To effectively protect critical infrastructure facilities (CIF), it is important to understand the focus of cybersecurity efforts. The concept of building security systems based on a variety of models describing various CIF functioning aspects is presented.

The development of the concept is presented as a sequence of solving the following tasks. The basic concepts related to cyberattacks on CIF were determined, which make it possible to outline the boundaries of the problem and determine the level of formalization of the modeling processes. The proposed threat model takes into account possible synergistic/emergent features of the integration of modern target threats and their hybridity. A unified threat base that does not depend on CIF was formed. The concept of modeling the CIF security system was developed based on models of various classes and levels. A method to determine attacker's capabilities was developed. A concept for assessing the CIF security was developed, which allows forming a unified threat base, assessing the signs of their synergy and hybridity, identifying critical CIF points, determining compliance with regulatory requirements and the state of the security system. The mathematical tool and a variety of basic models of the concept can be used for all CIFs, which makes it possible to unify preventive measures and increase the security level. It is proposed to use post-quantum cryptography algorithms on crypto-code structures to provide security services. The proposed mechanisms provide the required stability (230–235 group operations), the rate of cryptographic transformation is comparable to block-symmetric ciphers (BSC) and reliability (Perr 10–9–10–12)

Keywords: critical infrastructure, security system, threat classifier, concept, modeling method

UDC 681.32:007.5
DOI: 10.15587/1729-4061.2021.233533

DEVELOPMENT OF A CONCEPT FOR BUILDING A CRITICAL INFRASTRUCTURE FACILITIES SECURITY SYSTEM

Serhii Yevseiev
Corresponding author
Doctor of Technical Science, Professor*
E-mail: serhii.yevseiev@hneu.net
Yevgen Melenti
PhD
Special Department No. 2 «Tactical-Special Training, Marksmanship Training and Special Physical Training»
Juridical Personnel Training Institute for the Security Service of Ukraine
Yaroslav Mudryi National Law University
Pushkinska str., 77, Kharkiv, Ukraine, 61024
Oleksandr Voitko
PhD, Deputy Head of Department**
Vitalii Hrebeniuk
Doctor of Law, Senior Reseacher, Head of Laboratory
Scientific Laboratory
National Academy of Security Service of Ukraine
Mykhaylo Maksymovych str., 22, Kyiv, Ukraine, 03022
Anna Korchenko
Doctor of Technical Sciences, Associate Professor
Department of IT-Security
National Aviation University
Liubomyra Huzara ave., 1, Kyiv, Ukraine, 03058
Serhii Mykus
Doctor of Technical Sciences, Associate Professor, Head of Department **
Oleksandr Milov
Doctor of Technical Science, Professor*
Oleksandr Prokopenko
Adjunct
Center of Military and Strategic Studies***
Oleksandr Sievierinov
PhD, Associate Professor
Department of Information Technology Security
Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166
Dmytro Chopenko
Junior Researcher
Air Force Science Center
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
**Department of Information Technologies and Information Security Employment
Institute of the Troops (Forces) Support and Information Technologies***
***The National Defence University of Ukraine named after Ivan Cherniakhovskyi
Povitroflotskiy ave., 28, Kyiv, Ukraine, 03049

Received date: 06.04.2021
Accepted date: 10.05.2021
Published date: 30.06.2021

***How to Cite**: 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, 3 (9 (111)), 63–83. doi: https://doi.org/10.15587/1729-4061.2021.233533*

1. Introduction

The skyrocketing number of cyber incidents, which are becoming more serious, is driving the need to improve security, especially in the vulnerable area, which is critical infrastructure. One of the security challenges for critical infrastructures is the level of awareness of the impact of cyberattacks. The main reason for the escalation of critical

infrastructure (CI) cyberattacks may be that most of the CI control systems no longer use proprietary protocols and software, but use standard solutions. As a result, critical infrastructure systems are more vulnerable and prone to cyber threats than ever before. It is important to understand what types of attacks have occurred as this can help direct cybersecurity efforts to real threats to critical infrastructure.

Cyberspace has expanded significantly to become a large, dynamic and intricate network of computing devices. This situation also affected critical infrastructure systems. Apart from the positive effects of technological expansion, there are also disadvantages. Critical infrastructure is the backbone of everyday life in modern society, so its proper functioning is essential. For a long time, the most important infrastructure systems were considered immune to cyberattacks due to their dependence on proprietary networks and equipment. However, recent experience and cyberattacks show that this is unsustainable – the shift to open standards and web technologies makes critical infrastructure systems more vulnerable.

Unintentional or malicious actions in cyberspace have consequences for critical infrastructures in the physical world. Cyberspace attacks are not limited to government intelligence activities. Any part of critical infrastructure, from the banking system and utilities to the transportation or delivery of essential goods, can be attacked.

Attacks on critical infrastructure are diverse and include direct or anonymous access to secure networks through the Internet and supervisory control and data acquisition (SCADA) or employee violation of security procedures. All this leads to the spread of malware inside firewalls.

The problem with critical infrastructure cyberattack analysis is that some cyberattacks go unnoticed. However, some organizations are extremely reluctant to report incidents, believing that this leads to potential difficulties in doing business. One of the problems with cyberspace is that critical infrastructure protection is so imbalanced that it takes enormous resources, and only one infected computer disk is needed to start an attack. Thus, cyber defense has become one of the most important issues in national defense strategies.

Since the scale and nature of critical infrastructures preclude experimentation, the burden of understanding critical infrastructures and their relationships, emerging properties and resilience to malicious activity falls on modeling efforts. An attempt has been made to form the concept of building security systems based on a variety of models describing various aspects of critical infrastructure facilities.

2. Literature review and problem statement

Critical infrastructure (CI) supports basic services required by a complex modern society. Serious disruptions in the provision of services such as transport and energy can leave large populations vulnerable to shortages of food, electricity and fuel, as well as other necessities. Dependence on timely automated supply chains can also exacerbate the impact. Major natural disasters are good examples of how the destruction or degradation of such services affects populations. Large-scale disruption to these services can be triggered by cyberattacks aimed at undermining confidence in the state and designed to deplete emergency, medical and police services. CIs provide the foundation for the national economy, security, and health care. In [1], on the basis of intelligence data, the main results in the field of cyberterrorism focused on critical infrastructure facilities are presented (Table 1). However, the limitation of this work is only a description of the current state of cyberterrorism with the lack of recommendations on adequate countermeasures and measures to create a security system for critical infrastructure facilities.

Table 1

Aspects of critical infrastructure cyberterrorism

Key results	Emerging trends indicate that terrorists are expanding cyberattack capabilities
	Potential for economic damage, individually initiated and anonymous nature of cyberattacks are well aligned with the ideological beliefs, strategic goals and tactics of many terrorists
	Growing reliance of businesses on cyber technology, including interconnected networks and remote access, creates new and growing vulnerabilities that will be exploited by tech-savvy terrorists
	Proliferation of cyber technology and expertise, and availability of online hacking tools and "hackers for hire" encourage terrorists to adopt cyberattack strategies
Future strategies	Cyberattacks will become more attractive as companies' dependence on cyber technology grows, terrorists improve their cyberattack capabilities by keeping up with new technologies and overcoming countermeasures
	Availability of cyber technology and expertise, such as online hacking tools and hired hackers, provides resources to empower their cyberattack capabilities
	Emerging trend to post hacker-related content on their websites indicates their intention to develop more robust cyber strategies in the near future
Possible targets	Potential targets are likely to expand to include a wider range of organizations and critical infrastructure that terrorists associate with symbols of power
	International nature of cyberattacks means that many more attackers will be able to attack more remote targets (global communication makes the distance between the cyberattacker and the target irrelevant)
Possible indicators	Growing statements calling for the use of cyberattack methods
	Growing messages published on websites about committed cyber attacks
	Suspicious cyberattacks or increased frequency, creativity, or seriousness versus traditional targets
	Evidence that terrorists are recruiting or seeking services from persons with cyber capabilities

It can be assumed that control systems of critical infrastructure facilities are the most attractive targets for cyberattacks. Therefore, many works are devoted to the description of the structure, operation and safety of control systems, such as supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and other configurations, such as programmable logic controllers (PLC) [2–6].

In particular, [2] discusses the security issues of industrial control systems, the solution of which involves considering unique performance, reliability and safety requirements. The document provides an overview of ACS and typical system topologies, identifies typical threats and vulnerabilities for

these systems, and provides recommended security measures to mitigate associated risks. At the same time, the authors emphasize that their recommendations are focused exclusively on stand-alone use.

[3] provides specific recommendations for protection against cyberattacks on the UK's national critical infrastructure. An attempt is made to present the approach by outlining the magnitude of the challenges faced by the UK and what actions the government is taking to combat these threats. A number of recommendations aimed at mitigating these threats, increasing cyber resilience, and facilitating recovery plans as needed are offered. Full interaction and partnership with the owners and operators of critical national private sector infrastructure are vital to the success of the government's national cybersecurity strategy. This suggests that national and global actions are needed to ensure the efficient operation and cyber resilience of critical infrastructure facilities. These problems are relevant for all developed and developing countries. These conclusions should be considered the merit of the publication.

The papers [4–6] available for analysis are also focused either on the control system of critical infrastructure facilities or on its individual components that require protection from cyberattacks. At the same time, these works lack a unified concept and appropriate methodology for building a cybersecurity system for critical infrastructure facilities.

Of particular concern is the emergence of IoT and IIoT. IIoT consists of several industrial devices controlled by common software. IoT and IIoT have created many new attack vectors that can be exploited by cybercriminals and terrorists [5]. This evolution, combined with rapidly aging software platforms based on legacy CIs and outdated security policies, has made some CIs extremely vulnerable to cyberattacks.

CI has many internal vulnerabilities in its hardware and structure that could be easily exploited by attackers. Given these vulnerabilities, a terrorist organization is likely to attack CI. Specific examples of cyberattacks are presented in [7, 8]. The advantage of these works is the description of the so-called cascade effect, when a successful attack on one of the critical infrastructure facilities can cause a cascade effect of failures of other CI facilities.

Attention should be paid to the works devoted to the concept of sustainable development of developing states in an increasingly complex and unstable global world, and the concept of sustainability as a strategy for solving these problems [9]. The inclusion of a variety of new threats (such as economic, environmental and social) on the national security agenda, as well as ensuring the security of critical infrastructure, has created favorable conditions for a flexible approach to national security. In doing so, the nation state must fulfill its core responsibilities according to the traditional approach to national security, which is more preventive and not always consistent with the sustainability approach. Consequently, nation states must find an appropriate balance between proactive (security) and reactive (resilience) approaches that suit their specific needs as well as the values of society.

However, if the resilience of critical infrastructure remains a major national security concern, the government must nevertheless maintain the position that private operators and owners are responsible for the safety and resiliency of critical infrastructures.

The simulated events showed that a cyberattack on an adversary's CI can create an internal crisis situation with possible economic, psychological and physical damage. Such a cyberattack has not yet been fully performed as part of cyberwarfare by any state or non-state actor. Consequently, forecasting and preparing for computer network attacks are particularly difficult.

It should be noted that the description is focused on the situation of preparation or victim of cyberwarfare. However, the description is rather general, the problem is formulated, but solutions are not presented.

[10] warns that digital natives in terrorist organizations such as ISIS are likely to choose a cyber-kinetic attack method [11]. Cyber-natives means "young people, who entered the digital world, spend much time in the digital environment and use technological resources in their daily lives". In [10], it is argued that a digital terrorist would prefer to disable a power grid, causing cascading effects on the electricity-dependent CI, rather than conduct a ground attack that could directly endanger the attacker's own life. However, modern terrorist organizations may find martyrdom (suicide attacks) much more attractive, thus preferring the truck bomb to the logical one [12]. However, the ability to have a broader and more powerful impact on adversaries makes CI cyberattacks a powerful incentive to change tactics compared to traditional ground attacks carried out in the name of "martyrdom operations" [11]. Future terrorist operations will likely use cyberspace or a combination of cyber and ground-based attack methods, changing tactics as operational capabilities emerge. Therefore, it is imperative to understand the cyber dependencies built into CI and how vulnerable CIs can be to sophisticated cyber terrorist attacks.

Thus, the analysis of the literature [1–11] showed the lack of a single concept of building a system for protecting critical infrastructure facilities from cyberattacks and terrorist attacks, especially in the context of targeted threats with the manifestation of hybridity and synergy. This is noted in almost all publications. The proposed solutions for creating a holistic concept of protecting such facilities are either absent or local in nature and are aimed at protecting individual parts rather than critical infrastructure facilities as a whole.

3. The aim and objectives of the study

The aim of this work is to develop a concept for building a security system for critical infrastructure facilities based on a variety of models. The proposed models describe the structure and types of critical infrastructure facilities that reflect the typology of cyber terrorists and variety of their attacks in the form of classifiers. This approach will allow creating an effective security system, ensuring effective counteraction to modern hybrid threats to critical infrastructure elements emanating from cyber terrorists, and increasing the security of critical infrastructure facilities.

To achieve the aim, it is necessary to accomplish the following objectives:

– to form a classifier of critical infrastructure threats;

– to develop a concept for modeling the structure and functioning of the security system of critical infrastructure facilities;

– to develop models of a terrorist act and security of the critical infrastructure facility cybersystem;

– to develop a concept for assessing the security of critical infrastructure facilities.

4. Materials and research methods

Based on the analysis [13–15], the following definitions were introduced:

Systems of critical infrastructure facilities (CIF) – a set of automated control (dispatching) systems ensuring the interaction of CIF information and communication networks (ICN), destruction/failure of which significantly affects the information and/or cybersecurity of the state.

CIF information resources (IR) – information resources circulating in the CIF ICN, modification and/or destruction of which may lead to partial or complete destruction of CIF.

Confidentiality – protection of CIF IR from passive attacks.

Confidentiality of the CIF system – a property of the information security system (ISS) of CIF ensuring security during transmission.

Integrity – protection of CIF IR during storage and/or modification of CIF IR only by an authorized user (process).

Integrity of the CIF system – a property of the CIF ISS ensuring security during storage and/or modification of CIF IR only by an authorized user (process).

Availability – access of an authorized user to CIF IR.

Availability of the CIF system – a property of the ISS ensuring unlimited access to IR in accordance with the security model.

Authenticity – confirmation of CIF IR authenticity.

Authenticity of the CIF system – a property of the ISS ensuring the authenticity of the information source.

