В умовах появи повномасштабного квантового комп'ютера ставиться під сумнів стійкість практично всіх алгоритмів симетричної і несиметричної криптографії. При цьому бурхливе зростання обчислювальних ресурсів IT і технологій "G" сприяє збільшенню зростання атак на інформаційно-комунікаційні (ICS) і кіберфізичні системи (CPS). Ці системи є ядром сучасних інформаційно-критичних кібернетичних систем (CCIS). В таких умовах першочерговим завданням підтримки необхідного рівня безпеки є класифікація сучасних загроз, які комплексируються з методами соціальної інженерії і набувають ознак синергії і гибридности. У роботі пропонується синергетична модель загроз на ICS/CPS, яка враховує спрямованість загроз на синергію і гибридність, і комплексірований вплив складових безпеки: інформаційну безпеку (ІБ), кібербезпеку (КБ), безпеку інформації (БІ). Такий підхід дозволяє розробити методологічні основи побудови уніфікованого класифікатора загроз кіберфізичних систем, забезпечити формування множин критичних загроз, критичних точок в елементах інфраструктури ICS/CPS, на основі мінімальних обчислювальних, людських і економічних витрат. Розроблена методика визначення категорії зловмисника дозволяє систематизувати зловмисника і на основі аналізу вагових коефіцієнтів сформувати матрицю відповідності між можливостями зловмисників різних категорій і технічними засобами захисту інформації (ТСЗІ). Ці дії істотно знижують рівень ризику реалізації атаки певними категоріями зловмисників і дозволять забезпечити плановість у формуванні як політики ІБ, так і відповідних профілів захисту.

Ключові слова: синергетична модель загроз, класифікатор загроз кіберфізичних систем, інформаційна безпека, кібербезпека

UDC 681.32:007.5
DOI: 10.15587/1729-4061.2020.205702

DEVELOPMENT OF METHODOLOGICAL FOUNDATIONS FOR DESIGNING A CLASSIFIER OF THREATS TO CYBERPHYSICAL SYSTEMS

O. Shmatko
PhD, Associate Professor
Department of Software Engineering and Management Information Technologies
National Technical University "Kharkiv Polytechnic Institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002
S. Balakireva
PhD
Air Force Science Center*
A. Vlasov
PhD
Air Force Science Center*
N. Zagorodna
PhD, Associate Professor
Department of Cybersecurity
Ternopil Ivan Puluj National Technical University
Ruska str., 56, Ternopil, Ukraine, 46001
O. Korol
PhD, Associate Professor**
E-mail: olha.korol@hneu.net
O. Milov
PhD, Professor**
O. Petrov
PhD
Department of ACS Mathematical and Software Support*
S. Pohasii
PhD**
Kh. Rzayev
PhD, Associate Professor
Department of Computer Technology and Programming
Azerbaijan State Oil and Industry University
Azadlyg ave., 20, Baku, Azerbaijan, AZ1010
V. Khvostenko
PhD, Associate Professor, Patent Attorney of Ukraine**
*Ivan Kozhedub Kharkiv National Air Force University
Sumska str., 77/79, Kharkiv, Ukraine, 61023
**Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
Nauky ave., 9-A, Kharkiv, Ukraine, 61166

Received date 20.05.2020
Accepted date 15.06.2020
Published date 26.06.2020

1. Introduction

The development of computing resources and "G" technologies has predetermined the rapid growth of the Internet of things based on the synthesis of physical systems and Internet technologies. Given the fact that there is no single universally accepted definition of cyberphysical systems, a rather general definition of a cyberphysical system as a system

used to monitor and control objects of a physical nature (the physical world) is given in [1]. These systems are perceived as a new generation of embedded control systems. In addition, systems in which networks of sensors and actuators are integrated are also considered cyberphysical systems [2]. Due to the dependence on IT systems, cyber-physical systems can be defined as IT systems that are integrated into applications of the physical world [3]. This integration is the result of advances in information and communication technology (ICT) to improve interaction with physical processes. All these definitions emphasize the constant and intense interaction between the cyber and physical worlds. However, their development also determined a new direction in the development and/or modification of old threats, which is not only manifested in the possibility of hacking and unauthorized access to confidential (personal) information of users, but also in the possibility of conducting an "energy apocalypse". This approach allows cybercriminals to use cyberphysical systems to obtain a synergistic effect from the implementation of threats in cyberspace as a whole. There are many tasks that dictate the need for a unified approach based on the construction of classification of threats. These tasks include analyzing deviations from the normal operation of the security circuit in cyberphysical systems, ensuring the stable operation of the security circuit in cyberphysical processes, and preventing hacking of the security system. The construction of a classifier of threats should be carried out taking into account their synergy and hybridity for all security components, namely, information security (IS), cybersecurity (CS) and security of information (SI). The classifier should reflect the need to integrate security components with social engineering methods and take into account the lack of funds to ensure the required level of security.

2. Literature review and problem statement

Publications dealing with the development of methodological foundations for constructing classifiers of threats to cyberphysical systems can be divided into three groups. The first group combines publications describing various cyberphysical systems and their features and characteristics that make them vulnerable to various kinds of threats. The second group includes publications on a variety of threats and attacks directed specifically at cyber-physical systems. The publications of the third group describe various approaches to the construction of taxonomy and classification, which, ultimately, lead to the construction of threat classifiers for cyberphysical systems.

The most significant work of the first group is [1], in which existing studies on the safety of cyber physical systems (CPS) are collected and systematized within a single structure. The proposed structure is a three-dimensional system of orthogonal coordinates. The first axis corresponds to the well-known classifications (taxonomies) of threats, vulnerabilities, attacks and security controls. The second axis corresponds to the components and subsystems in terms of their nature, namely, cybernetic (computer information), physical and cyberphysical. The latter exhibits synergistic properties that were not possessed by the elements or subsystems of the first two. And finally, the third axis corresponds to the reflection of the integral (synergetic) functions of cyberphysical systems, as well as their manifestation in various typical cyberphysical systems (for example, intelligent networks, medical CPS and intelligent machines, and mechanisms). In Fig. 1, the relationship of the proposed structure with critical cybernetic information systems (CCIS) is proposed, using the banking sector as an example.

It is noted that the designed CPS model can be either abstract to show the general interactions of the CPS application, or specific to capture any details when necessary. This representation allows you to build a model that is abstract enough to be applicable to various heterogeneous CPS applications and to obtain a modular representation of closely related and interacting CPS components. In this case, the formation and manifestation of synergistic properties in the process of functioning are provided. This abstract separation allows you to build a systematic understanding of CPS security and highlight potential attack sources and defenses. The paper argues that identifying differences between traditional IT systems and cyberphysical systems is key in understanding CPS security issues and the subsequent construction of threat classifiers for such systems.

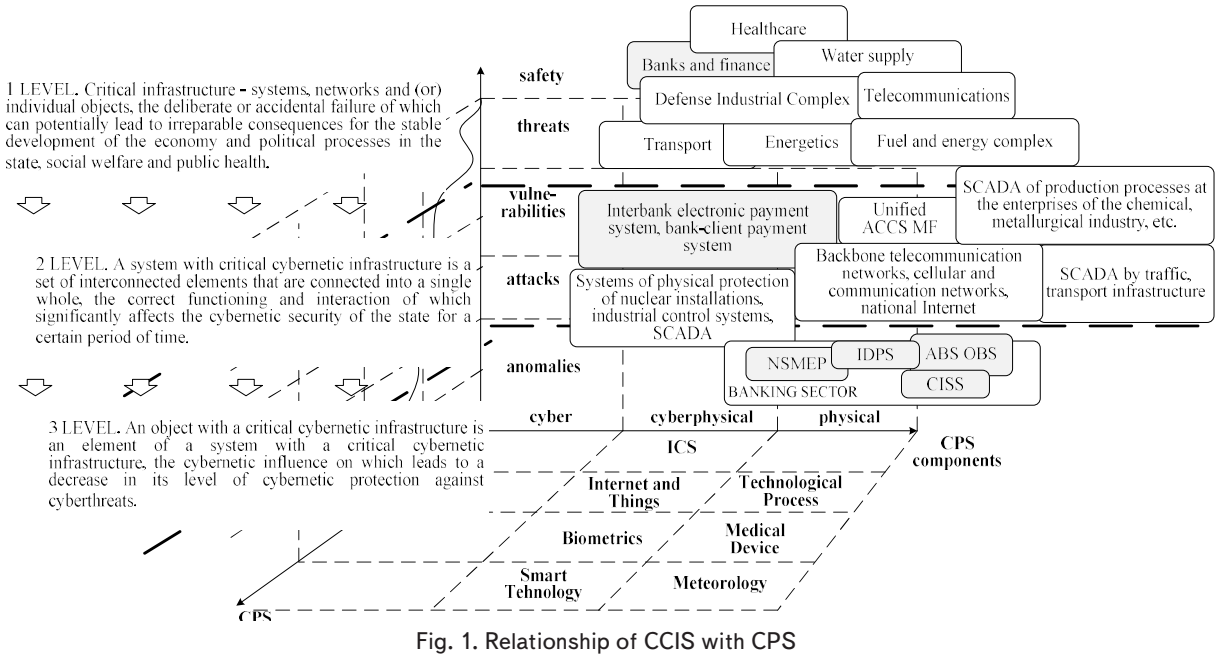

Fig. 1. Relationship of CCIS with CPS

Four specific cyberphysical systems are specifically considered, namely, power supply networks, medical systems, smart cars and industrial facilities control systems. For these systems, the issues of communication in these systems and their safety are discussed in detail. It is emphasized that security control is usually associated with mechanisms such as cryptography, access control, intrusion detection and many other solutions commonly used in IT systems. These mechanisms are very important for protecting the infrastructure of information and communication technologies. It is noted that security solutions require solutions that take into account cyber-physical aspects, and they can be supplemented by IT security solutions.

