The object of this study is the process of ensuring the security of cyber-physical systems under the influence of external destructive factors, in particular information, radio-electronic, and physical attacks aimed at disrupting continuous system operation. The paper addresses the problem of determining the optimal structure of an airborne mobile network within a cyber-physical system, specifically the ratio between operational and protective elements that ensures maximum system stability under targeted attacks. The presented modeling results are based on a minimax formulation of the interaction between the system and the external environment, which makes it possible to determine critical threshold values of stability parameters.

The applied mathematical model describes both the optimal strategy of the attacking environment and the optimal initial structure of the system itself. This enables the identification of relationships between the initial ratio of operational and protective components and the minimum adversary resources required for complete system destruction. It is shown that an optimal configuration of protective elements forces the attacking environment to expend 1.5–2 times more resources compared to suboptimal structures. A correctly selected ratio of system elements slows down the degradation of the protective contour. The developed mathematical model confirms the existence of an optimal strategy for external environment behavior and an optimal initial structure of the airborne mobile network of the cyber-physical system. This approach improves the design process of cyber-physical systems at early stages, enhances their survivability, and contributes to the development of a methodology for integrated protection of airborne mobile networks under challenging real-world conditions

Keywords: cyber-physical systems, unmanned aerial vehicles, mobile wireless network, protective elements

UDC 004.056
DOI: 10.15587/1729-4061.2025.345894

DEVELOPMENT OF A SECURITY SYSTEM ORGANIZATION MODEL TAKING INTO ACCOUNT THE IMPACT OF THE EXTERNAL ENVIRONMENT

Nataliia Dzheniuk
Doctor of Philosophy (PhD), Associate Professor
Department of Information Systems Named after V. O. Kravets*
Viktor Zaika
Doctor of Technical Sciences, Professor
Department of Telecommunication Systems
State University of Information and Communication Technologies
Solomyanska str., 7, Kyiv, Ukraine, 03110
Serhii Yevseiev
Corresponding author
Doctor of Technical Sciences, Professor, Head of Department
Department of Cybersecurity*
E-mail: Serhii.Yevseiev@gmail.com
Yevhen Tarasenko
Department of Information Systems Named after V. O. Kravets*
Artem Moskalenko
PhD
Department Computer Sciences and Software Engineering
International Scientific and Technical University named after academician Yury Buga
Khersonsky lane, 3, Kyiv, Ukraine, 02094
Vitalii Kryvosheiev
PhD, Associate Professor
Department of Command Control
State Military Management Institute**
Serhii Kravchenko
PhD, Associate Professor
Department of Land Forces**
Serhii Holdobin
Senior Lecturer
Department of Information and Communication Systems Security
National Academy of the Security Service of Ukraine
Mykhaila Maksymovycha str., 22, Kyiv, Ukraine, 03066
Artur Ismahilov
PhD Student***
Ihor Syvachenko
PhD Student***
*National Technical University "Kharkiv Polytechnic Institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002
**National Defence University of Ukraine
Povitryanich Sil ave., 28, Kyiv, Ukraine, 03049
***Institute of Software Systems of the National Academy of Sciences of Ukraine
Akademika Glushkova ave., 40, Kyiv, Ukraine, 03187

Received 29.09.2025
Received in revised form 17.11.2025
Accepted date 05.12.2025
Published date 30.12.2025

How to Cite: *Dzheniuk, N., Zaika, V., Yevseiev, S., Tarasenko, Y., Moskalenko, A., Kryvosheiev, V., Kravchenko, S., Holdobin,S., Ismahilov, A., Syvachenko, I. (2025). Development of a security system organization model taking into account the impact of the external environment. Eastern-European Journal of Enterprise Technologies, 6 (9 (138)), 114–124. https://doi.org/10.15587/1729-4061.2025.345894*

1. Introduction

Cyber-physical systems (CPS) represent a significant challenge in critical application domains such as aviation, transportation, defense, and autonomous robotic platforms. This complexity is further amplified when CPS incorporate unmanned aerial vehicles (UAVs). Such systems operate in dynamic environments, depend on sensor data, software,

and wireless communication channels, and function under real-time constraints.

Although many CPS analysis methods and design tools exist, their underlying models are typically developed from a single perspective. The ability to semantically reconcile multiple perspectives remains limited. In practice, assumptions made by one viewpoint about others are often not formalized, and even when they are, they are usually processed manually. As a result, current design approaches overly restrict the range of viable system solutions, highlighting the need for methods and tools that can formally integrate point-of-view models with corresponding analysis results [1, 2]. Traditional approaches, such as encryption, authentication, and integrity checking, do not ensure sufficient resilience against combined cyber and radio-electronic attacks. The vulnerability of UAVs is further increased by their autonomy, reliance on navigation signals, multi-channel positioning systems, and software components.

In particular, ongoing research in CPS that accounts for the influence of the external environment, interference characteristics, attacker capabilities, and available attacking resources can be grouped into several directions. These include studies focused on enhancing communication channel resilience, multilevel protection models, approaches to predicting system behavior under attack, methods for optimizing the structure of hybrid mobile networks, and resource reservation strategies.

All these directions demonstrate that cybersecurity is becoming an increasingly interdisciplinary domain encompassing multiple aspects. This underscores the necessity of a comprehensive approach to modeling and designing CPS protection mechanisms [3].

Key technologies for CPS development are closely associated with transdisciplinary technologies [4, 5] that integrate the physical and information worlds. However, CPS design remains a highly complex task. First, CPS are inherently complex due to network heterogeneity and the intricacy of software and hardware components, and there are currently no effective design approaches that systematically address these issues in a unified manner. Second, insufficient attention has been given to integrated design-stage methodologies for CPS, and no practical approaches to unified cyberspace modeling have yet been established.

The challenges associated with modeling realistic interference conditions, along with the growing vulnerability of radio-electronic and software components embedded directly within UAV platforms, remain highly relevant. This reinforces the need to develop a general mathematical model that describes the interaction between the external environment and the system itself.

2. Literature review and problem statement

Cyber-physical systems (CPS) are complex distributed systems controlled by computer algorithms that execute computational processes within a distributed environment using feedback mechanisms. In [6], the authors emphasize that CPS are closely related to widely used concepts such as the Internet of Things (IoT), Industry 4.0, the Industrial Internet, and unmanned aerial vehicles (UAVs). All of these rely on technologies that tightly integrate the physical and information worlds. Work [6] introduces the concepts of precision-timed processors (PRET) and programming temporally integrated distributed embedded systems (Ptides), which leverage emerging trends to create predictable and synchronized systems with well-defined temporal boundaries. These principles can be adapted for the design of mobile CPS, where precise time coordination between nodes enhances communication stability under interference and ensures controllability in the event of partial channel loss. CPS are described as systems that integrate computational resources into physical objects, thereby linking the physical and information domains and addressing the intellectual challenge of combining engineering solutions across these two worlds. A limitation of the temporal model presented in [6] is that, while effective in controlled environments, its application to hybrid systems with large numbers of nodes and stochastic delays lacks validated scaling methods.

