UDC UDC 681.32:007.5
DOI: 10.15587/1729-4061.2021.241638

DEVELOPMENT OF A METHOD FOR ASSESSING THE SECURITY OF CYBER-PHYSICAL SYSTEMS BASED ON THE LOTKA-VOLTERRA MODEL

Serhii Yevseiev
Corresponding author
Doctor of Technical Sciences, Professor*
E-mail: serhii.yevseiev@hneu.net
Serhii Pohasii
PhD, Associate Professor*
Stanislav Milevskyi
PhD, Associate Professor*
Oleksandr Milov
Doctor of Technical Sciences, Professor*
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
Myronosytska str., 71, Kharkiv, Ukraine, 61002
Ivan Grod
Doctor of Physical and Mathematical Sciences, Associate Professor
Department of Cybersecurity
Ternopil Ivan Puluj National Technical University
Ruska str., 56, Ternopil, Ukraine, 46001
Denis Berestov
PhD**
Ruslan Fedorenko
PhD**
Oleg Kurchenko
PhD, Associate Professor, Senior Researcher**
*Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
Nauky ave., 9-A, Kharkiv, Ukraine, 61166
**Department of Program Systems and Technology
Taras Shevchenko National University of Kyiv
Volodymyrska str., 60, Kyiv, Ukraine, 01033

The paper presents the results of the development of a method for assessing the security of cyber-physical systems based on the Lotka-Volterra model. Security models of cyber-physical systems are proposed: "predator-prey" taking into account the computing capabilities and focus of targeted cyberattacks, "predator-prey" taking into account the possible competition of attackers in relation to the "prey", "predato-prey" taking into account the relationships between "prey species" and "predator species", "predator-prey" taking into account the relationship between "prey species" and "predator species". Based on the proposed approach, the coefficients of the Lotka-Volterra model $\alpha=0.39$, $\beta=0.32$, $\gamma=0.29$, $\phi=0.27$ were obtained, which take into account the synergy and hybridity of modern threats, funding for the formation and improvement of the protection system, and also allow determining the financial and computing capabilities of the attacker based on the identified threats.

The proposed method for assessing the security of cyber-physical systems is based on the developed threat classifier, allows assessing the current security level and provides recommendations regarding the allocation of limited protection resources based on an expert assessment of known threats. This approach allows offline dynamic simulation, which makes it possible to timely determine attackers' capabilities and form preventive protection measures based on threat analysis. In the simulation, actual bases for assessing real threats and incidents in cyber-physical systems can be used, which allows an expert assessment of their impact on both individual security services and security components (cyber security, information security and security of information).

The presented simulation results do not contradict the graphical results of the classical Lotka-Volterra model, which indicates the adequacy of the proposed approach for assessing the security of cyber-physical systems

Keywords: critical infrastructure, security system, threat classifier, Lotka-Volterra model, simulation method, security level

Received date 01.09.2021
Accepted date 15.10.2021
Published date 29.10.2021

***How to Cite**: Yevseiev, S., Pohasii, S., Milevskyi, S., Milov, O., Melenti, Y., Grod, I., Berestov, D., Fedorenko, R., Kurchenko, O. (2021). Development of a method for assessing the security of cyber-physical systems based on the Lotka-Volterra model. Eastern-European Journal of Enterprise Technologies, 5 (9 (113)), 30–47. doi: https://doi.org/10.15587/1729-4061.2021.241638*

1. Introduction

The creation of large critical infrastructure systems, intensification of research on the dynamics of cyber-physical systems (CPS) require continuous improvement and updating of the existing apparatus for modeling and control of dynamic systems [1–5]. Recently, there has been a shift in the focus of research towards the development of a meth-

odology for dynamic time-variant systems. Using methods for analyzing such systems makes it possible to dramatically expand the range of tasks to be solved.

Modern practical requirements for the study of complex cyber-physical systems have led to the emergence of a new class of systems – developing ones [1–3]. These systems are characterized by the time dependence of their structure, changes in the development of a set of input and output system parameters, a significant level of a priori uncertainty about the system's functioning regularities. At present, there is no satisfactory solution to the problems of modeling developing cyber-physical systems based on causal information and data from periodically observed development processes. The fundamental difficulties of the structural synthesis of the model are usually replaced by assumptions about the laws of system evolution, followed by reducing the problem to parametric uncertainty within the framework of the classical theory of dynamical systems. The problems of decision-making in developing cyber-physical systems, when target settings are determined by a specialist using vague instructions are at the initial stages of research.

The development of cyber-physical systems in recent years has significantly changed the infrastructures of modern not only information-cybernetic systems (ICS), but also critical infrastructures (CI), as well as Internet-of-things systems (IoTS). Synthesis of these infrastructures makes it possible to significantly expand range of digital services, on the one hand, but also increases the level of cyber threats [6–9]. At the same time, the rapid growth of computing technologies allows attackers to form targeted, hybrid attacks that give a synergistic effect [6, 8, 9]. In such circumstances, an integral part of security systems is the ability not only to timely respond to incidents in infrastructure elements, but also to form them correctly. An important task is the timely and correct allocation of limited security resources in the face of constant changes in the vector of cyberattacks. To timely change the structure of protective resources, assess the necessary and current state of the security system, security models should be used. This approach can significantly reduce the cost of restoring the network infrastructure, allows taking timely preventive measures with the required costs of security mechanisms. However, the division of security into separate components: information security, cyber security, security of information in normative regulators leads to the formation of their models in each of the component [8, 9]. This approach does not allow taking into account the hybridity and synergy of threats, the possibility of their integration with social engineering methods, and formation of targeted attacks. One of the directions that provide the conceptual basis for building IoTS security systems is the security maturity model [1, 2]. At the same time, security maturity refers to the degree of confidence that the current state of security meets all the needs of the organization and security requirements [1]. Security maturity provides not only an assessment of the current security level, its necessity, benefits, but also the cost of maintaining it. The factors that need to be weighed in such an analysis include specific threats to the organization's industry vertical, regulatory requirements, unique risks in the environment, and the organization's threat profile [1]. However, it is proposed to build a security system according to a hierarchical structure with subsequent division into security segments. In addition, such a model does not take into account the capabilities of attackers to form their networks, to resist each other when implementing threats per "prey".

Thus, there is a need for a timely assessment of the current state of the security level of cyber-physical systems (CPS) in the face of modern threats, taking into account the synthesis of infrastructure elements of ICS with IoTS in conditions of dynamic changes in the situation.

2. Literature review and problem statement

The analysis of global trends in cyber threats showed that today security cannot be ensured in full. So, the works [3, 4] provide the analysis of cyber threats for 2017–2019. The analysis shows that the vector of cyber threats is changing with trends in the development of digital services, the Internet of Things and cryptocurrencies based on blockchain technology. The work [5] presents 10 main cybersecurity trends in 2021, which confirms the trends of cyberattacks in the context of a pandemic, first of all on cryptocurrency exchanges, secondly on private VPN channels (in connection with remote work), and thirdly based on social engineering methods – phishing emails in PDF format within corporate mail. In [6], methodological aspects of building a security system based on crypto-code constructions, their application in various critical infrastructure facilities, as well as the ability to resist modern threats are considered.

In [8], it is proposed to use dynamic models based on the methods of the theory of differential games and differential transformations, while assessing the current state of the system in offline mode. However, such methods require significant computing resources, which significantly reduces the possibility of their practical implementation. In [9], the authors consider the use of dynamic models in various systems of information space. However, the models do not take into account the possibility of increasing the computing capabilities of attackers, their combining into groups in order to achieve the attack objectives. In [10], the authors consider economic aspects that can affect the construction of not only a security model, but also its practical implementation in the information security system of the transport system. However, the authors do not take into account the aggregation of threats, their synergy and hybridity, which allows forming target (integrated) threats using social engineering methods.

The analysis of models for constructing protection systems [6–10] showed that an approach has developed based on the representation of the process of its processing in the form of the abstract computing environment. In this environment, a set of subjects (users and processes) operate simultaneously with a set of objects (resources and datasets). In this case, the construction of a protection system consists in creating a protective environment as a set of restrictions and procedures. It must be able, under the control of a security kernel, to prohibit unauthorized and implement authorized access of subjects to objects and protect the latter from intentional and accidental external and internal threats. This approach is based on the theoretical security models of Hartson, Bell-LaPadula, MMS Landwehr and McLean, Beebe, Clark-Wilson, etc. and is static in nature. These models are considered to be tools for developing security policies that define a set of requirements that must be met in a specific implementation of the system. However, theoretical models were developed in the 70s-80s of the last century, and do not take into account modern realities of computing technology, digital services, as well as signs of synergy and hybridity of targeted threats. It is only possible to provide a safety loop for continuous vital processes, which significantly reduces not only the quality of user services, but also threatens the

development of the company's/enterprise's production, etc. In addition, new types of cyber terrorists/intruders have appeared, whose actions are aimed at total destruction. New political hackers, whose actions are aimed at changing the course of countries, new and/or modified targeted cyberattacks with signs of hybridity and synergy perform hacking of security systems based on different models and concepts of their construction. At the same time, the rapid growth of cyber-physical systems, the Internet of things forms multisystems, which, on the one hand, expand the range of digital services, and, on the other, simplify targeted cyberattacks.

The second approach is to use the principle of sufficiency in the framework of a proactive protection strategy when potential threats are assessed at the design stage and protection mechanisms are implemented. However, the infrastructure of modern ICS is closely related to the elements of cyber-physical and Internet of things systems, which greatly complicates the security of such systems and networks.

One of the solutions proposed in [11] is the concept of building a security system based on the IIC IoT Security Maturity Model (IoT SMM). A systematic approach to the choice of protection options is provided by combining practices into appropriate domains according to the effect of their application: security management and organizational measures (Governance); security by design (Enablement); security strengthening (Hardening) [11]. The model allows making the right choice of security measures, forming the choice architecture based on a hierarchy of security practices. However, a significant drawback of such a system is the hacking of upper-level domains, followed by a chain reaction of hacking the entire system, the lack of taking into account the synergy and hybridity of targeted attacks and their modifications. In addition, as in theoretical models, modern computing resources of attackers, as well as signs of targeted threats, are not taken into account.

Dynamic models are a promising direction to form security systems. However, they often cannot be used due to management's misunderstanding of their expediency, significant growth in economic and computing costs compared to classical (stationary) models. Of particular interest in this direction is the Lotka-Volterra model and its modifications ("predator-prey"), which allows taking into account not only technical and economic aspects when building a security system, but also the possibility of attackers' "competition", formation of networks for targeted attacks on the "prey".

The work [12] provides a mathematical apparatus for using the Lotka-Volterra model in various fields – the environment, political science, biology, medicine and physics. However, the lack of research on their implementation does not allow using these models in the field of security. In [13], the authors consider using the "prey-predator" model in biology, which makes it possible to interpret approaches to the field of information and communication systems/cyberspace, considering it as an ecosystem. However, the work does not take into account the possibilities of modern threats, which significantly hinders their practical implementation.