Continuity of the business processes of the CIF system – a property of the ISS ensuring the formation of a security loop for the business processes of CIF, which makes it possible to resist the blocking of the main functions or destruction of CIF.

Security of CIF IR – the state of the CIF security ensuring security services.

Threats to CIF RI – a set of technogenic and anthropogenic threats, the integration of which can lead to a synergistic effect, which significantly increases the risks of the implementation of threats to CIF elements.

Information threats are expressed in availability, integrity, authenticity and confidentiality violations.

Fig. 1 shows a block diagram of a synergistic threat model for the CIF elements.

The presented threat model, using the principles of universality, takes into account not only possible synergistic/emergent features of the integration of modern target threats into security components, but also their hybridity. This approach allows forming a single (unified) classification base of CIF threats, taking into account their categories, goals and possible damage, which greatly simplifies the understanding of potential terrorist attacks on the CIF elements.

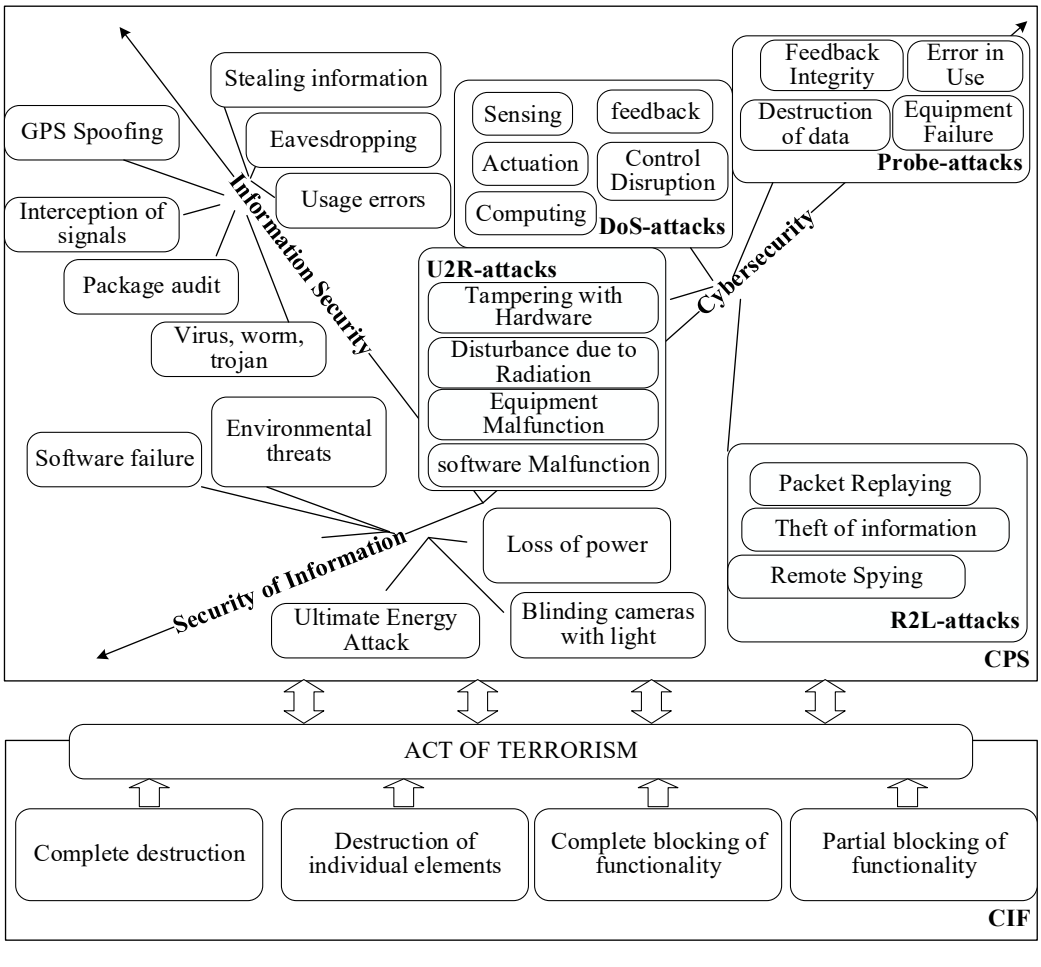

Fig. 1. Block diagram of a synergistic threat model for CIF elements

5. Results of research on the concept of building a security system for critical infrastructure facilities

5. 1. Development of a critical infrastructure threat classifier

To form a general classifier of threats to the CIF elements, it is proposed to divide the procedure (Fig. 2, 3) into two stages. At the first stage, based on the expert evaluation of threats and their impact on the security services of the CIF ISS, a single base of threat vectors is formed, which can be implemented by attackers at various CIF.

At the second stage, on the basis of the proposed expressions, the probabilities of threats, the possibility of their synergistic and/or hybrid impact on infrastructure elements are calculated. In this case, the synergistic effect is understood as the impact of threats on one of the security components: cybersecurity (CS), information security (IS) or security of information (SI). This approach makes it possible to significantly simplify the classification of threats and/or terrorist acts, to form relationships between threats and security services, to define hybrid threats to be understood as the aggregation of the impact on one of the security services in all security components. The classifier consists of 6 platforms.

The first platform defines the criticality of a threat (terrorist attack) as critical, high, medium, low, very low. The second platform – security components: CS, IS, SI. The third platform determines the focus of the threat on one of the security services, which allows assessing the possibility of a synergistic effect of threats on elements of critical infrastructure facilities.

The fourth platform defines the purpose of the terrorist attack – complete destruction of CIF (01), destruction of individual CIF elements (02), complete blocking of CIF functionality (03), partial blocking of functionality (04)).

The fifth platform allows determining the impact of the threat (terrorist attack) on the CIF elements, such as technical channel layer (H_0), ISO/OSI physical layer (H_1), data link layer (H_2), network layer (H_3), transport layer (H_4), application layer (H_5), layer of physical protection of CIF CPS elements (H_6), layer of possible secret intelligence devices (H_7).

The sixth platform defines the CIF category. For further research, it is proposed, in accordance with [15], to consider the following categories:

– fuel and energy complex (01);
– transport (02);
– public utilities (03);
– telecommunications and communication networks (04);
– banking and financial sector (05);
– public administration and law enforcement agencies (06);
– security and defense complex (07);
– chemical industry (08);
– emergency services and civil protection (09);
– food industry and agro-industrial complex (10).

To verify the expert evaluation, we use the approach proposed in [13]. In the expert evaluation of the objectivity of expert judgments, we use the weight factors of expert competence (k_k) presented in Table 2.

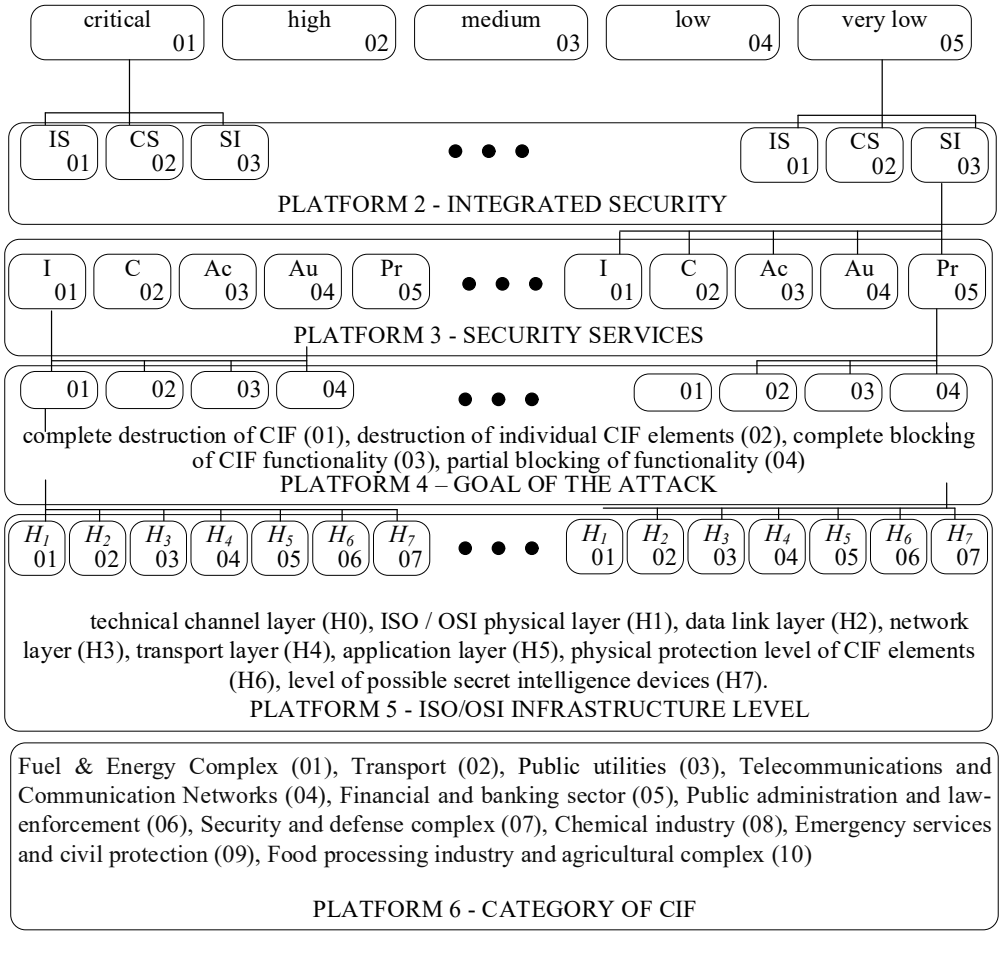

Fig. 2. Threat classifier structure (expert evaluation)

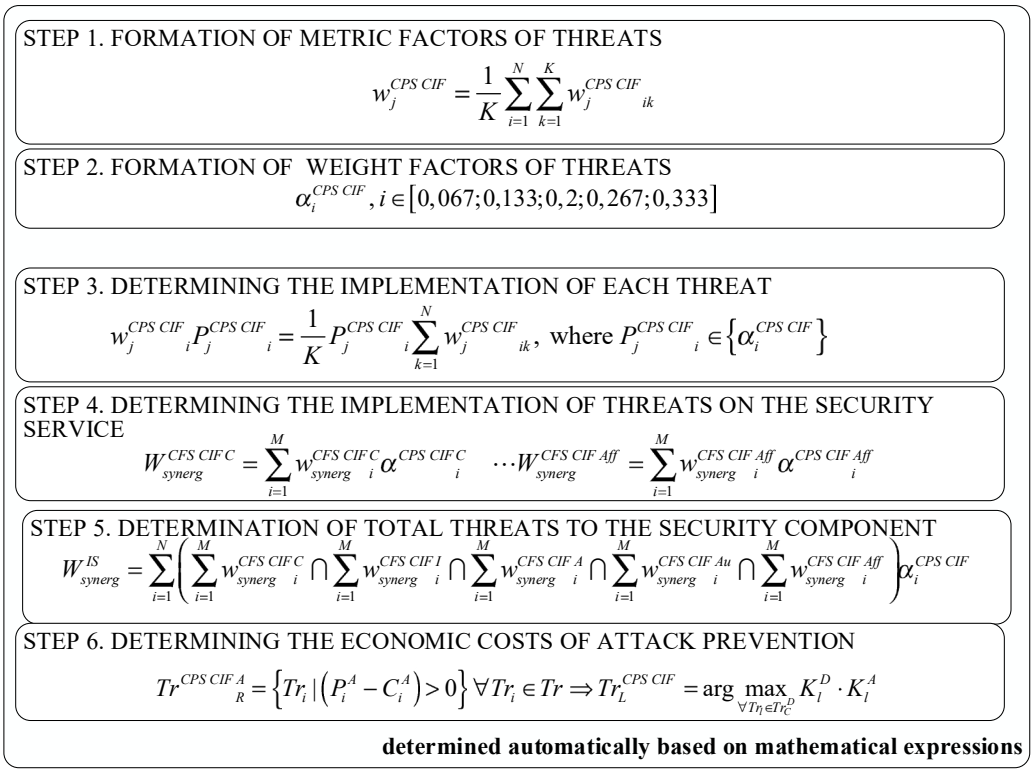

Fig. 3. Threat classifier structure (automatic calculations)

Table 2

Weight factors of expert competence

No.	Expert qualification	Weight factor value (k_k)
1	international expert in IS, CS, SI	1.0
2	national expert in IS, CS, SI	0.95
3	certified international specialist in IS, CS, SI	0.9
4	Full Doctor of Science in IS, CS, SI	0.9
5	chief security officer	0.85
6	Doctor of Philosophy in IS, CS, SI	0.8
7	security officer	0.7
8	system administrator	0.6
9	security engineer	0.5
10	postgraduate student in IS, CS, SI	0.4

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

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

where x_k is the k-th expert's estimate of the i-th threat; k_k is the expert's competence level; K is the number of experts.

A measure of the consistency of expert estimates is the variance, determined by the expression

$$\sigma_{\delta}^2 = \frac{1}{K}\sum_{k=1}^{K} k_k (x_k - \tilde{x}_i)^2. \quad (2)$$

The statistical probability of the results obtained $1 - \alpha_i$ is: $[\tilde{x}_i - \Delta, \tilde{x}_i + \Delta]$, where the value x_i is distributed according to the normal law with the center $\tilde{x}_i$ and variance σ_X^2. Then Δ is defined by the expression:

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

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

This approach allows forming an expert estimate of existing threats to security components (IS, CS, SI), taking into account their focus on hacking/termination of security services. The versatility of the approach lies in the objective assessment of experts' judgments, which allows using this mathematical tool when considering the entire range of threats, the possibility of their integration, synergy and hybridity.

To form metric (weight) factors of threats (Fig. 4) and their impact on security services, we introduce the following designations and offer the following mathematical tool:

1) j – security service for CIF. Basic security services:
– C – confidentiality;
– I – integrity;
– A – availability;
– Au – authenticity;
– Aff – affiliation.

Thus, a vector of security services $j = \{C, I, A, Au, Aff\}$ is formed in the classifier;

2) N – number of threats;

3) K – number of experts;

4) $\{i\}_1^N$ – current number of the i-th threat; $\{k\}_1^K$ – number of the expert.

To assess the hybrid and synergistic components of threats, we use the following procedure:

– Step 1. Assessment of the relationship between threats and security services:

$$w_j^{CPS\ CIF} = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_j^{CPS\ CIF}{}_{ik}, \quad (4)$$

where $w_j^{CPS\ CIF}{}_{ik}$ is the value of the factor set by the k-th expert for the i-th threat to the j-th security service.