Ensuring the security of CPS is associated with various problems, one of which is an understanding of potential threats [4]. Knowing who/from what CPS protection is organized is equally important for understanding existing vulnerabilities and attack mechanisms. A security threat is defined as "a set of circumstances that could lead to loss or harm" [5].

In [1], five factors are identified for each threat: source, target, motive, attack vector and potential consequences. The source of the threat is the initiator of the attack.

Sources of threats are divided into three types [6–10]:

– warring threats (intentions of individuals, group organizations or states/nations);

– random threats (threats that were caused by accident or using CPS components);

– environmental threats, including natural disasters (floods, earthquakes), man-made disasters (fires, explosions) and interruptions in the supporting infrastructure (power outages or loss of communication).

Goals are CPS applications, their components, or users. CPS attackers usually have one or more reasons to launch an attack: criminal, spyware, terrorist, political, or cyber warfare [10]. A threat can perform one or more of the four mechanisms of a successful attack: interception, interruption, modification, or fabrication [5]. The consequences of an attack may be a violation of the confidentiality, integrity, availability, confidentiality or security of the CPS.

Potential threats and vulnerabilities are investigated for the selected four applications of cyber-physical systems. The work contains summary tables reflecting the influence of each of the five factors noted on a particular type of cyberphysical system, as well as a list of characteristic attacks undertaken against such systems. Despite the fact that the listed factors can be considered as the foundation for constructing a classifier of threats to cyberphysical systems, the issues of taking into account the synergistic effects of the functioning of such systems have not been considered.

In general, the contribution of the mentioned work to the problem of constructing CPS threat classifiers can be formulated as follows:

1) the CPS security system, designed to distinguish between cyber, cyberphysical and physical components in this system is proposed;

2) the potential sources of threats and their motives are investigated;

3) existing vulnerabilities are presented and significant reasons for their occurrence are highlighted using real examples;

4) a review of recorded attacks on CPS was conducted to identify the main vulnerabilities and components susceptible to threats;

5) a comparative analysis of existing control mechanisms has been carried out and unresolved problems and problems in various CPS applications have been identified.

In [4], three key issues for protecting cyber physical systems are discussed: understanding the threats and possible consequences of attacks, identifying the unique properties of cyber physical systems and their differences from traditional IT security, and discussing security mechanisms applicable to cyber physical systems. In particular, security mechanisms are analyzed for: prevention, detection and recovery, resilience and deterrence of attacks.

A distinctive feature of the work is the development of an adversary model as a way to understand the extent of the problem and assess the risks. The work contains descriptions of some potential attackers, their motives and resources. An analysis of the behavioral aspects of attackers was made in [11, 12].

The work notes that the goal of cybercriminals is to compromise computers wherever they can be found (even in control systems). Attacks by cybercriminals may not necessarily be targeted. Cybercriminals may not have the intent to harm control systems, but their actions can cause negative side effects. For example, control systems infected with malware may not work properly.

Insiders are currently the main source of targeted computer attacks on control systems [13]. These attacks are important from a security point of view, because they are caused by persons with authorized access to computers and networks used by management systems. Therefore, even if control networks are completely isolated from public networks (and the Internet), insider attacks will still be possible. Since disgruntled employees tend to act alone, the potential consequences of their attacks may not be as devastating as the potential damage done by larger organized groups.

Terrorists, activists and organized crime groups are another potential threat to control systems. Attacks on extortion control systems are not new. Cyber attacks are a natural development of physical attacks: they are cheaper, less dangerous for an attacker, not limited by distance, they are easier to copy and coordinate.

States can also be a potential threat to governance systems. In general, it is not surprising that most military powers learn the technology of future attacks, including cyber attacks against the physical infrastructure of other countries.

The work emphasizes that the main objective of the research is to identify and classify a new type of attacks that are possible in control systems, and to study their possible consequences. For example, attackers can launch unique attacks on control systems (that is, attacks that are not possible in traditional IT systems). One possible example would be resonant attacks. In a resonant attack, an attacker who compromises some sensors or controllers will cause the physical system to oscillate at its resonant frequency. In [14], based on the definition of a cyberphysical system as a distributed control system with strict time constraints consisting of physical and cyber components, the differences between the IT system and the cyberphysical system are formulated. Physical Interface: Having a physical interface is what makes CPS security especially difficult. Unlike a standalone IT system, a security breach in a CPS system has disastrous consequences. An attacker can use a physical interface to undermine the security of CPS without the need to violate the access control mechanism. In traditional IT security, this can only happen if data is transmitted over an open network.

Control system: CPS is based on one or more core control networks, which are often integrated with a physical sensor/actuator, which differs markedly from the traditional point of view of IT security. Supervisory control and data acquisition systems (SCADA) are an integral part of modern industrial infrastructure. Unsurprisingly, vulnerabilities in this management network remain an attractive place for cyber attacks that continue to grow due to SCADA systems connected to the Internet [15]. A feature of the analyzed work is not only the classification of attacks, but also its connection with security standards. In addition, modern hybrid attacks on state-level computer systems do not just damage an isolated machine or disrupt the operation of a single corporate system [16]. Instead, new attacks target infrastructure, which is an integral part of the economy, national defense, and everyday life [17]. Studies of cyberphysical systems have shifted the focus from developing the optimization task of these computing components to the interaction involved between physical media and the computing elements with which they interact [18]. A classification consisting of four dimensions was proposed in [19], which allows one to simultaneously consider issues of both the functioning of the network and issues related to computer attacks. The first dimension of the classification covers the attack vector and the main scenario of the attack. The second dimension of classification identifies an attack by its primary purpose. Vulnerabilities are classified in the third dimension of the classification, and payloads in the fourth taxonomy. Similarly, the authors present an information security risk analysis methodology that links the assets, vulnerabilities, threats and controls of an organization. The approach uses a sequence of matrices that reflect the correlation of various elements in a risk analysis. The data are aggregated and cascaded by matrices in order to correlate assets with controls in such a way as to obtain priority ranking of controls based on the assets of the organization [20].

In addition, cyber-physical incidents were discussed and classified in [21] based on sectors, sources and impacts of incidents. This document provides an example of how organizing the process of collecting information about cyber incidents can be used by victims of cyber attacks. In addition, an attempt is described to help understand the threat of cyber incidents for various purposes, which may be useful to increase organizational focus from the point of view of cyber incident. In addition, the security ontology for investigating incident analysis [22] allows one to organize a classification similar to that presented in [23].

In the proposed classification, the stages of incidents were investigated taking into account additional extensions that reflect various categories of the entity involved in attacks and attack relationships. So, the authors distinguished the following classes of entities: an attacker, a vulnerability, a tool, a target, an action, goals, and an unauthorized result. Attackers use tools to perform actions that exploit target vulnerabilities. In [24], models of virtual control system environments (VCSE) are presented, which illustrates the corresponding parts of CPS and their threats. They are designed to analyze the influence of physical factors. Models were built from real, simulated and emulated components that were vulnerable to actual, simulated malicious and other hostile activities. In addition to the dynamic basis of cyber terrorism, a structure was proposed in [25] that describes the main components of cyber terrorism. Cyber terrorism was defined by a structure reflecting six points of view: motivation, goal, attack method, subject area, criminal actions and attack effects.

The classification of cyber attack and defense mechanisms for emergency management networks aims to support a common understanding of the associated cyber attack and defense mechanisms. Attack mechanisms are classified according to three aspects, according to the network, according to the attacked functions and attack factors, while the defense mechanism is determined by the type of protection, the degree of distribution and organizational elements [26]. In addition, the problems of cybersecurity in emergency management are divided into three groups determined by the criticality of time (refers to emergency situations), when decisions must be made and quickly transmitted. The National Institute of Standards and Technology (NIST) [27] presented a framework focused on using business drivers to guide cybersecurity activities and address cybersecurity risks as part of the organization's risk management processes. The classification structure is represented by three parts: the core of the structure, the profile of the structure, and the levels of implementation of the structure. The core of the structure is a set of cybersecurity measures, outcomes and information guides that are common to critical infrastructure sectors, providing detailed guidance for developing organizational personality profiles. Using the profile, the structure is designed to help the organization bring its cybersecurity activities in line with business requirements, acceptable risks and resources. Tiers provide a methodology for organizations to understand and consider the characteristics of a cybersecurity risk management approach. In addition, a threat-based mathematical quantitative structure is used in [28], which is used to evaluate and design the security of CPS.

To counter each element of the threat, it is proposed to be guided by the following three principles:

– principle 1: focusing on a critical system should include only basic functions;

– principle 2: the movement of key elements of the assets necessary for the mission, and security control, which is difficult for an attacker to achieve physically and logically (to reduce accessibility);

– principle 3: responding, detecting, adapting and misleading attackers by introducing system elements with dynamic response technologies (to counter the attacker's capabilities) [28].

The fundamental work in Ukraine, devoted to the construction of classification systems and classifiers of threats in the field of cybersecurity, is undoubtedly the work [29]. The paper presents the results of the analysis of modern protection of state information resources (SIR) in information and telecommunication systems. At the same time, the emphasis in the work is placed on the regulatory support for the SIR, the legal aspects of the formation of the SIR are described in detail, and new terms and definitions of the problems of their protection are introduced. A significant drawback is the lack of communication of threats with the OSI model, which allows you to identify critical penetration points.