The formation of CPS gives rise to insecure hybrid systems, which significantly complicates achieving the required level of security. A major security challenge in CPS is the reliance on wireless mobile data transmission channels between sensors and the switching infrastructure of the cyber-physical system. Work [7] examines CPS architectures, various attack types – including those targeting availability, integrity, and confidentiality – and methods for their detection and mitigation. Its key strengths lie in a systematic, multi-level approach to CPS modeling that encompasses both time-driven and event-driven systems. This framework enables the analysis of hybrid network architectures in which processes such as Discrete Event Systems (DES) are combined with continuous models, allowing for more accurate representation of CPS behavior when mobile sensor networks are involved. However, despite its focus on practical security considerations, most of the proposed models remain largely theoretical and are based on linear time-invariant (LTI) assumptions, which are poorly aligned with the inherently nonlinear nature of mobile wireless systems. Moreover, the study does not address inter-network interactions, such as the integration of Wi-Fi, 5G/6G, and ad hoc technologies, which form the foundation of modern CPS.

The existence of a complex set of UAV control tools and potential vulnerabilities in data transmission protocols, control software, data exchange, and navigation systems creates significant security threats to CPS. Paper [5] presents research results on ensuring the security of unmanned aerial vehicles, with a focus on cyber-physical and socio-cyber-physical systems. It analyzes UAV operation in transportation, energy, communications, and defense sectors and shows that the risks of control interception, navigation signal spoofing, and interference with automatic control systems are increasing. The main threat types to UAV control channels are identified, including spoofing, jamming, replay, man-in-the-middle, and command injection attacks. The study also examines how radio-electronic and cyber influences can be combined to form complex hybrid attacks. It is noted that widely used protection mechanisms – such as encryption, authentication, and integrity control – do not provide an adequate level of security when the physical layer of the network is affected or when targeted radio jamming is employed. The problem of building an integrated protection system that accounts for both the overall CPS architecture and the specific operational characteristics of airborne components remains unresolved. One possible solution is the development of a combined protection system that considers optimal interaction among different cyber-physical subsystems.

In [8], an overview of UAV control methods is presented, with particular attention given to modern approaches, key challenges, and prospective directions for further development. The strength of this work lies in its comprehensive and systematic analysis of various UAV control techniques. It provides a detailed discussion of issues related to hybrid systems, unexpected disturbances, and insecure wireless channels in CPS, emphasizing the importance of considering external factors and noise to ensure interference resilience. However, the proposed control methods are primarily focused on autonomous flight control and system stability under environmental influences. Less attention is devoted to encryption, authentication, and protection of network connections in mobile hybrid structures. In addition, the paper does not provide practical algorithms or schemes for ensuring continuous network operation under severe radio interference conditions.

Within the context of Industry 4.0 development, identifying optimal strategies for external environment behavior and designing critical infrastructure protection systems that reflect the complexity and dynamism of cyber-physical systems becomes particularly important. This issue is addressed in [9], where a universal threat classifier and an attacker behavior model are proposed, taking into account the hybrid and synergistic nature of attacks. One of the main strengths of this work is the extensive use of multidisciplinary models – economic, dynamic, agent-based, and game-theoretic – which capture complex interdependencies within the infrastructure and enable a comprehensive security assessment. The adoption of a multi-level protection framework incorporating Internet technologies, computer networks, and mobile solutions enhances the flexibility and scalability of the security system. Nevertheless, the work places greater emphasis on general concepts and modeling, while specific wireless communication technologies for hybrid mobile CPS networks are insufficiently detailed.

Paper [10] introduces the concept of a cyber-physical universe – a network of interconnected devices, systems, and infrastructures that integrate physical and digital components. It demonstrates that treating cyber and physical entities as a unified system enables the identification of patterns and a deeper understanding of the dynamics of modern complex systems. This concept is identified as an important step toward advancing approaches for complex system analysis. Real-time integration of data from sensors, devices, and digital networks makes it possible to model system behavior and more thoroughly analyze its properties. The paper proposes an integrated approach that combines data analytics, machine learning, and artificial intelligence to process large volumes of information generated within the cyber-physical universe. This enables the detection of hidden patterns, trend forecasting, and optimization of system operation in domains such as smart cities, transportation, healthcare, and industrial automation. At the same time, significant attention is given to confidentiality, security, and ethical challenges, which require a comprehensive approach that aligns technical solutions with social, political, and legal requirements. Hybrid wireless mobile communication networks operating within CPS must ensure stability and security under conditions of external interference and targeted attacks. The high dynamism of such networks – especially those involving aerial platforms and unmanned aerial vehicles – makes them particularly vulnerable to functional disruption and communication channel compromise.

Work [11] highlights the wide range of threats present in IoT environments, which is directly relevant to CPS, as socio-cyber-physical systems inherently integrate heterogeneous sensor networks and mobile nodes. A key strength of this work is its detailed classification of attacks across all layers of the IoT architecture, from the physical layer to the application layer. This classification can be effectively extended to mobile and wireless CPS segments, including UAV-based networks. However, several limitations exist with respect to mobile hybrid CPS networks. The analysis in [11] is largely based on static or low-mobility topologies, whereas CPS require support for wireless mobility, rapid topology changes, varying antenna characteristics, and dynamic communication channels – especially in UAV applications. In addition, the work does not address hybrid attack scenarios that combine radio-frequency interference, spoofing, manipulation of AI components, and cyberattacks on routing protocols, even though such multi-vector attacks largely determine the real threat level in CPS.

Based on this analysis, it can be concluded that issues related to reducing vulnerabilities in radio-electronic and software components remain insufficiently studied in the context of cyber-physical systems and their security assurance. This is largely due to the fact that modern cyber-physical and socio-cyber-physical systems are complex hybrid structures that integrate mobile wireless networks, sensor nodes, artificial intelligence components, and aerial platforms, significantly complicating both modeling and protection.

Developing a security system capable of ensuring controllability, stability, and continuity of UAV operation under interference conditions is therefore an urgent challenge. Addressing this problem requires the development of a security model that enables an integrated consideration of CPS architecture, threat characteristics, and radio-electronic influence. Such a model would support effective resource planning during both the development and operational phases of cyber-physical systems involving UAVs. In addition, it should enable a well-founded design of protection architectures that account for multi-contour infrastructure layouts and the diversity of CPS construction technologies in use.

3. The aim and objectives of the study

The aim of the study is to develop a mathematical model of the organization of the security system of a cyber-physical system, which allows determining the optimal ratio of working and protective elements of an air mobile network. This will make it possible to increase the stability and survivability of cyber-physical systems at the early stages of design.

To achieve this aim, the following objectives were accomplished:

– to determine the structural and functional relationships between the working, protective and communication elements of the CPS;

– to verify the model by numerical modeling and graphical analysis of the dependencies of the minimum attacker resource required for a complete system disruption.

4. Materials and methods

The object of this study is the process of ensuring the security of cyber-physical systems under the influence of external destructive factors, including information, radio-electronic, and physical attacks aimed at disrupting the continuous operation of the system.

The research hypothesis is that the stability and uninterrupted functioning of cyber-physical systems can be ensured through the construction of an optimal security system structure. The proposed model takes into account the interaction between the control components of unmanned aerial vehicles and the external environment, which determines the balance between offensive and defensive actions. It is assumed that an optimal initial ratio of functional and protective elements enables the efficient allocation of security resources.