The work [14] considers the possibility of practical use of the model in assessing the safety level of transport infrastructure facilities. However, the use of a security system as a "predator" does not allow taking into account changes in the vector of cyber threats, especially signs of synergy and hybridity, as well as conditions of limited economic resources. In [15, 16], studies of various cybersecurity models based on the Lotka-Volterra model are presented. The proposed approach allows determining vectors of cyber threats, however, without taking into account their synergy and hybridity, integration with social engineering methods, which significantly reduces their practical value. In [17, 18], cyberspace is viewed as a digital ecosystem, in which systems can adapt and evolve, allowing systems engineering to create "species" that function and adapt in that ecosystem. However, the authors do not take into account trends in the development of computing resources, capabilities of intruders, which does not allow adequate use of this approach in modern conditions. [19] explores the predator-prey analogy for the Internet and presents results on how different levels of species diversification affect network resilience, and discusses the relationship between diversification, competition, antitrust laws, and national security. In [20], an analogy is proposed between malware and ecological principles of "species" behavior – mediation, parasitism, predation, and density-dependent population regulation. However, the lack of studies of modern threats, their modifications and the emergence of new ones do not provide the required level of reliability in assessing the security of CPS. In [21], the authors propose to use the biological principles of ant-based cyber defense (ABCD) – mobile resilient defense that provides a set of wandering, bio-inspired, digital ant agents working with stationary agents in a hierarchy headed by a human supervisor. In [22], the authors propose a simplification of the Lotka-Volterra model by using the modulation function. The function is multiplied by both sides of the Lotka-Volterra model, and the model is converted to linear equations with parameters to be estimated by fractional integration. In [23], the authors propose an analysis of the predator-prey model based on characteristics such as the Allee effect, fear effect, cannibalism, and immigration. However, the works [17–23] do not take into account changes in the vector of cyber threats, their hybridity and synergy, which gives an emergent effect when implementing targeted attacks.

The work [24] proposes a conceptual approach to using the Lotka-Volterra model in describing the relationships and key elements of the information security system infrastructure in responding to incidents. However, the authors consider only the use of the model in one of the security components, without taking into account the integration of threats with social engineering methods, signs of hybridity and synergy.

In [25], it is proposed to use the Lotka-Volterra model to assess the dependence of personal data protection on the amount of information in the system and trust in social networks. As a result of research, the authors proved that the dependence of personal data protection on trust is proportional with other protection parameters unchanged. However, the assessment of threats does not consider trends of their development and improvement, the connection with social engineering methods, which does not allow taking into account the possibility of synergy and hybridity of threats.

Thus, this approach ("predator-prey" model) should be considered taking into account the modern development of computing resources, financial capabilities of both "attackers" and "defenders". It is also necessary to take into account changes in the vector of targeted attacks, considering their hybridity and synergy in all security components.

3. The aim and objectives of the study

The aim of the work is to develop a method for assessing the security of cyber-physical systems based on the Lotka-Volterra

predator-prey model. The method should take into account the computing and financial capabilities of attackers, signs of hybridity and synergy of targeted attacks on all security components, relationships between "prey species" and "predator species". This approach will allow timely dynamic changes in the security level, forming preventive measures in the offline mode based on pre-configured security scenarios/profiles while saving financial resources for security infrastructure components.

To achieve the aim, the following objectives were set:

– to develop security models for developing cyber-physical systems, taking into account the computing capabilities and focus of targeted cyberattacks, possible competition of attackers in relation to the "prey", the possibility of attackers/cyber groups grouping in order to achieve the cyberattack goals;

– to develop security models for cyber-physical systems based on the "predator-prey" model, taking into account relationships between "prey species" and "predator species";

– to develop a method for dynamic assessment of the security of cyber-physical systems based on the Lotka-Volterra "predator-prey" model;

– to conduct research on the practical implementation of the proposed approach.

4. Research materials and methods

To assess the security of cyber-physical systems under the influence of modern targeted cyber threats with signs of hybridity and synergy, their integration with social engineering methods on infrastructure elements is taken into account. At the same time, the classical Lotka-Volterra model uses the main approaches based on the following paradigms:

– in the absence of "predators", "prey" multiply exponentially;

– in the absence of "prey", "predators" die out exponentially.

At the same time, the works [8, 9, 12, 17–19, 24, 25] generally consider IS incidents/attackers as a "prey", and protection measures/protection system elements as a "predator". This looks illogical in terms of the ecosystem, which means cyberspace. Mathematically, the "predator–prey" model can be described as [14]:

$$\begin{cases} \dfrac{dN_1}{dt} = \alpha N_1 - \beta N_1 N_2; \\ \dfrac{dN_2}{dt} = -\varphi N_2 + \gamma N_2 N_1, \end{cases} \quad (1)$$

where N_1 is the number of prey, N_2 is the number of predators, α is the fertility rate of prey, β is the coefficient of predator's influence on the prey (predation coefficient), ϕ is the predator's mortality rate, γ is the coefficient of prey's influence on the predator.

However, to assess the security of cyber-physical systems, the following concepts are proposed:

– "prey" – a system or element of a system/infrastructure of an information and communication system/cyber-physical system that is subject to targeted threats with signs of synergy and hybridity;

– "predator" – a target threat or threat to separate security components (cybersecurity (CS), information security (IS), security of information (SI)), on a system or element of a system/infrastructure of an information and communication system/cyber-physical system or Internet of Things system;

– security of information resources (IR) – the state of IR security, characterized by the ability of users, technical means and information technologies to ensure confidentiality, integrity, authenticity and availability when processed in ICS with IoTS;

– cybersecurity of IR (CS IR) – a set of security tools, strategies, principles, security guarantees, risk management approaches, actions, training, insurance and technologies to protect the cybersecurity of ICS with IoTS, resources and users of cyber-physical systems;

– information security of IR (IS IR) – the state of security of the information environment of ICS with IoTS, ensuring its formation, use and development in the interests of citizens and ICS with IoTS;

– hybridity of IS, CS, SI threats – a set of several threats to information resources by security components: information security, cybersecurity, security of information, aimed at a separate security service: confidentiality, integrity or authenticity. This provides the maximum effect of their integration;

– synergy of IS, CS, SI threats – the combined impact of several threats on security components: information security, cybersecurity, security of information with security services: confidentiality, integrity, authenticity. It is characterized by the fact that their combined effect significantly exceeds the effect of each threat and their simple sum;

– emergence of ICS/CPS – a set of special ICS/CPS properties that do not belong to its subsystems and units, as well as the sum of elements that are not connected by special system-forming links. Based on the assessment of the synergy and hybridity of threats to security components, the costs of investing in a security system are minimized to ensure the efficiency and reliability of information transfer;

– security level of information resources – a qualitative (quantitative) indicator of the ability of the ICS/CPS protection system to resist synergistic and hybrid threats to security components: information security, cybersecurity, security of information;

– business continuity – a property of the system ensuring the uninterrupted operation of internal and external applications, which allows interrupted operation of subsystems and services during planned downtime and unplanned failures. It also ensures that critical business data is backed up and stored and can be recovered within a reasonable period of time in the event of an unexpected incident or disaster;

– security loop of business processes – the minimum permissible set of protection means for information resources and related business processes. The execution of business processes in a given sequence allows achieving the organization's goals.

Fig. 1 shows the relationship of the proposed definitions. The main difference from the known approaches is the ability to take into account not only the integration of threats, formation of targeted attacks, but also their impact on individual security components. This approach provides a detailed description of today's threats, and simplifies the understanding of their impact on the security level in general.

To determine the relationship between the "prey" and the "predator," the threat classifier and expert assessment steps proposed in [25] and presented in Fig. 2, 3 are used. This approach takes into account characteristics and signs of modern threats, minimizes funds to support information security systems (ISS), considering business continuity.

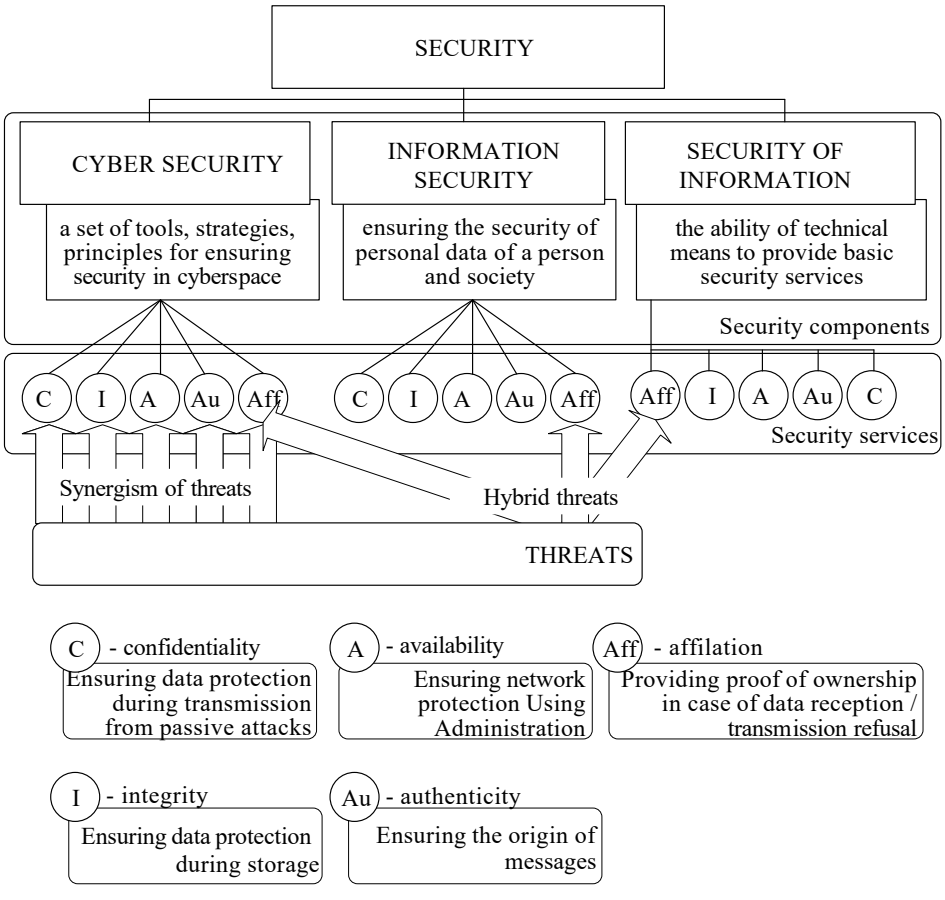

Fig. 1. Structure of the relationship of definitions

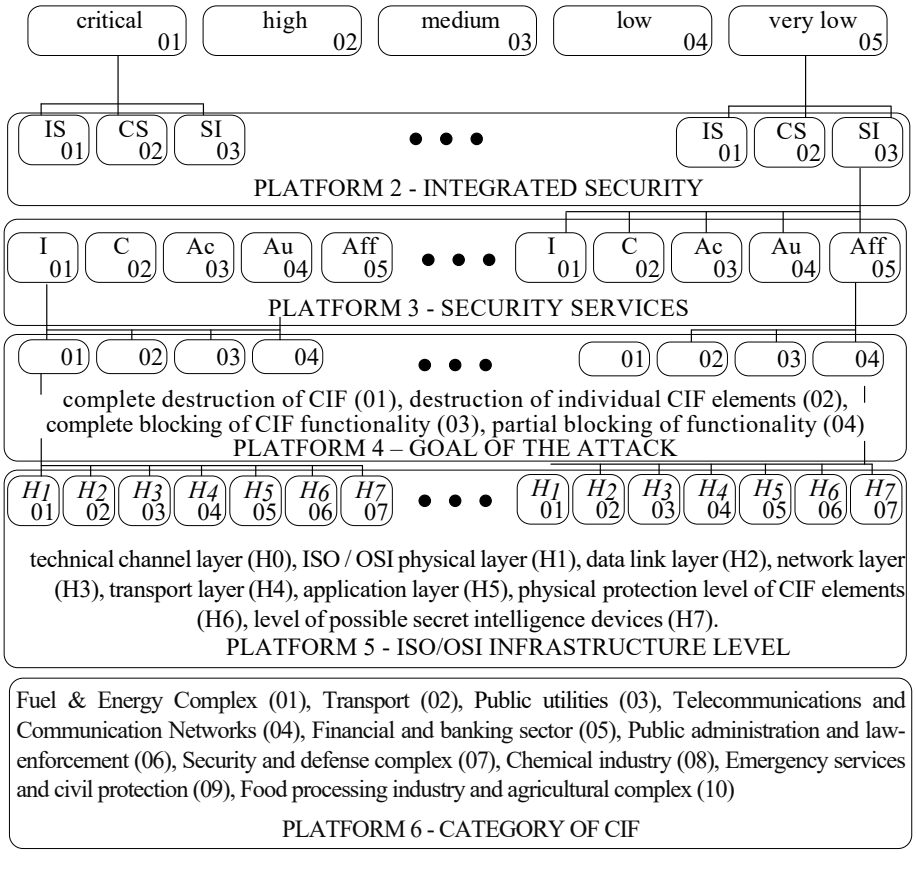

Fig. 2. Structure of the cyber threat classifier

STEP 1. FORMATION OF METRIC RATES OF THREATS

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

STEP 2. FORMATION OF WEIGHT COEFFICIENTS OF THE MANIFESTATION OF THREATS

$$\alpha_i^{CPS\ CIF}, i \in [0{,}067;0{,}133;0{,}2;0{,}267;0{,}333]$$

STEP 3. DETERMINATION THE IMPLEMENTATION OF EACH THREAT

$$w_j^{CPS\ CIF}{}_i P_j^{CPS\ CIF}{}_i = \frac{1}{K} P_j^{CPS\ CIF}{}_i \sum_{k=1}^{N} w_j^{CPS\ CIF}{}_{ik}, \text{ where } P_j^{CPS\ CIF}{}_i \in \left\{\alpha_i^{CPS\ CIF}\right\}$$

