easily repeat them, because there are no line connectors with the “Security Proxy” function. In addition, the use of the AES-128 algorithm in the formation of tunneling in the post-quantum period will not provide the required level of protection even for the inner contour.

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 – cyberphysical, which directly performs the functions of service, and socio-management – a combination of a social component and a control system that is deployed in the cloud. The use of security mechanisms of the second subsystem, as a rule, is not taken into account when assessing the current state of security. Formally, “it is considered” that cloud technologies provide the required level of security. The main security threats in the cloud are: data theft, data loss, account hacking, gaps in interfaces and Application Programming Interface (API), DDos attacks, insider actions, the possibility of penetration by hackers, as well as downtime due to the fault of the provider [25].

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

The goal of the article is to develop the concept of dual-contour protection of sociocyberphysical systems, which will allow forming a new approach to assessing the CPSS information security system, taking into account its scalability and integration of various technologies of wireless communication channels.

1. Development of the security concept for wireless networks based on mobile technologies

To ensure the security of sociocyberphysical systems and systems based on their infrastructure, it is necessary to take into account not only the rapid development of the computing capabilities of mobile technologies (wireless communication channels) with their ability to provide information transfer from 1 Tb/s and above, the growth of service capabilities and functionality of cloud technologies, but also the integration of modern threats based on the synthesis of social engineering mechanisms, cyber threats (with signs of hybridity and synergy), as well as the ability of special services to control a significant part of cloud technology resources. To implement this approach, it is proposed to divide CPSS into two subsystems of security and infrastructure – the inner contour, the cyber-physical system (cyber-physical system, CPS), which provides the required set of services and functionality, and the outer contour – the socio-managerial system (socio-managerial system, SMS) based on the synthesis of social networks and systems (messengers) of cloud technologies.

This approach provides a synthesis of internal and external contours, takes into account efficiency, energy intensity and relative safety (each contour builds security on its own mechanisms and principles), on the one hand. On the other hand, it allows to objectively assess the threats of each of the contours, taking into account the computing resources and financial capabilities of intruders. Fig. 2 presents a block diagram of the concept of dual-contour security of sociocyberphysical systems.

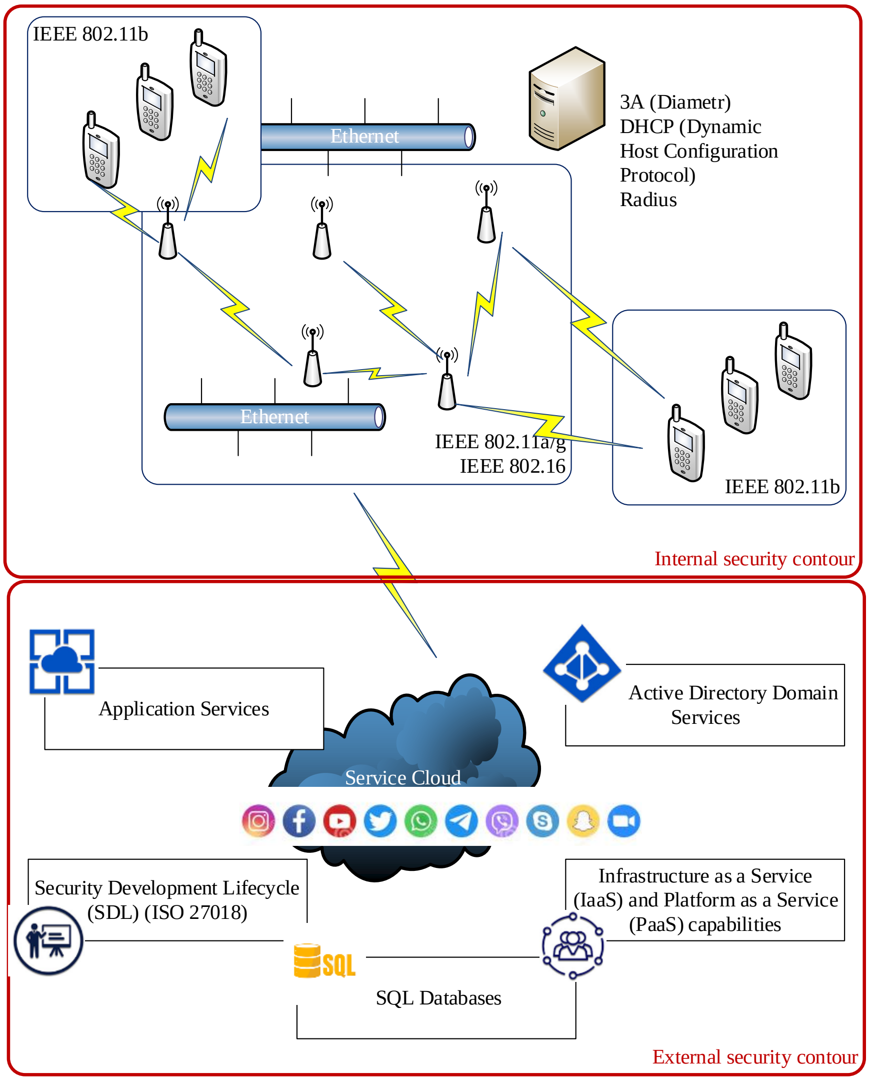

IEEE 802.11b
Ethernet
3A (Diametr)
DHCP (Dynamic Host Configuration Protocol)
Radius
Ethernet
IEEE 802.11a/g
IEEE 802.16
IEEE 802.11b
Internal security contour
Application Services
Active Directory Domain Services
Service Cloud
Security Development Lifecycle (SDL) (ISO 27018)
Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) capabilities
SQL
SQL Databases
External security contour

Fig. 2. Block diagram of the concept of dual-contour security of sociocyberphysical systems

To ensure the security of such systems, two classes of threats must be considered. The first class is threats and their integration with the methods of social engineering of the internal infrastructure (internal security contour). The second class is threats of the external contour (cloud technologies that provide not only the management of sociocyberphysical systems and networks, but also the storage/duplication of the database).

The works [10, 26] propose methodological foundations for building security systems, taking into account the synergy and hybridity of modern targeted attacks on critical infrastructure objects, which makes it possible to ensure security in the inner contour.