Since the effectiveness of the optimal ratio of security elements depends not only on the internal parameters of the model but also on the nature of system interaction with a dynamic external environment, it is necessary to analyze specific network structures that implement such interactions in practice. Particular attention should be paid to networks characterized by high mobility, distributed interaction, and strong dependence on radio communication channels, as these systems are the most sensitive to environmental changes and destructive influences [7]. In this context, hybrid airborne networks are of particular interest, as they represent one of the most complex classes of cyber-physical systems.

This study examines a typical cyber-physical system with an architecture in which hardware, software, and communication components interact to support real-time task execution. The central element of the system is an unmanned aerial vehicle equipped with hardware and software modules. The external security perimeter is represented by cloud technologies, servers, intelligent platform management systems, and other elements of cyber infrastructure. Within the system, an internal security contour operates, based on physical, software, and hardware smart technologies (Fig. 1). Communication between system components is ensured by wireless protocols, while the communication layer connects the UAV to the smart technology platform. The toolset of such a system enables multi-vector interaction between physical and cyber components, forming a unified cyber-physical space for data acquisition, analysis, and distribution, which necessitates an appropriate level of security [12, 13].

The basis of the hybrid wireless network is the airborne mobile peer-to-peer network FANET (Flying Ad Hoc Network) [14], which is a set of UAVs, each of which is equipped with its own switching module and functions as an element of a cyber-physical system. Through communication channels, these devices interact with each other, with ground control points and mobile base stations, forming a multi-level data exchange structure typical of cyber-physical systems. The integration of individual devices into the FANET network turns it into a complex dynamic system operating under conditions of significant a priori uncertainty. Its behavior is influenced by interactions between the external environment and the system itself, including radio-electronic, cybernetic and physical factors that determine the overall stability and efficiency of the network.

The defining condition for reliable and continuous operation of modern cyber-physical systems is ensuring protection and resistance to external influences. Existing approaches to providing protection use various mechanisms, but due to the complexity of the threat spectrum, the use of radio channels in environments with a high level of interference, and the use of UAVs in the network infrastructure, their effectiveness is reduced (Fig. 2).

Architectural approaches to security emphasize multi-layered protection, system segmentation to isolate critical components, reduction of the attack surface, and incident localization, as well as the application of the zero-trust principle. Multi-layered protection is achieved by introducing several independent security layers, ensuring that the compromise of a single layer does not lead to failure of the entire system. Segmentation and zoning make it possible to separate critical subsystems from the common information space, thereby limiting the propagation of attacks and facilitating incident containment. The zero-trust principle assumes continuous authentication, authorization, and verification of all requests, regardless of their origin. For critical infrastructures, systems are designed with redundancy, disaster recovery mechanisms, and uninterrupted operation as core requirements, which is especially important in environments characterized by high levels of interference.

Technical security solutions are primarily aimed at protecting communication channels and network devices. The key mechanisms include cryptographic protection and authentication, which ensure secure data transmission through protocols such as IPsec and TLS, as well as device and user authentication based on public key infrastructure (PKI). In the context of unmanned aerial vehicles, particular emphasis is placed on securing control and telemetry channels. Software-defined networking (SDN) technologies are employed to implement flexible security policies, dynamically redirect traffic during attacks, and support the deployment of intrusion detection and prevention systems (IDS/IPS) and firewalls. These technical solutions make it possible to maintain the required level of quality of service (QoS) and network redundancy, which is essential for the reliable transmission of critical service and control traffic.

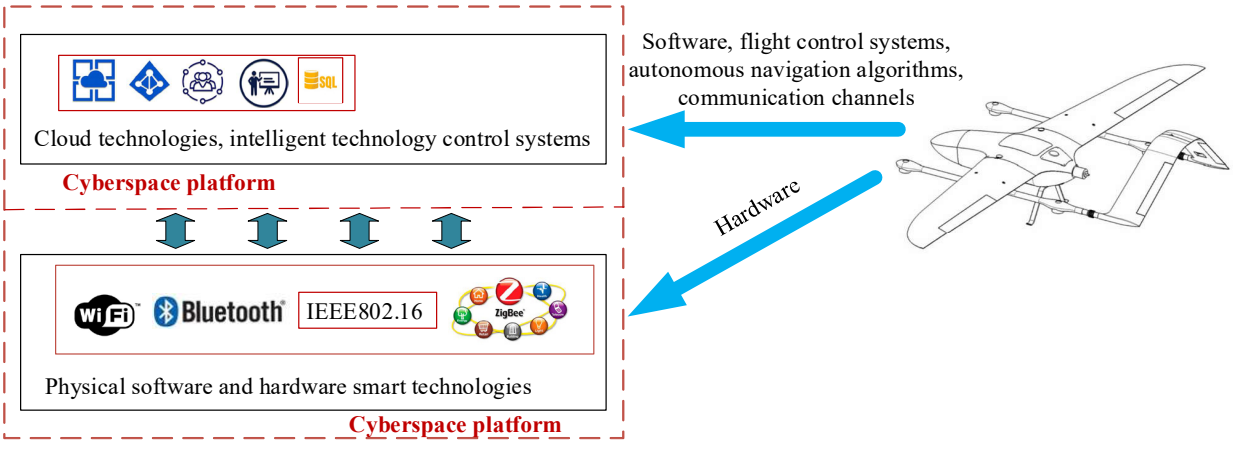

Fig. 1. Cyber-physical system with UAV elements

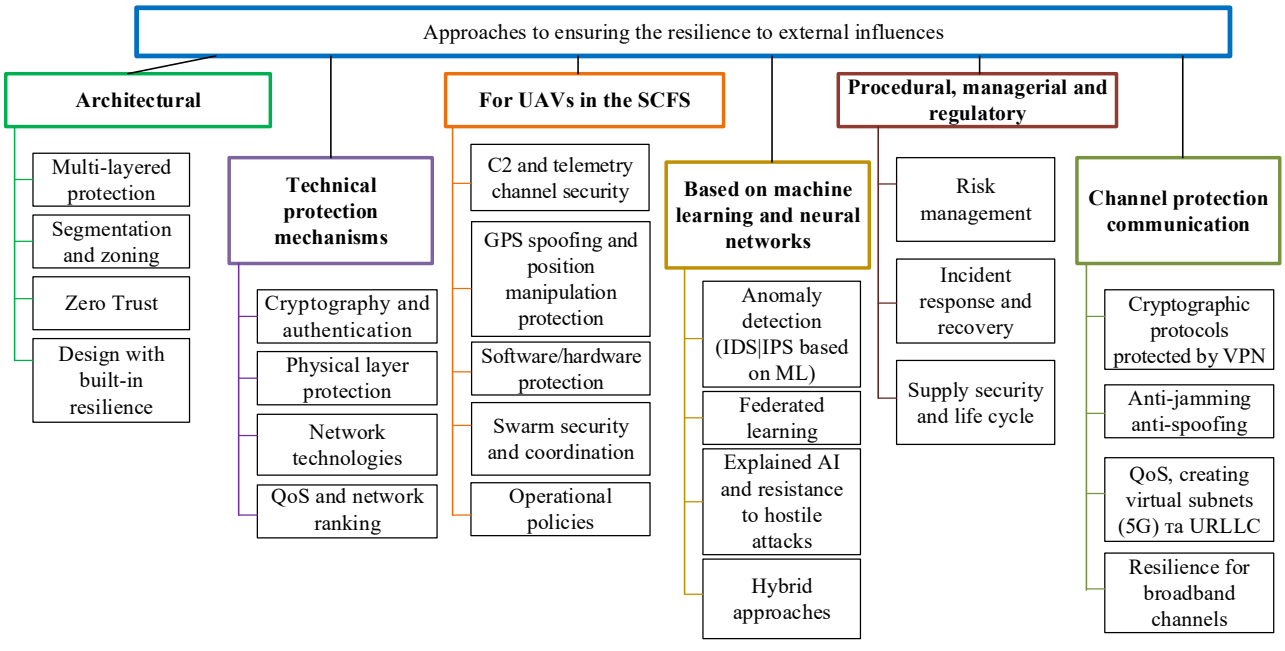

Fig. 2. Approaches to ensuring the resilience of cyber-physical systems to external influences