STEP 4. DETERMINATION OF THE IMPLEMENTATION OF THREATS TO THE SECURITY SERVICE

$$W_{synerg}^{CPS\ CIF\ C} = \sum_{i=1}^{M} w_{synerg}^{CPS\ CIF\ C}{}_i \alpha^{CPS\ CIF\ C}{}_i \quad \cdots W_{synerg}^{CPS\ CIF\ Aff} = \sum_{i=1}^{M} w_{synerg}^{CPS\ CIF\ Aff}{}_i \alpha^{CPS\ CIF\ Aff}{}_i$$

STEP 5. DETERMINATION OF THE TOTAL THREAT TO THE SECURITY COMPOSITION

$$W_{synerg}^{CPS\ CIF} = \sum_{i=1}^{N}\left(\sum_{i=1}^{M} w_{synerg}^{CPS\ CIF\ C}{}_i \cap \sum_{i=1}^{M} w_{synerg}^{CPS\ CIF\ I}{}_i \cap \sum_{i=1}^{M} w_{synerg}^{CPS\ CIF\ A}{}_i \cap \sum_{i=1}^{M} w_{synerg}^{CPS\ CIF\ Au}{}_i \cap \sum_{i=1}^{M} w_{synerg}^{CPS\ CIF\ Aff}{}_i\right)\alpha_i^{CPS\ CIF}$$

STEP 6. DETERMINATION THE ECONOMIC COSTS OF ATTACK PREVENTION

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

determined automatically based on mathematical expressions

Fig. 3. Steps of expert assessment of cyber threats

Note: $w_j^{CPS\ CIF}$ *– expert weighting factors of security services: confidentiality, integrity, availability, authenticity, and affiliation;* $\alpha_i^{CPS\ CIF}$ *– weighting factor of the security service: confidentiality, integrity, availability, authenticity and authenticity of manifestation of the attack of the i-th threat, while* $P_j^{CPS\ CIF}{}_i \in \left\{\alpha_i^{CPS\ CIF}\right\}$; $W_{synerg}^{CPS\ CIF_j}$ *– the total threat by security services;* $W_{synerg}^{CPS\ CIF}$ *– the total threat by security components;* Tr_R^A *– the set of potential threats, which are effective for the attacker;* Tr_i *– the threat to the i-th information resource;* P_i^A *– estimation of the cost of successful implementation of the attack on the i-th resource from the attacker side;* C_i^A *– the cost of the attack on the i-th resource from the attacker side.*

To account for the computing resources of attackers, the approach proposed in [26] is used. Simulation of models: "predator–prey" taking into account the computing capabilities and focus of targeted cyberattacks, "predator–prey" taking into account the possible competition of attackers in relation to the "prey", "predator–prey" taking into account relationships between "prey species" and "predator species", "predator–prey" taking into account relationships between "prey species" and "predator species" using a Java Script software package presented on the web resource [27]. In the expert assessment of threats ((https://bdu.fstec.ru/threat) [28], weighting factors of expert competence are proposed for the objectivity of expert judgments. The selection of experts from the scientific community is based on the analysis of publications in science-metric databases, research directions, as well as practical examination experience.

5. Results of the development of security models of cyber-physical systems based on the "predator-prey" model

5. 1. Development of security models for developing cyber-physical systems, taking into account the computing capabilities and focus of targeted cyberattacks, possible competition of attackers in relation to the "prey", the possibility of attackers/cyber groups grouping in order to achieve the cyberattack goals

Development of security models for developing cyber-physical systems, taking into account the computing capabilities and focus of targeted cyberattacks.

To use the "predator-prey" model for modeling the functioning dynamics and assessing cyber-physical systems, it is necessary not only to give a substantive interpretation of the basic model in terms and concepts of the security system, but also to parameterize the model. In other words, it is necessary to determine the values of the coefficients included in the model equations, as well as to set the initial values of the studied variables.

We begin the parametrization of the model with its first equation.

We estimate the number of protection elements of the business continuity security loop based on the following assumptions:

1. Threats are aimed at the corresponding security services, which are represented by the 3rd platform in the threat classifier [26].

2. For each of the security services, the security loop has means that provide those services. The distribution of these means over the considered range of services is described by the vector $\left(A_i^C, A_i^I, A_i^A, A_i^{Au}, A_i^{Aff}\right)$, where A_i^C is the weighting factor that provides the confidentiality service; A_i^I is the weighting factor that provides the integrity service; A_i^A is the weighting factor that provides the management availability service; A_i^{Au} is the weighting factor that provides the authenticity service; A_i^{Aff} is the weighting factor that provides the affiliation service. In this case, the equality holds $\sum_{i=1}^{j} A_i^j = 1$, where j is security services, i is the threat to the CPS infrastructure elements.

3. A threat is considered hybrid if it simultaneously targets all security services.

The number of objects representing the targets of attacks, taking into account their hybridity, can be represented as follows:

$$\tilde{N}_1 = \sum_{i=1}^{Q} \begin{pmatrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{pmatrix}, \quad (2)$$

where variable indices correspond to basic security services: C – confidentiality; I – integrity; A – availability; Au – authenticity, Aff – affiliation; $N_{1_i}^C$ – the number of objects providing the confidentiality security service; for other security services – the same; Q – the total number of known cyber threats.

We assume that the coefficient of introduction of new elements of the information security system α corresponds to the security level of the elements that provide security services for the CPS. The security level, according to [9], is estimated in relative units: 1 – corresponds to the maximum security level provided by the security system, 0 – the security system provides no protection of information resources.

We assume that the cost of attacks and the cost of protection measures have a normal distribution. In this case, the probability of the threat being realized with the maximum capabilities of defense A and attack B will be determined by the difference between the probability densities $F(B)-F(A)$, where A is the maximum defense capabilities, B is the maximum attack capabilities. In other words, $F(B)$ determines the proportion of attacks out of their total number, which can be implemented by attackers based on the resources available to them. Similarly, $F(A)$ determines the proportion of attacks that the security system can protect from based on the resources available to it. Under these assumptions, the value $S=F(B)-F(A)$ determines the proportion of unprotected targets of cyberattacks. Then the security level will be defined as the proportion of information resources protected from cyberattacks. This value can be calculated as:

$$S = 1 - F(B) - F(A) = \\ = \int_{-\infty}^{B} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)} \mathrm{d}t - \int_{-\infty}^{A} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)} \mathrm{d}t, \quad (3)$$

where S is the system security level, $F(B)$ and $F(A)$ are the shares of resources of the parties to the cyber conflict, t is the integration variable that determines the level of available resources of the "predator" and "prey", μ and σ are the values that determine the mathematical expectation and variance of the statistical distribution of the resources available to the parties.

The assessment of the maximum capabilities of the parties to a cyber conflict is based on the cost estimates of implementing and preventing the threat, as well as on the assessment of the benefits of implementing and preventing the threat [26].

The introduction of cost indicators of threats makes it possible to implement an algorithm for rating potential threats and importance of information resources to be protected.

When implementing the algorithm, it is assumed that the parties to the conflict determine the criticality of cyber threats, which are economically feasible and/or from which the IR must be protected first. Then we define the algorithm:

1st step. Identification of cyber threats, the effect of which exceeds their cost:

$$Tr_R^A = \left\{ Tr_i \,|\, \left(P_i^A - C_i^A\right) > 0 \right\} \forall Tr_i \in Tr, \quad (4)$$

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

2nd step. Determination of the direction of protection that provides a higher effect than its cost.

$$Tr_C^D = \left\{ Tr_j \,|\, \left(P_i^D - C_i^D\right) > 0 \right\} \forall Tr_j \in Tr, \quad (5)$$

where Tr_C^D – the set of threats, the protection from which is economically expedient; P_i^D – estimation of the cost of losing the i-th information resource for the defense side; P_i^D – the cost of protecting the i-th information resource for the defense side;

3rd step. Determination of importance coefficients for attackers. They are defined as the share of gain of the total gain that can be obtained potentially when implementing the entire complex of threats for attackers:

$$K_i^A = \frac{P_i^A - C_i^A}{\sum_{i=1}^{M} \left(P_i^A - C_i^A\right)}, \quad \forall Tr_i \in Tr_R^A, \quad M = \left|Tr_R^A\right|, \quad (6)$$

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

4th step. Determination of importance coefficients for defenders. They are defined as the share of gain of the total gain that can be obtained potentially when implementing the entire complex of protective measures:

$$K_j^D = \frac{P_i^D - C_i^D}{\sum_{i=1}^{N} \left(P_i^D - C_i^D\right)}, \quad \forall Tr_j \in Tr_C^D, \quad N = \left|Tr_C^D\right|, \quad (7)$$

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

5th step. Selection of critical threats for which, based on the assessment, the product of the attacker's and defender's importance coefficients is maximum:

$$Tr_l = \arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \cdot K_l^A. \quad (8)$$

Then the fertility rate of "prey" is proposed to be calculated as:

$$\alpha = \frac{\left|\{Tr_l\}\right|}{Q}, \quad (9)$$

where $\left|\{Tr_l\}\right|$ is the set of critical cyber threats against which the information security system (ISS) has no protection means or they are partially available, but the implementation of the threat can lead to significant and/or critical destruction of the security loop, Q is the total number of known cyber threats.

The coefficient obtained in this way provides management's understanding of the need for additional protection means against the identified critical attacks.

The equation for changes in the number of modern threats to the CPS with IoTS is presented as a set of threats to the CPS, taking into account the possibility of their signs of synergy and hybridity:

$$\tilde{N}_2 = N_2 \times \left| \left\{ W_{hybrid\ C,I,A,Au,Af} \right\} \right|_{synerg}, \quad (10)$$

where $\left| \left\{ W_{hybrid\ C,I,A,Au,Af} \right\} \right|_{synerg}$ is the cardinality of the set of hybrid threats (i. e., their number), and $\left\{ W_{hybrid\ C,I,A,Au,Af} \right\}_{synerg}$ is the set of hybrid threats, which, according to the accepted assumption, are defined as a set of threats to all security services simultaneously. The calculation of individual components is given in [26].

To assess the impact of modern threats on protection means, we use the expression in [26], then the coefficient β is represented as:

$$\beta = \sum_{i=1}^{M} \left(w_{CPSi}^{C} \cap w_{CPSi}^{I} \cap w_{CPSi}^{A} \cap w_{CPSi}^{Au} \cap w_{CPSi}^{Aff} \right) \chi_i^{CPS}, \quad (11)$$

where M – the number of threats chosen by the expert from the set $\{i\}_i^M$, which is the subset of the entire set of the classifier threats, that is, $M \le Q$. w_{CPSi}^{C}, w_{CPSi}^{I}, w_{CPSi}^{A}, w_{CPSi}^{Au}, w_{CPSi}^{Aff} – the expert weighting factors of security services: confidentiality, integrity, availability, authenticity and affiliation; χ_i^{CPS} – the weighting factor of security services: confidentiality, integrity, availability, authenticity and authenticity of manifestation of the attack of the i-th threat.

