DOI: https://doi.org/10.36910/6775-2524-0560-2024-56-08
UDC 004.49
Shkitov Andrii, Postgraduate student
https://orcid.org/0009-0005-4600-8467
Open International University of Human Development «Ukraine», Kyiv, Ukraine

FEATURES OF CREATING A MULTI-LEVEL MODEL OF CYBER SECURITY OF CRITICAL INFRASTRUCTURE DATA: AN INTERDISCIPLINARY APPROACH

Shkitov A. Features of creating a multi-level model of cyber security of critical infrastructure data: an interdisciplinary approach. The article examines the model of ensuring cyber security of Ukraine and documents the organizational and legal support for the protection of critical infrastructure objects from cyber attacks. The main concepts are described: multi-level data model, identification of cyber security, and critical infrastructure facilities. The levels of protection of critical infrastructure objects and measures at each level that ensure cyber security are highlighted and described. The stability of the critical infrastructure object is substantiated, and the formula for determining risks in critical infrastructure objects is described. The developed basic tuple model for the classification of critical information infrastructure objects by multi-level data models is highlighted. The prospects and risks of implementing multi-level data models in critical infrastructure facilities have been identified. It was concluded that multi-level data models are an important tool for ensuring cyber security in today's digital world and critical infrastructure enterprises in private. They allow for the effective protection of confidential information by isolating and controlling different levels of data access.
Keywords: cyber security, critical infrastructure, identification model, regulatory and legal support, multi-level data model

Шкітов А.А. Особливості створення багаторівневої моделі кібербезпеки даних критичної інфраструктури: міждисциплінарний підхід. У статті досліджено модель забезпечення кібербезпеки України та документи організаційно-правового забезпечення захисту об'єктів критичної інфраструктури від кібератак. Описано основні поняття: багаторівнева модель даних, ідентифікація кібербезпеки та об'єкти критичної інфраструктури. Висвітлено та описано рівні захисту об'єктів критичної інфраструктури та заходи на кожному рівні, що забезпечують кібербезпеку. Обґрунтовано стійкість об'єктів критичної інфраструктури та описано формулу для визначення ризиків в об'єктах критичної інфраструктури. Висвітлено розроблену базову модель кортежу для класифікації об'єктів критичної інформаційної інфраструктури за багаторівневими моделями даних. Визначено перспективи та ризики впровадження багаторівневих моделей даних на об'єктах критичної інфраструктури. Було зроблено висновок, що багаторівневі моделі даних є важливим інструментом для забезпечення кібербезпеки в сучасному цифровому світі та на підприємствах критичної інфраструктури, а заходи кібербезпеки забезпечують ефективний захист конфіденційної інформації шляхом ізоляції та контролю різних рівнів доступу до даних.
Ключові слова: кібербезпека, критична інфраструктура, модель ідентифікації, нормативно-правове забезпечення, багаторівнева модель даних

Introduction. In today's digital world, where cyber threats are becoming more complex and dangerous, ensuring the cyber security of critical infrastructure becomes an extremely important task. This requires the classification and improvement of approaches to protection against cyber threats and the implementation of effective innovative strategies. One of the classification leitmotifs of this problem is the development and implementation of a multilevel data model.

Cyber wars of the 21st century are relevant for the whole world and increase the importance of this issue. Ukrainian organizations should be maximally protected from cyber attacks. As noted in the State Service of Special Communications and Information Protection of Ukraine, «cyber security of critical infrastructure is one of the priorities of the national security of Ukraine». It is also worth noting that in today's world, where the regulatory environment is constantly changing and becoming increasingly complex, the identification of requirements becomes extremely important for businesses, government bodies, and critical infrastructure in general (Fig. 1).