Approaches aimed at securing UAVs as elements of cyber-physical systems focus primarily on protecting control channels, navigation subsystems, and onboard software. These approaches employ command authentication, cryptographic encryption, and digital signatures to prevent control substitution, spoofing, or interception. The use of firmware integrity verification mechanisms and secure key storage areas increases the resilience of both software and hardware components. For coordinated UAV groups and swarms, solutions include mutual participant authentication, mechanisms to mitigate the compromise of individual nodes, and the use of secure communication and key-exchange protocols to ensure reliable and trusted interaction.

Approaches based on machine learning and neural networks are particularly effective under conditions of complex system behavior and dynamically evolving threats. They enable the detection of anomalous network traffic and atypical device behavior, as well as the identification of distorted input data and compromised training samples. Hybrid approaches that combine physical process models with machine learning techniques make it possible to reduce false-positive rates and improve the overall reliability of decision-making in security systems.

Procedural, managerial, and regulatory approaches define the rules, processes, and requirements necessary for the safe operation of cyber-physical infrastructures. The application of international and industry standards makes it possible to systematically assess threats, determine risk levels, and implement appropriate protective measures throughout the system life cycle.

Despite the availability of effective countermeasures, significant risks remain. These are largely related to the decentralized nature of UAV control and the difficulty of managing flight dynamics in real time. This necessitates a more detailed analysis of the technical characteristics of such systems, as they directly determine the feasibility of complex and combined attack scenarios. When analyzing the operation of aerial networks, it is therefore essential to consider the capability of UAVs to perform autonomous motion along predetermined trajectories in real time. At the same time, the presence of sophisticated control tools and numerous potential vulnerabilities in communication protocols, control software, and navigation systems creates additional conditions for compromising the entire CPS. The most critical security threats are associated with wireless communication and control channels, as well as vulnerabilities in radio-electronic equipment and onboard software components.

An analysis of existing approaches shows that most solutions focus on protecting individual system elements, such as communication channels, UAV platforms, or information resources in isolation. They do not sufficiently account for the complex interaction between working and protective elements of the system under external threat conditions. Consequently, the development of a comprehensive model for organizing the security system is an urgent and scientifically justified task. Solving this problem will make it possible to substantiate the optimal structure of the security system at the early stages of cyber-physical system design, thereby significantly increasing its overall resilience and survivability.

In the developed mathematical model of the organization of the security system, it is assumed that the working and protective elements of the cyber-physical system are evenly distributed in space, and their number decreases over time without the possibility of resource replenishment. The external environment is assumed to have a fixed supply of attacking elements that act independently of each other and are fully consumed by the end of the interaction interval.

The probability of defeat of any system element is assumed to be identical and depends solely on the number of protective components present at the time of impact. It is further assumed that all changes in the system structure occur only at the beginning and at the end of the interaction interval. This assumption makes it possible to preserve the spatial uniformity of system elements. An additional simplification is that the probability-of-defeat function is differentiable.

The initial data used for modeling are typical and are formed based on the general characteristics of the cyber-physical system and the effects of the external environment. The initial number of working elements is determined by the typical CPS structure and reflects the key functional

components of the system. The number of protective elements is also specified as a typical initial characteristic, but it may vary, since it is used to study the optimal ratio between working and protective elements. The supply of attacking elements is treated as a fixed external resource that is not replenished and is completely exhausted before the end of the interaction period. The modeling interval and the time discretization step are defined as standard conditions necessary for a unified and consistent description of the interaction process between the system and the external environment.

To simulate the mathematical model of the security system, software implemented in C# within the .NET SDK 7.0 environment was used. To export the simulation results to Microsoft Excel, the ClosedXML library (a standard NuGet package) was employed. This library enables the creation and modification of Excel files in XLSX format based on the OpenXML standard and internally relies on the DocumentFormat.OpenXml library.

5. Results of developing a model for organizing a security system taking into account the influence of the external environment

5. 1. Determination of structural and functional relationships between working, protective and communication elements of the CPS, taking into account the influence of the external environment

Each cyber-physical system (CPS) is characterized by a specific structure and corresponding behavioral properties. The structure is defined by the number and types of interconnected elements, while behavior reflects the system's response to destabilizing influences from the external environment, in particular to the actions of functional damage agents. The behavior of the system is aimed at preserving continuity of operation under adverse conditions.

System survivability is understood as its ability to effectively counteract negative external influences. Traditionally, an increase in survivability is achieved through the introduction of structural redundancy, including duplication of critical functional elements and the incorporation of highly reliable protective components. Under such conditions, both working and protective elements of the system may be subjected to the impact of functional damage agents. The role of protective elements is to neutralize or reduce the intensity of destructive external effects [15].

To ensure the most effective compensation of external destructive influences, it is necessary to determine the optimal ratio between protective and working elements of the CPS.

Consider a system S with structure $|S|$, behavior $\overline{S}$ and behavior strategy of the external environment $\overline{Z}$. At any time t, the system has $K_w(t)$ working (w) and $K_d(t)$ protective (d) elements. All elements have ε-uniform placement in the system. This means that in the sphere of radius ε, which is completely located in the system S, there will be a constant number of $YK_w(0)$ working and $YK_d(0)$ protective elements. The coefficient Y is defined as $Y = v_0 / V$, V is the volume occupied by the system S; v_0 is the volume defined by the sphere of radius ε.

It is assumed that the probability of falling under the influence of destructive actions of attacking (z) elements of the external environment for all elements of the system S is the same. The time of unfavorable interaction of the external environment and the system S is limited by the interval $[0, T]$. The external environment has a supply of z-elements, which is not replenished. Its quantity is $L(0)$ pieces, which is completely spent on the system S by the time $t = T$. Thus, the number of z-elements $L(t)$ does not increase over time and at the time T is equal to 0. It is assumed that the time interval $[0, T]$ of the system's interaction with the external environment is divided into $k = T / h$ subintervals ($h > 0$).