To ensure the safety of the entire protection system, it is necessary to take into account the threats of the internal and external contours:

– internal contour threats considering hybridity and synergism [26]:

$$W^{CPSS\ ISL}_{hybrid\ C,I,A,Au,Af\ synerg} = W^{CPSS\ ISLC}_{synerg} \cap \\ \cap W^{CPSS\ \ ISLI}_{synerg} \cap W^{CPSS\ \ ISLA}_{synerg} \cap \\ \cap W^{CPSS\ ISLAu}_{synerg} \cap W^{CPSS\ \ ISLInv}_{synerg}, \tag{1}$$

where $W^{CPSS\ ISLC}_{synerg}$ – synergy of threats on confidentiality service, $W^{CPSS\ ISLI}_{synerg}$ – synergy of threats on integrity service, $W^{CPSS\ ISLA}_{synerg}$ – synergy of threats on availability service, $W^{CPSS\ ISLAu}_{synerg}$ – synergy of threats to the authenticity service, $W^{CPSS\ ISLInv}_{synerg}$ – synergy of threats to involvement service.

– outer contour threats considering hybridity and synergy [26]:

$$W^{SCPS\ ESL}_{hybrid\ C,I,A,Au,Af\ synerg} = W^{CPSS\ ESLC}_{synerg} \cap \\ \cap W^{CPSS\ \ ESLI}_{synerg} \cap W^{CPSS\ \ ESLA}_{synerg} \cap \\ \cap W^{CPSS\ \ ESLAu}_{synerg} \cap W^{CPSS\ \ ESLInv}_{synerg}, \tag{2}$$

where $W^{CPSS\ ESLC}_{synerg}$ – synergy of threats on confidentiality service, $W^{CPSS\ \ ESLI}_{synerg}$ – synergy of threats on integrity service, $W^{CPSS\ \ ESLA}_{synerg}$ – synergy of threats on availability service, $W^{CPSS\ ESLAu}_{synerg}$ – synergy of threats to the authenticity service, $W_{synerg}^{CPSS\ ESLInv}$ – synergy of threats to involvement service.

The analysis [10, 25, 26] showed that in the outer contour the main security services are integrity, confidentiality and availability, so the services of authenticity and involvement can be neglected. Then the threats of the outer contour can be written in the form:

$$W_{hybrid\ C,I,A,Au,Af\,synerg}^{CPSS\ ESL} = W_{synerg}^{CPSS\ ESLC} \cap \\ \cap W_{synerg}^{CPSS\ \ ESLI} \cap W_{synerg}^{CPSS\ \ ESLA}, \qquad (3)$$

Each element of information resources $I_{A_i} \in \{I_A\}$ can be described by a vector

$$I_{A_i} = \left(Type_i, A_i^C, A_i^I A_i^A, A_i^{Au}, A_i^{Inv}, \beta_i\right),$$

where $Type_i$ – information asset type, described by a set of basic values: $Type_i$={CI_i, PD_i, CD_i, TS_i, StR_i, $PubI_i$, $ContI_i$, PI_i}, where CI_i – confidential information, PD_i – payment documents, CD_i – loan documents, TS_i – commercial secret, StR_i – statistical reports, $PubI_i$ – public information, $ContI_i$ – control information, PI_i – personal Information. $A_i^C, A_i^I A_i^A, A_i^{Au}, A_i^{Inv}$ – security services (A_i^C – confidentiality, A_i^I – integrity, A_i^A – availability, A_i^{Au} – authenticity, A_i^{Inv} – involvement); β_i – a metric of the ratio of time and degree of confidentiality of information for an asset (critical – 1,0; high – 0,75; medium – 0,5; low – 0,25; very low – 0,01).

Then the general (current) level of security of sociocyberphysical systems based on wireless mobile technologies is described by the expression [26]:

– for additive convolution

$$L_{W_{security}^{CPSS}} = \sum_{W_{hybrid\ C,I,A,Au,Af\,synerg}^{CPSS\ ISL}} \sum_{i=1}^{8}\left(I_{A_i} \times \beta_i\right) + \\ + \sum_{W_{hybrid\ C,I,A,synerg}^{CPSS\ ESL}} \sum_{i=1}^{8}\left(I_{A_i} \times \beta_i\right); \qquad (4)$$

– for multiplicative convolution

$$L_{W_{security}^{CPSS}} = 1 - \\ - \left[1 - \sum_{W_{hybrid\ C,I,A,Au,Af\,synerg}^{CPSS\ ISL}} \sum_{i=1}^{8}\left(I_{A_i} \times \beta_i\right)\right] \times \qquad (5) \\ \times \left[1 - \sum_{W_{hybrid\ C,I,A,synerg}^{CPSS\ ESL}} \sum_{i=1}^{8}\left(I_{A_i} \times \beta_i\right)\right].$$

In (4), (5) index i refers to the corresponding type of information asset, and external summation is performed over all threats of the internal and external contours.

Thus, the proposed concept takes into account the level of security not only of the CPS, which directly provides services for the operation of smart and Internet of things systems, but also of the SMS, which directly provides the subsystem of the internal security contour.

2. Wireless network security assessment based on the dual-contour security concept

To determine the current security state of the inner contour, 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 synergy based on a synergistic threat model. The main stages are shown in Fig. 3.

To form an expert assessment, we use a modification of the threat classifier, which is proposed in [8, 9] and shown in Fig. 4. For the objectivity of expert judgments, we use the weight coefficients of expert competence (k_k), presented in Tabl. 1.

Table 1 – **Expert competence weight coefficient**

№	**Expert qualification**	**Weight value (k_k)**
1	International expert in the field of IS, CS, SI	1,0
2	National expert in the field of IS, CS, SI	0,95
3	Certified international specialist in the field of IS, CS, SI	0,9
4	Full doctorate in the field of IS, CS, SI	0,9
5	Head of security	0,85
6	Phd in the field of IS, CS, SI	0,8
7	Security officer	0,7
8	System administrator	0,6
9	Security engineer	0,5
10	Postgraduate student in the specialty in the field of IS, CS, SI	0,4

Summary score of i-th threat is determined by the number of experts according to the expression:

$$x_i = \sum_{k=1}^{K} x_k \times k_k \Big/ K, \qquad (6)$$

where x_k – evaluation of k-th expert for i-th threat influence; 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:

$$\sigma_x^2 = \frac{1}{K}\sum_{k=1}^{K} k_k \left(x_k - x_i\right)^2. \qquad (7)$$

Statistical probability of the received results 1 – α_i, will be: $\left[x_i - \Delta, x_i + \Delta\right]$, where 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:

$$\Delta = t\sqrt{\sigma_x^2 / N}, \qquad (8)$$

where t – Student's t-distribution value for K–1 degrees of freedom.