Under the conditions of cyber modernity, there are a number of normative documents that determine the classification and categorization leitmotifs of cyber protection of critical infrastructure objects, which are mandatory for enterprises, institutions, and organizations classified as critical infrastructure objects according to the legislation. These include: Resolution of the Cabinet of Ministers of Ukraine dated June 19, 2019, No. 519 «On approval of General requirements for cyber protection of critical infrastructure facilities»; Resolution of the Cabinet of Ministers of Ukraine dated November 11, 2020, No. 1176 «On approval of the Procedure for conducting a review of the state of cyber protection of critical information infrastructure state information resources and information the requirement for the protection of which is established by law»; Resolution of the Cabinet of Ministers of Ukraine dated December 23,

2020, No. 1295 «Some issues of ensuring the functioning of the system for detecting vulnerabilities and responding to cyber incidents and cyber attacks»; Resolution of the Cabinet of Ministers of Ukraine dated December 29, 2021, No. 1426 «On approval of the Regulation on the organizational and technical model of cyber protection»; Methodological recommendations for increasing the level of cyber protection of critical information infrastructure approved by the order of the State Special Communications Administration dated 06.10.2021 No. 601 (with changes introduced in accordance with the orders of the State Special Communications Administration dated 10.07.2022 No. 343); Order of the State Special Communications Administration dated December 1, 2023, No. 1011 «On the approval of Recommendations for the development of a plan for the protection of a critical infrastructure facility based on the project threat of a national level cyber attack/cyber incident» and others.

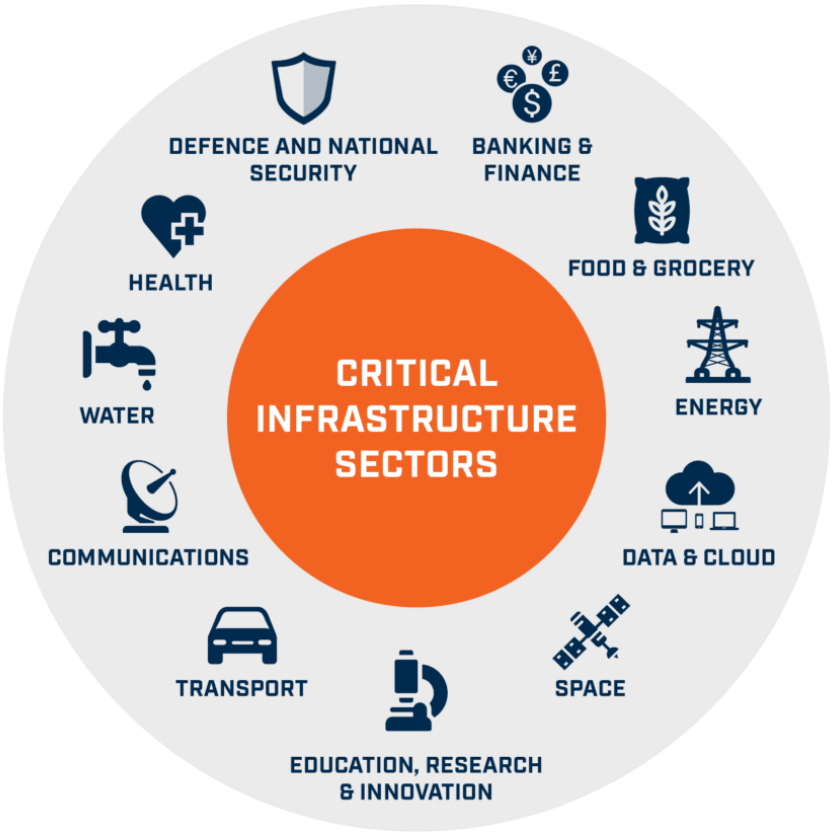

Fig. 1. General sectors of critical infrastructure

Implementing cyber protection measures involves: identification - detection of real and potential cyber threats for prevention and their neutralization; protection - development and implementation of methods, means, and procedures of cyber protection directed at software sustainability and reliability, functioning of information telecommunications, information, and telecommunications and technological systems; detection - conducting monitoring, definition, collection, and processing of atypical events in cyberspace; response - application of measures aimed at the prevention of cyber incidents, cyber attacks, minimization of their possible consequences (prevention of threats to life or health of people and infliction of damage to property), improvement of systems of cyber protection taking into account the necessity of proportionality and opportunities of such systems against real and potential risks; recovery - renewal of regular functioning of information and telecommunications technological systems after cyber attacks, recovery of information and information in case of their damage or deletion, creation of prerequisites for carrying out an investigation by consequences of cyber attacks. During the time of software functioning, the basic infrastructure of cyber protection has to provide protection in cyberspace, national electronic informative resources, communication, and technological systems; protection of objects of critical infrastructure; implementation of activities on forming a culture of cyber security on objects of critical infrastructure and enterprises regardless of their forms of property; informing citizens about the consequences of cyber incidents [1-3].