The number of z-elements $L(t)$ consists of the sum of the number of z-elements $L_w(t)$, which are spent on damage to the working elements of the system, and the number of z-elements $L_d(t)$, which are spent on damage to the protective elements of this system

$$L(t) = L_w(t) + L_d(t); \quad t = 0, h, ..., ih. \tag{1}$$

For the working (w) and protective (d) elements of the system S, the following number of z-elements is consumed at time intervals $(t, t + h)$:

$$l_w(t) = L_w(t) - L_w(t+h);$$

$$l_d(t) = L_d(t) - L_d(t+h). \tag{2}$$

At time $t + h$, the number of elements w and d in an arbitrary sphere of radius e inside the system S depends only on the number of elements w, d, and z in this sphere at time t. Portions of elements of the external environment $l_w(t)$ and $l_d(t)$ for each of the intervals t=0, h, $2h$, ..., kh e-uniformly complement the system S.

It is assumed that the appearance of the z-element at time t activates the protective mechanisms of all protective elements of the system S, which are located in the ε-environment. If these protective actions are effective, the corresponding element continues to work. If the protection does not work, the element fails. But the z-element itself in any case definitely fails.

System S does not receive new elements during the entire period of interaction with the external environment, therefore, over time, the working and protective elements of the system S gradually and evenly decrease. It is assumed that the system S fails if by the time t the number of its elements decreases below a certain critical threshold w_0, $K_w(t) \le Y_w K_w(0)$. If $K_w(t) > Y_w K_w(0)$, the system continues to function. Y_w is a fixed value $0 \le Y_w \le 1$ and is determined by the features of a particular system S.

It is assumed that if the system S contains $K_d(t)$ of protective elements, then the probability of damage to any of its elements (working or protective) at time t under the influence of one z-element of the external environment is $p[K_d(t)]$.

The redistribution of the working and protective elements of the system under the influence of z-elements occurs only at the beginning and end of the considered time interval, while the uniformity of the arrangement of elements in the system remains unchanged. The structure of the system $|S|$ at time t is determined only by the strategy of the external environment behavior $z = \{l_w(t), l_d(t)\}$ and the initial configuration of the system, i.e. the initial ratio of the number of protective and working elements $|S| = (K_w(0), K_d(0))$. In this case, the total initial number $L(0)$ of z-elements of the external environment is a function of the chosen environment strategy and the primary structure of the system $|S|$, on which this strategy affects

$$L(0) = L(\overline{z}, |S|) = f\left[l_w(t), l_d(t); K_w(0), K_d(0)\right]. \tag{3}$$

The optimal behavior of the external environment Z is the following behavior $\bar{Z}_{opt}$, at which it is achieved $\min_{\bar{Z}} L(0)$

$$\min_{\bar{Z}} L\left(\bar{Z},|S|\right)=L\left(\bar{Z}_{opt},|S|\right). \quad (4)$$

The optimal behavior of the external environment Z is the worst case of its action on the system S.

The structure of the system S tries to counteract the influence of the external environment and force it to spend as many of its z-elements as possible on its damage.

The optimal initial structure of the system S is such an initial structure $|S|^{opt}$ of the system S, due to which $\max_{|S|} L(0)$ is achieved with optimal behavior of the external environment

$$\max_{|S|} L(0)=\max_{|S|} L\left(\bar{Z}_{opt},|S|\right)=L\left(\bar{Z}_{opt},|S|_{opt}\right). \quad (5)$$

Determining the optimal initial structure of the CPS in the case when the external environment tries to damage the elements of the system, spending a minimum of its resources, is a task to increase the level of system protection. But the system, due to the optimal initial structure, must force the external environment to spend a maximum of its elements, which are necessary to influence the continuous operation of the system. A minimax problem arises in which the structure of the system is connected with the strategy of the external environment.

5. 2. Modeling and verification of a mathematical model of the security system organization taking into account the influence of the external environment

To solve the minimax problem, the time interval h = 1 is taken and the previous assumptions are taken into account. The number of elements of the external environment that must be spent on the destruction of the working and protective elements of the system is determined by the ratio

$$l_w(0)+l_w(1)+l_d(0)+l_d(1)=L(0), \quad (6)$$

where $L(0)$ – the total resource of the external environment, which is completely spent on the destruction of the system elements.

Taking into account the probability of failure of one working or protective element by one z-element and the uniform distribution of elements in the system, it is obtained that

$$l_w(0)p\left[K_d(0)\right]+l_w(1)p\left[K_d(1)\right]=\left(1-Y_w\right)K_w(0), \quad (7)$$

where

$$K_w(1)=K_w(0)-l_w(0)p\left[K_d(0)\right],$$

$$K_d(1)=K_d(0)-l_d(0)p\left[K_d(0)\right].$$

Under such conditions, the amount of external resource required to destroy the system's protective elements at the final moment of interaction with the external environment will be zero ($l_d(1)\equiv 0$), since by this moment all protective elements must be completely neutralized.

After determining what part of the resource, the external environment spends on destroying the system's working elements at the end of the time interval through the primary resource, the basic equation has the form

$$l_w(0)\left\{1-\frac{p\left[K_d(0)\right]}{p\left[K_d(1)\right]}\right\}+l_d(0)+\frac{\left(1-Y_w\right)K_w(0)}{p\left[K_d(1)\right]}=L(0). \quad (8)$$

The first component of the equation is always positive due to the fact that the probability of the previous event does not exceed the probability of the next $p[K_d(0)] \le p[K_d(1)]$ and increases with the increase in the resource that will be used to destroy the working elements $l_w(0)$. It cannot determine the minimum $L(0)$. Therefore $lw(0) \equiv 0$

$$l_d(0)+\frac{\left(1-Y_w\right)K_w(0)}{p\left[K_d(0)-l_d(0)p\left[K_d(0)\right]\right]}=L(0). \quad (9)$$

L_0 has a minimum depending on the number of protective elements $l_d(0)$. This is explained by the fact that with an increase in the number of protective elements, the first term in the ratio increases, while the second one decreases accordingly.

After assuming that the probability function of damage to a system element can be differentiated, the extreme value of $l_d^*(0)$ is found by differentiating the left-hand side of equation (9) with respect to $l_d(0)$ and comparing it with zero:

$$L'(0)=1+\frac{\left(1-Y_w\right)K_w(0)\cdot p'\left[K_d(1)\right]p\left[K_d(0)\right]}{p^2\left[K_d(1)\right]}=0,$$

$$-\frac{p^2\left[K_d(1)\right]}{p'\left[K_d(1)\right]p\left[K_d(0)\right]}=\left(1-Y_w\right)K_w(0). \quad (10)$$

The behavior of the external environment Z will be optimal $\bar{Z}_{opt}$ in case of:

$$l_w(0)\equiv l_d(1)\equiv 0,\ \ l_d(0)=l_d^*(0),$$

$$l_w(1)=l_w^*(1)=\frac{\left(1-Y_w\right)K_w(0)}{p\left\{K_d(0)-l_d^*(0)p\left[K_d(0)\right]\right\}}. \quad (11)$$

The optimal strategy of the external environment is compared with the suboptimal one and the relative gain in the number of attacking elements it spends is estimated. For this purpose, the suboptimal behavior of the environment $\bar{Z}_0$, is considered, in which the number of attacking elements aimed at defeating the protective elements of the system S is equal to the number used to defeat its working elements.