To determine the coefficient of the attacker's computing capabilities ϕ, we use the attacker classification, presented in [26], and represent it as:

$$\varphi = \frac{1}{M} \sum_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv}, \quad (12)$$

where $\nu_i^{CPS} = W_{cp}^{CPS} \cap W_{cash}^{CPS} \cap T$ – weighting factors of attacker's capabilities;

p_{rj} – the probability of implementation of at least one threat to the j-th asset, i – threat, $\forall i \in n$, n – number of threats, j – information resource (asset), $\forall j \in m$, m – number of assets;

r_{motiv} – the probability of the attacker's motivation to implement the threat;

W_{cp}^{CPS} – attacker's computing resources (from [27]);

W_{cash}^{CPS} – attacker's financial resources (from [27].

Table 1 shows the initial data of criteria and indicators of expert assessment of the weighting factor of the attacker's computing capabilities.

Table 1

Initial data of criteria and indicators of expert assessment of the weighting factor of the attacker's computing capabilities

Category	weighting factor				
	$\beta_i^{CPS} \in \{\beta_i^{CPS}\}$			p_{rj}	r_{motiv}
	W_{cp}^{CPS}	T^{CPS}	W_{cash}^{CPS}		
critical	1	1	1	1	1
high	0.75	0.75	0.75	0.75	0.75
medium	0.5	0.5	0.5	0.5	0.5
low	0.25	0.25	0.25	0.25	0.25
very low	0.001	0.001	0.001	0.001	0.001

The coefficient of the possibility of preventive measures is presented as:

$$\gamma^j = \frac{1}{K \times B} \sum_{k=1}^{K} \sum_{g=1}^{B} \left(\mu_{kg}^j \times w_{kg}^j \right), \quad (13)$$

where μ_{kg}^j – the weighting factor of the g-th metric of the j-th security service for the k-th expert. Rationing of weighting factors: $\sum_{k=1}^{K} \sum_{g=1}^{B} \mu_{kg}^j = 1$, w_{kg}^j – the value of assessment of the g-th characteristic of the ISS mechanism by the k-th expert for the j-th security service in the case when the degree of system security and the destructive actions of attackers are independent. Wherein B={*cryptographic resistance* (C_r), *Key data amount*, S_c, *encryption/decryption of data complexity*, O_E}. Thus, we have such a set of characteristics of the ISS technical means: $\mu^j = \left| \left\{ C_r^j, S_c^j, O_E^j \right\} \right| \ \mu^j = \left\{ C_r^j, S_c, O_E \right\}$, which corresponds to the security level of the ISS cryptographic means. To describe the set of characteristics, we use the index g: μ_g, where $\left(\{g\}_1^B \right)$.

Thus, using the expressions obtained, the Lotka-Volterra model can be represented as follows:

$$\begin{cases} \dfrac{dN_1}{dt} = \left(\arg \max\limits_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \\ \times \left(\sum\limits_{i=1}^{Q} \begin{pmatrix} N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \\ + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \end{pmatrix} \right) - \\ - \left(\sum\limits_{i=1}^{M} \begin{pmatrix} w_{CPSi}^{C} \cap w_{CPSi}^{I} \cap w_{CPSi}^{A} \cap \\ \cap w_{CPSi}^{Au} \cap w_{CPSi}^{Aff} \end{pmatrix} \chi_i^{CPS} \right) \times \\ \times \tilde{N}_1 \left(N_2 \times \left| W_{\text{hybrid } C,I,A,Au,Af\ synerg} \right| \right); \\ \dfrac{dN_2}{dt} = - \left(\dfrac{1}{M} \sum\limits_{i=1}^{M} \nu_i \times p_{rj} \times r_{motiv} \right) \tilde{N}_2 + \\ + \left(\dfrac{1}{KB} \sum\limits_{k=1}^{K} \sum\limits_{g=1}^{B} \left(\mu_{kg}^j \times w_{kg}^j \right) \right) \tilde{N}_2 \tilde{N}_1. \end{cases} \quad (14)$$

Thus, the proposed approach of the security model of cyber-physical systems allows, from a practical point of view, considering cyberspace as an ecosystem, taking into account the computing capabilities of attackers and focus of targeted cyberattacks. In addition, cyberattacks are considered taking into account their integration with social engineering methods, which allows attackers to form targeted attacks. The proposed model takes into account the possibility of manifestation of targeted attacks in the ecosystem of signs of synergy and hybridity, which significantly affects the quantitative indicators of assessing the current state of the security level.

Development of a security model for cyber-physical systems based on the "predator–prey" model, taking into account the possible competition of attackers in relation to the "prey".

One of the advantages of the Lotka-Volterra model is the ability to use the "biological" aspects of the "predator-prey" model, taking into account the possible struggle between the "predators" themselves under a decrease in the "prey" population. In terms of the modern development of the world community, certain manifestations of competition are already manifested in the environment of cyber intruders/cyber groups. This, on the one hand, can increase the population

of "prey", that is, increase the ability of the information protection system to resist threats, and/or timely prepare preventive measures to counter them. On the other hand, reduce the number of "predators", that is, reduce the variety of threats, which will allow a timely response to them.

Based on the above assumptions, the "predator-prey" model is presented as:

$$\begin{cases} \frac{dN_1}{dt}=\left(\arg\max_{\forall Tr_l\in Tr_C^D} K_l^D\times K_l^A\right)\times \\ \times\left(\sum_{i=1}^{Q}\left(\begin{matrix}N_{1_i}^C\times A_i^C+N_{1_i}^I\times A_i^I+N_{1_i}^A\times A_i^A+\\ +N_{1_i}^{Au}\times A_i^{Au}+N_{1_i}^{Aff}\times A_i^{Aff}\end{matrix}\right)\right)- \\ -\left(\sum_{i=1}^{M}\left(\begin{matrix}w_{CPSi}{}^C\cap w_{CPSi}{}^I\cap w_{CPSi}{}^A\cap \\ \cap w_{CPSi}{}^{Au}\cap w_{CPSi}{}^{Aff}\end{matrix}\right)\chi_i^{CPS}\right)\times \\ \times\tilde{N}_1\left(\tilde{N}_2^1\cap\tilde{N}_2^2\cap\ldots\cap\tilde{N}_2^w\right); \\ \frac{dN_2}{dt}=-\left(\frac{1}{M}\sum_{i=1}^{M}\nu_i\times p_{rj}\times r_{motiv}\right)\times \\ \times\left(\tilde{N}_2^1\cap\tilde{N}_2^2\cap\ldots\cap\tilde{N}_2^w\right)+\left(\frac{1}{KB}\sum_{k=1}^{K}\sum_{g=1}^{B}\left(\mu_{kg}^j\times w_{kg}^j\right)\right)\times \\ \times\left(\tilde{N}_2^1\cap\tilde{N}_2^2\cap\ldots\cap\tilde{N}_2^w\right)\tilde{N}_1, \end{cases} \quad (15)$$

where the number of "predators" belongs to the set $\overline{\left\{\tilde{N}_2^j\right\}}$, $j\in 1,\ldots w$.

Thus, the proposed security model of cyber-physical systems takes into account the possible competition of attackers in relation to the "prey". This makes it possible to timely determine not only the direction of threats, but also the attackers' computing resources, and their "simultaneous" impact can reduce the risk of cyber threats.

Development of a security model for cyber-physical systems based on the "predator–prey" model, taking into account the possibility of attackers/cyber groups grouping in order to achieve the cyberattack goals

The Lotka-Volterra model takes into account not only the competitiveness of "predators," but also their unification. At the same time, as in any ecosystem, the emergent properties of "predators" can be manifested, which in terms of security can lead to a significant decrease in the resistance of the protection system of the business process loop or to hacking and destruction of business continuity. Based on the above assumptions, the "predator–prey" model is presented as:

$$\begin{cases} \frac{dN_1}{dt}=\left(\arg\max_{\forall Tr_l\in Tr_C^D} K_l^D\times K_l^A\right)\times \\ \times\left(\sum_{i=1}^{Q}\left(\begin{matrix}N_{1_i}^C\times A_i^C+N_{1_i}^I\times A_i^I+N_{1_i}^A\times A_i^A+\\ +N_{1_i}^{Au}\times A_i^{Au}+N_{1_i}^{Aff}\times A_i^{Aff}\end{matrix}\right)\right)- \\ -\left(\sum_{i=1}^{M}\left(\begin{matrix}w_{CPSi}{}^C\cap w_{CPSi}{}^I\cap w_{CPSi}{}^A\cap \\ \cap w_{CPSi}{}^{Au}\cap w_{CPSi}{}^{Aff}\end{matrix}\right)\chi_i^{CPS}\right)\tilde{N}_1\left(\sum_{j=1}^{w}\tilde{N}_2^w\right); \\ \frac{dN_2}{dt}=-\left(\frac{1}{M}\sum_{i=1}^{M}\nu_i\times p_{rj}\times r_{motiv}\right)\left(\sum_{j=1}^{w}\tilde{N}_2^w\right)+ \\ +\left(\frac{1}{KB}\sum_{k=1}^{K}\sum_{g=1}^{B}\left(\mu_{kg}^j\times w_{kg}^j\right)\right)\left(\sum_{j=1}^{w}\tilde{N}_2^w\right)\tilde{N}_1, \end{cases} \quad (16)$$

Thus, the proposed security model of cyber-physical systems based on the "predator-prey" model takes into account the possibilities of intruders/cyber groups grouping in order to achieve the cyberattack goals. This approach makes it possible to predict the "worst" options for the development of cyberattacks, as well as to formulate appropriate preventive measures.

5. 2. Development of a security model for cyber-physical systems based on the "predator–prey" model, taking into account relationships between "prey species" and "predator species"

In [27], the authors consider the *m*-dimensional case, which takes into account interactions in the "environment" of "predators", as well as interactions in the "environment" of "prey". This model is interesting, first of all, in terms of the interaction of "prey", which are considered as means/mechanisms of the information security system. At the same time, one of the principles of ISS formation – the principle of sufficiency is taken into account. In addition to this interaction in the "environment" of "predators", various trends from simple cooperation to confrontation are taken into account. In the proposed model:

$$\tilde{N}_i=N_i\cdot f(N), \quad (17)$$

where $f(N)=r+\|A\|\times N$, N_1, ..., N_m are the sizes of populations of *m*-different "predator" and "prey" species that interact in one environment, N is the vector composed of these unknowns. The parameters in the vector r are responsible for the success (probability) of "fertility" (the emergence of new cyber threats, or means of protection, respectively, from species) (r_i>0) or "mortality" (r_i<0).

The matrix $\|A\|$ describes the relationships between "predators" or "prey" of different species, while [27] a_{ij} describes the influence of species *j* on species *i*, a_{ji} describes the influence of species *i* on species *j*. Moreover, if both values a_{ij} and a_{ji} are positive, the individuals benefit from the interaction, if both are negative, they are at enmity with each other.

If a_{ij}>0, a_{ji}<0, then species *i* is a predator, and species *j* is prey for it. The values a_{ii} describe the effect of the species on itself.