In [30], the authors propose an improved version of the classifier of threats to banking information as one of the resources of critical cybernetic information systems (CCIS) of the state, taking into account their synergies and synergies of security components. Fig. 2 shows a block diagram of the proposed solution.

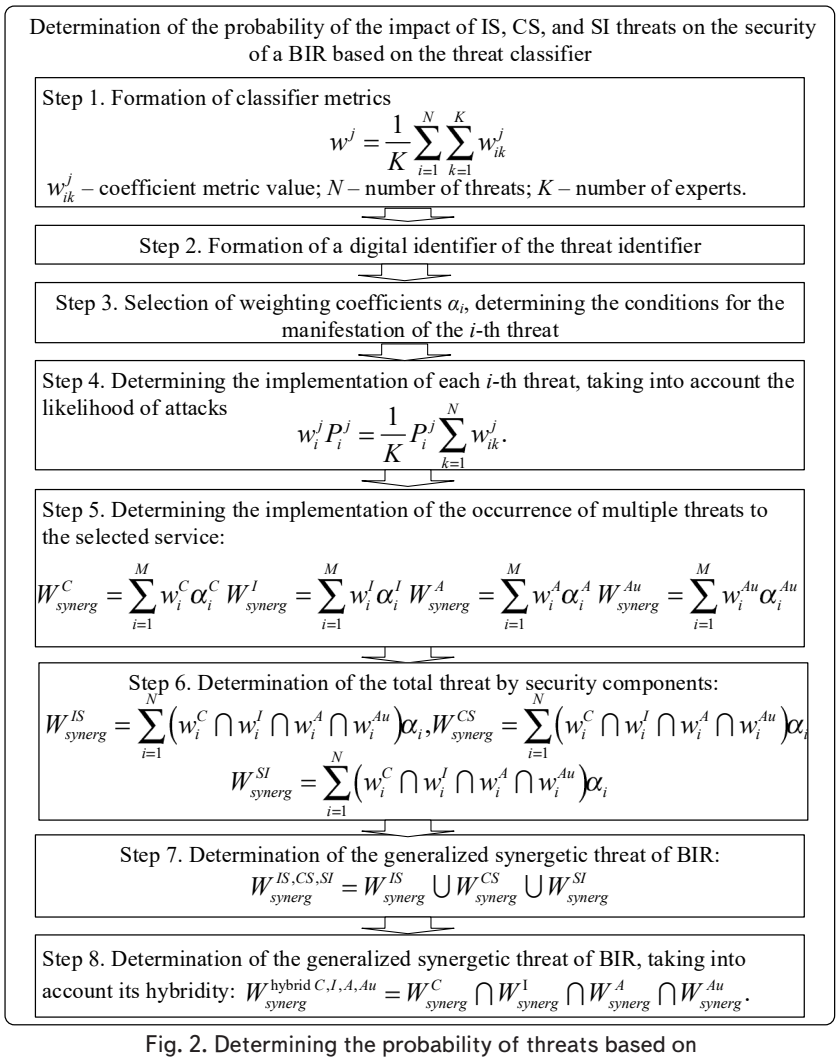

Fig. 2. Determining the probability of threats based on a synergistic model of threats

Thus, the analysis showed that the approaches considered do not take into account the combination of modern threats that are hybrid and synergistic with the elements of the cyberspace infrastructure of companies/organizations. Existing approaches practically do not take into account the economic aspects of ensuring security, which limits the minimization of economic costs for the construction of a comprehensive information protection system. It is the neglect of the economic aspects of security in the construction of the classifier of threats that makes the proposed study relevant.

3. The aim and objectives of the study

The aim of the study is to develop methodological foundations for constructing a unified classifier of threats to cyber systems based on a synergistic approach. This will allow taking into account the criticality of threats, taking into account the category of the attacker, identifying its category, the relationship between threats and infrastructure elements of the security chain of business processes to determine critical points of impact. This approach provides the economic costs of both the attacker and the comprehensive defense, which allows you to find a critical point of resistance and form a lot of critical attacks, taking into account the categories of the attacker.

To achieve the aim, the following objectives were set:

– consider the synergies of threats to the security components of cyber systems;

– develop a block diagram of a unified classifier taking into account the synergetic model of threats and economic costs to ensure the required level of security;

– develop models of the "danger" of the intruder based on their classification and the degree of protection of the cyber system;

– develop a methodology for determining the category of violator based on the proposed classifier.

4. Synergetic threat model for security components of cyber systems

To create a threat model, they usually use the adapted CIA triad model (confidentiality, integrity, availability), which is the basis for its further modifications in practical models (Hexad Parker model, 5A model, STRIDE model, etc.). However, in the conditions of post-quantum cryptography (in the context of the emergence of a full-scale quantum computer), US NIST experts question the provision of the required level of security with modern symmetric and asymmetric cryptosystems [31]. In addition, the rapid growth and use of "G" technologies can significantly change the vector of the use of cyberspace as the main channel for transmitting information between cyber systems and information and communication systems. Such changes significantly reduce the level of security and can practically reduce it to zero. Under such conditions, it is necessary to consider the complex of threats – their combination and hybridity, leading to the appearance of a synergistic effect with a subsequent increase in the likelihood of a threat based on a synthesis with social engineering methods. In [32], the authors proposed a fundamentally new approach to the methodology for constructing security systems based on the synergetic threat model, which provides the formation of methodological foundations for constructing a classifier of modern threats to cyberphysical systems. In Fig. 3, a block diagram of the synergetic model of synthesis threats to information-critical cybernetic systems (on the example of banking sector organizations) and CFS is proposed.

In accordance with ISO/IEC 27001:2013, threats are classified as intentional, incidental and/or environmental. Typical examples include technical failures, unauthorized actions, software interference, physical damage, compromised functions, etc. However, the standard, like other normative international acts, does not consider the synergy and hybridity of modern threats, their combination with social engineering methods, which significantly increases the risk of the threat.

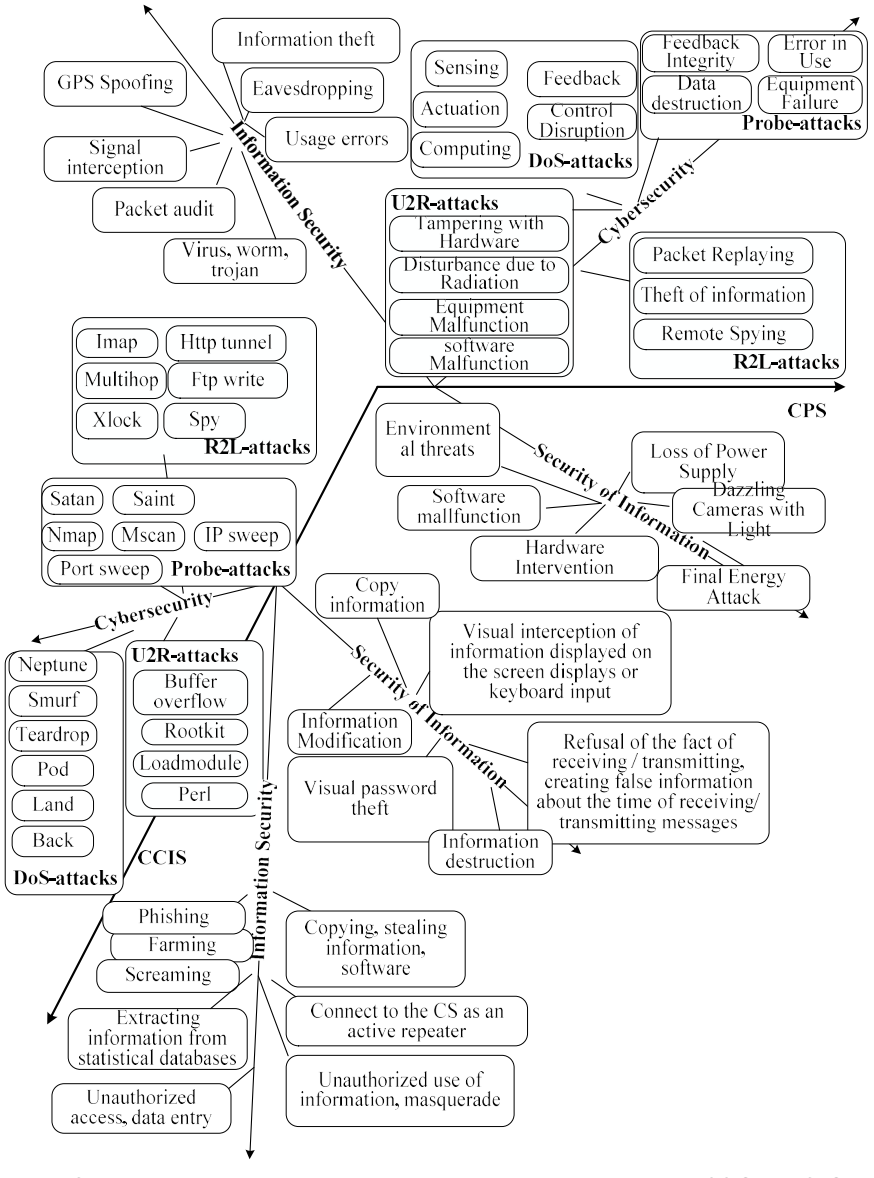

Fig. 3. Block diagram of a synergistic model of synthesis threats on CCIS and CFS

The proposed approach takes into account the possibilities of modern threats, their synergy and hybridity, the possibility of integration with social engineering methods.