When the environment Z uses the $\bar{Z}_{opt}$ behavior instead of the $\bar{Z}_0$ behavior, the relative gain in the number of attacking elements

$$\gamma=1-\frac{L(0)}{\tilde{L}(0)}. \quad (12)$$

It is assumed that the attacking elements act independently of each other. And the probability of disabling one attacking element by one protective element is a constant value F. The appearance of an attacking z-element in the system causes protective actions $YK_d(t)$ of protective d-elements located in its ε-surroundings. The probability of disabling a protective d-element:

$$p\left[K_d(0)\right]=e^{-fK_d(0)},\quad p\left[K_d(t)\right]=-fe^{-fK_d(t)}, \quad (13)$$

where $f = Y\ln(1-F)^{-1}$ is the efficiency coefficient of the d-element.

After substituting these values into the basic equation, the relationship is obtained $f^{-1}e^{f[K_d(0)-K_d(t)]}=(1-Y)K_w(0)$. It allows to determine such an environmental strategy that minimizes the total destructive resource:

$$l_d^*(0)=f^{-1}e^{fK_d(0)}\ln f(1-Y)K_w(0),$$

$$l_w^*(1)=\frac{(1-Y)K_w(0)}{p[K_d(t)]}=(1-Y)K_w(0)e^{fK_d(t)}=f^{-1}e^{fK_w(0)}. \quad (14)$$

The minimum number of attacking z-elements $L(0)$ is

$$L^*(0)=l_w^*(1)+l_d^*(0)=f^{-1}e^{fK_d(0)}\ln fe(1-Y)K_w(0). \quad (15)$$

One of the practical cases is considered, for which it is assumed that the probability of disabling one attacking z-element by one d-element is equal to a constant value $F = 0.99$, and the coefficient $Y = 0.01$.

Fig. 3 shows the dependence of the minimum number of $L^*(0)$ elements on the ratio of the number of working $K_w(0)$ and protective $K_d(0)$ elements, and Table 1 shows the calculated data.

Table 1

Results of calculations of the number of z-elements $L^*(0)$ under conditions of optimal behavior of the external environment

$K_d(0)$ \ $K_w(0$	10	12	14	16	18	20
10	524	565	598	626	651	675
15	5234	5643	5972	6251	6510	6750
20	52259	56340	59624	62412	65000	67389
25	522039	562808	595622	623464	649317	673182
30	5214468	5621693	5949460	6227565	6485805	6724181

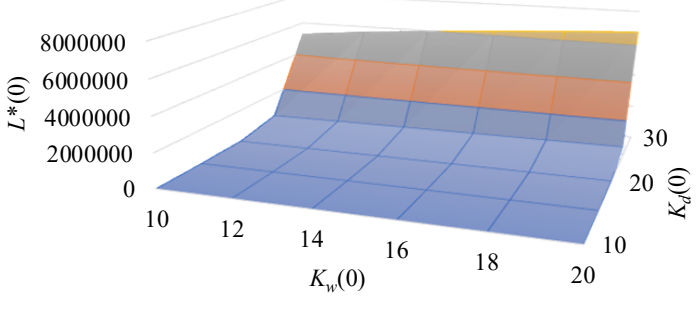

Fig. 3. Dependence of the number of elements of the external environment $L^*(0)$ on the number of working $K_w(0)$ and protective $K_d(0)$ elements of the system S under conditions of optimal behavior of the external environment

For a suboptimal external environment strategy, in which $l_d(0)=l_w(0)=\tilde{l}_d(0)$, taking into account the ratio:

$$K_w(1)=K_w(0)-l_w(0)p[K_d(0)],$$

$$K_d(1)=K_d(0)-l_d(0)p[K_d(0)]. \quad (16)$$

received

$$l_d(0)=\frac{(1-Y)K_w(0)}{P[K_d(1)]}=e^{fK_d(0)}(1-Y)K_w(0)e^{-fp[K_d(0)\tilde{l}_d(0)}. \quad (17)$$

Considering that $\ln(1 - Y)K_w(0) >> \ln fe$, and $\tilde{L}(0)=2\tilde{l}_d(0)$, received

$$\tilde{L}(0)=2f^{-1}e^{fK_d(0)}[dK_d(0)-\ln(1-Y)K_w(0)]. \quad (18)$$

Fig. 4 shows the dependence of the minimum number of $\tilde{L}(0)$ elements on the ratio of the number of working $K_w(0)$ and protective $K_d(0)$ elements, and Table 2 shows the calculated data.

Table 2

Results of calculations of the number of z-elements $\tilde{L}(0)$ under conditions of suboptimal behavior of the external environment

$K_d(0)$ \ $K_w(0)$	10	12	14	16	18	20
10	1039	961	896	836	784	736
15	20337	19558	18909	18303	17784	17308
20	302403	294626	288146	282098	276914	272162
25	4013436	3935756	3871024	3836499	3758820	3711349
30	50003272	49227359	48580765	47977277	47460002	46985834

In this case, the gain in the number of z-elements in comparing the optimal behavior of the external environment with the suboptimal one is

$$\gamma=1-\frac{L^*(0)}{\tilde{L}(0)}=1-\frac{1}{2}\frac{\ln(1-Y)K_w(0)}{1+fK_d(0)}. \quad (19)$$

Table 3 shows the results of calculating the gain from using optimal behavior of the external environment compared to suboptimal behavior, and Fig. 5 shows the corresponding dependencies.

From the analysis of the relation (19) it follows that the gain is always more than double, and increases significantly when $fK_d(0) >> \ln(1 - Y)K_w(0)$.

Table 3

Results of calculations of the gain in the number of z-elements under conditions of suboptimal and optimal behavior of the external environment

$K_d(0)$ \ $K_w(0)$	10	12	14	16	18	20
10	0.8	0.79	0.77	0.76	0.75	0.74
15	0.86	0.85	0.84	0.83	0.82	0.82
20	0.89	0.88	0.88	0.87	0.86	0.86
25	0.91	0.9	0.9	0.89	0.89	0.88
30	0.93	0.92	0.91	0.91	0.91	0.9

The analysis indicates that once the system S loses its protective elements, the effectiveness of the destructive actions of the external environment's attacking elements increases sharply. Therefore, the optimal strategy for the environment is to minimize the number of attacking elements required to disable system S. This strategy involves initially directing all available resources toward the destruction of the system's protective d-elements and only afterward targeting its working w-elements.

It is important to note that the number of working elements in system S is fixed and determined by its design specifications. In contrast, the number of protective elements can be selected to achieve an optimal balance between the system's structure and its capacity to withstand external influences.