To determine the economic costs of preventing an attack, we use an algorithm based on the cost indicators of threats. This approach makes it possible to estimate the economic costs of deliberate protection mechanisms, taking into account the ranking of potential threats and the importance of information resources to be protected [8]. Both sides of the attack are determined by the importance (ranking) of attacks that are economically feasible to carry out.

1-st step. Identification of attacks, the effect of which exceeds the cost of their implementation:

$$Tr_R^A = \left\{ Tr_i \mid \left(P_i^A - C_i^A \right) > 0 \right\} \forall Tr_i \in Tr, \qquad (9)$$

where Tr_R^A – set of potential threats, the implementation of which is effective for the attacker; Tr_i – threat for the *i*-th information resource; P_i^A – assessment of the cost of successful implementation of an attack on *i*-th resource from the side of the attacker; C_i^A – the cost of attacking the *i*-th resource from the side of the attacker.

2-nd step. Determination of the direction of protection, which provides an effect higher than the cost of their provision.

$$Tr_C^D = \left\{ Tr_j \mid \left(P_i^D - C_i^D \right) > 0 \right\} \forall Tr_j \in Tr, \qquad (10)$$

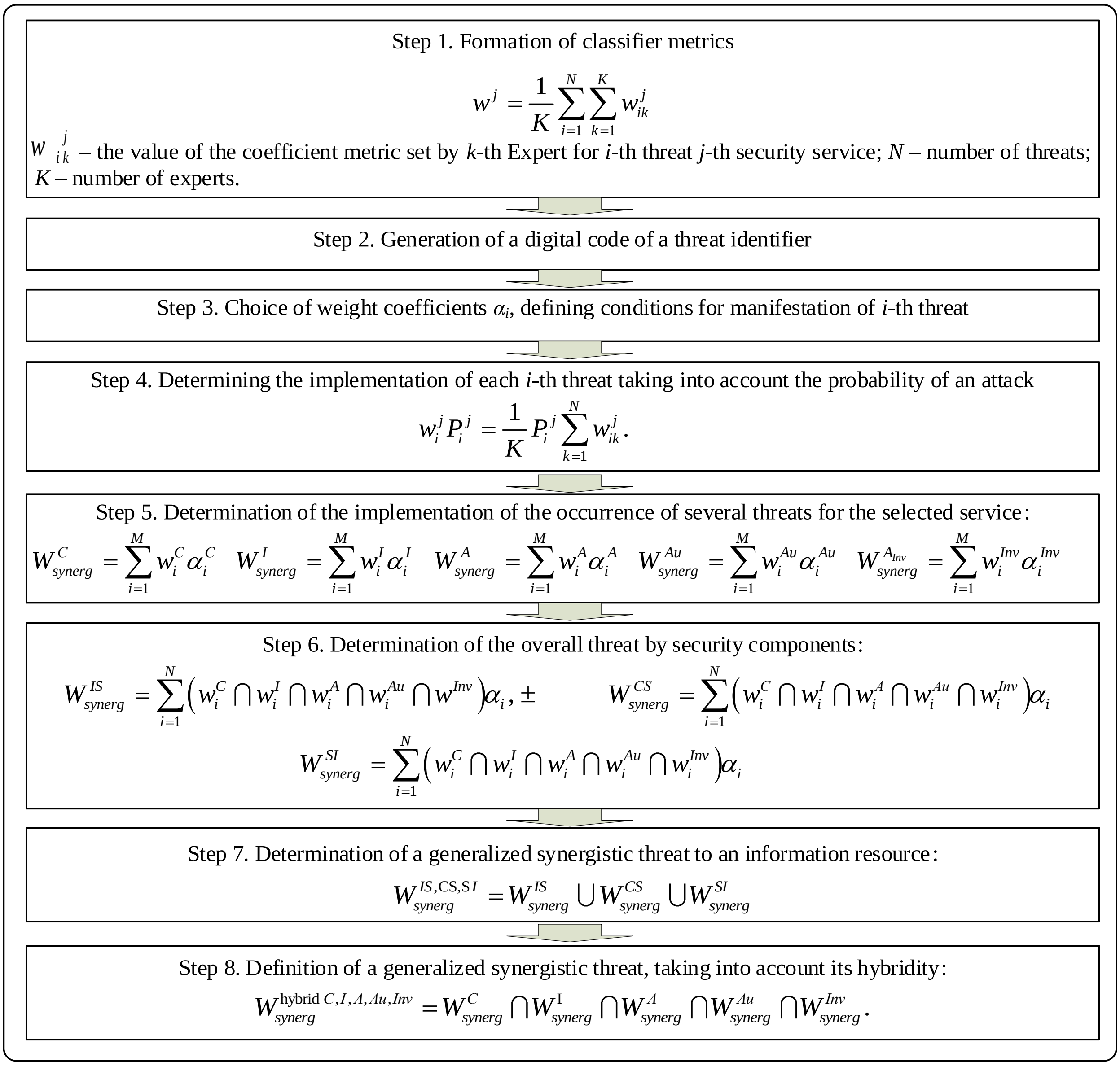
where Tr_C^D – set of threats against which it is economically feasible to build protection; P_i^D – estimate of the cost of *i*-th information resource loss for the defending side; C_i^D – protection cost for *i*-th information resource for the defense side;

3-th step. Determination of importance coefficients for attackers. Defined as the share of winnings from the total winnings, which can potentially be obtained from the implementation of the entire complex of attackers` threats:

$$K_i^A = \frac{P_i^A - C_i^A}{\sum_{i=1}^{M} \left(P_i^A - C_i^A \right)}, \ \ \forall Tr_i \in Tr_R^A, M = \left| Tr_R^A \right|, \qquad (11)$$

where K_i^A – rating coefficient (importance) of the threat realization for *i*-th information resource;

M – the power of the set of selected potentially effective threats for the attacking side.



Step 1. Formation of classifier metrics

$$w^j = \frac{1}{K} \sum_{i=1}^{N} \sum_{k=1}^{K} w_{ik}^j$$

w_{ik}^j – the value of the coefficient metric set by *k*-th Expert for *i*-th threat *j*-th security service; *N* – number of threats; *K* – number of experts.