5. Development of a block diagram of a unified classifier

To design a classifier of threats to cyberphysical systems, Fig. 4 provides a block diagram of the methodological foundations of a unified classifier taking into account the synergetic model of threats and economic costs of ensuring the required level of security.

Let us consider in more detail the proposed approach to the formation of a classifier of threats.

At the first stage, experts are invited, using their experience, to form tuples of a threat classifier based on 5 platforms.

The first platform determines the criticality level of the threat (critical, high, medium, low, very low), which allows you to calculate the economic "profitability" of critical threats in step 5.

The second platform defines the attitude towards the security component (information security (IS), cybersecurity (CS), security of information (SI)), which allows you to get an assessment of the synergistic effect on one of the threat components in step 5.

The third platform determines the direction of the threat to security services (integrity, confidentiality, accessibility, authenticity and involvement), which allows you to get an assessment of the impact of several threats on security services in step 4 and determine the direction vector of the impact on infrastructure elements.

The fourth platform determines the nature of the directions of the impact of threats (regulatory, organizational, engineering).

The fifth platform provides an assessment of focus on infrastructure elements and allows you to "identify" critical points in an integrated information security system (IISS).

Moreover, for the objectivity of expert judgments, we use the weighting coefficients of expert competence (k_k), presented in Table 1.

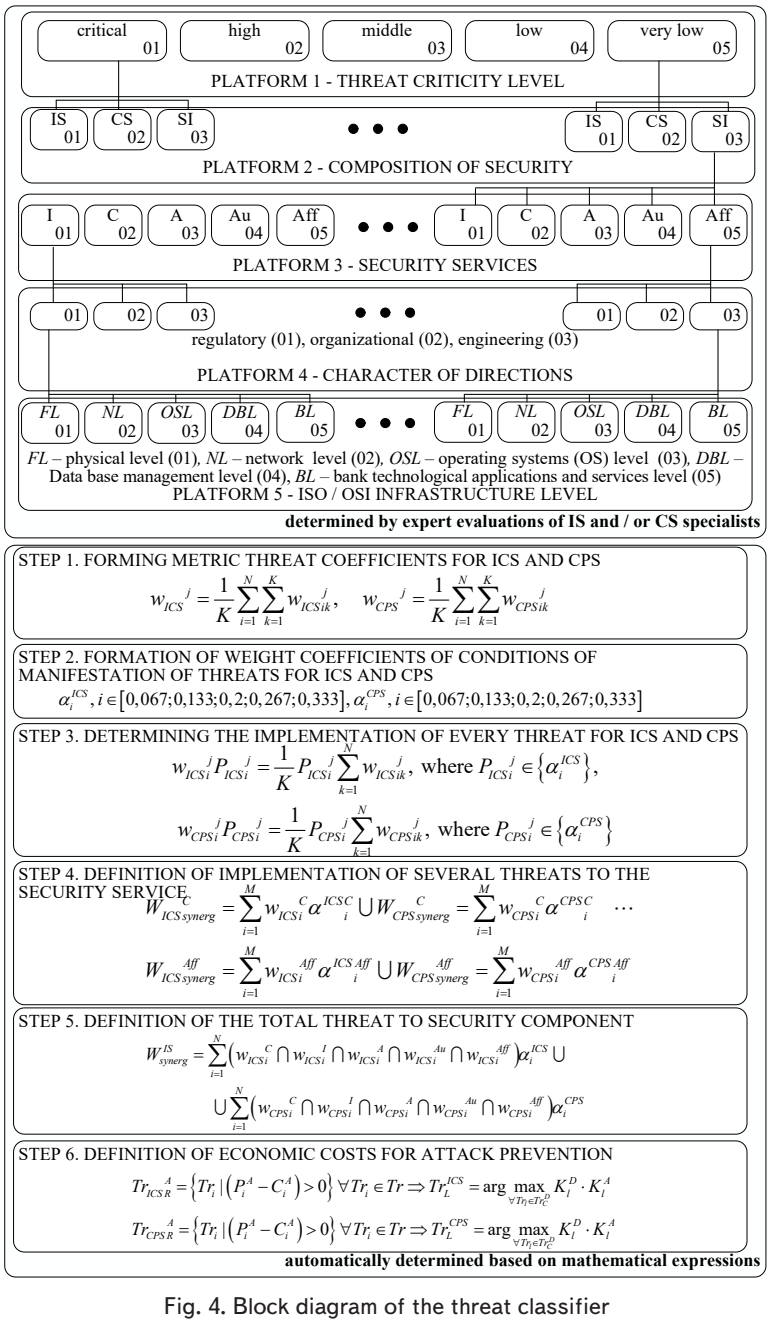

Fig. 4. Block diagram of the threat classifier

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

$$\widetilde{x}_i=\frac{\sum_{k=1}^{K}x_k\times k_k}{K}, \tag{1}$$

where x_k is the assessment of the of the i-th threat by the k-th expert; k_k – expert competency level; K is the number of experts.

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

$$\sigma_x^2=\frac{1}{K}\sum_{k=1}^{K}k_k\left(x_k-\widetilde{x}_i\right)^2. \tag{2}$$

The statistical probability of the obtained results $1-\alpha_i$, will be:

$$\left[\widetilde{x}_i-\Delta,\widetilde{x}_i+\Delta\right],$$

where the quantity x_i is distributed according to the normal law with center $\widetilde{x}_i$ and dispersion σ_X^2. Then Δ is determined by the expression:

$$\Delta=t\sqrt{\sigma_x^2/N}, \tag{3}$$

where t is the value according to the Student distribution for $K-1$ degrees of freedom.

To form metric (weighting) threat factors (Fig. 4) and their impact on security services, we introduce the following notation:

j is a security service for both ICS and CPS. Basic security services: C –confidentiality; I – integrity; A – availability; Au – authenticity, Aff – involvement (affiliation). Thus, a tuple of security services $j=\{C,I,A,Au,Aff\}$ is formed in the classifier; N – the number of threats; K – the number of experts who participated in the expert threat assessment; $\{i\}_1^N$ – current number of the i-th threat; $\{k\}_1^K$ – current number of the expert.

Table 1

Expert competency weight

No.	Expert Qualifications	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 doctor of science in the field of IS, CS, SI	0.9
5	Director of security service	0.85
6	Doctor of Philosophy 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	Graduate student in the field of IS, CS, SI	0.4

To evaluate the hybrid and synergetic components of the impact of modern threats, we use the following sequence of actions:

1st step. Determination of the average expert rating for all threats to a particular security service:

$$w_{ICS}{}^{j} = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{ICSik}{}^{j}, \quad w_{CPS}{}^{j} = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{CPSik}{}^{j}, \tag{4}$$

where $w_{ICSik}{}^{j}$ is the value of the metric coefficient set by the k-th expert for the i-th threat of the j-th security service for ICS, $w_{CPSik}{}^{j}$ is the value of the metric coefficient set by the k-th expert for the i-th threat of the j-th security service for CPS.

2nd step. Formation of weighting factors for the threat manifestation conditions for ICS and CPS (Table 2):

$$\alpha_i^{ICS}, \quad i \in [0.067;\ 0.133;\ 0.2;\ 0.267;\ 0.333],$$

$$\alpha_i^{CPS}, \quad i \in [0.067;\ 0.133;\ 0.2;\ 0.267;\ 0.333].$$

3rd step. Determining the implementation of each threat for ICS and CPS:

$$w_{ICSi}{}^{j} P_{ICSi}{}^{j} = \frac{1}{K} P_{ICSi}{}^{j} \sum_{k=1}^{N} w_{ICSik}{}^{j},$$

where

$$P_{ICSi}{}^{j} \in \{\alpha_i^{ICS}\},$$

$$w_{CPSi}{}^{j} P_{CPSi}{}^{j} = \frac{1}{K} P_{CPSi}{}^{j} \sum_{k=1}^{N} w_{CPSik}{}^{j},$$

where

$$P_{CPSi}{}^{j} \in \{\alpha_i^{CPS}\}. \tag{5}$$

Table 2

Selection of weights α_i of manifestations of the i-th threat

α_i	Manifestation conditions
0.067	The threat does not occur more than once every 5 years
0.133	The threat does not occur more than once a year
0.2	The threat does not occur more than once a month
0.267	The threat does not occur more than once a week
0.333	The threat is daily

For each security service and i-th threat:

1) for ICS:

$$w_{ICSi}{}^{C} \alpha_{ICSi}{}^{C} = \frac{1}{K} \alpha_{ICSi}{}^{C} \sum_{k=1}^{K} w_{ICSik}{}^{C}$$

– confidentiality service,

$$w_{ICSi}{}^{I} \alpha_{ICSi}{}^{I} = \frac{1}{K} \alpha_{ICSi}{}^{I} \sum_{k=1}^{K} w_{ICSik}{}^{I}$$

– integrity service,

$$w_{ICSi}{}^{A} \alpha_{ICSi}{}^{A} = \frac{1}{K} \alpha_{ICSi}{}^{A} \sum_{k=1}^{K} w_{ICSik}{}^{A}$$

– availability service,

$$w_{ICSi}{}^{Au} \alpha_{ICSi}{}^{Au} = \frac{1}{K} \alpha_{ICSi}{}^{Au} \sum_{k=1}^{K} w_{ICSik}{}^{Au}$$

– authenticity service,

$$w_{ICSi}{}^{Aff} \alpha_{ICSi}{}^{Aff} = \frac{1}{K} \alpha_{ICSi}{}^{Aff} \sum_{k=1}^{K} w_{ICSik}{}^{Aff}$$

– involvement service,

where $w_{ICSi}{}^{C}$, $w_{ICSi}{}^{I}$, $w_{ICSi}{}^{A}$, $w_{ICSi}{}^{Au}$, $w_{ICSi}{}^{Aff}$ are the expert weights of the security services: confidentiality, integrity, availability, authenticity and involvement; $\alpha_{ICSi}{}^{C}$, $\alpha_{ICSi}{}^{I}$, $\alpha_{ICSi}{}^{A}$, $\alpha_{ICSi}{}^{Au}$, $\alpha_{ICSi}{}^{Aff}$ $\alpha_{ICSi}{}^{Aff}$ – weighting factor of the security service: confidentiality, integrity, availability, authenticity and authenticity of the manifestation of the i-th threat attack.