– Step 2. Formation of threat factors (proposed in [13]):

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

– Step 3. Determination of threat implementation:

$$w_j^{CPS\ CIF}{}_i P_j^{CPS\ CIF}{}_i = \frac{1}{K} P_j^{CPS\ CIF}{}_i \sum_{k=1}^{N} w_j^{CPS\ CIF}{}_{ik},$$

where

$$P_j^{CPS\ CIF}{}_i \in \left\{\alpha_i^{CPS\ CIF}\right\}. \quad (5)$$

For security services and the i-th threat:

$$w_j^{CPS\ CIFC}{}_i P_j^{CPS\ CIFC}{}_i = \frac{1}{K} P_j^{CPS\ CIFC}{}_i \sum_{k=1}^{N} w_j^{CPS\ CIFC}{}_{ik},$$

where

$$P_j^{CPS\ CIFC}{}_i \in \left\{\alpha_i^{CPS\ CIFC}{}_i\right\};$$

$$w_j^{CPS\ CIFI}{}_i P_j^{CPS\ CIFI}{}_i = \frac{1}{K} P_j^{CPS\ CIFI}{}_i \sum_{k=1}^{N} w_j^{CPS\ CIFI}{}_{ik},$$

where

$$P_j^{CPS\ CIFI}{}_i \in \left\{\alpha_i^{CPS\ CIFI}{}_i\right\};$$

$$w_j^{CPS\ CIFA}{}_i P_j^{CPS\ CIFA}{}_i = \frac{1}{K} P_j^{CPS\ CIFA}{}_i \sum_{k=1}^{N} w_j^{CPS\ CIFA}{}_{ik},$$

where

$$P_j^{CPS\ CIFA}{}_i \in \left\{\alpha_i^{CPS\ CIFA}{}_i\right\}; \quad (6)$$

$$w_j^{CPS\ CIFAu}{}_i P_j^{CPS\ CIFAu}{}_i = \frac{1}{K} P_j^{CPS\ CIFAu}{}_i \sum_{k=1}^{N} w_j^{CPS\ CIFAu}{}_{ik},$$

where

$$P_j^{CPS\ CIFAu}{}_i \in \left\{\alpha_i^{CPS\ CIFAu}{}_i\right\};$$

$$w_j^{CPS\ CIFAff}{}_i P_j^{CPS\ CIFAff}{}_i = \frac{1}{K} P_j^{CPS\ CIFAff}{}_i \sum_{k=1}^{N} w_j^{CPS\ CIFAff}{}_{ik},$$

where

$$P_j^{CPS\ CIFAff}{}_i \in \left\{\alpha_i^{CPS\ CIFAff}{}_i\right\},$$

where $w_j^{CFS\ CIFC}{}_i$, $w_j^{CFS\ CIFI}{}_i$, $w_j^{CFS\ CIFA}{}_i$, $w_j^{CFS\ CIFAu}{}_i$, $w_j^{CFS\ CIFAff}{}_i$ are the weight factors of security services: *C*, *I*, *A*, *Au*, *Aff*; $\alpha^{CPS\ CIFC}{}_i$, $\alpha^{CPS\ CIFI}{}_i$, $\alpha^{CPS\ CIFA}{}_i$, $\alpha^{CPS\ CIFAu}{}_i$, $\alpha^{CPS\ CIFAff}{}_i$ are the weight factors of security services: *C*, *I*, *A*, *Au*, *Aff*, manifestations of the attack of the i-th threat.

– Step 4. Determination of implementation of several threats to the security service:

$$W_{synerg}^{CFS\ CIFC} = \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFC} \alpha^{CPS\ CIFC}{}_i;$$

$$W_{synerg}^{CFS\ CIFI} = \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFI} \alpha^{CPS\ CIFI}{}_i;$$

$$W_{synerg}^{CFS\ CIFA} = \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFA} \alpha^{CPS\ CIFA}{}_i; \quad (7)$$

$$W_{synerg}^{CFS\ CIFAu} = \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFAu} \alpha^{CPS\ CIFAu}{}_i;$$

$$W_{synerg}^{CFS\ CIFAff} = \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFAff} \alpha^{CPS\ CIFAff}{}_i,$$

where M is the number of threats selected by the expert from $\{i\}_i^M$, $M \le N$.

When forming the metric factors, it is considered that the results refer to independent threats. In the case of their dependence (coincidence of the threat tuples), it is necessary to use the expression for determining the total probability of dependent events:

$$P(AB) = P(A) + P(B) - P(AB). \quad (8)$$

In this case, only tuples of vectors that refer to the threats themselves are evaluated (platforms 1–5). This approach allows forming a common unified base of threats to all CIFs that can lead to terrorist attacks, the likelihood of their implementation and possible damage, without reference to the categories of critical infrastructure facilities.

– Step 5. Determination of a synergistic threat by security components:

$$W_{synerg}^{IS} = \sum_{i=1}^{N} \left(\begin{array}{l} \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFC} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFI} \cap \\ \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFA} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFAu} \cap \\ \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFAff} \end{array} \right) \alpha_i^{CPS\ CIF},$$

$$W_{synerg}^{CS} = \sum_{i=1}^{N} \left(\begin{array}{l} \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFC} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFI} \cap \\ \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFA} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFAu} \cap \\ \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFAff} \end{array} \right) \alpha_i^{CPS\ CIF}, \quad (9)$$

$$W_{synerg}^{SI} = \sum_{i=1}^{N} \left(\begin{array}{l} \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFC} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFI} \cap \\ \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFA} \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFAu} \cap \\ \cap \sum_{i=1}^{M} w_{synerg\ i}^{CFS\ CIFAff} \end{array} \right) \alpha_i^{CPS\ CIF}.$$

To determine the total synergistic threat:

$$W_{synerg}^{IS,CS,SI} = W_{synerg}^{IS} \cup W_{synerg}^{CS} \cup W_{synerg}^{SI}. \quad (10)$$

To determine the total hybrid threat:

$$W_{\text{hybrid } C,I,A,Au,Af\ synerg}^{CPS\ CIF\ \ CFS\ CIF\ I} = W_{synerg}^{CFS\ CIF} \cap W_{synerg} \cap \cap W_{synerg}^{CFS\ CIF\ A} \cap W_{synerg}^{CFS\ CIF\ Au} \cap W_{synerg}^{CFS\ CIF\ Aff}. \quad (11)$$

Step 6. Minimization of financial costs of preventive protection measures (we use the procedure proposed in [13]).

Thus, the main feature of the proposed approach is the possibility of forming a single unified base of threats to critical infrastructure facilities regardless of the CIF category. This makes it possible not only to simplify the formation of the CIF threat base, but also to timely take into account vectors of targeted attacks, the possibility of their integration, synergy and hybridity, as well as identify critical CIF points, their relationship with information resources. In addition, the proposed approach makes it possible to minimize funding for creating a security loop for CIF business processes, as well as timely formulate preventive measures and protection profiles.

5. 2. Development of a concept of modeling the structure and functioning of the security system of critical infrastructure facilities

Understanding and mitigating risks and threats to critical infrastructures highly depend on the ability to create and validate models, often involving physical systems or even human intervention.

The problem space of modeling includes both critical systems in general, such as industrial control systems at critical facilities, and interactions between several sectors of critical systems. Such a range of objects can be effectively described only by an equally wide range of modeling methods corresponding to the studied aspects of the infrastructure.

Formal identification of critical infrastructures has been made relatively recently [16], so the problem of modeling the construction of a CIF security system remains relevant. Such models were designed to solve relatively well-defined physical and engineering problems and therefore amenable to methods such as statistical reliability models for physical systems. These models are focused on designing technical systems with parametric fault tolerance.

However, the current understanding of critical infrastructures has revealed several additional dimensions to be mapped through modeling to ensure adequate reliability of the entire infrastructure. One of the most important aspects is the relationships between infrastructures and their components, as well as failure conditions leading to unavailability of infrastructure elements. This is unlikely to become apparent without a sufficient degree of abstraction allowing for a deeper understanding of such structural properties.

Obtaining such structural properties is a serious problem, since they are not limited only to obvious physical relationships, but must also reflect the information and communication aspects that define logical relationships.

More importantly, however, both information-based mechanisms and traditional physical vectors can be used by adversaries to degrade, damage or destroy infrastructure elements with disproportionate effects. Such hostility models are not common in many critical infrastructure sectors and, therefore, can be a source of serious vulnerabilities when threats are not fully understood and so not properly addressed. Thus, modeling is critical to obtain this information to design more robust infrastructure elements. The problem in any description of critical infrastructure models is a broad scope, as defined in [17, 18] and subsequently expanded in [19]. When it comes to critical infrastructure models, this can refer to several levels of abstraction, necessarily also aimed at answering different questions that the modeling concept has to address, as shown in Fig. 4.

In many models, the definition of CIF components was based on the impact of events or chains of events on infrastructure elements [20, 21]. This understanding, in particular of risk at different scales, leads to a classification mechanism originally proposed in [22] in the context of technical risk modeling and subsequently refined [23] into an infrastructure scale taxonomy, as shown in Fig. 4.

Verifying the applicability of the presented security analysis models requires significant effort. This is true even if the model takes into account all parameters related to security and reliability analysis.

For lower levels of abstraction, it may be possible to derive and test such models explicitly from the basic principles. At higher levels of abstraction, this leads to uncertainty in the validity of the model.

Such uncertainty is already problematic when it is not easy to determine whether the basic problem is ill-conditioned. Conditionality is defined as a situation where small variations in parameters lead to disproportionate changes in results. Poor conditioning can be a feature of the modeling method. This problem also arises in the context of combining several specialized models or models that address different levels of abstraction [24].

Moreover, in some cases, the same mathematical methods can be applied at different levels of abstraction, which is especially noteworthy for the case of game-theoretic models.

Economic models serve mainly to identify high-level relationships and can also reveal quantitative effects, albeit with a relatively low resolution. Most of the models used in the area of critical infrastructure are input-output models, focusing primarily on aspects driven by demand or supply. However, such models are necessarily limited to the state of equilibrium.

An application to critical infrastructures was originally proposed in [25], where several interrelated systems are considered, including intra-industry relationships. The purpose of the review is to identify inoperability caused by one or more failures. Such failures can be both natural and artificial. In the proposed model, inoperability is defined as the level of system dysfunction, i.e., as part of expected operability level, which is described by the Inoperability Input-Output model (IIM).

To capture the disturbance aspect, IIM extensions include demand reduction IIM, as well as variants of dynamic IIM that seek to reflect the effects of repeated recovery [23]. These models, summarized in [26], are also considered and applied in a variety of quantitative case studies at the regional and sectoral level [27], including [28] and in studies at larger scales, including studies on national economies [29]. The authors [30] applied the IIM to the case of damage caused by industrial espionage. Earlier works [31] sought to apply the modeling method to control systems, studying the effects of inoperability resulting from failures in the supervisory control and data acquisition (SCADA) systems.

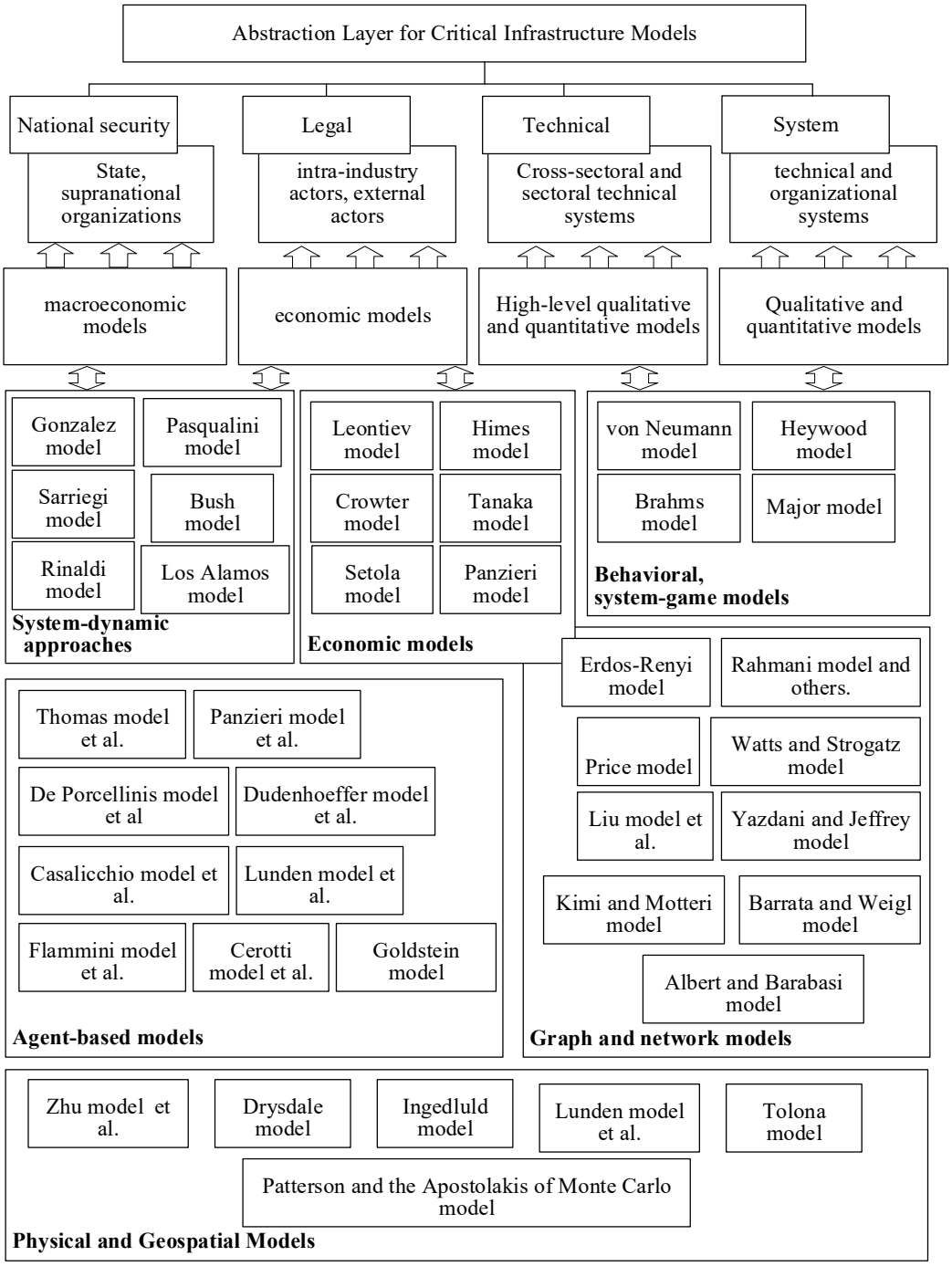

Fig. 4. Modeling concept of critical infrastructure facilities (according to [14, 15])

Moreover, the IIM approach was applied not only to describe and analyze existing relationships and related risks, but also as a basis for minimizing the relationships of critical infrastructure subsystems [32].