Step 2. Generation of a digital code of a threat identifier

Step 3. Choice of weight coefficients α_i, defining conditions for manifestation of *i*-th threat

Step 4. Determining the implementation of each *i*-th threat taking into account the probability of an attack

$$w_i^j P_i^j = \frac{1}{K} P_i^j \sum_{k=1}^{N} w_{ik}^j .$$

Step 5. Determination of the implementation of the occurrence of several threats for the selected service:

$$W_{synerg}^{C} = \sum_{i=1}^{M} w_i^C \alpha_i^C \quad W_{synerg}^{I} = \sum_{i=1}^{M} w_i^I \alpha_i^I \quad W_{synerg}^{A} = \sum_{i=1}^{M} w_i^A \alpha_i^A \quad W_{synerg}^{Au} = \sum_{i=1}^{M} w_i^{Au} \alpha_i^{Au} \quad W_{synerg}^{A_{Inv}} = \sum_{i=1}^{M} w_i^{Inv} \alpha_i^{Inv}$$

Step 6. Determination of the overall threat by security components:

$$W_{synerg}^{IS} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \cap w^{Inv} \right) \alpha_i , \pm \qquad W_{synerg}^{CS} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \cap w_i^{Inv} \right) \alpha_i$$

$$W_{synerg}^{SI} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \cap w_i^{Inv} \right) \alpha_i$$

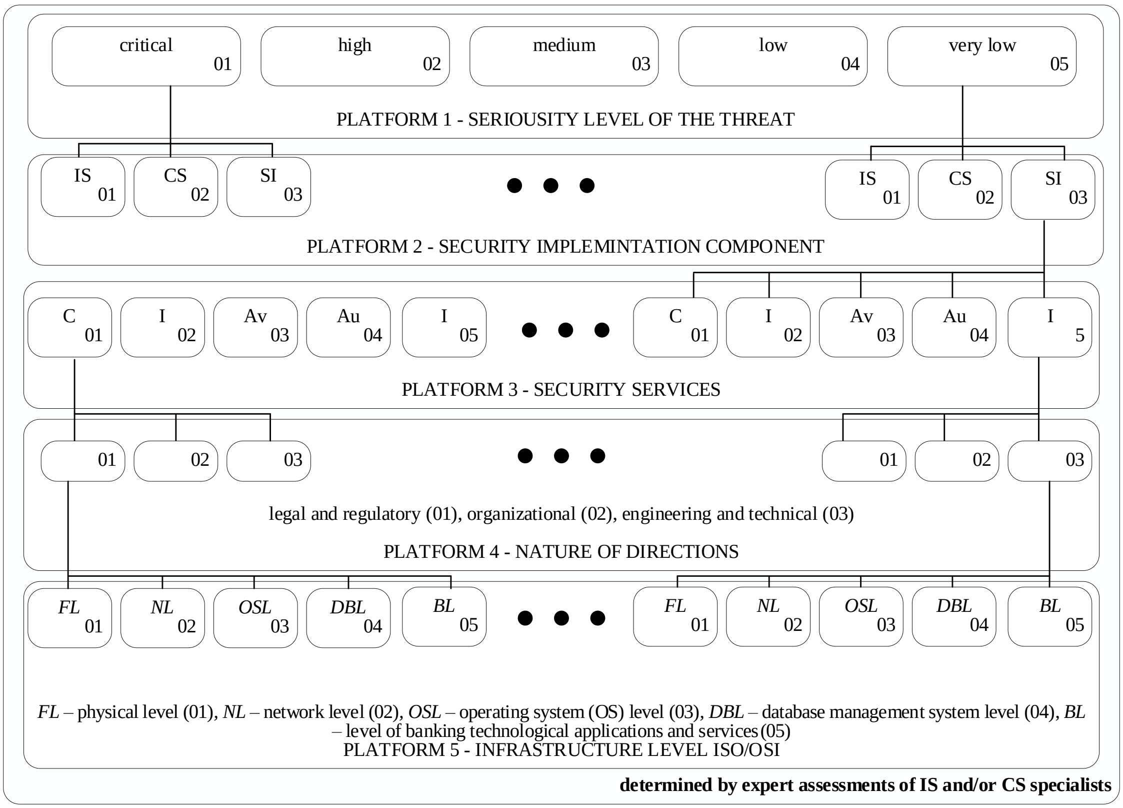
Step 7. Determination of a generalized synergistic threat to an information resource:

$$W_{synerg}^{IS,\mathrm{CS},\mathrm{S}I} = W_{synerg}^{IS} \cup W_{synerg}^{CS} \cup W_{synerg}^{SI}$$

Step 8. Definition of a generalized synergistic threat, taking into account its hybridity:

$$W_{synerg}^{\mathrm{hybrid}\ C,I,A,Au,Inv} = W_{synerg}^{C} \cap W_{synerg}^{\mathrm{I}} \cap W_{synerg}^{A} \cap W_{synerg}^{Au} \cap W_{synerg}^{Inv} .$$

Fig. 3. Determining the probability of threats based on the synergistic threat model


critical 01
high 02
medium 03
low 04
very low 05
PLATFORM 1 - SERIOUSITY LEVEL OF THE THREAT
IS 01
CS 02
SI 03
IS 01
CS 02
SI 03
PLATFORM 2 - SECURITY IMPLEMINTATION COMPONENT
C 01
I 02
Av 03
Au 04
I 05
C 01
I 02
Av 03
Au 04
I 5
PLATFORM 3 - SECURITY SERVICES
01
02
03
01
02
03
legal and regulatory (01), organizational (02), engineering and technical (03)
PLATFORM 4 - NATURE OF DIRECTIONS
FL 01
NL 02
OSL 03
DBL 04
BL 05
FL 01
NL 02
OSL 03
DBL 04
BL 05
FL – physical level (01), NL – network level (02), OSL – operating system (OS) level (03), DBL – database management system level (04), BL – level of banking technological applications and services(05)
PLATFORM 5 - INFRASTRUCTURE LEVEL ISO/OSI
determined by expert assessments of IS and/or CS specialists

STEP 1. FORMATION OF METRIC THREAT COEFFICIENTS FOR **CPSS ISL** AND **CPSS ESL**

$$w_{CPSS\ ESL}{}^{j}=\frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K}w_{CPSS\ ESLik}{}^{j},\quad w_{CPSS\ ISL}{}^{j}=\frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K}w_{CPSS\ ISLik}{}^{j}$$