When $G = fK_d(0) = \text{const}$, formula (15) takes the form

$$L(0)=\min L(\bar{Z},|S|)=$$
$$=G^{-1}K_d(0)e^G[\ln Ge(1-Y)K_w(0)-\ln K_d(0)]. \quad (20)$$

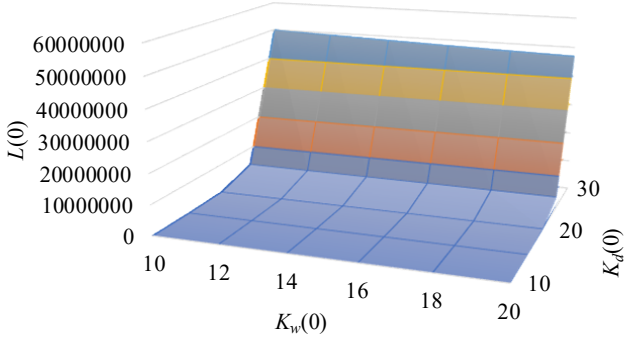

Fig. 4. Dependence of the number of elements of the external environment on the number of working $K_w(0)$ and protective $K_d(0)$ elements of the system S under conditions of suboptimal behavior of the external environment

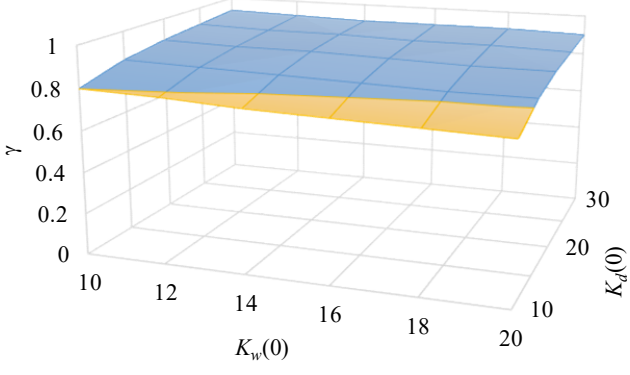

Fig. 5. Dependence of the gain γ on the number of elements of the external environment that are necessary to disable the system S

After differentiating relation (19) with respect to $K_d(0)$, a transcendental equation is obtained to determine $K_d^{**}(0)$

$$K_d^{**}(0)=\frac{G(1-Y)}{K_w(0)}. \quad (21)$$

In this case, the total number of attacking elements is determined by the ratio

$$L^{**}(0)=\max_{|S|}\min_{\bar{Z}} L(\bar{Z},|S|)=e^G(1-Y)K_w(0). \quad (22)$$

Table 4 shows the calculated data, and Fig. 5 shows the dependence of the number of $L^{**}(0)$ elements on the ratio of the number of working $K_w(0)$ and protective $K_d(0)$ elements for $F=0.99$, $Y=0.01$.

Table 4

Results of calculations of the number of z-elements $L^{**}(0)$ under conditions of optimal behavior of the external environment and optimal structure of the system

$K_d(0)$ \ $K_w(0)$	10	12	14	16	18	20
10	898	1077	1257	1437	1616	1796
15	8970	10764	12558	14352	16146	17940
20	89590	107508	125426	143344	161262	179180
25	894920	1073904	1252888	1431872	1610856	1789840
30	8939090	10726908	12514726	14302544	16090362	17878180

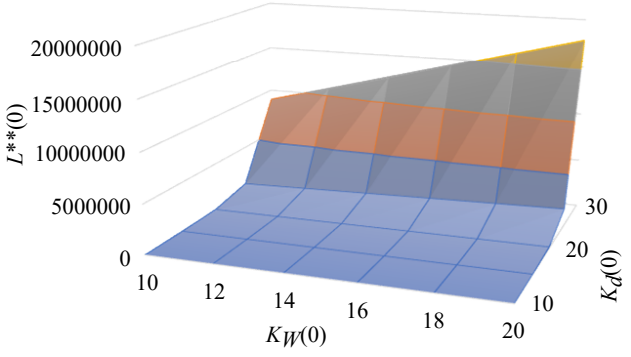

Fig. 6. Dependence of the number of $L^{**}(0)$ elements on the ratio of the number of working $K_w(0)$ and protective $K_d(0)$ elements

When compared with the suboptimal structure $|S|$, in which $K_w(0)=K_d(0)$, and

$$L(0)=e^G K_w(0)\frac{1+\ln G(1-Y)}{G},$$

the relative gain γ^{**} will be equal to

$$\gamma^{**}=1-\frac{1+\ln G(1-Y)}{G(1-Y)}. \quad (23)$$

The calculated dependence of the gain γ^{**} on the number of protective elements $K_d(0)$ is shown in Fig. 7.

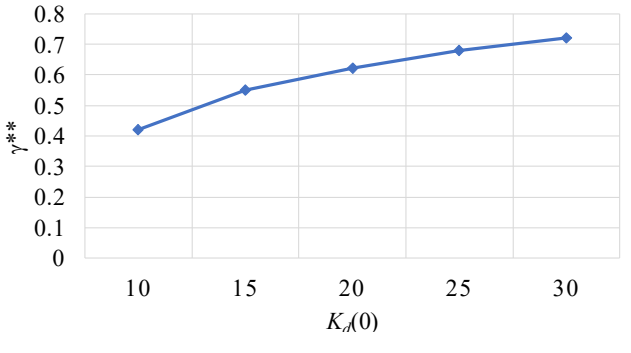

Fig. 7. Dependence of the gain γ^{**} on the number of protective elements $K_d(0)$

Comparing the values obtained for the optimal strategy of behavior of the external environment with the corresponding values under the condition of the optimal structure of the system itself, it is clear that optimizing the structure of the system requires increasing the number of attacking elements. Those elements that the enemy needs to disable the system. At the same time, the required number of protective elements is significantly reduced.

Thus, at a fixed value of $L(0)$, the optimal behavior of the external environment $\bar{Z}$ converts the value $(1-Y)K_w(0)$ to a maximum, and then the latter is converted to a minimum by the structure $|S|_{opt}$ of the system S.

6. Discussion of the results of developing a model for organizing a security system taking into account the influence of the external environment

The conducted studies provided a comprehensive understanding of the functioning of cyber-physical sys-

tems under destructive influences (Fig. 2) and highlighted the need to develop a mathematical model that accounts for the interactions between working, protective, and attacking elements.

The developed mathematical model of the security system organization in a cyber-physical system focuses on the structural and functional relationships between working, protective, and communication elements under the impact of external destructive factors. The model assumes that the CPS has a multi-component structure, which behavior is determined by the internal parameters and operational logic of its elements, as well as by the characteristics of the external environment (4), (5). It also considers that the attacking resource is expended on both working and protective elements, with its effectiveness dependent on the chosen strategy and the system's structural configuration (22).

This mathematical framework enables a quantitative description of the system's destruction processes and allows optimization of its initial structure at the early stages of design. It provides a means to determine the optimal initial configuration of the system that maximizes survivability under the worst-case scenario of enemy actions.

A key distinction of the proposed approach is the integration of the structural-functional organization of system elements with a minimax model of the attacking environment's behavior, enabling simultaneous consideration of both the internal system architecture and the enemy's optimal actions. Unlike traditional approaches that model attacks locally or focus on individual elements, this model accounts for the uniform spatial distribution of elements, their interactions, and the dependence of defeat probabilities. In contrast to methods aimed primarily at improving communication and mobility in aerial networks [14], the model mathematically defines the conditions under which the system maintains survivability even under deliberate and optimal destructive influence.

Unlike empirical and simulation methods described in the literature on UAV and radio-channel security [14, 16, 17], the proposed approach provides an accurate analytical description of interactions between system elements and attacking forces.

Modeling the CPS destruction process under attacking elements allowed for tracing the relationship between the internal system structure and the strategy of the external environment. The external resource is initially directed toward neutralizing protective elements, corresponding to the attacker's optimal tactic of first eliminating components capable of counteraction (15) (Fig. 3). Once protective components are destroyed, the attack shifts to the working elements, with their rate of loss determined by the effectiveness of the initial CPS organization.