An extension of the IIM model to study the impact of information technology and information security-based relationships is presented in [33]. A significant result of the work is quantitative indicators for identifying intersectoral relationships caused by information security problems.

In [26], a family of models is presented that reflect a decrease in efficiency indicators and economic losses of the system and allow estimating the impact of failures on information provision. However, models are limited to large-scale abstractions and are not suitable for obtaining quantitative data for subsystems or individual blocks. This is reflected in the mechanisms of attacker behavior modeling [34].

The dynamic IIM allows analyzing parameters such as optimization of buffering in the form of stocks to mitigate fluctuations in supply levels [35]. The use of explicit probabilistic vectors of disturbances from the demand side in the IIM increases the reliability of modeling results and the applicability of models for cybersecurity purposes [36–38].

Applicability for cybersecurity purposes may require the introduction of a cost metric for disparate facilities included in the critical infrastructure [39–41].

In [29], the role of individual infrastructures in the formulation of dynamic IIM is determined, which is of particular interest for understanding the potential of cascade

effects. It is proposed to use a qualitative parameter estimate [42] and map it to fuzzy sets with convex membership functions. It is proposed to implement this approach by introducing extensions based on intelligent agents.

System-dynamic approaches are considered in [43–46]. So, [43] considers the relationship between infrastructure facilities and information flows, [44, 45] study the structural properties of CIF. System dynamics provides insight into the types of threats to critical infrastructure, in particular, social engineering attacks [46].

Practice shows that it is difficult to avoid internal attacks, including attacks based on social engineering rather than technical measures. Therefore, when developing control mechanisms, it is necessary to focus on the ways in which control and interaction means can cause delays in implementing attackers' goals. In [47], an attempt is made to formalize similar aspects for the more general case of security management.

The systems dynamics approach is applied to both target and large-scale critical infrastructure environments [43, 48].

Larger-scale applications of systems dynamics for describing dynamic interactions are often based on simulation to help understand such relationships and cascading effects. These applications can use industry models, which are then combined through a better system dynamics approach.

One example of such a simulation environment is the Critical Infrastructure Protection Decision Support System (CIP/DSS) [49, 50]. This environment is based on discrete event modeling, rule-based expert systems and coupled differential equations for sector submodels. The simulation results were used in [51, 52] to identify clear economic impacts, their recovery and mitigation.

In [53], a system dynamics model is presented, which used the functional modeling mechanism (IDEF0 [54]) to determine the requirements and mechanisms for information exchange. This allows simulating local loss of function or bandwidth in the infrastructure as a whole, and then applying a decision support system using nonlinear optimization.

For large-scale models, there can be about 100 model elements, which usually requires an understanding of sector-specific aspects [49, 53]. System dynamics modeling helps to solve some of these problems using the so-called group model construction [55, 56], which seeks to integrate domain expertise into the overall model.

Behavioral and system-game models are proposed in [57–59]. Such methods are usually based on a combination of expert estimates and Bayesian statistics [57] or on explicit causal models. This approach may be useless assuming the adaptability of an intelligent adversary [58].

Behavioral and game-theoretic models provide for two or more agents whose interactions can be modeled under various constraints [59]. However, these interactions usually include:

– the ability to cooperate or act against the interests of other agents;

– the ability to interact with different levels of information about each other;

– the possibility of both one-time interaction and interaction over several rounds;

– the attainability of agents' solutions both simultaneously and sequentially.

This type of model assumes that agents are rational and act to maximize their utility. This is done by evaluating the results and choosing the actions that give the most preferable results, taking into account the actions of other players.

Of particular interest for considering hostile behavior is the assumption of complete information [60, 61] and the possibility of cooperation [62], which can be clear with full participation or unclear with varying participation levels. Game-theoretic security modeling, including strategic military models, is presented in [63, 64]. In the field of political science, applications are used that include arms control strategies [65], as well as applicability to information warfare [66]. Models of terrorist activities and related resource protection or allocation strategies are presented in [67, 69].

The use of game-theoretic models to protect critical information infrastructures is not well represented in the literature. Besides [66], examples include the use of two-player stochastic games [70] to capture the attackers' behavior under the Nash equilibrium. The model in [71] attempts to explicitly map the perception of attackers in the game-theoretic structure, as well as parameters, including resource allocation. Many of the physical security and counter-terrorism problems require careful analysis, taking into account various assumptions, which includes modeling of substitution effects and amount of mutual information [72]. Existing models [67] and subsequent developments [73, 74] not only estimate the parameters, but also assume the simultaneous play of attackers and defenders [70, 75].

Graph and network models provide rigorous formalization [76] and are easily adaptable to network infrastructures such as telecommunications, pipelines, and power distribution. By assigning a set of properties to nodes and edges and by defining flows along the graph edges, many aspects of critical infrastructures and their relationships for both physical assets and information flows can be covered. One of the main goals of such models is usually to capture the physical and logical relationships between network components, which may belong to several different infrastructure sectors.

Critical infrastructures are often long, and individual infrastructures can contain more than 105 elements. This explains the interest in studying graph-theoretic concepts to understand how a graph or interaction structures can be used to characterize the resilience of a network infrastructure.

Particular attention should be paid to the intensive study of random graphs such as the Erdös-Renyi graphs [76, 77].

Empirical research has shown that many networks, both in nature and human-created, are scaleless. To reflect the dynamics of the critical infrastructure, the processes of graph growth and the mechanism of preferential joining of new edges added to the graph are considered [78]. This work has resulted in a number of methods more widely used in statistical mechanics being applied to complex networks, including critical infrastructures and their relationships [79, 80]. The paper [81] provides a broader view of complex networks in general.

It is noteworthy that even relatively simple assumptions of graph theory make it possible to study the resistance of graphs to attacks. In [82], a process is described in which a dynamically evolving random graph is expanded using preferred attachment to achieve non-scalable properties and taking into account the adversary's ability to remove some of the vertices.

One of the areas associated with the ability to describe complex networks, of which critical infrastructure networks are only one instance, is the analysis of the resilience of such networks to attacks. The study [83] describes general classes of error vulnerabilities as well as deliberate attacks, while a number of authors analyzed specific infrastructure sectors using network complexity theory methods.

One area of particular interest that, however, has not been fully explored, but is critical for understanding the

implications of deliberate attacks on critical infrastructure networks, is the dynamic aspects of such graphs. Although the analysis was carried out on aspects such as individual failures, cascading failures have been investigated by a number of researchers, including early works [84, 85]. In [86], cost models for attackers were introduced.

The considered approaches are associated with the need to analyze information flows that can be mediated by human interaction. The study of such networks uses graph-theoretic concepts to understand such relationships and can rely on a large number of modeling methods specially adapted for social network analysis [87].

Agent-based models are often used to analyze the interdependencies of infrastructure facilities. Infrastructures or physical components are modeled as agents, which allows analyzing the performance and physical condition of the infrastructure and also capturing behavioral aspects, including irrational behavior [40]. Such agent-based systems have been widely used in other fields, which allows using the results to capture aspects such as the interaction of physical objects [88]. Descriptions of physical agent interaction were integrated into the model of interacting social agents, for example, to track the behavior of agents in the electricity and natural gas markets [89].

Most research has focused on using fewer explicit agents to describe the behavior of interacting agents in order to identify relationships in infrastructures [90, 91]. An example of such an agent-based modeling and simulation environment is [92] as a continuation of [93]. In [92, 93], the combined use of relationship analysis and qualitative methods to determine the parameters causing relationships is presented. With this approach, the model is built from composite elements, but with emergent properties of complex adaptive systems. Agents are represented as objects with a geospatial location, a number of domain-specific capabilities, and internal memory.

Obtaining comprehensive and complete datasets can be difficult even with analytical and simulation mechanisms. This has also led to several high-quality models and simulation environments, the main purpose of which is to enable an expert to visualize the relationships between sectors and infrastructure elements, without necessarily providing predictive capabilities. An example of such an environment is presented in [93, 94]. The critical infrastructure modeling system (CIMS) uses georeferenced features and graphs to simulate events, such as fires or floods, using a discrete event modeling environment.

Physical and geospatial models are usually designed to solve well-defined problems in a particular sector or for a specific facility. These models exhibit high computational complexity, while significantly varying the level of detail [43] from simple vulnerability analysis and intra-industry relationships to continuous physical models.

Such models are necessary to describe the operation of infrastructures [95], which allows for quantitative risk analysis [96]. External effects on critical infrastructures, such as cyberattacks, must be taken into account and even generated in the model.

Spatial proximity is an important parameter in the study of relationships and physical effects, which is not always clear from the analysis of only logical relationships. Therefore, a number of efforts have been aimed at creating models of critical infrastructures and their relationships based on geospatial information systems (GIS) [97, 98]. Examples of using GIS functions in the area of critical infrastructure include approaches based on the theory of multi-attribute utility for forecasting.

5. 3. Development of a model of a terrorist act and security of the critical infrastructure facility cybersystem

The formation of complex (echelon) protection of a critical infrastructure facility is based on the hierarchical structure of the synthesis of information security systems of cyber-physical systems, Internet technologies and computer networks, as well as mobile technologies. This approach allows forming a synergistic model of CIF threats, taking into account the impact of terrorists on its elements (Fig. 5).

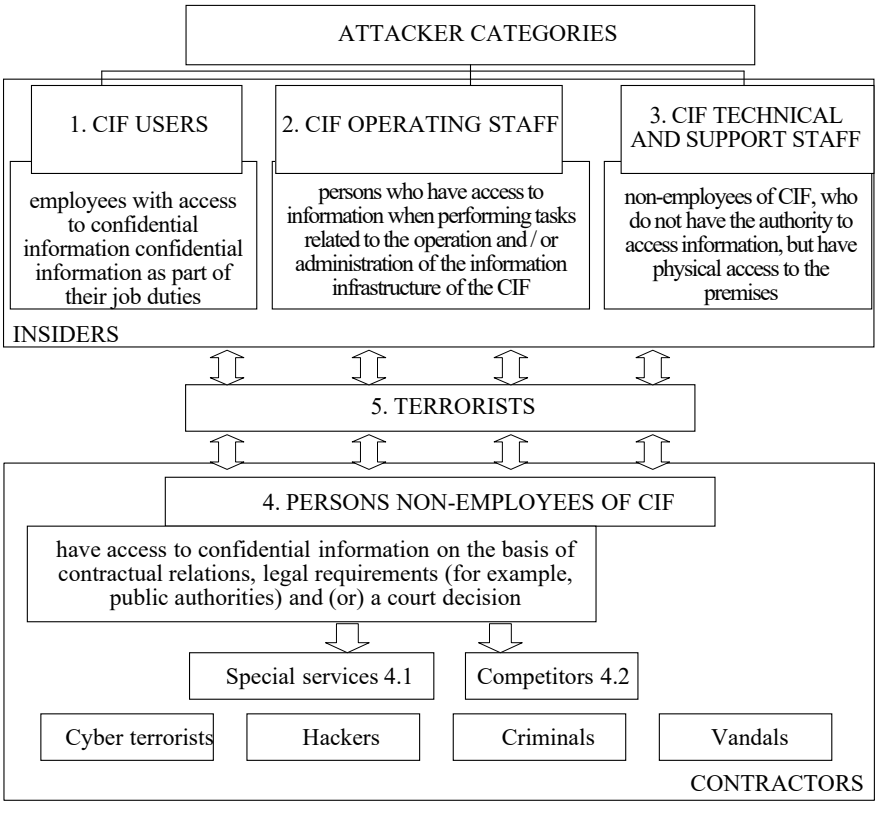

Fig. 5. Classification of attackers

To form a model of a terrorist act and security of the critical infrastructure facility cybersystem, a mathematical tool has been developed:

– classification allows entering elements of a set of attacker categories $L_i^{del} \in \{L^{del}\}$: L_1^{del} – CIF users; L_2^{del} – CIF operating personnel; L_3^{del} – CIF technical support staff; L_4^{del} – non-employees of CIF; L_5^{del} – terrorists and perpetrators of terrorist acts: L_{51}^{del} – cyber terrorists, L_{41}^{del} – in-

telligence agencies, L_{52}^{del} – hackers, $L_{4.2}^{del}$ – competitors, L_{53}^{del} – criminals, L_{54}^{del} – vandals;

– the model of a terrorist act is defined as:

$$G_{\text{terror}}^{CPS\,CIF}=\left\{L_i^{del},\beta_i^{C}\quad\in\left\{\beta_{\text{terror}}^{CPS\,CIF}\right\},p_{rj},r_{\text{motiv}},T\right\},\tag{12}$$

where $L_i^{del}\in\left\{L_i^{del}\right\}$ is the identifier of the terrorist-perpetrator; $\beta_i^{CPS\,CIF}\in\left\{\beta_{terror}^{CPS\,CIF}\right\}$ is the weight factor of the capabilities of the perpetrator of the terrorist attack on CIF;

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 is the information resource (asset); $\forall j\in m$, m is the number of assets; r_{motiv} is the motivation of the terrorist-perpetrator to carry out a terrorist attack on CIF, T is the time of the terrorist attack. Analysis of the attacker categories allows forming an expert estimate and obtaining a weight factor for the threat implementation probability (the i-th threat);

– the weight factor of the terrorist-perpetrator's capabilities is determined by:

$$\gamma_{terror}^{CPS\,CIF}=\frac{1}{N}\sum_{i=1}^{N}\beta_i^{CPS\,CIF}\times p_{rj}\times r_{motiv},\tag{13}$$

where $\beta_i^{CPS\,CIF}=W_{cp}^{CPS\,CIF}\bigcap W_{cash}^{CPS\,CIF}\bigcap T$ are the weight factors of the terrorist-perpetrator's capabilities;

$W_{cp}^{CPS\,CIF}$ is the terrorist-perpetrator's computing resources (from [13]);

$W_{cash}^{CPS\,CIF}$ is the terrorist-perpetrator's financial resources (from [13]).