2) for CPS:

$$w_{CPSi}{}^{C} \alpha_{CPSi}{}^{C} = \frac{1}{K} \alpha_{CPSi}{}^{C} \sum_{k=1}^{K} w_{CPSik}{}^{C}$$

– confidentiality service,

$$w_{CPSi}{}^{I} \alpha_{CPSi}{}^{I} = \frac{1}{K} \alpha_{CPSi}{}^{I} \sum_{k=1}^{K} w_{CPSik}{}^{I}$$

– integrity service,

$$w_{CPSi}{}^{A} \alpha_{CPSi}{}^{A} = \frac{1}{K} \alpha_{CPSi}{}^{A} \sum_{k=1}^{K} w_{CPSik}{}^{A}$$

– availability service,

$$w_{CPSi}{}^{Au} \alpha_{CPSi}{}^{Au} = \frac{1}{K} \alpha_{CPSi}{}^{Au} \sum_{k=1}^{K} w_{CPSik}{}^{Au}$$

– authenticity service,

$$w_{CPSi}{}^{Aff} \alpha_{CPSi}{}^{Aff} = \frac{1}{K} \alpha_{CPSi}{}^{Aff} \sum_{k=1}^{K} w_{CPSik}{}^{Aff}$$

– involvement service,

where $w_{CPSi}{}^{C}$, $w_{CPSi}{}^{I}$, $w_{CPSi}{}^{A}$, $w_{CPSi}{}^{Au}$, $w_{CPSi}{}^{Aff}$ are the expert weights of the security services: confidentiality, integrity, availability, authenticity and involvement; $\alpha_{CPSi}{}^{C}$, $\alpha_{CPSi}{}^{I}$, $\alpha_{CPSi}{}^{A}$, $\alpha_{CPSi}{}^{Au}$, $\alpha_{CPSi}{}^{Aff}$ – weighting factor of the security service: confidentiality, integrity, availability, authenticity and authenticity of the manifestation of the i-th threat attack.

4th step. Determining the implementation of several threats to a security service:

$$W_{ICS\,synerg}{}^{C} = \sum_{i=1}^{M} w_{ICSi}{}^{C} \alpha^{ICSC}{}_{i} \cup W_{CPS\,synerg}{}^{C} = \sum_{i=1}^{M} w_{CPSi}{}^{C} \alpha^{CPSC}{}_{i}$$

– synergistic effect on the confidentiality service,

$$W_{ICS\,synerg}{}^{I} = \sum_{i=1}^{M} w_{ICSi}{}^{I} \alpha^{ICSI}{}_{i} \cup W_{CPS\,synerg}{}^{I} = \sum_{i=1}^{M} w_{CPSi}{}^{I} \alpha^{CPSI}{}_{i}$$

– synergistic effect on the integrity service,

$$W_{ICS\,synerg}{}^{A} = \sum_{i=1}^{M} w_{ICSi}{}^{A} \alpha^{ICSA}{}_{i} \cup W_{CPS\,synerg}{}^{A} = \sum_{i=1}^{M} w_{CPSi}{}^{A} \alpha^{CPSA}{}_{i}$$

– synergistic effect on the availability service,

$$W_{ICS\,synerg}^{\;\;Au}=\sum_{i=1}^{M}w_{ICS\,i}^{\;\;Au}\alpha_{i}^{ICS\,Au}\cup W_{CPS\,synerg}^{\;\;Au}=\sum_{i=1}^{M}w_{CPS\,i}^{\;\;Au}\alpha_{i}^{CPS\,Au}$$

– synergistic effect on the authenticity service,

$$W_{ICS\,synerg}^{\;\;Aff}=\sum_{i=1}^{M}w_{ICS\,i}^{\;\;Aff}\alpha_{i}^{ICS\,Aff}\cup W_{CPS\,synerg}^{\;\;Aff}=\sum_{i=1}^{M}w_{CPS\,i}^{\;\;Aff}\alpha_{i}^{CPS\,Aff}$$

– synergistic effect on the involvement service, (6)

where M is the number of several threats that are selected by the expert from the set $\{i\}_i^M$, which is a subset of the entire set of threats of the classifier, that is, $M \le N$.

When forming metric coefficients, it is believed that the results obtained are independent threats, in case of their dependence (coincidence of tuples of threats), it is necessary to use the expression for determining the total probability of dependent events:

$$P(AB)=P(A)+P(B)-P(AB).$$

5th step. Determination of the total threat by security components, taking into account the expression (6):

$$W_{synerg}^{IS}=\sum_{i=1}^{N}\left(\begin{matrix}w_{ICS\,i}^{\;\;C}\cap w_{ICS\,i}^{\;\;I}\cap w_{ICS\,i}^{\;\;A}\cap\\ \cap w_{ICS\,i}^{\;\;Au}\cap w_{ICS\,i}^{\;\;Aff}\end{matrix}\right)\alpha_i^{ICS}\cup$$
$$\cup\sum_{i=1}^{N}\left(w_{CPS\,i}^{\;\;C}\cap w_{CPS\,i}^{\;\;I}\cap w_{CPS\,i}^{\;\;A}\cap w_{CPS\,i}^{\;\;Au}\cap w_{CPS\,i}^{\;\;Aff}\right)\alpha_i^{CPS},$$

$$W_{synerg}^{CS}=\sum_{i=1}^{N}\left(\begin{matrix}w_{ICS\,i}^{\;\;C}\cap w_{ICS\,i}^{\;\;I}\cap w_{ICS\,i}^{\;\;A}\cap\\ \cap w_{ICS\,i}^{\;\;Au}\cap w_{ICS\,i}^{\;\;Aff}\end{matrix}\right)\alpha_i^{ICS}\cup$$
$$\cup\sum_{i=1}^{N}\left(w_{CPS\,i}^{\;\;C}\cap w_{CPS\,i}^{\;\;I}\cap w_{CPS\,i}^{\;\;A}\cap w_{CPS\,i}^{\;\;Au}\cap w_{CPS\,i}^{\;\;Aff}\right)\alpha_i^{CPS},$$

$$W_{synerg}^{SI}=\sum_{i=1}^{N}\left(\begin{matrix}w_{ICS\,i}^{\;\;C}\cap w_{ICS\,i}^{\;\;I}\cap w_{ICS\,i}^{\;\;A}\cap\\ \cap w_{ICS\,i}^{\;\;Au}\cap w_{ICS\,i}^{\;\;Aff}\end{matrix}\right)\alpha_i^{ICS}\cup$$
$$\cup\sum_{i=1}^{N}\left(w_{CPS\,i}^{\;\;C}\cap w_{CPS\,i}^{\;\;I}\cap w_{CPS\,i}^{\;\;A}\cap w_{CPS\,i}^{\;\;Au}\cap w_{CPS\,i}^{\;\;Aff}\right)\alpha_i^{CPS}. \quad (7)$$

To determine the generalized synergistic threat:

$$W_{synerg}^{IS,CS,SI}=W_{synerg}^{IS}\cup W_{synerg}^{CS}\cup W_{synerg}^{SI}. \quad (8)$$

To determine the generalized synergistic threat, taking into account its hybridity for ICS:

$$W_{ICS\,synerg}^{\;\;\text{hybrid}\,C,I,A,Au,Aff}=W_{ICS\,synerg}^{\;\;\;C}\cap W_{ICS\,synerg}^{\;\;\;\text{I}}\cap$$
$$\cap W_{ICS\,synerg}^{\;\;\;A}\cap W_{ICS\,synerg}^{\;\;\;Au}\cap W_{ICS\,synerg}^{\;\;\;Aff}. \quad (9)$$

To determine the generalized synergistic threat, taking into account its hybridity for CPS:

$$W_{CPS\,synerg}^{\;\;\text{hybrid}\,C,I,A,Au,Aff}=W_{CPS\,synerg}^{\;\;\;C}\cap W_{CPS\,synerg}^{\;\;\;\text{I}}\cap$$
$$\cap W_{CPS\,synerg}^{\;\;\;A}\cap W_{CPS\,synerg}^{\;\;\;Au}\cap W_{CPS\,synerg}^{\;\;\;Aff}. \quad (10)$$

To determine the generalized hybrid synergistic threat:

$$W_{synerg}^{\text{hybrid}\,IS,CS,SI}=W_{ICS\,synerg}^{\;\;\text{hybrid}\,C,I,A,Au,Aff}\cup W_{CPS\,synerg}^{\;\;\text{hybrid}\,C,I,A,Au,Aff}. \quad (11)$$

6th step. Determining the economic costs of preventing an attack.

The introduction of cost indicators of threats allows implementing an algorithm for constructing a rating of potential threats and the importance of information resources to be protected.

The algorithm proposed in [36] implements the following actions. Both sides of the attack are determined by the importance (rating) of the attacks that are economically feasible.