The optimal ratio of protective to working elements is critical for enhancing CPS stability. A correctly selected ratio forces the external environment to expend more attacking resources (22) (Fig. 6), thereby extending the system's operational duration even under conditions of targeted destructive influence.

The modeling results demonstrated that the initial ratio of protective to working elements in a CPS determines the amount of attacking resource required for the system's complete destruction. At low ratios of working to protective elements (approximately 0.1–0.5), the attacking resource required is minimal because the small number of protective elements is quickly neutralized, allowing the attack to immediately target the working components and accelerating system destruction.

Conversely, ratios within the range of 1.5–2.0 were found to significantly increase CPS stability. The results showed that when the number of protective elements exceeds 2.0, further increases in attacking resource requirements are less pronounced, indicating diminishing returns from adding additional protective elements.

The main limitation of the proposed model is that the probability of defeat is fixed and identical for all elements. It does not account for dynamic changes in system topology, energy constraints, equipment degradation, or the emergence of new communication channels. Another limitation is that the CPS is assumed to be a uniformly filled space with protective and working elements evenly distributed.

Despite these limitations, the proposed approach allows for a more comprehensive design of CPS, where the system structure, protection methods, and predictions of adversary actions are considered jointly as part of a single optimization process. In real conditions, multiple types of destructive factors act simultaneously, and the model can be further improved by incorporating combined social, cybernetic, and radio-electronic attacks.

7. Conclusions

1. It is determined that the structural and functional relationships between the working, protective, and communication elements of the CPS are critical for enhancing resistance to external influences. The efficiency of the system depends not on the absolute number of elements, but on their optimal ratio. The existence of an optimal strategy for the behavior of the external environment and an optimal initial structure of the system is demonstrated.

2. Modeling results indicate that the most effective strategy for the external environment is to prioritize the destruction of protective elements. This approach minimizes the total resources required to disable the system. Comparison with a suboptimal strategy, where the attack is evenly distributed between working and protective components, shows that the optimal strategy reduces the attacking resource expenditure by approximately 1.5–2.0 times. Consequently, an optimally structured CPS forces the external environment to expend 1.5–2 times more resources to compromise it, thereby extending the system's operational life.

Conflict of interest

The authors declare that they have no conflict of interest regarding this study, including financial, personal, authorship, or other, that could influence the study and its results presented in this article.

Financing

The study was conducted without financial support.

Data availability

The manuscript has no associated data.

Using artificial intelligence tools

The authors confirm that they did not use artificial intelligence technologies when creating the presented work.

Authors' contributions

Nataliia Dzheniuk – Conceptualization, Methodology, Writing – original draft, Writing – review & editing; **Serhii Yevseiev** – Conceptualization, Methodology, Project administration; **Vitalii Kryvosheiev** – Software, Validation; **Viktor Zaika** – Software, Validation; **Serhii Holdobin** – Software, Validation; **Yevhen Tarasenko** – Software; **Artem Moskalenko** – Formal analysis, Investigation, Resources; **Serhii Kravchenko** – Formal analysis, Investigation, Resources; **Artur Ismahilov** – Formal analysis, Investigation, Resources; **Ihor Syvachenko** – Formal analysis, Investigation, Resources.

References

1. Graf, S., Quinton, S., Girault, A., Gössler, G. (2018). Building Correct Cyber-Physical Systems: Why We Need a Multiview Contract Theory. Formal Methods for Industrial Critical Systems, 19–31. https://doi.org/10.1007/978-3-030-00244-2_2
2. Bereket Abera, Y., Naudet, Y., Panetto, H. (2020). A new Paradigm and Meta-Model for Cyber-Physical-Social Systems. IFAC-PapersOnLine, 53 (2), 10949–10954. https://doi.org/10.1016/j.ifacol.2020.12.2841
3. Kampourakis, V., Gkioulos, V., Katsikas, S. (2023). A systematic literature review on wireless security testbeds in the cyber-physical realm. Computers & Security, 133, 103383. https://doi.org/10.1016/j.cose.2023.103383
4. Tyagi, A. K., Sreenath, N. (2021). Cyber Physical Systems: Analyses, challenges and possible solutions. Internet of Things and Cyber-Physical Systems, 1, 22–33. https://doi.org/10.1016/j.iotcps.2021.12.002
5. Yaacoub, J.-P., Noura, H., Salman, O., Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. Internet of Things, 11, 100218. https://doi.org/10.1016/j.iot.2020.100218
6. Lee, E. (2015). The Past, Present and Future of Cyber-Physical Systems: A Focus on Models. Sensors, 15 (3), 4837–4869. https://doi.org/10.3390/s150304837
7. Duo, W., Zhou, M., Abusorrah, A. (2022). A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. IEEE/CAA Journal of Automatica Sinica, 9 (5), 784–800. https://doi.org/10.1109/jas.2022.105548
8. Zuo, Z., Liu, C., Han, Q.-L., Song, J. (2022). Unmanned Aerial Vehicles: Control Methods and Future Challenges. IEEE/CAA Journal of Automatica Sinica, 9 (4), 601–614. https://doi.org/10.1109/jas.2022.105410
9. Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S. et al. (2021). Development of a concept for building a critical infrastructure facilities security system. Eastern-European Journal of Enterprise Technologies, 3 (9 (111)), 63–83. https://doi.org/10.15587/1729-4061.2021.233533
10. Lombardi, M., Vannuccini, S. (2022). Understanding emerging patterns and dynamics through the lenses of the cyber-physical universe. Patterns, 3 (11), 100601. https://doi.org/10.1016/j.patter.2022.100601
11. Tariq, U., Ahmed, I., Bashir, A. K., Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors, 23 (8), 4117. https://doi.org/10.3390/s23084117
12. Zhao, H. (2022). Multi-vue Design Pour Cyber-physical Systems. Université Côte d'Azur, 170.
13. Greer, C., Burns, M., Wollman, D., Griffor, E. (2019). Cyber-physical systems and internet of things. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.1900-202
14. Ayass, T., Coqueiro, T., Carvalho, T., Jailton, J., Araújo, J., Francês, R. (2022). Unmanned aerial vehicle with handover management fuzzy system for 5G networks: challenges and perspectives. Intelligence & Robotics. https://doi.org/10.20517/ir.2021.07
15. Serkov, A., Jammine, A., Kudii, D., Nataliia, D., Farid, N.-A., Bogdan, L. (2023). Security Models and Methods of Socio-Cyberphysical Systems. 2023 7th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 1–6. https://doi.org/10.1109/ismsit58785.2023.10304955
16. Khan, M. A., Kumar, N., Alsamhi, S. H., Barb, G., Zywiołek, J., Ullah, I. et al. (2025). Security and Privacy Issues and Solutions for UAVs in B5G Networks: A Review. IEEE Transactions on Network and Service Management, 22 (1), 892–912. https://doi.org/10.1109/tnsm.2024.3487265
17. Tsao, K.-Y., Girdler, T., Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. Ad Hoc Networks, 133, 102894. https://doi.org/10.1016/j.adhoc.2022.102894