The proposed approach makes it possible to unify the procedure for determining the probability of a terrorist attack on CIF, taking into account the terrorist-perpetrator's capabilities, both financial and computing resources.

The analysis of the CIF infrastructure level and terrorist-perpetrator categories allows forming the set $\{H_j\}$, which forms the levels of impact on CIF: technical channel layer (H_0); ISO/OSI physical layer (H_1); ISO/OSI link layer (H_2); ISO/OSI network layer (H_3); ISO/OSI transport layer (H_4); ISO/OSI application layer (H_5); layer of physical protection of CIF elements (video surveillance, sensors, grilles, locks, etc.) (H_6); layer of possible secret intelligence devices (ventilation ducts, power lines, etc.) (H_7);

– the relationship matrix for the terrorist-perpetrator category and the level of impact on CIF is defined as:

$$M_{L_i^{del}}^{H_i}=\left\|L_i^{del}\right\|\times\left\|H_i\right\|=\begin{matrix}0&0&0&0&0&0&0&1\\1&1&1&1&1&0&1&0\\0&0&0&0&0&0&1&1\\1&1&1&1&0&1&1&0\\1&1&1&1&1&1&1&1\\1&1&1&1&0&1&1&0\\1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1\\1&1&1&1&0&1&1&0\\1&1&1&1&1&1&1&0\\1&0&0&0&0&1&1&0\\1&0&0&0&0&1&0&0\end{matrix}.\tag{14}$$

Thus, the relationship matrix for the terrorist-perpetrator categories and the levels of impact on CIF allows determining the terrorist-perpetrator category by the threat classifier according to the proposed method:

– Stage 1. Determination of the level of impact on CIF from the set $\{H\}$;

– Stage 2. Determination of the threat according to the CIF threat classifier;

– Stage 3. Determination of the relationship matrix for the terrorist-perpetrator category and the level of impact on CIF;

– Stage 4. Determination of a possible terrorist-perpetrator from the relationship matrix.

Thus, based on the proposed methodology, a list of critical threats for each attacker category is constructed. Taking into account the modern approaches proposed in [99–108] for assessing the layer of possible secret intelligence devices (H_7), the time and financial costs of preventive protection measures are significantly reduced.

5. 4. of a concept for assessing the security of critical infrastructure facilities

To determine the current state of security, we use the approach proposed in [14], which takes into account the proposed approach to the formation of a synergistic threat model, categories of attackers, their goals and capabilities. Fig. 6 shows the concept of assessing the security of critical infrastructure facilities.

To assess the current state, it is proposed to use the following mathematical tool:

– the formally improved model of CIF is defined as:

$$G^{CIF}=\{\{O^{CIF}\},\{L^{CIF}\},\{I_A\}\},\tag{15}$$

where $\{O^{CIF}\}$ is the set of environment objects describing the CIF elements; $\{L^{CIF}\}$ is the set of links between the elements, defined by an adjacency matrix; $\{I_A\}$ is the set of information asset elements.

Each element $I_{A_i}\in\left\{I_A\right\}$ is described by the vector $I_{A_i}=\left(Type,A^C,A^IA^A,A^{Au},A^{Aff},A^{cont}\right)$. *Type* is the type of information asset, described by a set of basic values: T*ype*= ={*CI, PD, CD, TS, StR, PubI, ContI, PI*}, where *CI* is confidential information, *PD* is payment documents, *CD* is credit documents, *TS* is trade secret, *StR* is statistical reports, *PubI* is public information, *ContI* is control information, *PI* is personal information.

A^C, A^I, A^A, A^{Au}, A^{Aff}, A^{cont} are security services.

Each element of $O_l^{CIF}\in\left\{O^{CIF}\right\}$, is described by the vector $O_l^{CIF}=\left\{L^{CIF},TC^{CIF}\right\}$, where L^{CIF} is the level of the CIF information structure, defined by the set $L^{CIF}=\left\{H_0,H_1,H_2,H_3,H_4,H_5,H_6,H_7\right\}$, where the technical channel layer (H_0), ISO/OSI physical layer (H_1), data link layer (H_2), network layer (H_3), transport layer (H_4), application layer (H_5), layer of physical protection of CIF CPS elements (H_6), layer of possible secret intelligence devices (H_7);

– formally, the relationship between the CIF IR and elements:

$$TC^{CIF}=\left\|TC_{il}^{CIF}\right\|,\tag{16}$$

where TC_{il}^{CIF} determines the relationship between the i-th IR and the l-th element of CIF, while

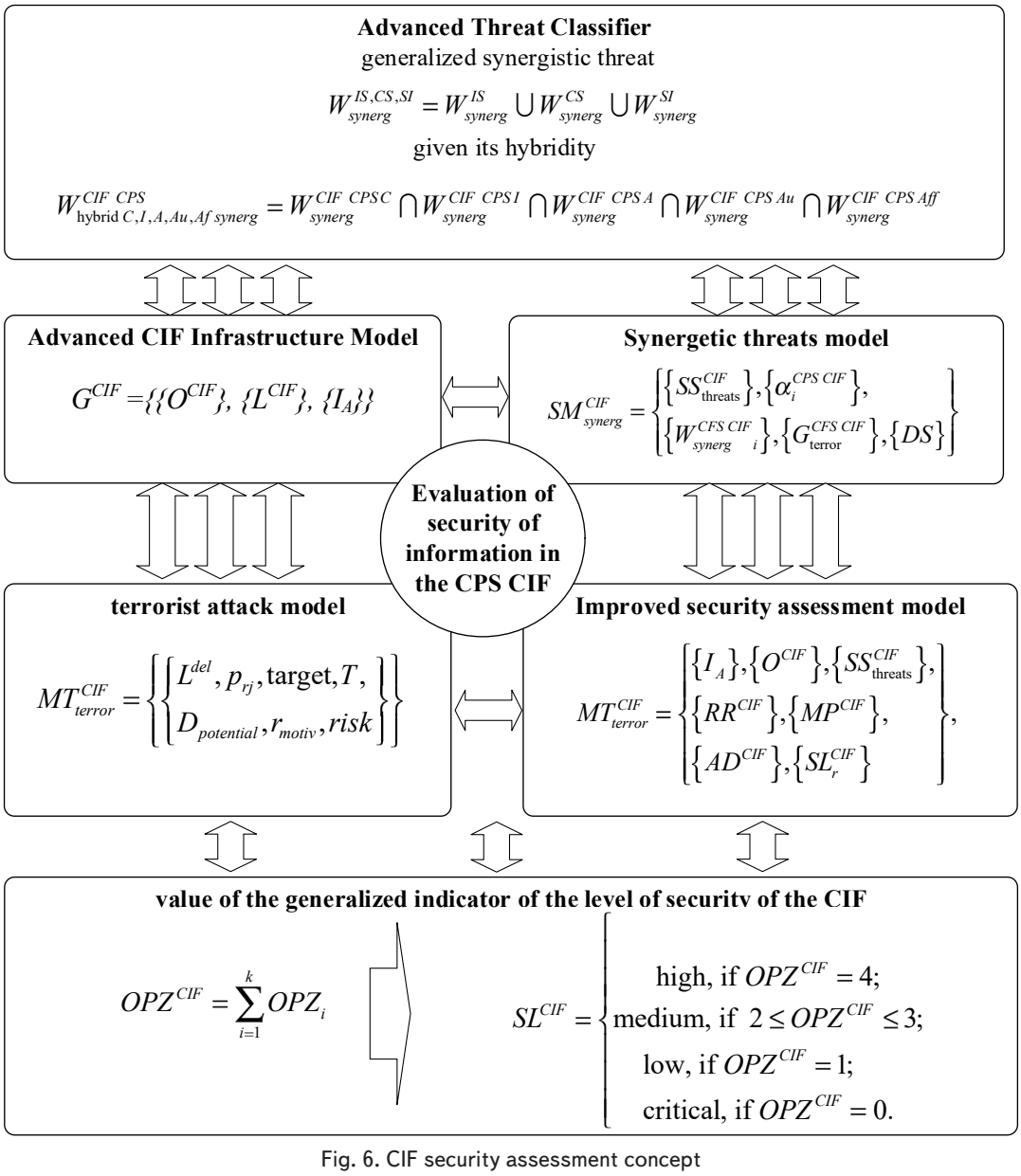

Fig. 6. CIF security assessment concept

$$\forall i \in \{I_A\}, \forall l \in \{O^{CIF}\} \Rightarrow TC_{il}^{CIF} = \\ = \begin{cases} 0, \text{ no relationship;} \\ is, \text{ includes and stores;} \\ pt, \text{ processes and transfers;} \\ mf, \text{ maintains the functioning;} \end{cases} \quad (17)$$

– the proposed synergistic model of CIF threats:

$$SM_{synerg}^{CIF} = \left\{ \{SS_{\text{threats}}^{CIF}\}, \{\alpha_i^{CPS\ CIF}\}, \{W_{synerg\ i}^{CFS\ CIF}\}, \{G_{\text{terror}}^{CFS\ CIF}\}, \{DS\} \right\}, \quad (18)$$

where $SS_{\text{threats}}^{CIF} = \left\{ \{SS_{MMS}^{CIF}\}, \{AS_{\text{threats}}^{CIF}\} \right\}$ is the set of possible threats, in which $\{SS_{MMS}^{CIF}\}$ is man-made threats; $SS_{MMS}^{CIF} = \left\{ \{SS_{IS}^{CIF}\}, \{SS_{CS}^{CIF}\}, \{SS_{SI}^{CIF}\} \right\}$ are the anthropogenic threats. The set of anthropogenic threats is proposed to be considered based on the synergetic approach according to security components.

Wherein $\{SS_{IS}^{CIF}\}$ is IS threats, $\{SS_{CS}^{CIF}\}$ is CS threats, $\{SS_{SI}^{CIF}\}$ is SI threats. $\{\alpha_i^{CPS\ CIF}\}$ is the set of threat weight factors, $\{W_{synerg\ i}^{CFS\ CIF}\}$ is the set of threats to the security service, $\{G_{\text{terror}}^{CFS\ CIF}\}$ is the set of damage from a terrorist attack, $\{DS\}$ is the set of destructive states of CIF elements, which mean complete destruction of CIF (01), destruction of CIF elements (02), complete blocking of CIF functionality (03), partial blocking of functionality (04);

– synergistic effect of modern threats:

$$SS_{\text{threats}}^{CIF} = \{SS_{MMS}^{CIF}\} \cup \{AS_{\text{threats}}^{CIF}\},$$

where

$$SS_{MMS}^{CIF} = \{SS_{IS}^{CIF}\} \cap \{SS_{CS}^{CIF}\} \cap \{SS_{SI}^{CIF}\}, \quad (19)$$

– each threat to the CIF elements is formalized by the tuple:

$$SS_{\text{threats}}^{CIF}=\left(p_{rj},D_{potential},risk\right), \quad (20)$$

where p_{rj} is the probability of a threat to the j-th asset, i is the threat for all i that belong to n – the number of threats, j is the IR (asset) for all j that belong to m – the number of IR; $D_{potential}$ is the potential damage, *risk* is the risk expressed in a qualitative form and taking one of the values $risk=\left(\alpha_{r_1},\alpha_{r_2},\alpha_{r_3},\alpha_{r_4},\alpha_{r_5}\right)$, where α_{r_1} – critical, α_{r_2} – high, α_{r_3} – medium, α_{r_4} – low, α_{r_5} – very low;

– destructive states of the CIF elements (the set $\{DS\}$) from [13]. The formal model of the terrorist-perpetrator is defined as:

$$MT_{terror}^{CIF}=\left\{\left\{L^{del},p_{rj},\text{target},T,D_{potential},r_{motiv},risk\right\}\right\}, \quad (21)$$

where L_{del} is the attacker categories; target is the attacker' target, $\text{target}\in\{DS\}$; T is the time of successful implementation of the threat; r_{motiv} is the probability of the terrorist-perpetrator's motivation.

– formally, the relationship between the categories of attackers and their impact on the CIF elements is defined by the matrix $CT_{\text{impact}}^{CIF}=\left\|a_{ij}^{CIF}\right\|$, where $a_{ij}^{CIF}=1$, if the threat source $SS_{\text{threats}}^{CIF}$ can implement a threat against the j-th CIF asset $O_l^{CIF}\in\{O^{CIF}\}$, otherwise $a_{ij}^{CIF}=0$.

– CIF security assessment model:

$$MT_{terror}^{CIF}=\begin{Bmatrix}\{I_A\},\{O^{CIF}\},\{SS_{\text{threats}}^{CIF}\},\{RR^{CIF}\},\\ \{MP^{CIF}\},\{AD^{CIF}\},\{SL_r^{CIF}\}\end{Bmatrix}, \quad (22)$$

where $\{I_A\}$ is the set of IR; { O^{CIF} } is the set of CIF elements; $\{SS_{\text{threats}}^{CIF}\}$ is the set of threats; $\{RR^{CIF}\}$ is the set of IS regulatory requirements; $\{MP^{CIF}\}$ is the set of information security elements; $\{AD^{CIF}\}$ is the result of CIF security assessment; $\{SL_r^{CIF}\}$ is the CIF security level;

– formally, the relationship between threats and IR:

$$TI^{CIF}=\left\|\beta_{ij}^{CIF}\right\|,\forall j\in\{I_A\},\forall i\in\{SS_{\text{threats}i}^{CIF}\}, \quad (23)$$

where 1 – the threat to the IR, 0 – no threat to the IR;

– the protection mechanism is formed by the tuple:

$$MP^{CIF}{}_i=\left(T_{pe},T_{\text{introducing}},\ {}_{pe}\right), \quad (24)$$

where T_{pe} is the type of the IS tool, $T_{introducing}$ is the introducing time, C_{pe} is the cost of the IS tool;

– formally, the relationship between threats and information security systems:

$$L_{ThIS}^{CIF}=\left\|\gamma_{ij}^{ThIS}\right\|, \quad (25)$$

where MP^{CIF} – the threat can be repelled by the ISS, NMP^{CIF} – the threat is imlemented.