STEP 2. FORMATION OF WEIGHT COEFFICIENTS OF THE CONDITIONS OF MANIFESTATION OF THREATS FOR **CPSS ISL** AND **CPSS ESL**

$$\alpha_i^{CPSS\ ISL},\ i\in\left[0,067;0,133;0,2;0,267;0,333\right],\ \alpha_i^{CPSS\ ESL},\ i\in\left[0,067;0,133;0,2;0,267;0,333\right]$$

STEP 3. DEFINING THE IMPLEMENTATION OF EACH THREATS FOR **CPSS ISL** \and **CPSS ESL**

$$w_{CPSS\ ISLi}{}^{j}P_{CPSS\ ISLi}{}^{j}=\frac{1}{K}P_{{}_{CPSS\ ISL}i}{}^{j}\sum_{k=1}^{N}w_{I_{CPSS\ ISL}ik}{}^{j},\ \text{где}\ P_{{}_{CPSS\ ISL}i}{}^{j}\in\left\{\alpha_i^{CPSS\ ISL}\right\},$$

$$w_{CPSi}{}^{j}P_{CPSi}{}^{j}=\frac{1}{K}P_{CPSS\ ESLi}{}^{j}\sum_{k=1}^{N}w_{CPSS\ ESLik}{}^{j},\ \text{где}\ P_{CPSS\ ESLi}{}^{j}\in\left\{\alpha_i^{CPSS\ ESL}\right\}$$

STEP 4. DEFINITION OF THE IMPLEMENTATION OF MULTIPLE THREATS TO A SECURITY SERVICE

$$W_{CPSS\ ISLsynerg}{}^{C}=\sum_{i=1}^{M}w_{CPSS\ ISLi}{}^{C}\alpha^{CPSS\ ISLC}{}_{i}\bigcup W_{CPSS\ ESLsynerg}{}^{C}=\sum_{i=1}^{M}w_{CPSi}{}^{C}\alpha^{CPSS\ ESLC}{}_{i}$$

$$W_{CPSS\ ISLsynerg}{}^{I}=\sum_{i=1}^{M}w_{CPSS\ ISLi}{}^{I}\alpha^{CPSS\ ISLC}{}_{i}\bigcup W_{CPSS\ ESLsynerg}{}^{I}=\sum_{i=1}^{M}w_{CPSi}{}^{I}\alpha^{CPSS\ ESLC}{}_{i}$$

$$W_{CPSS\ ISLsynerg}{}^{A}=\sum_{i=1}^{M}w_{CPSS\ ISLi}{}^{A}\alpha^{CPSS\ ISLC}{}_{i}\bigcup W_{CPSS\ ESLsynerg}{}^{A}=\sum_{i=1}^{M}w_{CPSi}{}^{A}\alpha^{CPSS\ ESLC}{}_{i}$$

$$W_{CPSS\ ISLsynerg}{}^{Aff}=\sum_{i=1}^{M}w_{{}_{CPSS\ ISL}i}{}^{Aff}\alpha^{CPSS\ ISLAff}{}_{i};\quad W_{CPSS\ ISLsynerg}{}^{Inv}=\sum_{i=1}^{M}w_{CPSS\ ISLi}{}^{Inv}\alpha^{CPSS\ IS\,Inv}{}_{i}$$

STEP 5. DETERMINATION OF THE TOTAL THREATS TO THE SAFETY COMPONENT

$$W_{synerg}^{IS}=\sum_{i=1}^{N}\left(w_{CPSS\ ISLi}{}^{C}\bigcap w_{CPSS\ ISLi}{}^{I}\bigcap w_{CPSS\ ISLi}{}^{A}\bigcap w_{CPSS\ ISLi}{}^{Au}\bigcap w_{CPSS\ ISLi}{}^{Aff}\right)\alpha_i^{CPSS\ ISL}\bigcup$$

$$\bigcup\sum_{i=1}^{N}\left(w_{CPSS\ ESLi}{}^{C}\bigcap w_{CPSS\ ESLi}{}^{I}\bigcap w_{CPSS\ ESLi}{}^{A}\right)\alpha_i^{CPSS\ ESL}$$

STEP 6. DETERMINING THE ECONOMIC COST OF ATTACK PREVENTION

$$Tr_{CPSS\ ISLR}{}^{A}=\left\{Tr_i\mid\left(P_i^{A}-C_i^{A}\right)>0\right\}\ \forall Tr_i\in Tr\Rightarrow Tr_L^{ICS}=\arg\max_{\forall Tr_l\in Tr_C^D}K_l^D\cdot K_l^A$$

$$Tr_{CPSS\ ESLR}{}^{A}=\left\{Tr_i\mid\left(P_i^{A}-C_i^{A}\right)>0\right\}\ \forall Tr_i\in Tr\Rightarrow Tr_L^{CPS}=\arg\max_{\forall Tr_l\in Tr_C^D}K_l^D\cdot K_l^A$$

determined automatically based on mathematical expressions

Fig. 4. Modification of the threat classifier

4-th step. Determination of coefficients of importance for defenders. Defined as the share of the gain from the total amount of the gain, which can potentially be obtained from the implementation of the entire complex of protective measures:

$$K_j^D = \frac{P_i^D - C_i^D}{\sum_{i=1}^{N}\left(P_i^D - C_i^D\right)}, \qquad (12)$$
$$\forall Tr_j \in Tr_C^D, N = \left|Tr_C^D\right|,$$

where K_j^D – rating coefficient (importance) of building defense for *j*-th information resource.

5-th step. The selection of critical threats based on the evaluation of the product of the coefficients of importance, the attacker and the attacker is the maximum:

$$Tr_l = \arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \cdot K_l^A. \qquad (13)$$

Thus, the use of this classifier, as well as the introduction of economic indicators of the cost of carrying out an attack and the cost of measures to counter it, make it possible to obtain an integral assessment of the security of the system.

To obtain an assessment of the current state of information security based on the proposed concept of a two-contour information security system CPSS, let's assume that "1" will correspond to the maximum level of security that is provided by the security system as a whole, and "0" – corresponds to the absence of the required level of information protection.

To determine the probability of a threat being realized under the limiting possibilities of defense *A* and the limiting possibilities of attack *B*, we will use the probability density function of a random variable *x* – *F*(*x*).

The specified probability is determined by the difference

$$F(B) - F(A),$$

where *A* – marginal level of protection side capabilities, *B* – the limiting level of the attacking side's ability to implement an attack.