So, in the modern cyber age, protecting critical infrastructure is one of the primary tasks of the state, taking into account the fact that the latest information and communication technologies are being implemented in Ukraine in all areas. At the same time, the issue of classification and regulation of the multi-level data model, specifically regarding the cyber protection system of critical infrastructure objects and the diagnosis of the state of cyber security, is one of the important and relevant in the conditions of Ukraine.

Literature review. The following scientists investigated the issue of cyber security of critical infrastructure in their works: Hnatiuk S.O. [4], Ivanyuta S.P. [5], Kondratov S.I. [6], Lukyanchuk R.V. [7], Leonov B.D. [8], Ryzhov I.M. [9], Seryogin V.S. [6], Sukhodolya O.M. [10], Tkachuk N.A. [11], Tsiapa S.M. [12], etc. The directions of the development of cyber security were considered in their works by V. Lebedev, D. Ogorodnikov, M. Oleynik, D. Prozorov, A. Svishchev, E.V. Kovalenko, O.O. The question of the multi-level model in cyber security Kharchenko V.P., Korchenko O.G., Hnatyuk S.O. [13, 14] and others.

In the research work [15], a logical-probabilistic model of cyber security for critical infrastructure objects in the power industry was developed for protection against cyber threats and the study of event probabilities. A research article [16] presents a simulator based on agents for evaluating cyber threats in interconnected critical infrastructures that support Italian legislative requirements of cyber protection measures. The article [17] suggests a taxonomy for modeling relationships in critical infrastructure to improve analysis of cyber security by detecting vulnerabilities and critical components in complex systems. Another paper [18] proposes a model for protecting critical informative infrastructure by analyzing functions, connections, threat objects, and implementing methods for minimizing damage from security violations and material costs.

From a literature review, it is evident that scientists all over the world are dealing with cyber security issues and forming information protection models for higher authorities and powerful commercial structures. Since the main damage to information is usually caused by criminal actions (viruses, hacking of secret keys, data theft, etc.), various security mechanisms are created to combat them, including organizational, technical, and software measures and means of information protection [6]. However, a systematic analysis of the multi-level data model in cyber security identification needs further research. The purpose of this work is to consider the main features of creating a multi-level model of cyber security of critical infrastructure data and to determine the main directions of development of this model

Methodology. The model of the regulatory environment allows one to view data at multiple levels of abstraction, from specific requirements to high-level policies and strategies. Fundamentally, the multi-level security model is built on models of authority and truth verification, providing authorized access to users to closed information in databases based on predetermined powers. However, this is not enough for protection, as such models do not have secrecy classes, and databases usually store information from open to completely confidential. For such purposes, the Bell-LaPadula multi-level security model, which is also called the «model of the highest level of secrecy» [19, 20], is intended, which provides users with access to secret data in databases according to different classes of secrecy and is a classic model of an authorized demarcation of access to data. The Bell-LaPadula model uses concepts such as the level of secrecy, the set and current levels of user access, the level of the hierarchy of objects, and others [21].

Thus, the benefits of using a multi-level data model include enabling a more precise definition of requirements, improving the effectiveness of risk analysis, and ensuring compliance with regulatory requirements.

The use of a multi-level data model also helps to avoid duplication of information and improves knowledge management in the organization, which is the prerogative of special services.

In the classification-categorical nature of priority algorithms in information protection, it is worth noting that Identification (lat. Identifico) — is the recognition of something or someone. In this sense, the term is used in general engineering and legal psychology, where it is understood as the process of comparing one object with another on the basis of any feature or property, as a result of which their similarity or difference is established. Identification is the act of establishing an identity [22]. In this context, Identification in particular (information security) is a procedure for recognizing a user in the system, as a rule, with the help of a preventively determined name (identifier) or other a priori information about them, which is perceived by the system.