1st step. Determination of attacks, the effect of which exceeds the costs of their implementation:

$$Tr_R^A=\left\{Tr_i\,|\left(P_i^A-C_i^A\right)>0\right\}\forall Tr_i\in Tr, \quad (12)$$

where Tr_R^A – a set of the potential threats, the implementation of which is effective for the attacker; Tr_i – threat to the i-th information resource; P_i^A – cost assessment of the success of the attack on the i-th resource by the attacker; C_i^A – the cost of an attack on the i-th resource by the attacker.

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

$$Tr_C^D=\left\{Tr_j\,|\left(P_i^D-C_i^D\right)>0\right\}\forall Tr_j\in Tr, \quad (13)$$

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

3rd step. Determination of importance factors for attackers. Defined as a share of the winnings of the total winnings that can be obtained potentially when implementing the entire range of threats to attackers:

$$K_i^A=\frac{P_i^A-C_i^A}{\sum_{i=1}^{M}\left(P_i^A-C_i^A\right)},$$
$$\forall Tr_i\in Tr_R^A, M=\left|Tr_R^A\right|, \quad (14)$$

where K_i^A is the rating coefficient (importance) of the threat to the i-th information resource; M is the power of a set of selected potentially effective threats to the attacking side.

4th step. Determination of importance factors for defenders. Defined as the share of the winnings of the total winnings that can be obtained potentially when implementing the entire range of protective measures

$$K_j^D=\frac{P_i^D-C_i^D}{\sum_{i=1}^{N}\left(P_i^D-C_i^D\right)},$$
$$\forall Tr_j\in Tr_C^D, N=\left|Tr_C^D\right|, \quad (15)$$

where K_j^D is the rating coefficient (importance) of building the protection of the j-th information resource.

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

$$Tr_l = \arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \cdot K_l^A. \quad (16)$$

Thus, the main difference of the proposed approach is the ability to take into account not only the opinion of experts, but also to form an objective assessment and integration of threats, which allows forming their synergistic effect and hybridity. In addition, the use of the ISO model in the classifier allows you to "identify" critical places in the infrastructure not only of cyberphysical systems, but also in synthesis with Internet technologies of cyberspace and "G" technologies. This approach intuitively allows you to focus on the weak points of comprehensive protection, taking into account economic costs in the face of low funding and the "profitability" of an attack by attackers.

6. Development of a model of "danger" of the intruder based on their classification and the degree of protection of the cyber system

Assessing the level of threats is impossible without assessing the capabilities of the attackers themselves (attackers, cybercriminals, etc.). The possibility of implementing a threat largely depends on their "competence", computing resources, time characteristics, and motivation. Thus, an integral part of the threat analysis is the development of a "danger" model of the intruder. This approach allows you to generate many threats, depending on the capabilities of the attackers, to form many possible impacts, to assess the state of preventive protection. It is proposed to use the following classification of violators to form weight coefficients of "danger" of violators, Fig. 5, while CCIS can be both part of the CPS and make up a separate cyberphysical system. The basis of category 5 (Fig. 5) is the taxonomy in [35].

Thus, the classification allows you to introduce elements of many categories of attackers $L_i^{del} \in \{L_i^{del}\}$: L_1^{del} – ICS (CPS) users; L_{11}^{del} – ICS (CPS) management, L_{12}^{del} – ICS (CPS) employee, L_{13}^{del} – users "at risk"; L_2^{del} – operational staff; L_3^{del} – technical support staff; L_4^{del} – non-ICS (CPS) employees, L_5^{del} – external attackers: L_{51}^{del} – cyber terrorists, L_{52}^{del} – special services, L_{53}^{del} – hackers, L_{54}^{del} – cybercriminals, L_{55}^{del} – competitors, L_{56}^{del} – criminals, L_{57}^{del} – vandals.

We define the formal model of the "danger" of the violator taking into account the authors' suggestions [32–34]:

$$G_{CPS}^{ICS} = \left\{aid_i, \beta_i^{ICS} \in \{\beta_i^{ICS}\}, \beta_i^{CPS} \in \{\beta_i^{CPS}\}, p_{rj}, r_{\text{motiv}}, T\right\}, \quad (17)$$

where $aid_i \in \{aid\}$ is the identifier of the intruder (category of intruder), $\beta_i^{ICS} \in \{\beta_i^{ICS}\}$ is the weighting coefficient of the capabilities of the violator for ICS, $\beta_i^{CPS} \in \{\beta_i^{CPS}\}$ is the weighting coefficient of the capabilities of the CPS violator, T is the time of successful implementation of the threat, p_{rj} is the probability of implementation of at least one threat to the j-th asset, i is the threat, $\forall i \in n$, n is the number of threats, j – information resource (asset), $\forall j \in m$, m – number of assets; r_{motiv} – the probability of the attacker's motivation to implement the threat.

Analysis of the classification of attackers allows you to form an expert assessment and obtain a weight coefficient of the possibility of threats (i-th threat).

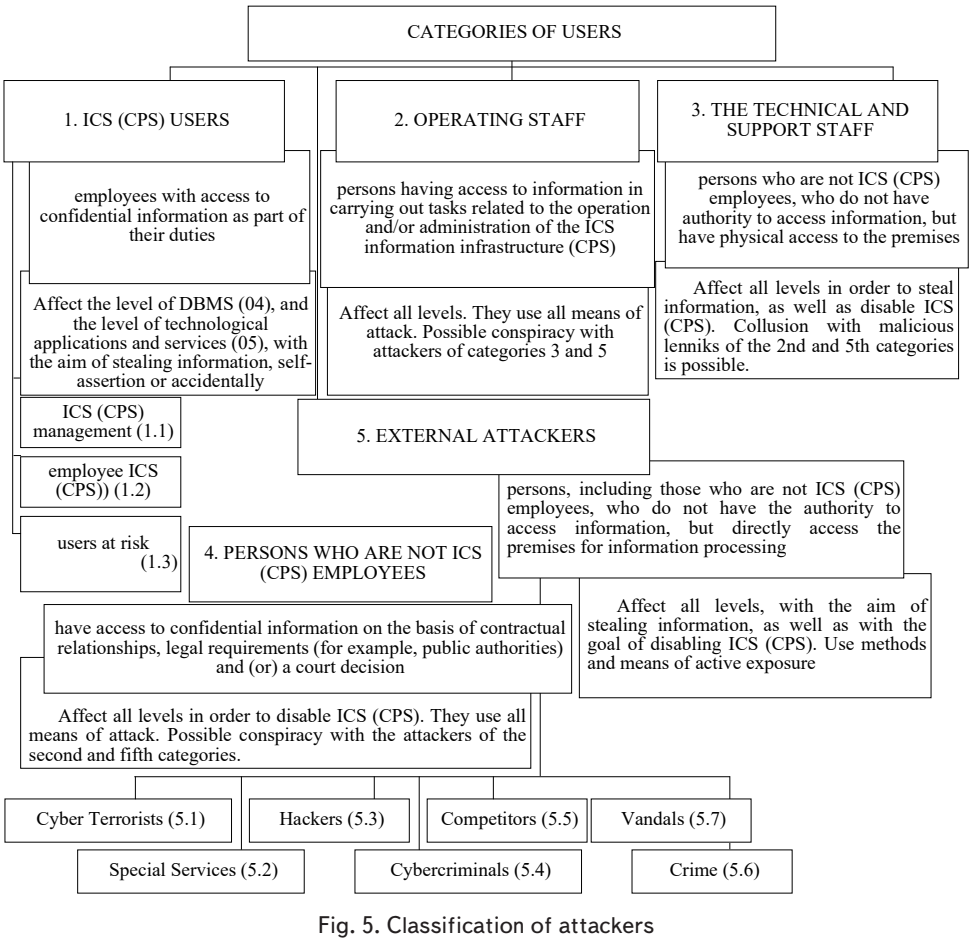

Fig. 5. Classification of attackers

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

$$\gamma_{ICS}^{CPS} = \frac{1}{N}\sum_{i=1}^{N}\gamma_{ICS\,i}^{CPS},$$

where

$$\gamma_{ICS\,i}^{CPS} = \left(\beta_i^{ICS} \cup \beta_i^{CPS}\right) \times p_{rj} \times r_{motiv}, \quad (18)$$

where

$$\beta_i^{ICS} = W_{cp}^{ICS} \cap W_{cash}^{ICS} \cap T^{ICS}, \;\; \beta_i^{CPS} = W_{cp}^{CPS} \cap W_{cash}^{CPS} \cap T^{CPS}$$

are the weights of the intruder's capabilities for ICS and CPS (respectively), $W_{cp}^{ICS}\left(W_{cp}^{CPS}\right)$ are the intruder's computing resources (1 – unlimited resources of cyberterrorists, 0.75 – resources of the state (special services), 0.5 – resources of cybercriminals, 0.25 – resources of criminals, competitors , hackers, 0.001 – vandal resources);

T^{ICS} (T^{CPS}) – time to complete the threat (1 – the threat is implemented daily, 0.75 – the threat is implemented within a week, 0.5 – the threat is implemented within a month, 0.25 – the threat is implemented during the year, 0.001 – unlimited time);

$W_{cash}^{ICS}\left(W_{cash}^{CPS}\right)$ – economic opportunities of attackers (1 – unlimited resources of cyberterrorists, 0.75 – resources of the state (special services), 0.5 – resources of cybercriminals, 0.25 – resources of criminals, competitors, hackers, 0.001 – resources of vandals).

Table 3 shows the initial data of the criteria and indicators of the expert assessment of its location.