Taking into account the above assumptions, the "predator-prey" model is presented as:

$$\begin{cases} \frac{dN_1}{dt}=\left(\arg\max_{\forall Tr_l\in Tr_C^D} K_l^D\times K_l^A\right)\times \\ \times\left(\sum_{i=1}^{Q}\left(\begin{matrix}N_{1_i}^C\times A_i^C+N_{1_i}^I\times A_i^I+N_{1_i}^A\times A_i^A+\\ +N_{1_i}^{Au}\times A_i^{Au}+N_{1_i}^{Aff}\times A_i^{Aff}\end{matrix}\right)\right)- \\ -\left(\sum_{i=1}^{M}\left(\begin{matrix}w_{CPSi}{}^C\cap w_{CPSi}{}^I\cap w_{CPSi}{}^A\cap \\ \cap w_{CPSi}{}^{Au}\cap w_{CPSi}{}^{Aff}\end{matrix}\right)\chi_i^{CPS}\right)\times \\ \times\tilde{N}_1\left(\sum_{j=1}^{w}\tilde{N}_2^w\right)-\varepsilon\tilde{N}_2^2; \\ \frac{dN_2}{dt}=-\left(\frac{1}{M}\sum_{i=1}^{M}\nu_i\times p_{rj}\times r_{motiv}\right)\left(\sum_{j=1}^{w}\tilde{N}_2^w\right)+ \\ +\left(\frac{1}{KB}\sum_{k=1}^{K}\sum_{g=1}^{B}\left(\mu_{kg}^j\times w_{kg}^j\right)\right)\left(\sum_{j=1}^{w}\tilde{N}_2^w\right)\tilde{N}_1-\xi\tilde{N}_2^2, \end{cases} \quad (18)$$

where the coefficients ε, ζ>0, and describe the damage inflicted by the "prey" and "predator" on themselves, respectively.

5. 3. Development of a method for assessing the security of cyber-physical systems based on the Lotka–Volterra "predator–prey" model

One of the features of cyber-physical systems is the absence of ISS in the infrastructure elements, signal transmission from sensors over open channels, and provision of management and administration based on cloud technologies. This significantly reduces the possibility of forming a security loop, and increases the number of critical points for implementing cyberattacks. In such conditions, security assessment must be carried out offline, which makes it possible to take into account the dynamics of both cyber threats, on the one hand, and the ability of protection means to resist them.

Fig. 4 shows the block diagram of the proposed assessment method.

At *the first stage*, the following are formed and/or calculated:

– metric coefficients of threats;

– weighting factors of threat manifestation;

– determination of the implementation of each threat;

– determination of the implementation of threats to the security service;

– determination of the total threat to the security component;

– determination of economic costs of attack prevention.

At *the second stage*. Based on the analysis of stage 1, the Lotka-Volterra model is chosen, and the corresponding coefficients and components of expressions are calculated using formulas (2)–(18).

At *the third stage*, based on expressions (19)–(21), the current state of security of the cyber-physical system is determined.

The proposed method is based on assessing the security of cyber-physical systems over time. A descriptive characteristic of changes in the current state of CPS security is its *intensity* $l(t)$ – the average number of changes that happened to the current state of CPS security per unit of time. To estimate the time intervals $\Delta t_{[i-q]}$ between changes in the CPS security level, we use the formula:

$$\Delta t_{[i-q]}(t) = \frac{K}{l(t)}, \tag{19}$$

where K – total number of security level changes;

$l(t)$ – intensity of security level changes;

$i, q \in [1; n]$ – serial numbers of changes; $i \geq q$.

We describe changes in security levels as a finite-state machine H^{CPS}, the states of which are described by the formula:

$$H^{CPS} = \left\langle S^I, value, T, S_0^I \right\rangle, \tag{20}$$

where S^I is the finite state of the CPS security level;

value is the value of changes in the CPS security level;

T is the function of transitions of the CPS security level from state k to state j;

S_0^I is the initial state of the CPS security level.

We estimate the function of transitions of the CPS security level T from state k to state j by the formula:

$$T = S_0^I \times value \rightarrow S^I. \tag{21}$$

To determine security states, we use one of the proposed Lotka-Volterra models, taking into account the capabilities of both "prey" and "predators".

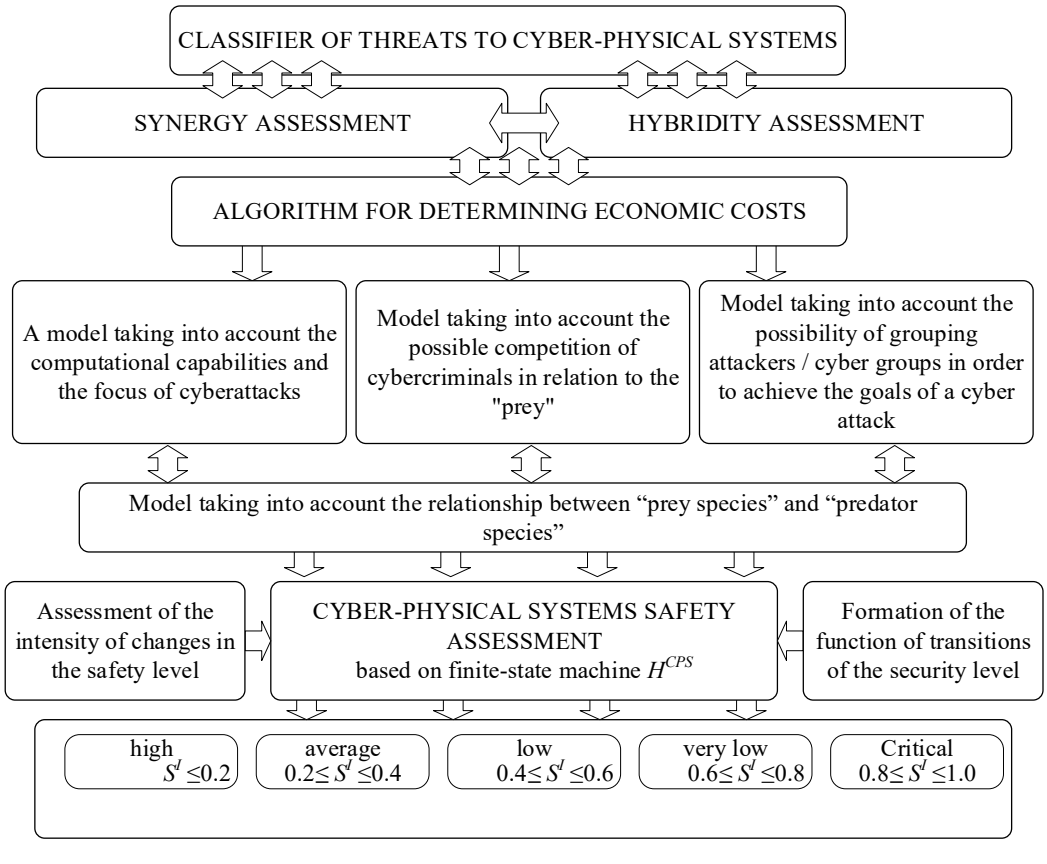

Fig. 4. Block diagram of the method for assessing the security of cyber-physical systems based on the Lotka-Volterra "predator-prey" model

The use of the proposed models for the method of assessing the security of cyber-physical systems based on the Lotka-Volterra model is determined in Fig. 3. For modeling, the values of the parameters included in the expressions for the coefficients of the Lotka-Volterra equations are determined using the threat classifier, which already partially contains quantitative indicators. Thus, the values of the weighting factors of the manifestation of threats are determined quantitatively. On the other hand, some of the indicators contained in the threat classifier need to be quantified.

As a conditionally real CPS, we consider the automated banking system (ABS) of banking sector organizations, which not only belongs to the CPS, but also to critical infrastructure systems. To assess the ABS security, we assume that the information security system has 25 technical means of information protection, which provide security services to bank information resources (BIR), that is, N_1=25, the number of threats Q=194 (https://bdu.fstec.ru/threat). Their description and expert assessment of the distribution of impact on security services are given on the resource (http://skl.hneu.edu.ua/), which allows using the proposed models to automate the calculations of the remaining indicators. Fig. 5 shows the relationship between security services and special security mechanisms, which allows determining the number of required technical protection means (security mechanisms) to provide the corresponding security services.

The formation of a dynamic model for assessing the security of cyber-physical systems begins with the formation of metric coefficients of threats, calculated as

$$w_j^{CPS\ CIF} = \frac{1}{K}\sum_{i=1}^{Q}\sum_{k=1}^{K} w_{ijk}^{CPS\ CIF}, \qquad (22)$$

where w_{CPSi}^{C}, w_{CPSi}^{I}, w_{CPSi}^{A}, w_{CPSi}^{Au}, w_{CPSi}^{Aff} are the expert weighting factors of the security services: confidentiality, integrity, availability, authenticity, and affiliation, as specified earlier.

It is proposed for experts in [26] to form the weighting factors of the cyber threat impact on security services using the values $w_j^{CPS\ CIF} \in \{0;\ 0.1;\ 0.25;\ 0.33;\ 0.5;\ 0.66;\ 0.75;\ 0.9;\ 1\}$. 27 experts were involved in the expert assessment.

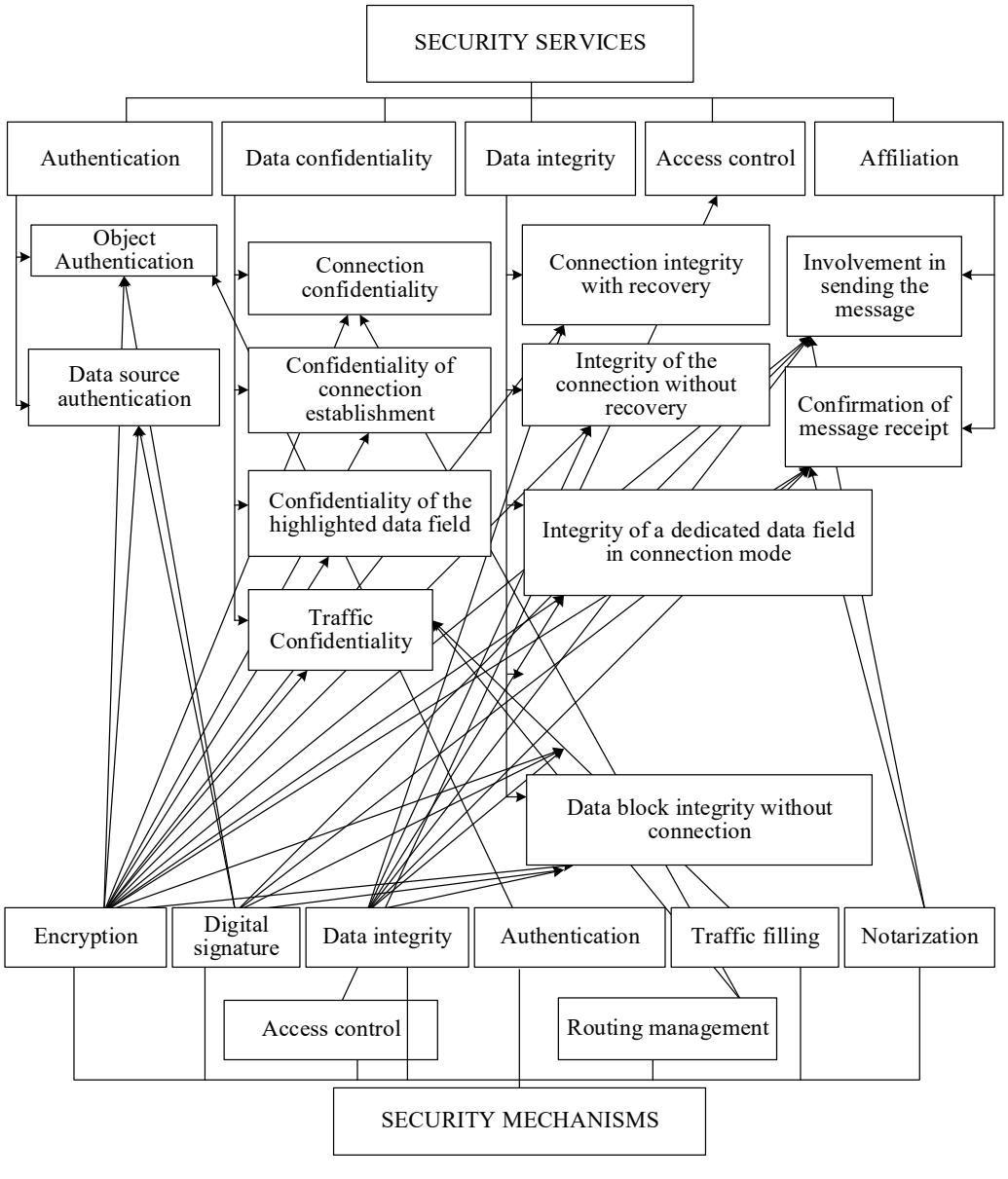

Fig. 5. Relationship between services and special security mechanisms

Table 2 shows the results of distribution of the weighting factors of the main services by experts: confidentiality, integrity, availability and authenticity, as well as average values of the weighting factors of the distribution of technical protection means for security services.