Identification is used to obtain information about the subject of the system based on the identifier provided by them. It is the initial procedure for granting access to the system. After it, authentication and authorization are carried out [23].

In our opinion, the multi-level data model of cyber security provides for the integration of classification-categorical leitmotifs of protection levels and measures at each level of implementation. This model is based on the idea that no single defense can be completely effective in addressing all cyber threats, so a combination of measures at different levels of the infrastructure must be used.

The first level of logical conditioning with respect to the multi-level model is network and systems level safeguards. This includes the use of network firewalls, interface filters, user authentication and authorization, and other technologies to prevent unauthorized access to the system.

The second level is protection at the level of applications and services. This includes the use of anti-virus programs, data integrity mechanisms, protection against software vulnerabilities, and other technologies to prevent cyber attacks on applications and services.

The third level is protection at the data level. This includes data encryption, access control to confidential information, auditing, and monitoring of user activity to identify suspicious activities.

In the classification-categorical nature, one of the main advantages of the multi-level data model of cyber security is its comprehensive approach to protection against cyber threats. The integration of different levels of protection allows you to create a reliable barrier against various types of attacks and ensure full protection of critical infrastructure.

In addition, multi-level data models allow you to effectively manage access rights by identifying them in accordance with regulatory and legal provisions and providing the ability to precisely control who has access to which information. This provides an additional layer of protection, preventing possible security breaches due to unauthorized access.

In view of this, modern domestic scientists O.G. Korchenko, Yu.O. Dreys, and Romanenko O.O. proposed a basic tuple model for the classification of critical information infrastructure (CII) objects of the state, which contains the main identifiers of the object and is suitable for the topic of our research [24]:

$$ID =\leq ID_1, ID_2, \ldots, ID_i, \ldots, ID_n >, \quad (1)$$

where $ID_i \subseteq ID \ (i = 1, n)$ is the component of the tuple displaying the i-th object identifier, and n is their number.

For example, to form the list of the state [19, 20, 5, 11], with n =≤ 8, tuple (1) is defined as:

$$ID = < ID, ID, ID, ID, ID, ID, ID, ID >=<S,U,O,N,I,R,H,M >,1\ 2\ 3\ 4\ 5\ 6\ 7\ 8 \quad (2)$$

The first component of the tuple S - the KII sector can be represented as a set of sectors:

Taking (4) into account, expression (3) can be represented in the following form: 3 {,,..., }},

$$S = \left\{\bigcup_{i=1}^{n_1} S_i\right\} = \{S_1, S_2, \ldots, S_{n_1}\}, \quad (3)$$

Where $S_i \subseteq S \ (i = \overline{1, n_1})$ is the i-th subset of groups of KII sector identifiers, and n_1 is the total number of groups. For the i-th subset S_i we define as:

$$S_i = \left\{\bigcup_{j=1}^{n_{1j}} S_{ij}\right\} = \{S_{i1}, S_{i2}, \ldots, S_{in_{1i}}\}, \quad (1)$$

Where $S_{ij} \subseteq S_i \ (j = \overline{1, n_{1i}})$ are identifiers of sectors of the i-th group, and n_{1i} - their number. Taking into account **Помилка! Джерело посилання не знайдено.**, the expression **Помилка! Джерело посилання не знайдено.** can be presented in the following form:

$$S = \{\bigcup_{i=1}^{n_1} S_i\} = \left\{\bigcup_{i=1}^{n_1} \left\{\bigcup_{j=1}^{n_1 j} S_{ij}\right\}\right\} = \left\{\{S_{11}, S_{12}, \ldots, S_{1n_{11}}\}, \{S_{21}, S_{22}, \ldots, S_{2n_{12}}\}, \ldots, \left\{S_{n_1 1}, S_{n_1 2}, \ldots, S_{n_1 n_{1mu1}}\right\}\right\}, \left(i = \overline{l, n_1}, \ j = \overline{l, n_{1i}},\right). \quad (5)$$