Table 3

Initial data of the criteria and indicators of the expert assessment of the weight coefficient of the "danger" of the offender

Category	weighting score indicators							
	$\beta_i^{ICS} \in \{\beta_i^{ICS}\}$			$\beta_i^{CPS} \in \{\beta_i^{CPS}\}$			p_{rj}	r_{motiv}
	W_{cp}^{ICS}	T^{ICS}	W_{cash}^{ICS}	W_{cp}^{CPS}	T^{CPS}	W_{cash}^{CPS}		
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
Average	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

7. Development of methods for determining the category of violator

Analysis of Table 3 allows you to create a table of correspondence between the category of cybercriminals and the infrastructure elements of ICS, CPS, and allows you to reversely determine the category of cybercriminals.

Analysis of the classification of attackers allows you to create a set $\{H_j\}$ that determines the levels of impact on ICS (CPS):

– level of technical channels (H_0);
– physical layer of the TCP/IP protocol stack (H_1);
– link layer of the TCP/IP protocol stack (H_2);
– network layer of the TCP/IP protocol stack (H_3);
– transport layer of the TCP/IP protocol stack (H_4);
– level of harmful effects (H_5);
– level of embedded devices (H_6);
– application layer of the TCP/IP protocol stack (H_7);
– level of the information security system (H_8).

In Table 4, the correlation of categories of violator and levels of their impact is determined.

Table 4

Correlation of categories of violator and 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

Thus, to determine the category of the attacker based on the analysis of (Table 4) the threat classifier, a methodology for determining the category of intruder is proposed, which boils down to the following algorithm:

1) a classification attribute is selected from the set $\{H\}$, which determines the levels of impact on ICS (CPS);

2) the threat tuple is determined by the proposed classifier;

3) the vector V_{ij} is formed on the basis of the tuple and the generated set of critical threats (based on the evaluation of the product of the importance coefficients of the attacker);

4) using the vector V_{ij}, the maximum category of the intruder is determined in accordance with Table 4, starting with the offender of the first category $\left(L_1^{del}\right)$.

Thus, on the basis of the proposed methodology, a list of critical threats for each category of violators is built.

If the subjects of attacks are excluded from the list of potential violators, the maximum category of the violator can be reduced, and, consequently, the number of critical threats.

8. Discussion of the results of the study assessing the degree of "danger" of an attacker

To assess indicators of the degree of "danger" of attackers and the degree of implementation of protective measures, we define sets of weighted metrics that acquire a value in the

range [0; 1]. Each metric characterizes the degree to which a particular trait of an attacker or a defensive means corresponds to a given target value.

To assess the degree of "danger" of the attacker, we use the proposed model

$$G_{CPS}^{ICS} = \left\{ \overline{dld}_i, \beta_i^{ICS} \in \left\{ \beta_i^{ICS} \right\}, \beta_i^{C} \in \left\{ \beta_i \right\}, p_{rj}, r_{\text{motiv}}, T \right\}.$$

To describe the set of characteristics, we use the index h:

$$G_{CPS_h}^{ICS},$$

where $\left(\{h\}_1^{G_{CPS}^{ICS}} \right)$.

Denote j – security services for both ICS and CPS. Basic security services: C – confidentiality; I – integrity; A – availability; Au – authenticity, Aff – involvement (affiliation). Thus, a tuple of security services $j = \{C, I, A, Au, Aff\}$. is formed. Denote by i the current number of the attacker $\left(\{i\}_1^{L} \right)$, k – the current number of the expert who evaluated $\left(\{k\}_1^{K} \right)$, L – the number of attackers, K – the number of experts, w_{kih}^{j} – the expert assessment of the k^{th} expert for the h^{th} characteristic of the i^{th} attacker for the j^{th} security service.

Then the average value of all experts' ratings over the entire set of characteristics of all attackers for the j-th security service will be:

$$w^j = \frac{1}{KLG_{CPS}^{ICS}} \sum_{k=1}^{K} \sum_{i=1}^{L} \sum_{h=1}^{G_{CPS}^{ICS}} \gamma_{ICS\,kih}^{CPS\,j} \times w_{kih}^{j}, \tag{19}$$

where $\gamma_{ICS\,kih}^{CPS\,j}$ is the weight coefficient of the h^{th} metric of the i-th attacker for the j-th service. Rationing weights:

$$\sum_{k=1}^{K} \sum_{i=1}^{L} \sum_{h=1}^{G_{CPS}^{ICS}} = 1.$$

Similarly, you can describe the degree of protection of the technical means of information security (TMIS). To do this, we use a set of characteristics B={cryptographic resistance, TMIS strength (C_r), key data amount (S_c), the complexity of performing forward and reverse cryptographic transformations (encryption/decryption of data, O_E)}. Thus, we have such a set of TMIS characteristics: B={C_r, S_c, O_E}. To describe the set of characteristics, we use the index g: B_g, where $\left(\{g\}_1^{B} \right)$. We denote by w_{kg}^{j} the value of the estimate of the g^{th} characteristic of the TMIS by the k^{th} expert for the j^{th} security service in the case when the degree of system security and the destructive actions of the attackers are independent.

Then the average value of all experts' estimates of the degree of implementation of protective measures for the j-th security service will be:

$$\psi^j = \frac{1}{KB} \sum_{k=1}^{K} \sum_{g=1}^{B} \left(\beta_{kg}^{j} \times w_{kg}^{j} \right), \tag{20}$$

where β_{kg}^{j} is the weight coefficient of the g^{th} metric of the j^{th} security service for the k^{th} expert. Rationing weights:

$$\sum_{k=1}^{K} \sum_{g=1}^{B} \beta_{kg}^{j} = 1.$$

To correlate between the degree of "danger" of the attacker and the characteristics of the system protection, that is, between the sets G_{CPS}^{ICS} and B, we use the matrix M of size $\left[G_{CPS}^{ICS} \times B \right]$, which is sometimes called the matrix of pairwise comparisons. If the g^{th} security characteristic Bg completely blocks the h^{th} property of the attacker (or the threat implemented by this attacker), then M_{hg}=1, otherwise M_{hg}=0. Intermediate values are also possible when the threat/characteristic of the attacker is not completely closed. Thus, $\left\| M_{hg} \right\|$ – the matrix of coefficients linking the threats/characteristics of the attacker with the protective measures of the security system.

Then the new values of the protective measures estimates can be written using the matrix M:

$$\left\| w_{kg}^{j} \right\|_{cor} = \left\| M_{hg} \times w_{kg}^{j} \right\|. \tag{21}$$

Then

$$\psi^j = \frac{1}{KB} \sum_{k=1}^{K} \sum_{g=1}^{B} \left(\beta_{kg}^{j} \times \left\| w_{kg}^{j} \right\|_{cor} \right). \tag{22}$$

The expansion of the classifier by introducing economic indicators of the cost of an attack and the cost of countermeasures allows you to get an integrated assessment of the system security. Safety assessment will be carried out in relative units. Let 1 correspond to the maximum level of security provided by the security system as a whole, and 0 corresponds to the situation when the security system does not protect any of the resources.

To determine the probability of threat with the maximum defense capabilities A and the maximum attack capabilities B, we will use the probability density function $x - F(x)$. The indicated probability is determined by the difference $F(B)–F(A)$, where A is the limit level of capabilities of the defense side, B is the limit level of attack opportunities of the attack side.

Security level is defined as the share of those resources that are protected from cyber attacks. It is easy to see that this value can be determined as follows:

$$S = F(B) - F(A) = \int_{-\infty}^{B} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} \mathrm{d}t - \int_{-\infty}^{A} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} \mathrm{d}t. \tag{23}$$

A graphical representation of the current level of security when changing the capabilities of the parties to the cyber conflict (relative values) is shown in Fig. 6.

Thus, the above expressions (19)–(23) allow, on the basis of the proposed classifier of threats, the "danger" model of the attacker, and the methodology for determining the intruder category, determining:

– many critical threats;

– critical points of ICS/CPS infrastructure elements (CCIS);

– preventive measures;

– system security in conditions of underfunding of the security field, taking into account the synergy and hybridity of modern threats.

The proposed approach has certain limitations that should be taken into account in the practical use of the research results. The main limitation follows from the fact that the application of the security level assessment formula assumes that the attacker uses all the resources to organize an attack on a single resource. In addition, it is necessary to take into account

the category of the attacker, which allows you to determine its capabilities (computing and financial resources, economic interest). Then the attack is determined by a comprehensive criterion that takes into account the cost of the conduct and the computing capabilities available to the attacker. There is no doubt that all attacks with a lower cost can be implemented. In the case of simultaneous implementation of several attacks of lower cost, the maximum threshold of threats from the attacker will be lower. Similar reasoning can be applied to the defense side. In this case, protection of several less valuable resources can be organized at the same time, rather than a single but more expensive resource. Formed restrictions allow you to identify a group of resources that will not be targeted by a certain category of attackers, whereby exempted funds can be used to organize the protection of other resources. On the other hand, resources can be defined whose protection cannot be ensured due to the limited funding of the security system.

