UDC 351.861:004.056
JEL: F52; H56; L86
DOI: https://doi.org/10.32983/2222-4459-2024-9-139-147

IMPROVING CYBERSECURITY MECHANISMS IN UKRAINE: THE POLITICAL AND ADMINISTRATIVE ASPECTS

©2024 BABICHEV A. V., PELIUKH O. I.

UDC 351.861:004.056
JEL: F52; H56; L86

Babichev A. V., Peliukh O. I. Improving Cybersecurity Mechanisms in Ukraine: The Political and Administrative Aspects

The article examines the political and administrative aspects of improving the State mechanisms for ensuring cybersecurity in Ukraine based on international experience. A comparative analysis of approaches to cybersecurity in the United States of America, the European Union, and Ukraine was conducted. Particular attention is paid to the analysis of the national regulatory framework, administrative structures and international cooperation in the field of cybersecurity. Based on this, specific recommendations are proposed to improve the effectiveness of Ukrainian cybersecurity mechanisms. Among the main measures are the harmonization of legislation with European standards, the creation of the National Cybersecurity Center and the implementation of the system of key performance indicators (KPI). The proposed recommendations will help strengthen Ukraine's cyber resilience and improve its interaction with international partners in the face of growing cyber threats. The article analyzes the main problems of the regulatory framework regulating the functioning of the management system, as well as recommendations for improving national cybersecurity mechanisms based on international experience. On the basis of the conducted analysis and taking into account international experience, a certain number of recommendations for improving cybersecurity mechanisms in Ukraine are proposed. The recommendations cover political, administrative and international aspects, forming a comprehensive approach to strengthening national cyber resilience. The key success factor is the development of the cybersecurity system in the context of the national security of the State, effective coordination between various State bodies, the private sector and international partners. Undoubtedly, it is important to ensure constant monitoring and evaluation of the effectiveness of implemented mechanisms for timely adaptation to new challenges in the field of cybersecurity.

Keywords: *administrative reforms, State policy, cybersecurity, national security, security mechanism.*
Fig.: *2.* ***Tabl.:*** *5.* ***Bibl.:*** *17.*

Babichev Anatolii V. *– PhD (Public Administration), Associate Professor, Pro-rector for Scientific and Pedagogical Work, V. N. Karazin Kharkiv National University (4 Svobody Square, Kharkiv, 61022, Ukraine)*
E-mail: *babichev@karazin.ua*
ORCID: *https://orcid.org/0000-0002-7587-4824*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=58577438400*

Peliukh Oleksandr I. *– Student of the Educational and Scientific Institute "Institute of Public Administration" of V. N. Karazin Kharkiv National University (75 Heroiv Kharkova Ave., Kharkiv, 61001, Ukraine)*
E-mail: *oleksandr.peliukh@karazin.ua*
ORCID: *https://orcid.org/0000-0003-0507-0262*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=58290509500*

УДК 351.861:004.056
JEL: F52; H56; L86

Бабічев А. В., Пелюх О. І. Удосконалення механізмів кібербезпеки в Україні: політичний і адміністративний аспекти

У статті досліджено політико-адміністративні аспекти вдосконалення державних механізмів забезпечення кібербезпеки в Україні на основі міжнародного досвіду. Проведено порівняльний аналіз підходів до кібербезпеки у Сполучених Штатах Америки, Європейському Союзі та Україні. Особлива увага приділяється аналізу національної нормативно-правової бази, адміністративних структур та міжнародного співробітництва у сфері кібербезпеки. Виходячи з цього, пропонуються конкретні рекомендації щодо підвищення ефективності українських механізмів кібербезпеки. Серед основних заходів – гармонізація законодавства згідно з європейськими стандартами, створення Національного центру кібербезпеки та впровадження системи ключових показників ефективності (КПЕ). Запропоновані рекомендації сприятимуть зміцненню кіберстійкості України та покращенню її взаємодії з міжнародними партнерами в умовах зростання кіберзагроз. У статті проаналізовано основні проблеми нормативно-правової бази, що регулює функціонування системи управління, а також надано рекомендації щодо вдосконалення національних механізмів кібербезпеки на основі міжнародного досвіду. На основі проведеного аналізу та з урахуванням міжнародного досвіду запропоновано певну кількість рекомендацій щодо вдосконалення механізмів кібербезпеки в Україні. Рекомендації охоплюють політичні, адміністративні та міжнародні аспекти, формуючи комплексний підхід до посилення національної кіберстійкості. Ключовим фактором успіху є розвиток системи кібербезпеки в контексті національної безпеки держави, ефективна координація між різними державними органами, приватним сектором та міжнародними партнерами. Безумовно, важливим є забезпечення постійного моніторингу та оцінки ефективності впроваджених механізмів своєчасної адаптації до нових викликів у сфері кібербезпеки.