The next component of the tuple U is the set of identifiers of the administrative-territorial units of Ukraine, within which the OKI is located and displayed as:

$$S = \left\{\bigcup_{i=1}^{n_2} U_i\right\} = \{U_1, U_2, \ldots, U_{n_2}\} = \{»01», »02», »03», \ldots, »n_2»\} \quad (6)$$

Where $Ui \subseteq U \ (i = \overline{1, n_2})$ is the identifier of the administrative-territorial unit, and n_2 is their total number.

It is also necessary to consider it expedient to disclose the concept of stability of a critical infrastructure object, which was clearly disclosed by O.P. Ermenchuk.

In other words, the stability of a critical infrastructure object is its ability to counter threats, minimize the consequences of their impact and negative factors, and quickly recover. For operators, the ideal model for ensuring the stability of CI objects is one where even the active direct action of various threats does not interfere with guaranteeing the provision of basic functions and services, and the restoration of basic functions and services is carried out in the shortest possible time. It is important to identify risks at the earliest possible stage using the proposed formula:

$$P = f(\Pi, B, \text{C}, T) \quad (7)$$

Each of these risk components can be evaluated by experts on the appropriate point scale using the methods evaluations mentioned above. In the simplest version, taking into account the coefficients of significance, b_i the function P has the following form:

$$P = b_1\Pi + b_2B + b_3C + b_4T, \text{де } b_1 + b_2 + b_3 + b_4 = 1 \quad (2)$$

Where risk is *P*, the state of protection of the object (C) against a certain threat, the potential of the threat (P) and the duration of its action, the predicted period of restoration of the functioning of the CI object (T), the importance of the object (B) for a certain type subjects (state, society, business) [11].

However, it must be taken into account that the implementation of multi-level data models can require significant efforts and resources. It requires careful design and implementation, as well as constant monitoring and adaptation to changes in cyber security threats.

In the future, the development of artificial intelligence and machine learning technologies may contribute to further improvements of multi-level data models, specifically for critical infrastructure enterprises. They can become more adaptive and effective in responding to new cyber threats by automating the processes of detection and response to potential attacks.

Results and Discussion. Multi-level data models are an important tool for ensuring cyber security in today's digital world and critical infrastructure enterprises in particular. They allow one to effectively protect confidential information by isolating and controlling different levels of data access. With the right approach and the use of modern technologies, multi-level data models can provide a high level of protection against cyber threats.

Therefore, the normative-legal regulation of the classification-categorical nature of the multi-level data model should be understood as a subject of jurisdiction enshrined in the Constitution of Ukraine regarding the foundations of national security, the foundations of internal and external policy, electronic communications, and the protection of state information resources and information. In accordance with this, the legal and organizational bases for ensuring the protection of the vital interests of man and citizen, society, and the state, national interests of Ukraine in cyberspace, the main goals, directions, and principles of state policy in the field of cyber security, the powers of state bodies, enterprises, institutions, and organizations must be determined [22]. At the same time, cyber security protects the vital interests of a person and citizen, society, and the state in cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention, and neutralization of real and potential threats to the national security of Ukraine in cyberspace [22].

In our opinion, the ISO/IEC 27032 standard defines «cyber security» through the category of cyberspace security as preserving the confidentiality, integrity, and availability of information in cyberspace.

According to the Law of Ukraine «On the Basic Principles of the Development of the Information Society in Ukraine for 2007-2015», the problem of information security should be solved by:

- creating a fully functional information infrastructure of the state and ensuring the protection of its critical elements;
- increasing the level of coordination of the activities of state bodies regarding the identification, assessment and forecasting of threats to information security, prevention of such threats and ensuring the elimination of their consequences, implementation of international cooperation on these issues;

- improvement of the legal framework for ensuring information security, in particular protection of information resources, countering computer crime, protection of personal data, as well as law enforcement activities in the information sphere;
- deployment and development of the National Confidential Communication System as a modern protected transport base capable of integrating territorially distributed information systems in which confidential information is processed [25].