If $\lambda_{ij}^{LThIS}=NMP^{CIF}$, it is concluded that the CIF ISS is not able to protect the IR from the threat, and it is necessary to introduce additional protection means and mechanisms to increase the CIF security;

– requirements of international and national standards and legislation:

$$\{RR^{CIF}\}=\{R_{INS}^{CIF}\}\cup\{A_{DSR}^{CIF}\}, \quad (26)$$

where $\{R_{INS}^{CIF}\}$ is the international and national regulatory requirements, $\{A_{DSR}^{CIF}\}$ is the set of information security assessments.

The current state of the CIF IS is determined by the following indicators:

– OPZ_{one} – assessment of threat risks and the presence of critical points in the CIF elements;

– OPZ_2 – assessment of possible attacks on the CIF elements;

– OPZ_3 – assessment of compliance with regulatory requirements.

$$OPZ^{CIF}=\sum_{i=1}^{k}OPZ_i. \quad (27)$$

The proposed mathematical tool of the concept of assessing the security of critical infrastructure facilities provides a qualitative estimate of the current state of information security:

$$SL^{CIF}=\begin{cases}\text{high, if } OPZ^{CIF}=4;\\ \text{medium, if } 2\le OPZ^{CIF}\le 3;\\ \text{low, if } OPZ^{CIF}=1;\\ \text{critical, if } OPZ^{CIF}=0.\end{cases} \quad (28)$$

Thus, the proposed approach is understandable to an average person, allows one to intuitively understand the main critical points of CIF, possibilities of a terrorist attack on them, as well as necessary preventive measures, in conditions of minimizing the financial support of the information security system.

6. Discussion of the results of research on developing a concept of building a security system for critical infrastructure facilities

To assess the likelihood of a terrorist attack and the readiness of protective measures, sets of weighted metrics were determined, which acquire a value in the range of [0; 1]. Each metric characterizes the degree of compliance of a certain attribute of a terrorist-perpetrator or protective agent with a given target value.

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

$$G_{\text{terror}}^{\text{ES CIF}}=\left\{L_i^{del},\beta_i^{C}\quad\in\left\{\beta_{\text{terror}}^{\text{ES CIF}}\right\},p_{rj},r_{\text{motiv}},T\right\}. \quad (29)$$

To describe the set of characteristics, we use the index h: $G_h^{CPS\ CIF}$, where $\left(\{h\}_i^{G_h^{CPS\ CIF}}\right)$.

Let j be the security services for both ICS and CPS. Basic security services: *C*; *I*; *A*; *Au*, *Aff*. Thus, the tuple of security services j={*C*; *I*; *A*; *Au*, *Aff*} is formed. Let i denote the current attacker's number $\left(\{i\}_i^{L}\right)$, k – the current number of the expert who performed the assessment $\left(\{k\}_i^{K}\right)$,

L – the number of attackers,

K – the number of experts,

w_{kih}^{j} – the k-th expert estimate for the h-th characteristic of the i-th attacker for the j-th security service.

Then the average estimate of all experts for the entire set of characteristics of all attackers for the j-th security service is as follows:

$$w^{PS\_CIF\_j} = \frac{1_j}{KLGG_h^{CPS\ CIF}} \sum_{k=1}^{K} \sum_{i=1}^{L} \sum_{h=1}^{G_h^{CPS\ CIF}} \gamma_{ki}^{C} {}_h \times w_{kih}, \quad (30)$$

where $\gamma_{ki}^{PS\ CIF\ j}{}_h$ is the weight factor of the h-th metric of the i-th attacker for the j-th service. Normalization of weight factors: $\sum_{k=1}^{K} \sum_{i=1}^{L} \sum_{h=1}^{G_h^{CPS\ CIF}} = 1.$

The level of CIF security can be described in a similar way. To do this, we use the set of characteristics $B=\{$*cryptographic resistance*, strength of ISS mechanisms (C_r), key data amount (K_{da}), complexity of direct and reverse cryptographic transformation (*encryption/decryption of data*, O_{ED})$\}$. Thus, we have a set of ISS characteristics: $B=\{C_r, K_{da}, O_{ED}\}$. To describe the set of characteristics, we use the index g: B_g, where $\left(\{g\}_i^B\right)$. Let w_{kg}^j be the value of the k-th expert's estimate of the g-th characteristic of the ISS mechanism for the j-th security service in the case when the system security and the destructive actions of attackers are independent.

Then the average value of all experts' estimates of implementation of protective measures for the j-th security service is as follows:

$$\psi^j = \frac{1}{KB} \sum_{k=1}^{K} \sum_{g=1}^{B} \left(\beta_{kg}^j \times w_{kg}^j\right), \quad (31)$$

where β_{kg}^j is the weight factor of the g-th metric of the j-th security service for the k-th expert. Normalization of weight factors: $\sum_{k=1}^{K} \sum_{g=1}^{B} \beta_{kg}^j = 1.$

To correlate between the probability of a terrorist attack and the system security characteristics, that is, between the sets $G_{\text{terror}}^{CFS\ CIF}$ and B, we use the matrix M of size $\left[G_{\text{terror}}^{CFS\ CIF} \times B\right]$, sometimes referred to as a pairwise comparison matrix. If the g-th security characteristic B_g 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/attacker category is not completely closed. Thus, $\|M_{hg}\|$ is the matrix of factors connecting the threats/attacker categories with the protective measures of the security system.

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

$$\left\|w_{kg}^j\right\|_{cor} = \left\|M_{hg} \times w_{kg}^j\right\|. \quad (32)$$

Then

$$\psi^j = \frac{1}{KB} \sum_{k=1}^{K} \sum_{g=1}^{B} \left(\beta_{kg}^j \times \left\|w_{kg}^j\right\|_{cor}\right). \quad (33)$$

Expansion of the classifier due to the introduction of economic indicators of the cost of attack/terrorist act and the cost of countermeasures provides an integrated estimate of system security in relative units. Thus, 1 corresponds to the maximum security provided by the security system as a whole, and 0 corresponds to a situation where the security system does not protect any of the resources. An additional indicator can be an integrated indicator of the quality of service of an information and communication network, proposed in [109]. To increase the level of security (basic security services), it is proposed to use post-quantum algorithms based on crypto-code stuctrures proposed in [110–114]. The proposed mechanisms provide the required stability (2^{30}–2^{35} group operations), efficiency (the speed of cryptographic transformations is comparable to BSC) and re liability (P_{err} 10^{-9}–10^{-12}) in the face of growing computing resources.

To assess the current state of IS, complexes of systems for detecting attacks/deviations from normal operation and risk assessment methods are commonly used (Fig. 7), which allow qualitative and/or quantitative assessment of the current state of IS.

Table 3 shows a comparative assessment with the proposed approach, which not only unifies the mathematical tool for IS assessment, but also significantly simplifies its implementation, taking into account the minimization of financial costs for IS.

The analysis of Table 3 and Fig. 7 showed the lack of a single approach for assessing the current state. Each of the presented ones consists of a complex of systems and methods that do not have a unified threat classification approach. As a rule, open databases are used, such as KDD-99, CAPEC, CVE, which contain more than a million threats without appropriate classification, which largely does not allow for their prompt analysis. In addition, threats are not classified by security mechanisms, which makes it impossible to take into account their integration, synergy and hybridity, which does not allow for the objectivity of their assessment and possible damage. The methods do not allow determining the relationship between threats, information resources, communication channels between the CIF elements, determining critical points, between threats and information security means, which makes it possible to determine preventive protection measures in a timely manner. None of the considered systems and methods allows determining the attacker's characteristics and capabilities by threats, which greatly increases the risk of unauthorized penetration/hacking of the information security system.

The presented conceptual framework, together with the proposed mathematical tool, allows forming a unified base based on the classifier, taking into account the direction of attack vectors, assessing the possibilities of their synergy and hybridity, which allows taking preventive measures in a timely manner, assessing the attacker, and determining his capabilities.

Based on the proposed models, the requirements for computing resources to assess the current state of information security are significantly reduced, taking into account the national and international regulatory requirements. This approach will allow a self-assessment of the information security state, forming preventive measures and ISS based on the analysis of critical points in the CIF elements, taking into account the relevant relationships. The main limitations of the proposed approach are the formation of a unified base of threats, their assessment by cybersecurity and/or information security experts. To ensure objectivity, practical implementation is required, followed by testing in one of the CIF areas, which will provide a practical component and optimize the formation of preventive measures based on the proposed concept.

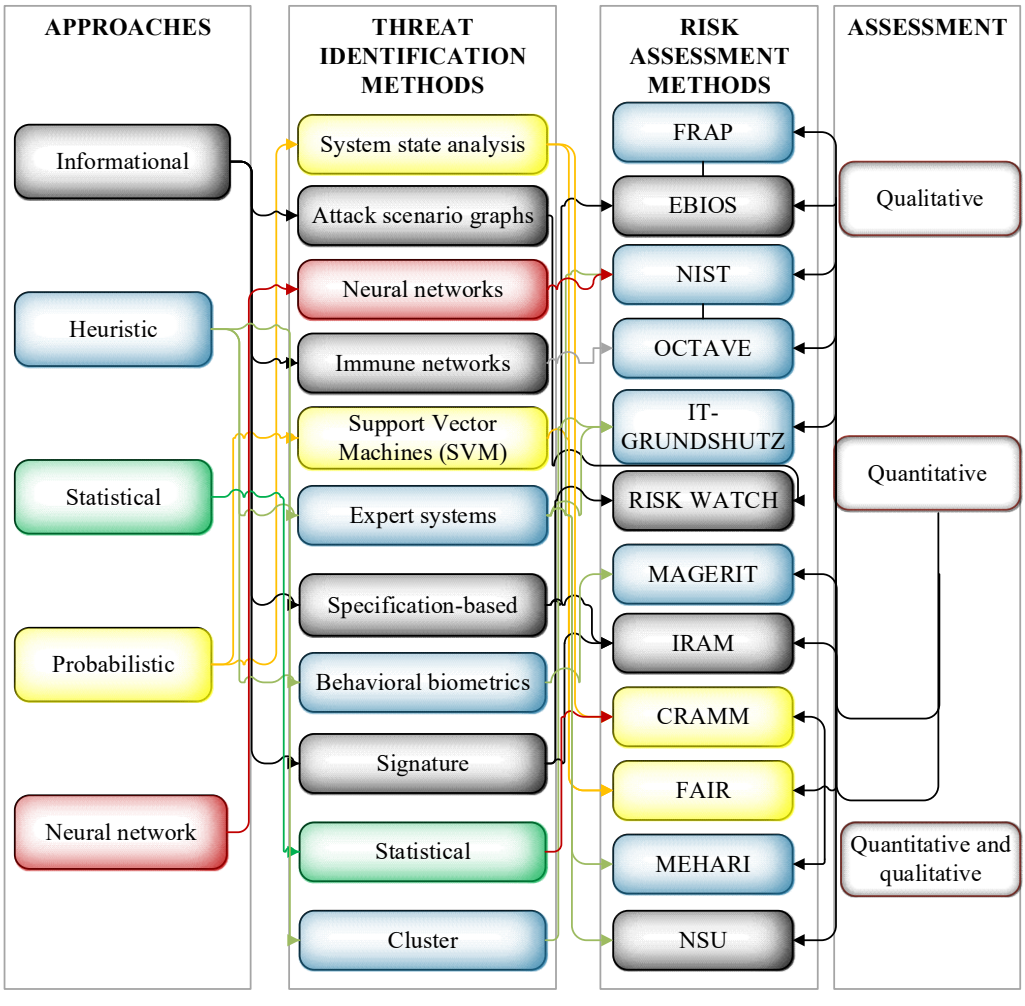

Fig. 7. Relationship between attack detection and risk assessment methods

Table 3

Results of the study of risk assessment methods

Method	Criteria								
	qualitative assessment	quantitative assessment	comprehensive assessment	assessment of threat characteristics		economic optimization	assessment of compliance with regulatory standards	effectiveness of preventive measures	ease of understanding
				hybridity	synergy				
NIST	+	–	–	–	–	–	–	–	–
FAIR		–	+	–	–	–		+	+
EBIOS	+		–	–	–	–	–	+	–
MEHARI		–	+	–		–	–	–	–
OCTAVE	+	–	–	–	–	–	–	–	–
IT-GRUND-SHULTZ	+	–	–	–	–	–	–	+	–
IRAM	+	–	–	–	–	–	–	–	+/–
RISK WATCH	–	+	–	–	–	–		+	+
FRAP	+	–	–	–	–	–	–	–	–
CRAMM			+	–	–	–	–	+/–	+/–
MAGERIT	+	+	–	–	–	–	–	–	–
Proposed method	+	+	+	+	+	+	+	+/–	+

7. Conclusions

1. The basic concepts related to cyber-terrorist attacks on critical infrastructure facilities were identified and formalized. Definitions of the security of information resources of critical infrastructure facilities, basic mechanisms and procedures of building a security model for CIF IR on the basis of a synergistic approach were developed. Security characteristics of critical infrastructure facilities such as availability, integrity, confidentiality and security are detailed. The definitions served as the basis for solving subsequent problems. A threat classifier was developed, which allows systemizing threats, forming a unified base of CIF threats, determining the synergistic effect and hybridity of threats, their impact not only on security components, but also on the infrastructure elements of CIF. This approach makes it possible not only to form preventive measures, but also to determine the terrorist-perpetrator's capabilities.

2. The concept of modeling the structure and functioning of the security system of critical infrastructure facilities was developed. The concept is based on a variety of models of different classes and levels currently used to model both critical infrastructures and the implementation of various threats on critical infrastructure facilities. The basic models of the modeling concept are as follows: economic, system-dynamic, behavioral game-theoretic, graph and network, agent-based, physical and geospatial.

3. Models of a terrorist act and security of the critical infrastructure facility cybersystem were developed. It is proposed to assess the integrated (echelon) security of a critical infrastructure facility on the basis of the hierarchical structure of the synthesis of security systems, Internet technologies and computer networks with information security tools based on mobile technologies. This approach allows forming a synergistic model of threats to critical infrastructure facilities, taking into account the impact of terrorists on the elements. A method for determining the terrorist-perpetrator category was developed based on analyzing the table of the relationship between the terrorist-perpetrator category and infrastructure elements. This allows pre-determining the category of the attacker by the impact on CIF and his ability to conduct a terrorist attack. An analysis of the CIF infrastructure level and terrorist-perpetrator categories allows forming a set of levels of impact on CIF. Based on the proposed method, a list of critical threats is determined for each attacker category.