Ключові слова: *адміністративні реформи, державна політика, кібербезпека, національна безпека, безпековий механізм.*
Рис.: *2.* ***Табл.:*** *5.* ***Бібл.:*** *17.*

Бабічев Анатолій Валерійович *– кандидат наук з державного управління, доцент, проректор з наукової та педагогічної роботи, Харківський національний університет імені В. Н. Каразіна (майдан Свободи, 4, Харків, 61022, Україна)*
E-mail: *babichev@karazin.ua*
ORCID: *https://orcid.org/0000-0002-7587-4824*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=58577438400*

Пелюх Олександр Іванович *– студент, Навчально-науковий інститут «Інститут державного управління» Харківського національного університету імені В. Н. Каразіна (просп. Героїв Харкова, 75, Харків, 61001, Україна)*

E-mail: *oleksandr.peliukh@karazin.ua*

ORCID: *https://orcid.org/0000-0003-0507-0262*

Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=58290509500*

In today's world, cybersecurity is becoming one of the key components of national security for every country. The increasing number and complexity of cyber incidents poses new challenges for countries in protecting their information infrastructure and responding to cyber threats. Cyber incidents can have serious consequences for public administration, the economy, and the private sector, so countries are forced to improve their response mechanisms to these threats.

The experience of leading countries, such as the United States of America (USA) and the European Union (EU), demonstrates the effectiveness of comprehensive approaches to cybersecurity that combine regulatory frameworks, administrative coordination, and international cooperation. The United States is actively implementing standards, such as NIST SP 800-61 and CSF 2.0, which are focused on creating mechanisms for responding to and managing cyber incidents. The EU, in turn, is developing a pan-European cybersecurity system through the NIS directives and institutions such as ENISA.

The *aim* of this article is to study the political and administrative aspects of improving the State cybersecurity instruments in Ukraine by comparing them with the approaches used in the United States and the EU.

Ukraine, as a country in a state of hybrid war, is particularly acutely aware of the need to strengthen its cybersecurity mechanisms. Since 2014, the Ukrainian State has made significant progress in developing its own regulatory framework, in particular through the Law of Ukraine «On the Basic Principles of Cybersecurity of Ukraine» dated 05.10.2017 No. 2163-VIII [1]. However, the effectiveness of Ukraine's cyber incident response mechanisms still needs to be improved, especially in the area of political and administrative coordination.

In the context of the study, it is advisable to compare the approaches of different countries to building up cybersecurity.

Summarizing the experience of the United States of America allows us to state certain practical aspects and implement the experience in the development of the configuration of the cybersecurity system in Ukraine.

The United States of America is one of the leaders in cybersecurity, thanks to the development of a regulatory framework and effective mechanisms for responding to cyber incidents. The high level of protection of the U. S. information systems is ensured through the implementation of standardized documents, such as NIST Special Publication SP 800-61 [2] and the Cybersecurity Framework (CSF) [3], which provide detailed instructions on cyber incident management and cyber risk minimization.

One of the key documents in the field of cybersecurity is NIST SP 800-61 [2], which offers a holistic model for responding to cyber incidents that defines the main stages of the incident life cycle: preparation, detection, analysis, containment, elimination and recovery, as well as follow-up actions for incident analysis. The document is aimed at all levels of organizations, from technical specialists to management, and allows you to customize the processes of detecting and responding to cyber threats to ensure efficiency and effectiveness.