Critical infrastructure facilities are strategically important enterprises and institutions necessary for the functioning of the country's society and its economy.

Enterprises related to critical infrastructure objects:

1. In order and provision of the most important public (administrative) services;
2. Energy supply (including the supply of thermal energy);
3. Water supply and drainage;
4. Genealogical support;
5. Health care;
6. Pharmaceutical industry.

The term «critical infrastructure» usually includes those objects, systems, networks, or their parts, the malfunctioning or destruction of which will lead to the most serious consequences for the social and economic sphere of the state, will negatively affect the level of its defense capability and national security. In addition, the functioning of critical infrastructure in peacetime is associated with the maintenance of vital functions in society, the protection of the basic needs of its members, and the formation of a sense of safety and security in them. The Green Paper on Critical Infrastructure Protection interprets Ukraine's critical infrastructure as a system and resources, physical or virtual, so vitally important to the country that their incapacity or destruction undermines national security, the national economy, the health or safety of the population, or has as a result any combination of the above [6].

Today, the state actively addresses of the questions of implementation and increasing the efficiency of the national systems of cyber security for critical infrastructure objects with the purpose of ensuring stable and safe functioning of national critical infrastructure in cyberspace, creating prerequisites for the association of efforts of subjects responsible for cyber security to solve the task of increasing the cyber resilience of the critical infrastructure of the state. This includes communication and information systems, whose sustainability and reliability are critically important for the functioning of state bodies, enterprises, institutions, and organizations.

The main task of technological infrastructure for cyber defense is the operational and effective protection of cyberspace in opposition to cyberattacks, cybercrimes, cyberterrorism, cyberespionage, including: collection, analysis, evaluation, generalization and spread of information about cyber incidents; granting methodical help to other subjects of cyber protection; mutual informing of subjects of cyber protection about new real and potential threats; creation of conditions for responsible and trusted exchange of information between subjects of cyber protection in every aspect [26, 27]. Thus, reviewing the state of cyber security in relevant sectors of the Ukrainian economy is crucial for strengthening the protection of critical infrastructure. It will help to improve state cyber security, increase the security of information resources and communication systems of critical infrastructure objects, as well as raise the level of the fuel and energy sector to provide a functioning safe integrated informative environment of communication.

Conclusion. The multi-level model data is a powerful tool for identifying requirements for regulatory and legal provision. Its implementation will become a key step in improving the process of identifying requirements for regulatory and legal provision, contributing to more effective organizations and analysis of information, and may improve business efficiency, provide compliance with regulatory requirements, and reduce risks for organizations in all industries. In particular, such a model allows for integrating different data sources, increasing the accuracy and completeness of analysis, and contributing to more operational decision-making. The multi-level data model also provides flexibility in adaptation to changes in the legislative and regulatory base, which is important for maintaining actuality and compliance with normative requirements.

As a result, the multi-level data model for the software cyber security of critical infrastructure is an effective approach to protection from cyber threats. The integration of different levels of protection allows creating reliable and comprehensive protection that ensures the safety and stability of critical infrastructure systems in the digital world. It is especially relevant in the conditions of growing complexities and

interdependence of informative systems, where even insignificant violations can have serious consequences.