4. A concept for assessing the security of critical infrastructure facilities was developed. The assessment is based on an approach to forming a synergistic threat model, attacker categories, their goals and capabilities. The CIF security estimate obtained as a result of the audit allows determining the most valuable information assets and effectiveness of protection means. The solutions make it possible to assess the compliance of the CIF ISS with the regulatory security requirements, identify the most vulnerable spots and develop recommendations for increasing the CIF security.

References

1. (U//FOUO) Leftwing Extremists Likely to Increase Use of Cyber Attacks over the Coming Decade (2016). Washington: Department of Homeland Security. Available at: https://fas.org/irp/eprint/leftwing.pdf
2. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hans, A. (2015). Guide to Industrial Control Systems (ICS) Security. National Institute of Standard and Technology. Available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
3. Stoddart, K. (2016). UK cyber security and critical national infrastructure protection. International Affairs, 92 (5), 1079–1105. doi: http://doi.org/10.1111/1468-2346.12706
4. Konstantas, J. (2016, April 19). Dam Hackers! The Rising Risks to ICS and SCADA Environments. Security Week. Available at: http://www.securityweek.com/dam-hackers-rising-risks-ics-and-scada-environments
5. Westervelt, R. (2012). Old Application Vulnerabilities, Misconfigurations Continue to Haunt. TechTarget. Available at: https://searchsecurity.techtarget.com/
6. Ashford, W. (2014). Industrial control systems: What are the security challenges? Computer Weekly. Available at: http://www.computerweekly.com/news/2240232680/Industrial-control-systems-What-are-the-security-challenges
7. Schneider, J., Obermeier, S., Schlegal, R. (2015). Cyber Security maintenance for SCADA systems. 15 Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research, 89–94. doi: http://doi.org/10.14236/ewic/ics2015.10
8. Russon, M. (2016). How hackers could cripple the UK: Doomsday infrastructure cyber attacks would cost country £442bn. International Business Times. Available at: http://www.ibtimes.co.uk/how-hackers-could-cripple-uk-critical-infrastructure-cyberattacks-would-cost-country-442bn-1554509
9. Fjäder, C. (2014). The nation-state, national security and resilience in the age of globalisation. Resilience, 2 (2), 114–129. doi: http://doi.org/10.1080/21693293.2014.914771
10. Holt, T. J., Bossler, A. M., Seigfried-Spellar, K. C. (2015). Cybercrime And Digital Forensics: An Introduction. New York: Routledge, 500. doi: http://doi.org/10.4324/9781315777870
11. Charlton, C. (2017). Armchair Warriors: Terrifying new generation of 'cybernative' ISIS terrorists could target 'Facebook and West's energy grids' in a bid to cause mass panic and mayhem. The Sun. Available at: https://www.thesun.co.uk/news/2643688/cyber-terrorism-attacks-threat-level-isis-facebook-energy/
12. Denning, D. E. (2000). Cyber terrorism: The Logic Bomb versus the Truck Bomb. Global Dialogue, 2 (4), 29–37.
13. Shmatko, O., Balakireva, S., Vlasov, A., Zagorodna, N., Korol, O., Milov, O. et. al. (2020). Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 3 (9 (105)), 6–19. doi: http://doi.org/10.15587/1729-4061.2020.205702

14. Hryshchuk, R., Yevseiev, S., Shmatko, A. (2018). Construction methodology of information security system of banking information in automated banking systems. Vienna: Premier Publishing s. r. o., 284. doi: http://doi.org/10.29013/r.hryshchuk_s.yevseiev_a.shmatko.cmissbiabs.284.2018
15. Kondratov, S., Bobro, D., Horbulin, V. et. al.; Sukhodolia, O. (Ed.) (2017). Developing The Critical Infrastructure Protection System in Ukraine. Kyiv: NISS, 184.
16. Marsh, R. T. (Ed.) (1997). Critical Infrastructures: Protecting America's Infrastructures. United States Government Printing Office. Report of the President's Commission on Critical Infrastructure Protection. Washington.
17. Abele-Wigert, I., Dunn, M., Wenger, A., Mauer, V. (Eds.) (2006). International CIIP Handbook 2006: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies. Center for Security Studies. Vol. I. ETH Zurich. Zurich, 495.
18. Dunn, M., Mauer, V., Abele-Wigert, I. (Eds.) (2006). Ineternational CIIP Handbook 2006: Analyz- ing Issues, Challenges, and Prospects. Center for Security Studies. Vol. II. ETH Zurich. Zurich, 238.
19. Assaf, D. (2008). Models of critical information infrastructure protection. International Journal of Critical Infrastructure Protection, 1, 6–14. doi: http://doi.org/10.1016/j.ijcip.2008.08.004
20. Lagadec, P.(1981). La Civilisation du Risque: Catastrophes Technologiques et Responsabilite´ Sociale. Science Ouverte. Paris: E´ditions du Seuil, 21.
21. Beck, U. (1986). Risikogesellschaft: Auf dem Weg in eine andere Moderne. Frankfurt: Suhrkamp.
22. Perrow, C. (1984). Normal Accidents: Living with High-Risk Technologies. New York: Basic Books, 386.
23. Rinaldi, S. M., Peerenboom, J. P., Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems, 21 (6), 11–25. doi: http://doi.org/10.1109/37.969131
24. Casalicchio, E., Galli, E., Tucci, S.; Setola, R., Geretshuber, S. (Eds.) (2009). Modeling and Simulation of Complex Interdependent Systems: A Federated Agent-Based Approach. CRITIS 2008. LNCS. Heidelberg: Springer, 5508, 72–83. doi: http://doi.org/10.1007/978-3-642-03552-4_7
25. Haimes, Y. Y., Jiang, P. (2001). Leontief-Based Model of Risk in Complex Interconnected Infrastructures. Journal of Infrastructure Systems, 7 (1), 1–12. doi: http://doi.org/10.1061/(asce)1076-0342(2001)7:1(1)
26. Haimes, Y. Y., Horowitz, B. M., Lambert, J. H., Santos, J. R., Lian, C., Crowther, K. G. (2005). Inoperability Input-Output Model for Interdependent Infrastructure Sectors. I: Theory and Methodology. Journal of Infrastructure Systems, 11 (2), 67–79. doi: http://doi.org/10.1061/(asce)1076-0342(2005)11:2(67)
27. Santos, J. R., Haimes, Y. Y. (2004). Modeling the Demand Reduction Input Output (I O) Inoperability Due to Terrorism of Interconnected Infrastructures*. Risk Analysis, 24 (6), 1437–1451. doi: http://doi.org/10.1111/j.0272-4332.2004.00540.x
28. Haimes, Y. Y., Horowitz, B. M., Lambert, J. H., Santos, J., Crowther, K., Lian, C. (2005). Inoperability Input-Output Model for Interdependent Infrastructure Sectors. II: Case Studies. Journal of Infrastructure Systems, 11 (2), 80–92. doi: http://doi.org/10.1061/(asce)1076-0342(2005)11:2(80)
29. Setola, R.; Goetz, E., Shenoi, S. (Eds.) (2007). Analysis of Interdependencies Between Italy's Economic Sectors. Critical Infrastructure Protection: Proceedings of the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection. IFIP. Springer: Hanover, 253, 311–321. doi: http://doi.org/10.1007/978-0-387-75462-8_22
30. Andrijcic, E., Horowitz, B. (2006). A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property. Risk Analysis, 26 (4), 907–923. doi: http://doi.org/10.1111/j.1539-6924.2006.00787.x
31. Haimes, Y. Y., Chittester, C. G. (2005). A Roadmap for Quantifying the Efficacy of Risk Management of Information Security and Interdependent SCADA Systems. Journal of Homeland Security and Emergency Management, 2 (2). doi: http://doi.org/10.2202/1547-7355.1117
32. Crowther, K. G. (2008). Decentralized risk management for strategic preparedness of critical infrastructure through decomposition of the inoperability input–output model. International Journal of Critical Infrastructure Protection, 1, 53–67. doi: http://doi.org/10.1016/j.ijcip.2008.08.009
33. Tanaka, H. (2009). Quantitative Analysis of Information Security Interdependency between Industrial Sectors. Proceedings of the 3rd International Symposium on Empirical Software Engineering and Measurement (ESEM 2009). Lake Buena Vista: IEEE Computer Society Press, 574–583. doi: http://doi.org/10.1109/esem.2009.5314218
34. Lian, C., Haimes, Y. Y. (2006). Managing the risk of terrorism to interdependent infrastructure systems through the dynamic inoperability input–output model. Systems Engineering, 9 (3), 241–258. doi: http://doi.org/10.1002/sys.20051
35. Barker, K., Santos, J. R. (2010). Measuring the efficacy of inventory with a dynamic input–output model. International Journal of Production Economics, 126 (1), 130–143. doi: http://doi.org/10.1016/j.ijpe.2009.08.011
36. Santos, J. R. (2008). Interdependency analysis with multiple probabilistic sector inputs. Journal of Industrial & Management Optimization, 4 (3), 489–510. doi: http://doi.org/10.3934/jimo.2008.4.489
37. Jung, J. (2009). Probabilistic Extension to the Inoperability Input-Output Model: P-IIM. Charlottesville: University of Virginia.
38. Santos, J. R., Haimes, Y. Y., Lian, C. (2007). A Framework for Linking Cybersecurity Metrics to the Modeling of Macroeconomic Interdependencies. Risk Analysis, 27 (5), 1283–1297. doi: http://doi.org/10.1111/j.1539-6924.2007.00957.x
39. Nieuwenhuijs, A., Luiijf, E., Klaver, M.; Papa, M., Shenoi, S. (Eds.) (2008). Modeling Dependencies In Critical Infrastructures. Critical Infrastructure Protection II: Proceedings of the Second Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection. IFIP. Heidelberg: Springer, 290, 205–213. doi: http://doi.org/10.1007/978-0-387-88523-0_15

40. Rosato, V., Issacharoff, L., Tiriticco, F., Meloni, S., Porcellinis, S. D., Setola, R. (2008). Modelling interdependent infrastructures using interacting dynamical models. International Journal of Critical Infrastructures, 4 (1/2), 63–79. doi: http://doi.org/10.1504/ijcis.2008.016092
41. Panzieri, S., Setola, R. (2008). Failures propagation in critical interdependent infrastructures. International Journal of Modelling, Identification and Control, 3 (1), 69–78. doi: http://doi.org/10.1504/ijmic.2008.018186
42. Oliva, G., Panzieri, S., Setola, R. (2010). Agent-based input-output interdependency model. International Journal of Critical Infrastructure Protection, 3(2), 76–82. doi: http://doi.org/10.1016/j.ijcip.2010.05.001
43. Rinaldi, S. M. (2004). Modeling and Simulating Critical Infrastructures and Their Interdependencies. Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS 2004). Big Island: IEEE Computer Society Press, 1–8. doi: http://doi.org/10.1109/hicss.2004.1265180
44. Forrester, J. W. (1961). Industrial Dynamics. Waltham: Pegasus Communications, 480.
45. Forrester, J. W. (1961). Principles of Systems. Waltham: Pegasus Communications.
46. Gonzalez, J. J., Sarriegi, J. M., Gurrutxaga, A.; Lo pez, J. (Ed.). A Framework for Conceptualizing Social Engineering Attacks. CRITIS 2006. LNCS. Heidelberg: Springer, 4347, 79–90. doi: http://doi.org/10.1007/11962977_7
47. Sarriegi, J. M., Santos, J., Torres, J. M., Imizcoz, D., Egozcue, E., Liberal, D.: Lopez, J., Hammerli, B. M. (Eds.) (2008). Modeling and Simulating Information Security Management. CRITIS 2007. LNCS. Heidelberg: Springer, 5141, 327–336. doi: http://doi.org/10.1007/978-3-540-89173-4_27
48. Pasqualini, D., Witkowski, M. S., Klare, P. C., Patelli, P., Cleland, C. A.; Gro ler, A., Rouwette, E. A. J. A., Langer, R. S., Rowe, J. I., Yanni, J. M. (Eds.) (2006). A Model for a Water Potable Distribution System and its Impacts resulting from a Water Contamination Scenario. Proceedings of the 24th International Conference of the System Dynamics Society. Nijmegen: Wiley, 99–100.
49. Bush, B. B., Dauelsberg, L. R., LeClaire, R. J., Powell, D. R., DeLand, S. M., Samsa, M. E. (2005). Critical Infrastructure Protection Decision Support System (CIP/DSS) Project Overview. Tech. Rep. LA-UR-05-1870. Los Alamos: Los Alamos National Laboratory.
50. LeClaire, R., Bush, B., Dauelsberg, L., Powell, D.; Sterman, J. D., Repenning, N. P., Langer, R. S., Rowe, J. I., Yanni, J. M. (Eds.) (2005). Critical Infrastructure Protection Decision Support System. Proceedings of the 23rd International Conference of the System Dynamics Society. Boston: System Dynamics Society, 97.
51. Dauelsberg, L., Outkin, A.; Sterman, J. D., Repenning, N. P., Langer, R. S., Rowe, J. I., Yanni, J. M. (Eds.) (2005). Modeling Economic Impacts to Critical Infrastructures in a System Dynamics Framework. Proceedings of the 23rd International Conference of the System Dynamics Society. Boston: System Dynamics Society, 63.
52. LeClaire, R., O'Reilly, G.; Sterman, J. D., Repenning, N. P., Langer, R. S., Rowe, J. I., Yanni, J. M. (Eds.) (2005). Leveraging a High Fidelity Switched Network Model to Inform a System Dynamics Model of the Telecommunications Infrastructure. Proceedings of the 23rd In- ternational Conference of the System Dynamics Society. Boston: System Dynamics Society, 97.
53. Min, H.-S. J., Beyeler, W., Brown, T., Son, Y. J., Jones, A. T. (2007). Toward modeling and simulation of critical national infrastructure interdependencies. IIE Transactions, 39 (1), 57–71. doi: http://doi.org/10.1080/07408170600940005
54. United States Department of Commerce, National Institute of Standards and Technology, Computer Systems Laboratory: Integration Definition for Function Modeling (IDEF0) (1993). United States Draft Federal Information Standard, 183.
55. Berard, C. (2010). Group Model Building Using System Dynamics: An Analysis of Methodological Frameworks. Electronic Journal of Business Research Methods, 8 (1), 35–45.
56. Hernantes, J., Lauge, A., Labaka, L., Rich, E. H., Sveen, F. O., Sarriegi, J. M. et. al. (2011). Collaborative Modeling of Awareness in Critical Infrastructure Protection. Proceedings of the 44th Hawaii International International Conference on Systems Science (HICSS-44 2011). Koloa: IEEE Press. doi: http://doi.org/10.1109/hicss.2011.113
57. Bier, V. M., Ferson, S., Haimes, Y. Y., Lambert, J. H., Small, M. J. (2004). Risk of Extreme and Rare Events: Lessons from a Selection of Approaches. Risk Analysis and Society: An Interdisciplinary Characterization of the Field. Cambridge: Cambridge University Press, 74–118. doi: http://doi.org/10.1017/cbo9780511814662.004
58. Bier, V. M. (2001). Game Theoretic Models for Critical Infrastructure Protection. Risk Analysis in an Interconnected World.
59. von Neumann, J., Morgenstern, O. (1947). Theory of Games and Economic Behavior. Princeton: Princeton University Press.
60. Fudenberg, D., Tirole, J. (1991). Game Theory. Cambridge: MIT Press.
61. Osborne, M. J., Rubinstein, A. (1994). A Course in Game Theory. Cambridge: MIT Press.
62. Branzel, R., Dimitrov, D., Tijs, S. (2008). Models in Cooperative Game Theory. Heidelberg: Springer. doi: http://doi.org/10.1007/978-3-540-77954-4
63. Haywood, O. G. (1954). Military Decision and Game Theory. Journal of the Operations Research Society of America, 2(4), 365–385. doi: http://doi.org/10.1287/opre.2.4.365]
64. Hamilton, T., Mesic, R. (2004). A Simple Game-Theoretic Approach to Suppression of Enemy Defenses and Other Time Critical Target Analyses. Santa Monica. doi: http://doi.org/10.7249/rb108
65. Brams, S., Kilgour, M. D. (1988). Game Theory and National Security. Oxford: Basil Blackwell, 199.
66. Burke, D.A. (1999). Towards a Game Theory Model of Information Warfare. Air Force Institute of Technology, Wright-Patterson Air Force Base.
67. Major, J. A. (2002). Advanced Techniques for Modeling Terrorism Risk. The Journal of Risk Finance, 4 (1), 15–24. doi: http://doi.org/10.1108/eb022950