We define the security level as the share of those resources that are protected from cyberattacks. It is easy to see that this quantity can be defined as follows:

$$S = F(B) - F(A) = \int_{-\infty}^{B} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} dt - \qquad (14)$$
$$- \int_{-\infty}^{A} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} dt.$$

To assess the category of an attacker and determine his capabilities (computing and financial resources, economic interest), we use the attacker model and the method for determining the attacker category on CPSS applied in the work [9].

An analysis of the classification of intruders allows to form a set $\{H_j\}_{CPSS\ ISL}$, determining the levels of influence on the CPSS of the internal contour [9]:

– technical channels level (H_0);

– protocol stack physical level TCP/IP(H_1);

– protocol stack link level TCP/IP (H_2);

– network level protocol stack TCP/IP (H_3);

– protocol stack transport level TCP/IP (H_4);

– level of harmful impact (H_5);

– embedded device level (H_6);

– protocol stack application-level TCP/IP (H_7);

– information security system level (H_8).

In Table 2, the ratio of the categories of the intruder and the levels of their impact on the internal loop security system is determined.

Table 2 – **The ratio of the categories of the violator and the levels of their impact**

Category	**Impact levels**								
	H_0	H_1	H_2	H_3	H_4	H_5	H_6	H_7	H_8
L_1^{del}	0	0	0	0	0	0	0	1	1
L_{11}^{del}	1	1	0	0	0	0	1	1	1
L_{12}^{del}	0	0	0	0	0	0	0	1	1
L_{13}^{del}	0	0	0	0	0	0	0	1	1
L_2^{del}	1	1	1	1	1	0	1	0	1
L_3^{del}	0	0	0	0	0	0	1	1	0
L_4^{del}	1	1	1	1	0	1	1	0	0
L_5^{del}	1	1	1	1	1	1	1	1	0
L_{51}^{del}	1	1	1	1	1	1	1	1	1
L_{52}^{del}	1	1	1	1	1	1	1	1	1
L_{53}^{del}	1	1	1	1	0	1	1	0	0
L_{54}^{del}	1	1	1	1	1	1	1	0	1
L_{55}^{del}	1	1	1	1	0	1	1	0	0
L_{56}^{del}	1	0	0	0	0	1	1	0	0
L_{57}^{del}	1	0	0	0	0	1	0	0	0

Elements of the set of categories of intruders $L_i^{del} \in \left\{L_i^{del}\right\}$:

L_1^{del} – users of CPSS;

L_{11}^{del} – management of CPSS,

L_{12}^{del} – employee of CPSS,

L_{13}^{del} – users “at risk”;

L_2^{del} – operating personnel;

L_3^{del} – technical support staff;

L_4^{del} – persons who are not employees of CPSS,

L_5^{del} external intruders:

L_{51}^{del} – cyberterrorists,

L_{52}^{del} – special services,

L_{53}^{del} – hackers,

L_{54}^{del} – cybercriminals,

L_{55}^{del} – competitors,

L_{56}^{del} – criminality,

L_{57}^{del} – vandals.

Let's form a set $\{H_j\}_{CPSS\,ESL}$, determining the levels of influence on the CPSS of the external contour:

– the level of technical channels of cloud technologies (H_0);

– database management system level (H_1);

– service application layer (H_2);

– Azure Active Directory Domain Services level (H_3);

– the level of harmful effects on Security Development Lifecycle (H_4);

– SQL Databases (H_5);

– information security system level (H_6).

In Table 3, the ratio of the categories of the intruder and the levels of influence of the external contour of the protection system is determined.

The weight coefficient of the "danger" of the attacker is determined by the formula [9]:

$$\gamma_{ICS}^{CPS} = \frac{1}{N}\sum_{i=1}^{N}\gamma_{ICS\ i}^{CPS}, \qquad (15)$$

where $\gamma_{ICS\ i}^{CPS} = \left(\beta_i^{ICS} \cup \beta_i^{CPS}\right) \times p_{rj} \times r_{motiv}$,

$\beta_i^{CPSS\ ISL} = W_{cp}^{CPSS\ ISL} \cap W_{cash}^{CPSS\ ISL} \cap T^{CPSS\ ISL}$,

$\beta_i^{CPSS\ ESL} = W_{cp}^{CPSS\ ESL} \cap W_{cash}^{CPSS\ ESL} \cap T^{CPSS\ ESL}$ – weighting coefficients of the intruder capabilities for CPSS ISL and CPSS ESL (respectively),

$W_{cp}^{CPSS\ ISL}\left(W_{cp}^{CPSS\ ESL}\right)$ – computing resources of the intruder (1 – unlimited resources of cyberterrorists, 0,75 – state resources (special services), 0,5 – resources of cybercriminals, 0,25 – resources of criminality, competitors, hackers, 0,001 – vandal resources); $T^{CPSS\ ISL}$ ($T^{CPSS\ ESL}$) – time to carry out the threat (1 – the threat is realized daily, 0,75 – the threat is realized within a week, 0,5 – the threat is realized within a month, 0,25 – the threat is realized within a year, 0,001 – unlimited time); $W_{cash}^{CPSS\ ISL}\left(W_{cash}^{CPSS\ ESL}\right)$ – economic opportunities of attackers (1 – unlimited resources of cyberterrorists, 0,75 – state resources (special services), 0,5 – resources of cybercriminals, 0,25 – resources of criminality, competitors, hackers, 0,001 – vandal resources).

Table 3 – **The ratio of the categories of the violator and the levels of their impact**

category	impact levels						
	H_0	H_1	H_2	H_3	H_4	H_5	H_6
L_1^{del}	0	0	0	0	0	0	0
L_{11}^{del}	1	1	0	0	0	0	1
L_{12}^{del}	0	0	0	0	0	0	0
L_{13}^{del}	0	0	0	0	0	0	0
L_2^{del}	1	1	1	1	1	0	1
L_3^{del}	0	0	0	0	0	0	1
L_4^{del}	1	1	1	1	0	1	1
L_5^{del}	1	1	1	1	1	1	1
L_{51}^{del}	1	1	1	1	1	1	1
L_{52}^{del}	1	1	1	1	1	1	1
L_{53}^{del}	1	1	1	1	0	1	1
L_{54}^{del}	1	1	1	1	1	1	1
L_{55}^{del}	1	1	1	1	0	1	1
L_{56}^{del}	1	0	0	0	0	1	1
L_{57}^{del}	1	0	0	0	0	1	0

Table 4 shows the initial data of the criteria and indicators of the expert assessment of its location.