References

1. Limba, T., et al. (2017) Cyber security management model for critical infrastructure. Entrepreneurship and Sustainability Issues, 4(4),P. 559-573. https://doi.org/10.9770/jesi.2017.4.4(12)
2. Ten, C.-W., Govindarasu, M., & Liu, C.-C. (2010) Cybersecurity for critical infrastructures: Attack and defense modeling. IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, 40(4), P.853-865.
3. Sarker, I. H., Janicke, H., Ferrag, M. A., & Abuadbba, A. (2024) Multi-aspect rule-based AI: Methods, taxonomy, challenges, and directions towards automation, intelligence, and transparent cybersecurity modeling for critical infrastructures. Internet of Things, 25, 101110.
4. Hnatyuk, S.O. (2013) Cyberterrorism: History of development, current trends, and countermeasures. Information Security, 19(2), P. 118-129.
5. Ivanyuta, S.P. (2018) Priority areas of legislative and organizational support for certification of critical infrastructure objects.
6. Biryukov, D.S., Kondratov, S.I., Nasvit, O.I., & Sukhodolya, O.M. (2015) Green book on critical infrastructure protection in Ukraine: Analytical report. Kyiv: NISD.
7. Lukyanchuk, R.V. (2016) State strategic planning in the field of cyber security: Realities today. Herald National Academy of State Management at the President of Ukraine. Series: State Management, 3, P. 131-137.
8. Leonov, B.D., Shostak, R.M., & Seryogin, V.S. (2020) Development of methodical provision of anti-terrorist protection of critical infrastructure objects (using the example of the USA). Information and Law, 3(34),P. 88-95.
9. Ryzhov, I.M. (2016) Basic concepts of anti-terrorist security: Monograph. Kyiv: National Academy of SBU.
10. Kondratov S. I., Sukhodolia O. M. (2020) The state system of critical infrastructure protection in the national security system: an analyst. add. / edited by OHM. Dried fruits Kyiv: NISD, P. 28.
11. Yermenchuk, O.P. (2018) Basic approaches to the organization of critical infrastructure protection in European countries: Experience for Ukraine: Monograph. Dnipro: Dniprop. State University of Internal Affairs.
12. Alekseieva O. (2021) Legal and organizational support for the protection of critical information infrastructure objects from cyber attacks. Information and law. No. 4(39). https://doi.org/ 10.37750/2616-6798.2023.4(47).291633
13. Kharchenko, V.P., Korchenko, O.G., & Hnatyuk, S.O. (2016) The basic model of the formation of requirements for ensuring cybersecurity of civil aviation. Security of Information, 22(2).
14. Kharchenko, V.P., Korchenko, O.G., & Hnatyuk, S.O. (2016) Multi-level data model for identification of the security of requirements in accordance with the regulatory and legal provision of cybersecurity of civil aviation information protection.
15. Alekseichuk, L., Novikov, O., Yakobchuk, D., & Rodionov, A. (2023).Cyber security logical and probabilistic model of a critical infrastructure facility in the electric energy industry. Theoretical and Applied Cybersecurity.
16. Bonagura, V., Foglietta, C., Panzieri, S., Rossi, M., Santini, R., & Scannapieco, M., et al. (2023) Modeling and assessing the impacts of cyber threats on interdependent critical infrastructures. In Proceedings of the 2023 International Conference on Cybersecurity.
17. Jiang, Y., Jeusfeld, M. A., & Ding, J. (2023) Model-based cybersecurity analysis. Business & Information Systems Engineering.
18. Gasimov, V., & Mammadov, J. I. (2023) Model and method for determining the optimal structure of the security system for critical information infrastructure. Reports of the Belorussian State University of Computer Science and Radio Electronics.
19. Decree of the President of Ukraine No. 155. (2002, February 19) On the procedure for organizing and monitoring the execution of decrees, orders, and instructions of the President of Ukraine.
20. Decree of the President of Ukraine No. 447. (2021, August 26) On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 «On the Cybersecurity Strategy of Ukraine».
21. Netesin, I. (2001). Approach to security of distributed databases. Legal Regulatory and Metrological Support of the Information Protection System in Ukraine: Scientific and Technical Collection, 2, P.118-124.
22. Electronic resource, access mode URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
23. Electronic resource, access mode URL: https://uk.wikipedia.org/wiki/ Identification
24. Electronic resource, access mode URL: https://jrnl.nau.edu.ua/index.php/ZI/article/view/12448
25. Electronic resource, access mode URL: https://coordynata.com.ua/pravove-zabezpecenna-kiberzahistu-v-ukraini
26. Tsantikidou, K., & Sklavos, N. (2024) Threats, attacks, and cryptography frameworks of cybersecurity in critical infrastructures. Cryptography, 8(1).
27. Varma, V. V. (2024) Cybersecurity of critical infrastructure. International Machine Learning Journal and Computer Engineering, 7(7), P.1-17.