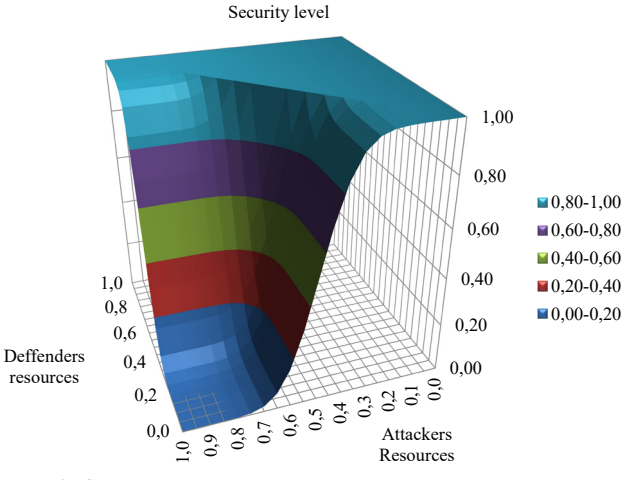

Fig. 6. Security level depending on the ratio of resources of the parties to the cyber conflict

From these limitations, the direction for further research follows. Namely, how the decision to simultaneously protect several less valuable resources instead of protecting a single more expensive resource will affect the overall level of system security. It is also necessary to develop approaches to assessing the level of security while simultaneously implementing several critical threats aimed at various resources and for different categories of users, while taking into account the synergy and hybridity of threats, as well as their integration with social engineering methods.

9. Conclusions

1. The analysis of threats in the context of the rapid growth of computing resources, both of cyber technologies and "G" technologies, showed their vector of focus on the integration with social engineering methods to obtain new characteristics, such as synergy and hybridity. Humanity's entry into the era of post-quantum cryptography (the emergence of a full-scale quantum computer) puts forward more stringent security requirements in both ICS and CPS, which form the core of CCIS. In the conditions of possible security chaos (hacking ~~by~~ of symmetric and asymmetric cryptosystems by quantum algorithms), the synergetic threat model is put first in the analysis of the current security state, which allows for the integration of threats by security components: IS, CS, SI. The proposed synergetic model allows one to take into account threats not only to ICS, but also their synergy with CPS threats, which greatly simplifies its use in security assessment methods in general.

2. The paper proposes a scheme of a unified classifier, taking into account the synergetic model of threats and economic costs of ensuring the required level of security. This approach allows us to formulate the methodological foundations of its construction and confirms its unification. The proposed classifier provides an intuitive approach to understanding its structure, allows you to generate critical threats, identify critical points in the construction of the ICS/CPS (CCIS) infrastructure. At the same time, the formation of preventive measures in the context of cost savings on TMIS is ensured at low computational and human costs.

3. The proposed model of the "danger" of the intruder based on their classification and degree of cyber system protection allows for the formation of the required security profiles based on the analysis of identified attempts to implement threats and/or to identify deviations from normal operation. This approach allows us to take into account the growth in the computing resources of attackers, the possibility of their motivation and the economic potential for implementing threats in a timely manner. It allows, in the context of the synergy and hybridity of modern threats, to respond in a timely manner to the formation of preventive measures to eliminate critical points in the infrastructure elements, to conduct a planned policy to increase the level of security based on the analysis of simulation results.

4. The developed methodology for determining the category of the intruder on the basis of the proposed classifier and the model of the "danger" of the attacker allows you to generate sets of critical threats, to model the identification of critical points based on the analysis of modeling the "danger" of various categories of attackers. Such an approach without significant computational, human, and economic costs significantly reduces many critical threats, allows to systematize them, and to form profiles of preventive protection measures.

References

1. Alguliyev, R., Imamverdiyev, Y., Sukhostat, L. (2018). Cyber-physical systems and their security issues. Computers in Industry, 100, 212–223. doi: https://doi.org/10.1016/j.compind.2018.04.017
2. Cárdenas, A. A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y., Sastry, S. (2011). Attacks against process control systems. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security - ASIACCS '11. doi: https://doi.org/10.1145/1966913.1966959
3. Gollmann, D. (2013). Security for Cyber-Physical Systems. Lecture Notes in Computer Science, 12–14. doi: https://doi.org/10.1007/978-3-642-36046-6_2

4. Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., Sastry, S. (2009). Challenges for securing cyber physical systems. Workshop on future directions in cyber-physical systems security.
5. Pfleeger, C. P., Pfleeger, S. L. (2006). Security in Computing. Prentice Hall, 880.
6. Cebula, J. J., Young, L. R. (2010). A taxonomy of operational cyber security risks. Technical report, DTIC Document.
7. Kang, D.-J., Lee, J.-J., Kim, S.-J., Park, J.-H. (2009). Analysis on cyber threats to SCADA systems. 2009 Transmission & Distribution Conference & Exposition: Asia and Pacific. doi: https://doi.org/10.1109/td-asia.2009.5357008
8. Nicholson, A., Webber, S., Dyer, S., Patel, T., Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. Computers & Security, 31 (4), 418–436. doi: https://doi.org/10.1016/j.cose.2012.02.009
9. Guide for conducting risk assessments (2012). NIST. doi: https://doi.org/10.6028/nist.sp.800-30r1
10. Cyber threat source descriptions. US-CERT. Available at: https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions
11. Milov, O., Korol, O., Khvostenko, V. (2019). Development of the classification of the cyber security agents bounded rationality. Control, Navigation and Communication Systems. Academic Journal, 4 (56), 82–90. doi: https://doi.org/10.26906/sunz.2019.4.082
12. Yevseiev, S. (2017). Intruder model of access rights in the automated banking system based on a synergistic approach. Naukovo-tekhnichnyi zhurnal "Informatsiyna bezpeka", 2 (26), 110–120.
13. Kravets, D. (2009). Feds: Hacker disabled offshore oil platforms' leak-detection system. Available at: https://www.wired.com/2009/03/feds-hacker-dis/
14. Chattopadhyay, A., Prakash, A., Shafique, M. (2017). Secure Cyber-Physical Systems: Current trends, tools and open research problems. Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017. doi: https://doi.org/10.23919/date.2017.7927154
15. Dell security annual threat report. Available at: https://proconics.co.za/wp-content/uploads/2017/10/2425.pdf
16. Walker, J. J. (2012). Cyber Security Concerns for Emergency Management. Emergency Management. doi: https://doi.org/10.5772/34104
17. Ali, N. S. (2016). A four-phase methodology for protecting web applications using an effective real-time technique. International Journal of Internet Technology and Secured Transactions, 6 (4), 303. doi: https://doi.org/10.1504/ijitst.2016.10003854
18. Park, K.-J., Zheng, R., Liu, X. (2012). Cyber-physical systems: Milestones and research challenges. Computer Communications, 36 (1), 1–7. doi: https://doi.org/10.1016/j.comcom.2012.09.006
19. Hansman, S., Hunt, R. (2005). A taxonomy of network and computer attacks. Computers & Security, 24 (1), 31–43. doi: https://doi.org/10.1016/j.cose.2004.06.011
20. Goel, S., Chen, V. (2005). Information security risk analysis – a matrix-based approach. Proceedings of the Information Resource Management Association (IRMA) International Conference. San Diego.
21. Kjaerland, M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. Computers & Security, 25 (7), 522–538. doi: https://doi.org/10.1016/j.cose.2006.08.004
22. Blackwell, C. (2010). A security ontology for incident analysis. Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW '10. doi: https://doi.org/10.1145/1852666.1852717
23. Yevseiev, S., Karpinski, M., Shmatko, O., Romashchenko, N., Gancarczyk, T. (2019). Methodology of the cyber security threats risk assessment based on the fuzzy-multiple approach. 19th International Multidisciplinary Scientific GeoConference (SGEM 2019). Sofia, 437.
24. Pollock, G. M., Atkins, W. D., Schwartz, M. D., Chavez, A. R., Urrea, J. M., Pattengale, N. et. al. (2010). Modeling and simulation for cyber-physical system security research, development and applications. doi: https://doi.org/10.2172/1028942
25. Ahmad, R., Yunos, Z. (2012). A dynamic cyber terrorism framework. International Journal of Computer Science and Information Security, 10 (2), 149–158.
26. Loukas, G., Gan, D., Vuong, T. (2013). A taxonomy of cyber attack and defence mechanisms for emergency management networks. 2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops). doi: https://doi.org/10.1109/percomw.2013.6529554
27. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0 (2014). National Institute of Standards and Technology. Available at: http://securityaffairs.co/Downloads/cybersecurity-framework-021214-final.pdf
28. Hughes, J., Cybenko, G. (2014). Three tenets for secure cyber-physical system design and assessment. Cyber Sensing 2014. doi: https://doi.org/10.1117/12.2053933
29. Buchyk, S. (2016). The methodology of analysis of risks of tree that identifiers the state informative resources. Ukrainian Information Security Research Journal, 18 (1), 81–89. doi: https://doi.org/10.18372/2410-7840.18.10116
30. Yevseiev, S., Rzayev, K., Mammadova, T., Samedov, F., Romashchenko, N. (2018). Classification of cyber cruise of informational resources of automated banking systems. Cybersecurity: Education, Science, Technique, 2 (2), 47–67. doi: https://doi.org/10.28925/2663-4023.2018.2.4767
31. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. NIST. doi: https://doi.org/10.6028/nist.ir.8105
32. Nurdinov, R. A., Batova, T. N. (2013). Approaches and methods of rationale choosing of information protection facilities. Sovremennye problemy nauki i obrazovaniya, 2, 395. Available at: https://www.elibrary.ru/item.asp?id=21285749
33. Katorin, Yu. F., Nurdinov, R. A., Zaytseva, N. M. (2015). Model' kolichestvennoy otsenki riskov bezopasnosti informatsionnoy sistemy. Vestnik mezhdunarodnyh nauchnyh konferentsiy, 12 (16), 77–86. Available at: https://www.elibrary.ru/item.asp?id=25663945
34. Howard, J. (1997). An Analysis of Security Incidents on the Internet 1989–1995. Pennsylvania. Available at: https://resources.sei.cmu.edu/asset_files/WhitePaper/1997_019_001_52455.pdf