Analysis of tables 2–4 takes into account that the attack is determined by a complex criterion that includes account the cost of conducting and the computational capabilities available to the attacker. This approach ensures timely response to computer incidents depending on the category of intruder and ensures the required level of security.

Table 4 – **Initial data of criteria and indicators of expert evaluation of the weight coefficient of the “danger” of the violator**

Category	Weighting indicators							
	$\beta_i^{ICS} \in \left\{\beta_i^{ICS}\right\}$			$\beta_i^{CPS} \in \left\{\beta_i^{CPS}\right\}$			p_{rj}	r_{motiv}
	$W_{cp}^{CPSS\ ISL}$	$T^{CPSS\ ISL}$	$W_{cash}^{CPSS\ ISL}$	$W_{cp}^{CPSS\ ESL}$	$T^{CPSS\ ESL}$	$W_{cash}^{CPSS\ ESL}$		
critical	1	1	1	1	1	1	1	1
high	0,75	0,75	0,75	0,75	0,75	0,75	0,75	0,75
median	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5
low	0,25	0,25	0,25	0,25	0,25	0,25	0,25	0,25
very low	0,001	0,001	0,001	0,001	0,001	0,001	0,001	0,001

Conclusions

In the context of the rapid growth of computing resources of wireless networks, their integration with the technologies of the mobile Internet and the Internet of Things allows to form an expansion of the range of services based on smart technologies and wireless networks. This approach ensures further integration and formation of sociocyberphysical networks, on the one hand. On the other hand, the emergence of new targeted attacks on the rapidly developing areas of the IT industry. In addition, the emergence of a quantum computer significantly increases the capabilities of cyber-intruders and cyber-terrorists. Under such conditions, the proposed approach to the formation of the security system of sociocyberphysical systems based on the two-contour Security Concept provides an objective assessment of the current state of the CPSS security level.

The paper proposes a scheme of a unified classifier, taking into account the synergetic model of threats and economic costs to ensure the required level of security, including the construction of a security system consisting of two subsystems – the CPS protection system (internal security contour) and the SMS protection system (external security contour). This approach not only takes into account targeted attacks on individual elements of the CPSS, but also ensures the objectivity of the obtained results of assessing the security level.

References

1. Gryshchuk, RV and Danyk, Yu. G. (2016), *Fundamentals of cyber security*, ZhNAEU, Zhytomyr, 2016, 636 p.
2. Yevseiev, S., Ryabukha, Yu., Milov, O., Milevskyi, S., Pohasii, S., Ivanchenko, Ye., Ivanchenko, I., Melenti, Ye., Opirskyy, I. and Pasko, I. (2021), "Development of a method for assessing forecast of social impact in regional communities", *Eastern-European Journal of Enterprise Technologies*, 6/2 (114), pp. 30–47.
3. Feng, Xia and Jianhua, Ma (2011), "Building smart communities with cyber-physical systems", *SCI '11: Proceedings of 1st international symposium on From digital footprints to social and community intelligence*, September 2011, pp. 1–6, DOI: https://doi.org/10.1145/2030066.2030068.
4. Guo, B., Yu, Z. and Zhou, X. (2015), "A Data-Centric Framework for Cyber-Physical-Social Systems", *IT Prof*., 17, pp. 4–7, availble at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7332207.
5. Kuang, L., Yang, L. and Liao, Y. (2015), "An Integration Framework on Cloud for Cyber Physical Social Systems Big Data", *IEEE Trans. Cloud Comput*., availble at: https://ieeexplore.ieee.org/document/7364232.
6. Lin, C.C., Deng, D.J. and Jhong, S.Y. (2017), "A Triangular NodeTrix Visualization Interface for Overlapping Social Community Structures of Cyber-Physical-Social Systems in Smart Factories", *IEEE Trans. Emerg. Top. Comput*., DOI: https://dl.acm.org/doi/10.1145/2030066.2030068.
7. (2017), *Cyber–Physical–Social Frameworks for Urban Big Data Systems: A Survey*, DOI: http://dx.doi.org/10.3390/app7101017.
8. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021), *Synergy of building cybersecurity systems*, PC TECHNOLOGY CENTER, Kharkiv, 188 p., DOI: http://doi.org/10.15587/978-617-7319-31-2.
9. Shmatko, O., Balakireva, S., Vlasov, A., Zagorodna, N., Korol, O., Milov, O., Petrov, O., Pohasii, S., Rzayev, Kh. and Khvostenko V. (2020), "Development of methodological foundations for a classifier of threats to cyberphysical systems design", *Eastern-European Journal of Enterprise Technologies*, 3/9 (105), pp. 6–19.
10. (2021), *Report on Post-Quantum Cryptography*, available at: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.
11. Parthasarathy S. (2011), "Community discovery in social networks: applications, methods and emerging trends", *Social Network Data Analytics,* pp 79–113, DOI: https://doi.org/10.1007/978-1-4419-8462-3_4.
12. Jimeng, Sun & Jie, Tang (2011), "A survey of models and algorithms for social influence analysis", *Social Network Data Analytics,* pp 177–214, DOI: https://doi.org/10.1007/978-1-4419-8462-3_7.
13. Anagnostopoulos, A., Kumar, R. and Mahdian, M. (2008), "Influence and correlation in social networks" *Proceeding of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD'08)*, pp. 7–15, DOI: https://doi.org/10.1145/1401890.1401897.
14. Goyal, A., Bonchi, F. and Lakshmanan L. V. (2010), "Learning influence probabilities in social networks", *Proceedings of the 3st ACM International Conference on Web Search and Data Mining (WSDM'10)*, pp. 207–217, DOI: https://doi.org/10.1145/1718487.1718518.
15. Xiang, R., Neville, J. and Rogati, M. (2010), "Modeling relationship strength in online social networks", *Proceeding of the 19th international conference on World Wide Web (WWW'10)*, pp. 981–990, DOI: https://doi.org/10.1145/1772690.1772790.
16. Scripps, J., Tan, P.-N. and Esfahanian, A.-H. (2009), "Measuring the effects of preprocessing decisions and network forces in dynamic network analysis", *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD'09)*, pp. 747–756, DOI: https://doi.org/10.1145/1557019.1557102.
17. Merz, H., Hansemann, T. and Hübner, C. (2009), *Building Automation: Communication systems with EIB/KNX*, LON und BACnet / Springer-Verlag Berlin Heidelberg, 293 p.
18. (2017), *KNX Technical Manual 2CKA001473B8668. KNX Technical Manual. Busch-Presence detector KNX*, Busch-Watchdog Sky KNX, Busch-Jaeger Elektro GmbH, 198 p.
19. (2006), *Technical documentation on KNX devices*, ABB.
20. (2004), *KNX Handbook*, Version 1.1 Revision 1. Konnex Association.
21. (2016), *ABB i-bus KNX KNX Security Panel GM/A 8.1 Product Manual*, Busch-Watchdog Sky KNX lektro GmbH, 648 p.
22. Schilder Jü. and Reibel T. (2016), *ABB GPG Building Automation Webinar ABB i-bus® KNX Basics and Products*, March 3, 2016, Busch-Watchdog Sky KNX Busch-Jaeger Elektro GmbH, 86 p.
23. (2017), *Manual for KNX Planning*, Siemens Switzerland Ltd, 100 p.
24. (2010), *Security Technology KNX-Intrusion Alarm System L240 Installation, Commissioning, Operation*, Busch-Watchdog Sky KNX, Busch-Jaeger Elektro GmbH, 116 p.