68. Sandler, T., Arce, D. G. (2003). Terrorism & Game Theory. Simulation & Gaming, 34 (3), 319–337. doi: http://doi.org/10.1177/1046878103255492
69. Sandler, T., Siqueira, K. (2008). Games and Terrorism. Simulation & Gaming, 40 (2), 164–192. doi: http://doi.org/10.1177/1046878108314772
70. Liu, D., Wang, X., Camp, J. (2008). Game-theoretic modeling and analysis of insider threats. International Journal of Critical Infrastructure Protection, 1, 75–80. doi: http://doi.org/10.1016/j.ijcip.2008.08.001
71. Jenelius, E., Westin, J., Holmgren, Å. J. (2010). Critical infrastructure protection under imperfect attacker perception. International Journal of Critical Infrastructure Protection, 3 (1), 16–26. doi: http://doi.org/10.1016/j.ijcip.2009.10.002
72. Yoshida, M., Kobayashi, K. (2010). Disclosure Strategies for Critical Infrastructure against Terror Attacks. Proceedings of the 2010 IEEE International Conference on Systems Man and Cybernetics (SMC 2010). Istanbul: IEEE Press, 3194–3199. doi: http://doi.org/10.1109/icsmc.2010.5642277
73. Lakdawalla, D.N., Zanjani, G. (2004). Insurance, Self-Protection, and the Economics of Terrorism. Tech. Rep. WR-171-ICJ, RAND Corporation. Santa Monica.
74. Woo, G. (2002). Quantitative Terrorism Risk Assessment. The Journal of Risk Finance, 4 (1), 7–14. doi: http://doi.org/10.1108/eb022949
75. Bier, V., Oliveros, S., Samuelson, L. (2007). Choosing What to Protect: Strategic Defensive Allocation against an Unknown Attacker. Journal of Public Economic Theory, 9 (4), 563–587. doi: http://doi.org/10.1111/j.1467-9779.2007.00320.x
76. Bolloba´s, B. (1998). Modern Graph Theory. Graduate Texts in Mathematics. Vol. 184. Berlin: Springer.
77. Bolloba´s, B., Kozma, R., Miklo´s, D. (Eds.) (2008). Handbook of Large-Scale Random Networks. Bolyai Society Mathematical Studies. Vol. 18. Budapest: Ja´nos Bolyai Mathematical Society and Springer. doi: http://doi.org/10.1007/978-3-540-69395-6
78. Barabási, A.-L., Albert, R. (1999). Emergence of Scaling in Random Networks. Science, 286 (5439), 509–512. doi: http://doi.org/10.1126/science.286.5439.509
79. Albert, R., Barabási, A.-L. (2002). Statistical mechanics of complex networks. Reviews of Modern Physics, 74 (1), 47–97. doi: http://doi.org/10.1103/revmodphys.74.47
80. Newman, M. E. J. (2003). The Structure and Function of Complex Networks. SIAM Review, 45 (2), 167–256. doi: http://doi.org/10.1137/s003614450342480
81. Newman, M., Baraba´si, A. L., Watts, D. J. (Eds.) (2006). The Structure and Dynamics of Networks. Princeton Studies in Complexity. Princeton: Princeton University Press, 592.
82. Flaxman, A. D., Frieze, A. M., Vera, J. (2007). Adversarial Deletion in a Scale-Free Random Graph Process. Combinatorics, Probability and Computing, 16 (2), 261–270. doi: http://doi.org/10.1017/s0963548306007681
83. Albert, R., Jeong, H., Barab si, A.-L. (2000). Error and attack tolerance of complex networks. Nature, 406 (6794), 378–382. doi: http://doi.org/10.1038/35019019
84. Cohen, R., Erez, K., ben-Avraham, D., Havlin, S. (2001). Breakdown of the Internet under Intentional Attack. Physical Review Letters, 86 (16), 3682–3685. doi: http://doi.org/10.1103/physrevlett.86.3682
85. Motter, A. E., Lai, Y.-C. (2002). Cascade-based attacks on complex networks. Physical Review E, 66 (6), 378–382. doi: http://doi.org/10.1103/physreve.66.065102
86. Wang, X., Guan, S., Heng Lai, C. (2009). Protecting infrastructure networks from cost-based attacks. New Journal of Physics, 11 (3), 033006. doi: http://doi.org/10.1088/1367-2630/11/3/033006
87. Borgatti, S. P. (2005). Centrality and network flow. Social Networks, 27 (1), 55–71. doi: http://doi.org/10.1016/j.socnet.2004.11.008
88. Barton, D. C., Stamber, K. L. (2000). An Agent-Based Microsimulation of Critical Infrastructure Systems. Tech. Rep. SAND2000-0808C. Sandia National Laboratories. Albuquerque.
89. North, M.; Sallach, D., Wolsko, T. (Eds.) (2000). Agent-Based Modeling of Complex Infrastructures. Proceedings of the Workshop on Simulation of Social Agents: Architectures and Institutions. ANL/DIS/TM-60. Chicago: University of Chicago and Argonne National Laboratory, 239–250.
90. Panzieri, S., Setola, R., Ulivi, G. (2004). An Agent Based Simulator for Critical Interdependent Infrastructures. Proceedings of the 2nd International Conference on Critical Infrastructures (CRIS 2004). Grenoble.
91. Balducelli, C., Bologna, S., Pietro, A. D., Vicoli, G. (2005). Analysing interdependencies of critical infrastructures using agent discrete event simulation. International Journal of Emergency Management, 2 (4), 306–318. doi: http://doi.org/10.1504/ijem.2005.008742
92. Porcellinis, S. D., Setola, R., Panzieri, S., Ulivi, G. (2008). Simulation of heterogeneous and interdependent critical infrastructures. International Journal of Critical Infrastructures, 4 (1/2), 110–128. doi: http://doi.org/10.1504/ijcis.2008.016095
93. Dudenhoeffer, D. D., Permann, M. R., Manic, M. (2006). CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis. Proceedings of the 2006 Winter Simulation Conference (WSC 2006). Phoenix: IEEE Press, 478. doi: http://doi.org/10.1109/wsc.2006.323119
94. Dudenhoeffer, D. D., Permann, M. R., Sussman, E. M. (2002). A Parallel Simulation Framework for Infrastructure Modeling and Analysis. Proceedings of the 34th Winter Simulation Conference (WSC 2002). San Diego: IEEE Press, 1971. doi: http://doi.org/10.1109/wsc.2002.1166498

95. Zhu, G.-Y., Henson, M. A., Megan, L. (2001). Dynamic modeling and linear model predictive control of gas pipeline networks. Journal of Process Control, 11 (2), 129–148. doi: http://doi.org/10.1016/s0959-1524(00)00044-5
96. Han, Z. Y., Weng, W. G. (2010). An integrated quantitative risk analysis method for natural gas pipeline network. Journal of Loss Prevention in the Process Industries, 23 (3), 428–436. doi: http://doi.org/10.1016/j.jlp.2010.02.003
97. Wolthusen, S. D. (2005). GIS-based Command and Control Infrastructure for Critical Infrastructure Protection. Proceedings of the First IEEE International Workshop on Critical Infrastructure Protection (IWCIP 2005), 40–47. doi: http://doi.org/10.1109/iwcip.2005.12
98. Patterson, S. A., Apostolakis, G. E. (2007). Identification of critical locations across multiple infrastructures for terrorist actions. Reliability Engineering & System Safety, 92 (9), 1183–1203. doi: http://doi.org/10.1016/j.ress.2006.08.004
99. Yevseiev, S., Korolyov, R., Tkachov, A., Laptiev, O., Opirskyy, I., Soloviova, O. (2020). Modification of the algorithm (OFM) S-box, which provides increasing crypto resistance in the post-quantum period. International Journal of Advanced Trends in Computer Science and Engineering, 9(5), 8725–8729. doi:10.30534/ijatcse/2020/261952020
100. Barabash, O., Laptiev, O., Kovtun, O., Leshchenko, O., Dukhnovska, K., Biehun, A. (2020). The Method dynavic TF-IDF. International Journal of Emerging Trends in Engineering Research, 8 (9), 5712–5718. doi: http://doi.org/10.30534/ijeter/2020/130892020
101. Barabash, O., Laptiev, O., Tkachev, V., Maystrov, O., Krasikov, O., Polovinkin, I. (2020). The Indirect method of obtaining Estimates of the Parameters of Radio Signals of covert means of obtaining Information. International Journal of Emerging Trends in Engineering Research, 8 (8), 4133–4139. doi: http://doi.org/10.30534/ijeter/2020/17882020
102. Savchenko, V., Ilin, O., Hnidenko, N., Tkachenko, O., Laptiev, O., Lehominova, S. (2020). Detection of Slow DDoS Attacks based on User's Behavior Forecasting. International Journal of Emerging Trends in Engineering Research, 8 (5), 2019–2025. doi: http://doi.org/10.30534/ijeter/2020/90852020
103. Berkman, L., Barabash, O., Tkachenko, O., Musienko, A., Laptiev, O., Salanda, I. (2020). The Intelligent Control System for infocommunication networks. International Journal of Emerging Trends in Engineering Research, 8 (5), 1920–1925. doi: http://doi.org/10.30534/ijeter/2020/73852020
104. Laptiev, O., Shuklin, G., Hohonianc, S., Zidan, A., Salanda, I. (2019). Dynamic model of Ceber Defence Diagnostics of information Systems with the Use of Fozzy Technologies IEEE ATIT 2019 Conference Proceedings. Kyiv, 116–120. doi: http://doi.org/10.1109/atit49449.2019.9030465
105. Laptiev, O., Stefurak, O., Polovinkin, I., Barabash, O., Savchenko, V., Zelikovska, O. (2020). The method of improving the signal detection quality by accounting for interference. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings. Kyiv, 172–176.
106. Laptiev, O., Savchenko, V., Yevseiev, S., Haidur, H., Gakhov, S., Hohoniants, S. (2020). The new method for detecting signals of means of covert obtaining information. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings. Kyiv, 176–181.
107. Sobchuk, V., Pichkur, V., Barabash, O., Laptiev O., Kovalchuk, I., Zidan, A. (2020). Algorithm of control of functionally stable manufacturing processes of enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings. Kyiv, 206–211.
108. Savchenko, V., Laptiev, O., Kolos O., Lisnevskyi R., Ivannikova V., Ablazov, I. (2020). Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings Kyiv, 246–251.
109. Yevseiev, S., Ponomarenko, V., Ponomarenko, V., Rayevnyeva, O., Rayevnyeva, O. (2017). Assessment of functional efficiency of a corporate scientificeducational network based on the comprehensive indicators of quality of service. Eastern-European Journal of Enterprise Technologies, 6 (2 (90)), 4–15. doi: http://doi.org/10.15587/1729-4061.2017.118329
110. Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S. et. al. (2018). Practical implementation of the Niederreiter modified cryptocode system on truncated elliptic codes. Eastern-European Journal of Enterprise Technologies, 6 (4 (96)), 24–31. doi: http://doi.org/10.15587/1729-4061.2018.150903
111. Yevseiev, S., Tsyhanenko, O., Gavrilova, A., Guzhva, V., Milov, O., Moskalenko, V. et. al. (2019). Development of Niederreiter hybrid crypto-code structure on flawed codes. Eastern-European Journal of Enterprise Technologies, 1 (9 (97)), 27–38. doi: http://doi.org/10.15587/1729-4061.2019.156620
112. Tsyhanenko, O., Yevseiev, S., Milevskyi, S. (2019). Using the Flawed Codes In Niederreiter Crypto-Code Structure. Short Paper Proceedings of the 1st International Conference on Intellectual Systems and Information Technologies (ISIT 2019). Odessa, 17–19.
113. Yevseiev, S., Kots, H., Minukhin, S., Korol, O., Kholodkova, A. (2017). The development of the method of multifactor authentication based on hybrid cryptocode constructions on defective codes. Eastern-European Journal of Enterprise Technologies, 5 (9 (89)), 19–35. doi: http://doi.org/10.15587/1729-4061.2017.109879
114. Yevseiev, S., Korol, O., Kots, H. (2017). Construction of hybrid security systems based on the crypto-code structures and flawed codes. Eastern-European Journal of Enterprise Technologies, 4 (9 (88)), 4–21. doi: http://doi.org/10.15587/1729-4061.2017.108461