Table 2

Results of expert assessment of the weighting factors of the impact of cyber threats on security services

No. of threat, i	Weighting factors of impact of cyber threats on security services				
	A_i^C	A_i^{Au}	A_i^A	A_i^I	A_i^{Aff}
1	0.28	0.22	0.2	0.21	0.09
2	0.19	0.22	0.23	0.23	0.13
3	0.22	0.15	0.25	0.28	0.1
4	0.21	0.19	0.13	0.3	0.17
5	0.15	0.2	0.36	0.22	0.07
...	...	...	...	...	...
190	0.24	0.21	0.15	0.4	0
191	0.15	0.19	0.15	0.5	0.01
192	0.35	0.17	0.12	0.36	0
194	0.32	0.31	0.12	0.18	0.07
average values of weighting factors for security service					
$w_j^{CPS\,CIF}$	w_{CPSi}^{C}	w_{CPSi}^{Au}	w_{CPSi}^{A}	w_{CPSi}^{I}	w_{CPSi}^{Aff}
	0.26	0.22	0.26	0.25	0.01

Then, based on the average values of the weighting factors for the security service, we determine the distribution of the ISS technical means as:

$$\lambda_j^{CPS\,CIF} = N_1^j \times w_j^{CPS\,CIF}, \quad (23)$$

where j is the security service, N_1^j is the number of "prey" objects (ISS technical means). A limitation of the modeling is the assumption that the technical means of the ISS cannot provide several security services.

To determine the cost indicators of attacks, we use the table of probable loss magnitude of the FAIR (Factor Analysis of Information Risk) risk assessment method [29, 30].

We estimate the costs of attackers for attacks on the assumption that they amount to no more than 10 % of the probable loss magnitude of the prey (Table 3).

Table 3

Probable loss magnitude (PLM) (USD)

No.	losses	lower limit	upper limit
1	Critical	10,000,000	–
2	High	1,000,000	9,999,999
3	Significant	100,000	999,999
4	Medium	10,000	99,999
5	Low	1,000	9,999
6	Very Low	0	999

Then the coefficients of the model are calculated according to the previously derived relationships.

The fertility rate of "prey" in accordance with the proposals on the available resources of "prey" and "predators" (Table 2) and the total number of threats

$$\alpha = \frac{\left|\{Tr_l\}\right|}{Q} = \frac{29}{194} = 0.15. \quad (24)$$

To calculate the coefficient of predator's influence on the prey (β), assume that the number of "predators" (intruders and/or groups of cyber intruders) is N_2=5, and $\left|W_{\text{hybrid } C,I,A,Au,Af\ synerg}\right| = 0.03$, we choose the maximum weighting factor of the impact of each threat 0.33, i. e. each of 194 threats is implemented by cybercriminals every day. The coefficient β of the impact of modern threats on protection means, presented earlier as $\beta = \sum_{i=1}^{M}\left(w_{CPSi}^{C} \cap w_{CPSi}^{I} \cap w_{CPSi}^{A} \cap w_{CPSi}^{Au} \cap w_{CPSi}^{Aff}\right)\chi_i^{CPS}$, largely depends on expert assessments. Based on expert opinions, we obtain the value of the coefficient β=0.32.

To calculate the predator mortality rate (φ), we use the data from Table 1, and we also consider that $M = \left|\{Tr_l\}\right|$. Based on the estimates given in [25, 26, 28], as well as expert estimates, we obtain the numerical value of the coefficient φ, which determines the mortality rate of "predators" in the Lotka-Volterra model φ=0.29.

To calculate the coefficient of prey's influence on the predator (γ), we use the indicator B=3 – security services, where cryptographic protection means (confidentiality, integrity, authenticity) are used. In this case, we assume that the set of characteristics of cryptographic protection means of the security information system $\mu^j = \left|\{C_r^j, S_c^j, O_E^j\}\right|$, the weighting factors for symmetric systems are equal to 0.75, for asymmetric cryptosystems 0.9. The final value of the coefficient γ, which determines the prey's influence on the predator, is 0.27.

The initial values of "prey" and "predators" are, respectively.

$$\tilde{N}_1 = 55 \times 0.26 + 49 \times 0.22 + 73 \times 0.26 + 17 \times 0.25 \approx 48,$$

$$\tilde{N}_2 = N_2 \times \left|W_{\text{hybrid } C,I,A,Au,Af\ synerg}\right| = 5 \times 9 = 45.$$

The number of hybrid threats is determined according to the threat classifier.

The calculations performed provide the numerical values of the coefficients included in the Lotka-Volterra equations.

Parameterized equations allow modeling the dynamics of the development of the cyber-physical system in conditions of hybridity and synergy of threats. The results of modeling the behavior of the conditionally real system are shown in Fig. 6–12.

Fig. 6 shows the dynamics of changes in the number of potential targets and threats.

As the number of critical attacks increases, the interaction between prey and predators becomes more intense, i. e. the period between the growth and decline in the number of both sides of the cyber conflict decreases (Fig. 7).

A more visual representation of the simulation results can be obtained by presenting the results as a phase portrait. A phase portrait (phase diagram) is a graphical representation of how the quantities describing the system state (dynamic variables) depend on each other. In our case, this is the number of predators and prey. A typical phase portrait for dynamic variables of the Lotka-Volterra model is shown in Fig. 8 (the model coefficients correspond to the calculated ones of the considered problem).

As the number of critical threats increases, the total number of threats also increases, and therefore the coefficient α changes. For the new values of the number of critical threats and fertility rate of "prey", the phase portrait is as shown in Fig. 9.

As the coefficient β increases, i. e. the influence of predators on prey becomes more intense even with increasing potential targets (prey), the number of predators decreases rather than grows. This can be explained by the fact that with a more intense impact, the same amount of compromised resources can be reached by fewer predators (Fig. 10).

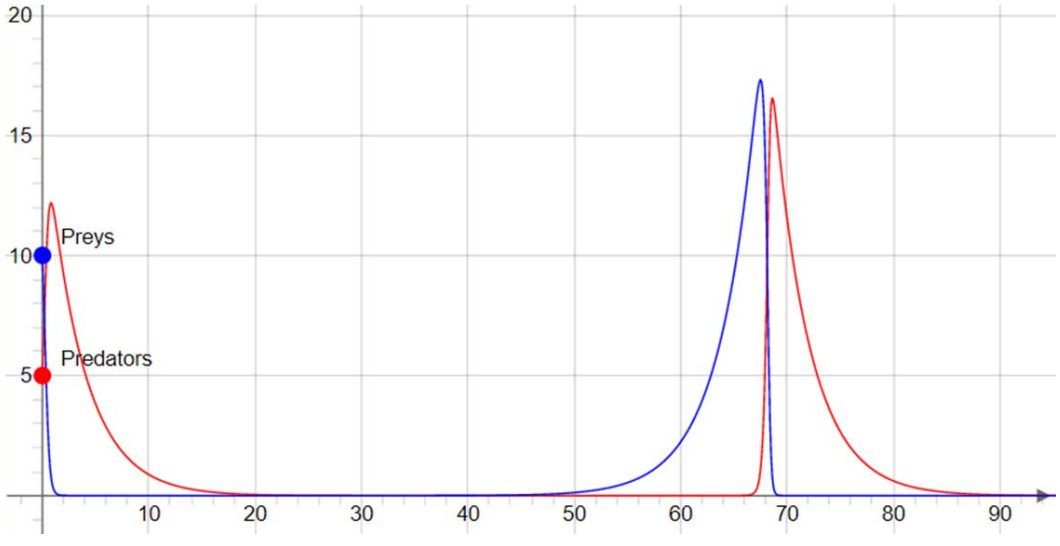

Fig. 6. Dynamics of changes in the number of potential targets and threats, with α=0.29, β=0.39, γ=0.29, φ=0.28

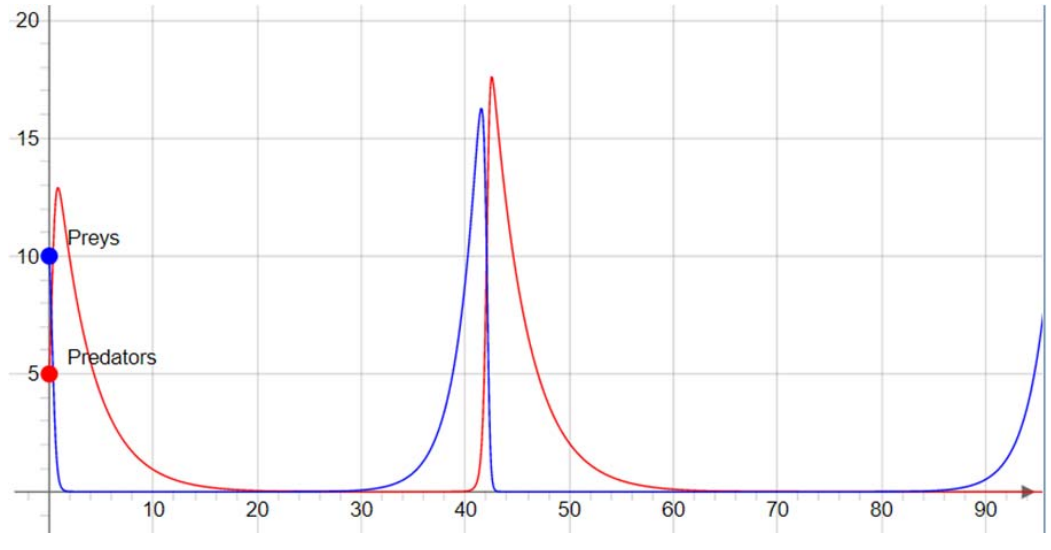

Fig. 7. Reduction of the oscillation period in the "predator" – "prey" system, α=0.49, β=0.39, γ=0.29, φ=0.28

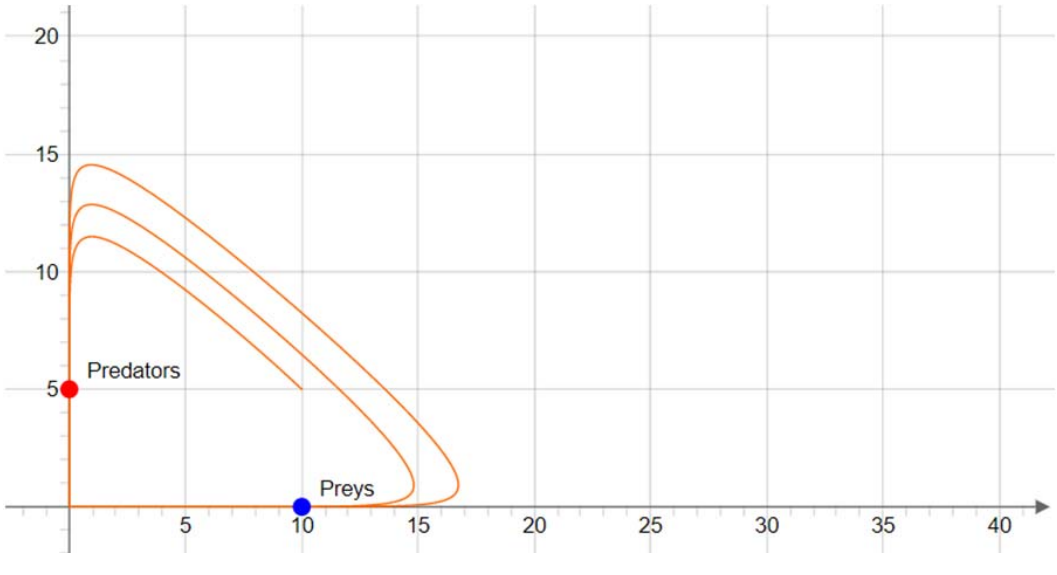

Fig. 8. Phase portrait of CFR dynamics (basic version), with α=0.25, β=0.32, γ=0.29, φ=0.27

An increase in the mortality rate of predators, as shown by simulation experiments, has little effect on the increase in the number of prey, but leads to more intensive predator attacks (Fig. 11).