25. (2021), *"Cloud" 10 years old. From a startup in the emerging market to a successful company and new heights*, available at: https://tadviser.com.
26. Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S., Milov, O., Prokopenko, O., Sievierinov O. & Chopenko, D. (2021), "Development of a concept for building a critical infrastructure facilities security system" ,*Eastern-European Journal of Enterprise Technologies*, Vol. 3(9(111), pp. 63–83, DOI: https://doi.org/10.15587/1729-4061.2021.233533.

Received (Надійшла) 21.02.2022
Accepted for publication (Прийнята до друку) 27.04.2022

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Погасій Сергій Сергійович – кандидат економічних наук, доцент, доцент кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Serhii Pohasii – Candidate of Economic Sciences, Associate Professor, Department of Cyber Security, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: spogasiy1978@gmail.com; ORCID ID: https://orcid.org/0000-0002-4340-3693.

Мілевський Станіслав Валерійович – кандидат економічних наук, доцент кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Stanislav Milevskyi – Candidate of Economic Sciences, Associate Professor, Department of Cyber Security, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: milevskiysv@gmail.com; ORCID ID: https://orcid.org/0000-0001-5087-7036.

Томашевський Богдан Паїсійович – кандидат технічних наук, старший науковий співробітник, кафедра кібербезпеки, Тернопільський національний технічний університет ім. І. Пулюя, Тернопіль, Україна;
Bogdan Tomashevsky – Candidate of Engineering Sciences, Senior researcher, Department of Cyber Security, Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine;
e-mail: bogdan_tomashevsky@tntu.edu.ua; ORCID ID: https://orcid.org/0000-0002-1934-4773.

Воропай Наталя Ігорівна – кандидат технічних наук, асистент кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Natalya Voropay – Candidate of Engineering Sciences, Assistant, Department of Cyber Security, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: Natalia_Voropay@gmail.com; ORCID ID: https://orcid.org/0000-0003-1321-7324.

Розробка концепції двоконтурного захисту соціокіберфізичних систем

С. С. Погасій, С. В. Мілевський, Б. П. Томашевський, Н. І. Воропай

Анотація. Бурхливий розвиток мобільних інтернет-технологій LTE (Long-Term Evolution) не тільки зумовив подальший розвиток кіберфізичних систем, що ґрунтуються на синтезі технологій класичних комп'ютерних систем та технологій та LTE, а також комплексуванні з технологіями інтернет-речей. Внаслідок чого поява соціокіберфізичних систем визначає подальший розвиток на основі даного комплексування. Створення mesh-, сенсорних мереж дозволяє також розвивати смарттехнології, і системи, засновані на їх конгломерації. Розвиток та створення квантового комп'ютера з одного боку дозволить зробити технічний прорив у обчислювальних ресурсах, використовувати штучний інтелект, а з іншого боку може призвести до "хаосу" у забезпеченні безпеки сучасних технологій та систем. Так на підставі алгоритмів квантової криптографії Шора та Гровера можуть бути зламані симетричні криптосистеми на основі алгоритмів традиційної криптографії, а також несиметричні криптосистеми, включаючи системи на основі криптографії на еліптичних кривих. У роботі пропонується використовувати новий підхід до побудови систем безпеки на основі Концепції внутрішнього та зовнішнього контурів безпеки. У цьому розглядаються контури безпеки безперервних бізнес-процесів. Такий підхід забезпечує об'єктивну оцінку поточного стану безпеки соціокіберсистеми загалом.

Ключові слова: двоконтурна Концепція безпеки; постквантовий період; квантовий комп'ютер; синергізм; гібридність кібератак.

Разработка концепции двухконтурной защиты социокиберфизических систем

С. С. Погасий, С. В. Милевский, Б. П. Томашевский, Н. И. Воропай

Аннотация. Бурное развитие мобильных интернет-технологий LTE (Long-Term Evolution) не только предопределило дальней шее развитие киберфизических систем, которые основаны на синтезе технологий классических компьютерных систем и технологий и LTE, а также комплексировании с технологиями интернет-вещей. В следствии чего появление социо-киберфизических систем предопределяет дальнейшее развитие на основе данного комплексирования. Создание mesh-, сенсорных сетей позволяет так же развивать и смарт-технологии, и системы, основанные на их конгломерации. Развитие и создание квантового компьютера с одной стороны позволит сделать технический прорыв в вычислительных ресурсах, использовать искусственный интеллект, а с другой стороны может привести к "хаосу" в обеспечении безопасности современных технологий и систем. Так на основании алгоритмов квантовой криптографии Шора и Гровера могут быть взломаны симметричные криптосистемы на основе алгоритмов традиционной криптографии, а также несимметричные криптосистемы, включая и системы на основе криптографии на эллиптических кривых. В работе предлагается использовать новый подход к построению систем безопасности на основе Концепции внутреннего и внешнего контуров безопасности. При этом рассматриваются контуры безопасности непрерывных бизнес-процессов. Такой подход обеспечивает объективную оценку текущего состояния безопасности социо-киберсистемы в целом.

Ключевые слова: двухконтурная Концепция безопасности; постквантовый период; квантовый компьютер; синергизм; гибридность кибератак.