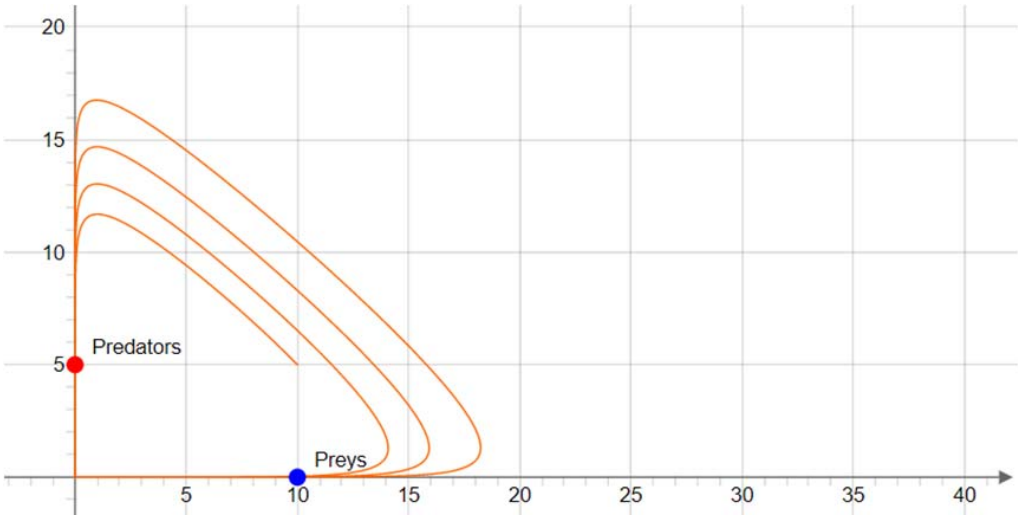

Fig. 9. Phase portrait depending on prey fertility rate, with α=0.39, β=0.32, γ=0.29, φ=0.27

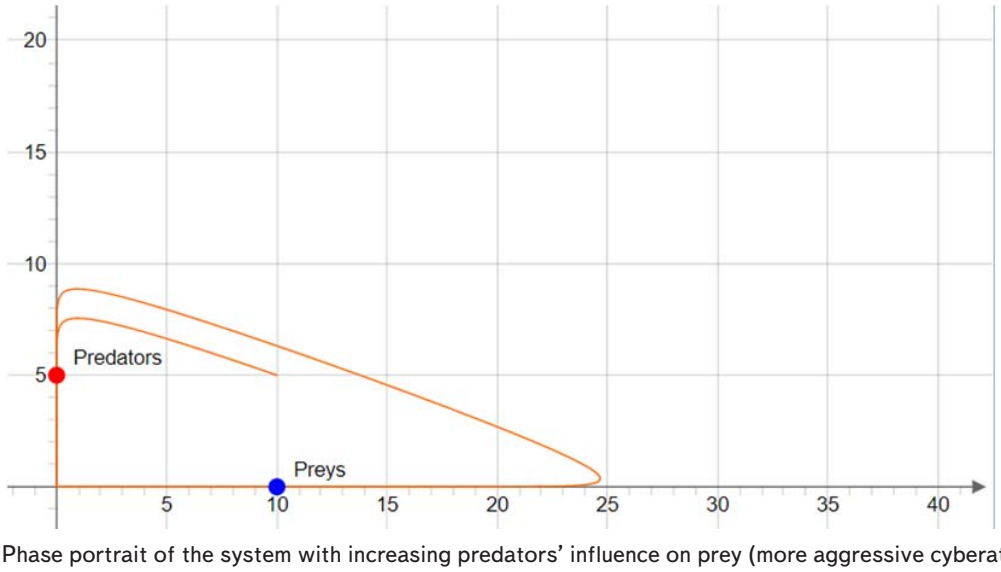

Fig. 10. Phase portrait of the system with increasing predators' influence on prey (more aggressive cyberattacks), with α=0.25, β=0.76, γ=0.29, φ=0.27

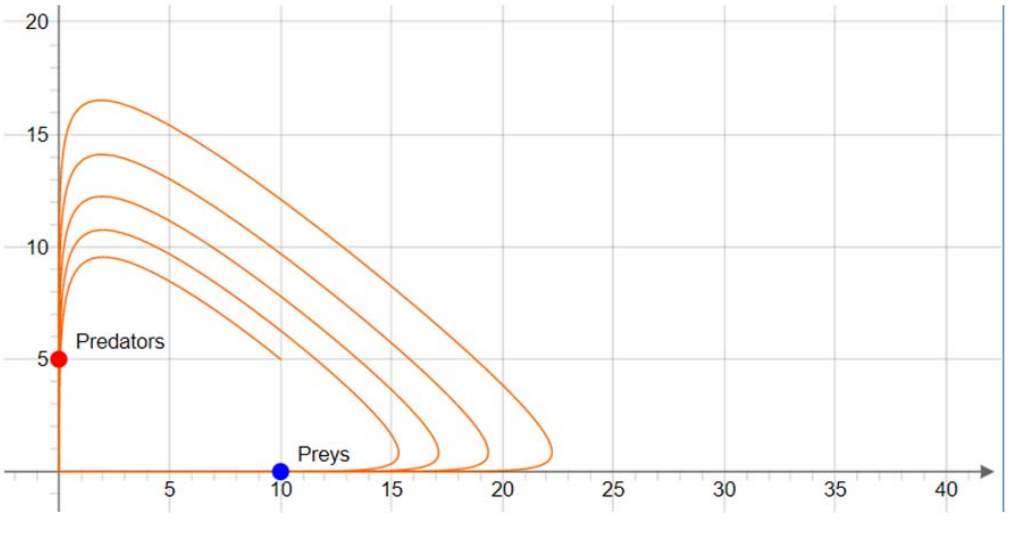

Fig. 11. Phase portrait with increasing mortality rate of predators, with α=0.25, β=0.32, γ=0.58, φ=0.27

As the coefficient of prey's influence on the predator increases, the phase portrait is as shown in Fig. 12. The results obtained can be interpreted as the need to increase the number of predators in order to achieve goals with the same or even smaller number of prey.

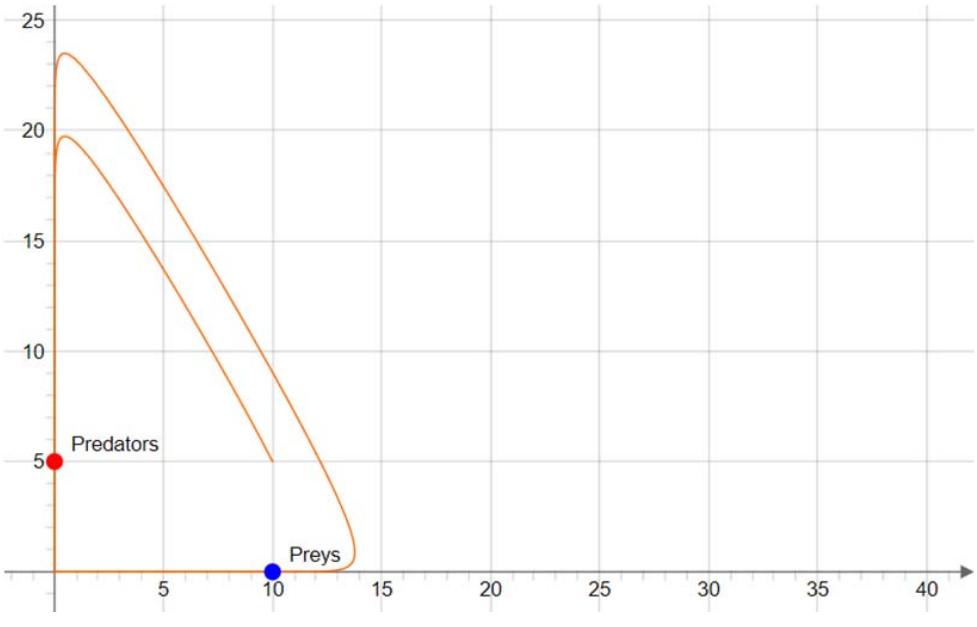

Fig. 12. Phase portrait of the system with increasing coefficient of prey's influence on the predator, with α=0.25, β=0.32, γ=0.29, φ=0.54

6. Discussion of the results of the study of security models of cyber-physical systems based on the Lotka-Volterra model

The analysis of the simulation results (Fig. 6–12) allows us to make a general conclusion that in conditions of limited financial resources for the development and implementation of new security service tools, they should be allocated as follows. The coefficient, the change of which leads to more significant changes in security level, is determined. The most significant factor that leads to changes in the considered coefficient is defined. Measures leading to such changes are determined. Table 4 shows the comparative results of the analysis of the practical use of the method for assessing the security state of cyber-physical systems based on the Lotka-Volterra model.

The analysis of Table 4 shows that almost all practical security assessment approaches operate in the static mode, that is, during working hours, incident detection systems (deviations from normal operation) record incidents/threats, and their analysis is carried out during non-working hours. This approach does not allow timely consideration of the synergy and hybridity of targeted attacks, the need for preventive measures. The proposed method and the methods in [14, 24] use security assessment approaches based on the Lotka-Volterra model, which allows for dynamic assessment (real-time assessment of the dynamics and capabilities of threats). However, the works [14, 24] do not take into account the synergy and hybridity of modern threats, the possibility of integrating them with social engineering methods. In the proposed method, based on the proposed classifier, these signs of threats are taken into account, which makes it possible to obtain the coefficients of the model and, knowing the number of threats, to determine the number of threats with these signs.

Table 4

Results of the study of the practical use of the method for assessing the security state of cyber-physical systems based on the Lotka-Volterra model

Method	Criteria								
	qualitative assessment	quantitative assessment	comprehensive assessment	assessment of threat characteristics		economic optimization	assessment of compliance with regulatory standards	effectiveness of preventive measures	assessment mode
				hybridity	synergy				
NIST	+	–	–	–	–	–	–	–	stat.
FAIR		–	+	–	–	–		+	stat.
EBIOS	+		–	–	–	–	–	+	stat.
MEHARI		–	+	–		–	–	–	stat.
OCTAVE	+	–	–	–	–	–	–	–	stat.
IT-GRUNDSHULTZ	+	–	–	–	–	–	–	+	stat.
IRAM	+	–	–	–	–	–	–	–	stat.
RISK WATCH	–	+	–	–	–	–		+	stat.
FRAP	+	–	–	–	–	–	–	–	stat.
CRAMM			+	–	–	–	–	+/–	stat.
MAGERIT	+	+	–	–	–	–	–	–	stat.
Method in [14]	+	+	–	–	–	–	–	+/–	dynamic
Method in [24]	+	+	–	–	–	–	–	+/–	dynamic
Proposed method	+	+	+	+	+	+	+	+/–	dynamic

So in the reviewed example, with the total number of threats Q=194, the coefficient of predators' influence on the prey (predation coefficient) allows determining the number of threats with signs of synergy and hybridity (with β=0.32, the number of threats $Q_{synerg}=Q\times\beta=194\times0.32=62.08$). In addition, it depends on the introduction of new security service means; as an investment, it makes sense to choose those protection means (confidentiality, integrity, authenticity), the weighting factor of which has the maximum value. As mentioned earlier, the weighting factor for asymmetric cryptographic protection means is 0.9, unlike symmetric (0.75). Available resources should be first directed to the development of these protection means.

The threat assessment analysis presented in [31–35] shows that the number of targeted attacks (attacks with signs of synergy and hybridity, as well as integration with social engineering methods) on cyber-physical systems is growing every year in direct proportion with the growth of computing resources and digital services. Various channels are used to hack systems, but usually mobile Internet channels (59 %), while external sources of attacks account for 26 % [35]. In the simulation, statistics on attacks on the banking sector were used, and the models made it possible to determine the coefficient of predators' influence on the prey (predation coefficient). This corresponds to the assessment of static data and gives 31 % of threats with signs of synergy and hybridity. All this confirms the adequacy of the proposed approach.

It is necessary to point out the limitations of the research performed. First of all, these are the limitations that follow from the constraints of the model itself. The model equations used are linear, since the values of "predators" and "prey" are included in the linear equation and there are no terms that include both variables simultaneously. This simplified representation of the model does not allow obtaining and investigating more complex nonlinear effects that can demonstrate synergistic effects. The second limitation of the study is the assumption that the "predator-prey" community is closed. This assumption means that the processes of the emergence of new attackers and new types of attacks are not considered, that is, the variety of attacks is determined using the existing threat classifier.

Overcoming these limitations can be considered as directions for the development of the research performed. As additional areas of research, it is proposed to study the stability of the existing "predator–prey" system, in particular, the relationship between the model coefficients (and, accordingly, the processes defining them), describing equilibrium points.

7. Conclusions

1. Security models of cyber-physical systems have been developed, taking into account the computing capabilities and focus of targeted cyberattacks, possible competition of attackers in relation to the "prey". The models also reflect the possibilities of grouping in order to achieve the cyberattack goals, relationships between "prey species" and "predator species". Based on the proposed approach, the coefficients of the Lotka-Volterra model α=0.39, β=0.32, γ=0.29, φ=0.27 were obtained, which take into account the synergy and hybridity of modern threats, funding for the formation and improvement of the protection system, and also allows determining the financial and computing capabilities of the attacker based on the identified threats.

2. Modification of the "predator-prey" model allows grouping not only "prey species", but also "predator species", which affects not only the formation of collective protection, but also gives a synergistic effect of cyber threats in order to achieve the cyberattack goals based on the relationships between "prey species" and "predator species".

3. A method for assessing the security of cyber-physical systems based on the Lotka-Volterra predator-prey model has been developed. The method is based on the proposed threat classifie, taking into account hybridity and synergy. The classifier structure reflecting the hybridity and synergy of threats is presented. The proposed method, unlike the existing ones, makes it possible to assess the security level of developing cyber-physical systems and security systems, that is, to make a dynamic assessment rather a static one, as suggested in previous studies.

4. Studies on the practical implementation of the proposed approach have been carried out. In the course of practical implementation, not only assessment of the security level of the cyber-physical system was carried out, but also simulation of the development dynamics of the "predator-prey" system for the conditional cyber-physical system and its security system. The assessment provides recommendations regarding the allocation of limited resources to effectively protect objects that are targets of hybrid and synergistic attacks. The simulation allowed not only visualizing the relationships between "predators" and "prey", but also determining research areas, in which the dynamic behavior indicators of the parties to a cyber conflict can be reduced. This ultimately eliminates drastic changes in the number of potential threats and resulting prevention measures.

References

1. IoT Security Maturity Model: Description and Intended Use (2018). Available at: https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf
2. IoT Security Maturity Model: Practitioner's Guide (2019). Available at: https://iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2019-02-25.pdf
3. Global'noe issledovanie tendentsiy informatsionnoy bezopasnosti na 2017. Available at: https://www.pwc.ru/ru/publications/gsiss-2017.html
4. Otchet Antifishinga o zaschischennosti sotrudnikov v 2020 godu (2021). Available at: https://antiphish.ru/tpost/88km7s0a01-otchyot-antifishinga-o-zaschischennosti
5. Gartner nazvala 10 glavnyh trendov v sfere kiberbezopasnosti v 2021 godu. Available at: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%93%D0%BB%D0%B0%D0%B2%D0%BD%D1%8B%D0%B5_%D1

%82%D0%B5%D0%BD%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B8_%D0%B2_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D0%B5_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8#.2Agartner_.D0.BD.D0.B0.D0.B7.D0.B2.D0.B0.D0.BB.D0.B0_10_.D0.B3.D0.BB.D0.B0.D0.B2.D0.BD.D1.8B.D1.85_.D1.82.D1.80.D0.B5.D0.BD.D0.B4.D0.BE.D0.B2_.D0.B2_.D1.81.D1.84.D0.B5.D1.80.D0.B5_.D0.BA.D0.B8.D0.B1.D0.B5.D1.80.D0.B1.D0.B5.D0.B7.D0.BE.D0.BF.D0.B0.D1.81.D0.BD.D0.BE.D1.81.D1.82.D0.B8_.D0.B2_2021_.D0.B3.D0.BE.D0.B4.D1.83

6. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et. al.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021). Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 188. doi: https://doi.org/10.15587/978-617-7319-31-2
7. Hryshchuk, R., Yevseiev, S. (2016). The synergetic approach for providing bank information security: the problem formulation. Ukrainian Scientific Journal of Information Security, 22 (1), 64–74. doi: https://doi.org/10.18372/2225-5036.22.10456
8. Hryshchuk, R. V. (2010). Teoretychni osnovy modeliuvannia protsesiv napadu na informatsiu metodamy teoriy dyferentsialnykh ihor ta dyferentsialnykh peretvoren. Zhytomyr: Ruta, 280.
9. Hryshchuk, R. V., Danyk, Yu. H.; Danyk, Yu. H. (Ed.) (2016). Osnovy kibernetychnoi bezpeky. Zhytomyr: ZhNAEU, 636.
10. Petrov, O., Lahno, V. (2016). Povyshenie informatsionnoy bezopasnosti avtomatizirovannyh sitsem obrabotki dannyh na transporte. Information Technology in Selected Areas of Management. Krakow, 65–78.
11. Model' zrelosti bezopasnosti interneta veschey: tolchok k razvitiyu bezopasnyh sistem. Available at: https://ics-cert.kaspersky.ru/reports/2019/08/14/the-internet-of-things-security-maturity-model-a-nudge-for-iot-cybersecurity/
12. Trubetskov, D. I. (2011). Phenomenon of Lotka–Volterra mathematical model and similar models. Izvestiya VUZ. Applied Nonlinear Dynamics, 19 (2), 69–88. doi: https://doi.org/10.18500/0869-6632-2011-19-2-69-88
13. Bratus', A. S., Novozhilov, A. S., Platonov, A. P. Dinamicheskie sistemy i modeli biologii. Available at: https://avmaksimov.ucoz.ru/_ld/1/109_-Bratus_A-Novoz.pdf
14. Dormidontov, A. V., Mironova, L. V., Mironov, V. S. (2018). Possibility of the mathematical model of counteraction application to the assessment of transport infrastructure security level. Civil Aviation High Technologies, 21 (3), 67–77. doi: https://doi.org/10.26467/2079-0619-2018-21-3-67-77
15. Kononovich, I. V. (2014). Dynamics of the number of information security incidents. Informatics and Mathematical Methods in Simulation, 4 (1), 35–43. Available at: http://immm.opu.ua/files/archive/n1_v4_2014/n1_v4_2014.pdf
16. Kononovich, I., Mayevskiy, D., Podobniy, R. (2015). Models of system of the cibersecurity providing with delay of reaction on incidents. Informatics and Mathematical Methods in Simulation, 5 (4), 339–346. Available at: http://immm.opu.ua/files/archive/n4_v5_2015/n4_v5_2015.pdf
17. Lippert, K. J., Cloutier, R. (2021). Cyberspace: A Digital Ecosystem. Systems, 9 (3), 48. doi: https://doi.org/10.3390/systems9030048
18. Mazurczyk, W., Drobniak, S., Moore, S. (2016). Towards a Systematic View on Cybersecurity Ecology. Combatting Cybercrime and Cyberterrorism, 17–37. doi: https://doi.org/10.1007/978-3-319-38930-1_2
19. Gorman, S. P., Kulkarni, R. G., Schintler, L. A., Stough, R. R. A Predator Prey Approach to the Network Structure of Cyberspace. Available at: https://www.researchgate.net/publication/255679706_A_predator_prey_approach_to_the_network_structure_of_cyberspace
20. Crandall, J. R., Ensafi, R., Forrest, S., Ladau, J., Shebaro, B. (2008). The ecology of Malware. Proceedings of the 2008 Workshop on New Security Paradigms - NSPW '08. doi: https://doi.org/10.1145/1595676.1595692
21. Fink, G. A., Haack, J. N., McKinnon, A. D., Fulp, E. W. (2014). Defense on the Move: Ant-Based Cyber Defense. IEEE Security & Privacy, 12 (2), 36–43. doi: https://doi.org/10.1109/msp.2014.21
22. Wu, L., Wang, Y. (2011). Estimation the parameters of Lotka–Volterra model based on grey direct modelling method and its application. Expert Systems with Applications, 38 (6), 6412–6416. doi: https://doi.org/10.1016/j.eswa.2010.09.013
23. Diz-Pita, É., Otero-Espinar, M. V. (2021). Predator–Prey Models: A Review of Some Recent Advances. Mathematics, 9 (15), 1783. doi: https://doi.org/10.3390/math9151783
24. Minaev, V. A., Sychev, M. P., Vayts, E. V., Gracheva, Yu. V. (2016). Matematicheskaya model' "hischnik-zhertva" v sisteme informatsionnoy bezopasnosti. Informatsiya i bezopasnost', 19 (3), 397–400. Available at: https://elibrary.ru/item.asp?id=27186929
25. Yevseiev, S., Laptiev, O., Lazarenko, S., Korchenko, A., Manzhul, I. (2021). Modeling the protection of personal data from trust and the amount of information on social networks. EUREKA: Physics and Engineering, 1, 24–31. doi: https://doi.org/10.21303/2461-4262.2021.001615
26. 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. doi: https://doi.org/10.15587/1729-4061.2021.233533
27. Ya dogonyayu, ty ubegaesh'. Chto takoe model' Lotki-Vol'terry i kak ona pomogaet biologam. Available at: https://nplus1.ru/material/2019/12/04/lotka-volterra-model

28. 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: https://doi.org/10.15587/1729-4061.2020.205702
29. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. Available at: https://www.iso.org/standard/54534.html
30. An Introduction to Factor Analysis of Information Risk (FAIR). Available at: https://www.yumpu.com/en/document/read/7271140/an-introduction-to-factor-analysis-of-information-risk-fair
31. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. NISTIR. doi: https://doi.org/10.6028/nist.ir.8105
32. Lohachab, A., Lohachab, A., Jangra, A. (2020). A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks. Internet of Things, 9, 100174. doi: https://doi.org/10.1016/j.iot.2020.100174
33. Ugrozy bezopasnosti yadra paketnoy seti 4G (2017). Available at: https://www.ptsecurity.com/ru-ru/research/analytics/epc-2017/
34. Uyazvimosti protokola Diameter v setyah 4G (2018). Available at: https://www.ptsecurity.com/ru-ru/research/analytics/diameter-2018/
35. Godovoy otchet o podverzhennosti kiberatakam sotrudnikov kompaniy v Rossii i SNG. Available at: https://welcome.tiger-optics.ru/антифишинг-годовой-отчет?_ga=2.171180576.1827066423.1631692491-524698473.1631692491