In addition to NIST SP 800-61, the United States has developed and implemented a structured approach [3], which has become the main tool for assessing the risks and cyber resilience of organizations. The CSF was developed for different sectors of the economy, which enabled organizations to adapt protection mechanisms to their needs. The CSF defines five main functions that help organizations identify threats, protect against them, detect incidents in time, respond to them, and recover systems after attacks. It provides a systematic approach to cyberspace risk management, making it applicable to both large and small organizations.

Despite the high effectiveness of the regulatory framework, there are certain challenges. First of all, NIST SP 800-61 requires significant resources for implementation, which may be unaffordable for some organizations, in particular SMEs. In addition, the CSF framework is flexible enough to be adapted to different conditions, but this sometimes leads to insufficiently stringent regulation in critical sectors of the economy. A generalized description of the U. S. regulatory framework governing the functioning of cybersecurity is presented in *Tbl. 1.*

The U. S. approach to cybersecurity is based on close cooperation between public and private entities. In particular, agencies such as US-CERT (Computer Emergency Readiness Team) play a key role in coordinating incident response, collecting and disseminating threat information, and assisting victims of attacks. This approach facilitates rapid detection of threats and

Table 1

Generalized description of the USA documents regulating the functioning of cybersecurity

Parameter	CSF 2.0 [3]	NIST SP 800-61 [2]
Purpose	Providing a high-level classification system for cybersecurity compliance outcomes	Providing detailed guidance on establishing and improving cyber incident response systems
Scope, details of content	The outcome classification system and its recommendations	Detailed recommendations and instructions for their implementation
Use in the world	Wide	
Relevance (year of last update)	2023	2021
Resources for implementation	Medium	Significant
Time to implement	Long	
Flexibility	High	
Availability	Publicly available	

effective response, which is important for maintaining a high level of cybersecurity in the country.

Summarizing the experience of the European Union allows us to state certain practical aspects and implement the experience in the development of the configuration of the cybersecurity system in Ukraine.

The European Union (EU) pays considerable attention to cybersecurity, recognizing its importance for protecting digital space and ensuring the stability of critical infrastructures. The European approach to cybersecurity is based on several key regulatory documents, the most important of which are the Network and Information Security Directive (NIS Directive) and the Cybersecurity Act.

The NIS Directive, adopted in 2016 [4], sets minimum cybersecurity requirements for operators of critical services such as energy, transportation, and finance, as well as for digital service providers. The main objective of the NIS is to ensure the resilience of networks and information systems within the EU. It obliges the Member States to establish national cybersecurity authorities, as well as to introduce mechanisms to coordinate actions between them.

The Cybersecurity Law [5], adopted in 2019, strengthens the role of the EU Cybersecurity Agency (ENISA) in promoting the protection of digital networks. ENISA has been given expanded powers to support the Member States in developing and implementing cybersecurity standards. In addition, the law introduced a European cybersecurity certification system for products, processes and services that ensures a high level of protection of digital infrastructure throughout the EU.

The European approach is characterized by a strong focus on regulation and ensuring a pan-European harmonized approach to cybersecurity. For example, the European Electronic Communications Code (EECC) [6] also regulates the security of networks and services. Article 40 of the Code describes the requirements for the protection of information systems and communication networks, which include the protection of both infrastructure and information from cybersecurity threats. ENISA is responsible for coordinating efforts between the Member States and for introducing new standards that allow systems to adapt to new challenges.

When it comes to responding to cyber incidents, the EU also relies on a network of CSIRTs (Computer Security Incident Response Teams) that coordinates national response teams. This allows for the rapid exchange of information about threats and ensures a quick response to cyber incidents. Below is *Fig. 1*, presenting a comparison of the international cybersecurity index between the EU countries and Ukraine.

A comparative analysis of the key documents regulating the functioning of EU cybersecurity is presented in *Tbl. 2*.

Thus, cybersecurity in the EU is based on the creation of pan-European standards and bodies that ensure a high level of coordination and certification in the field of cybersecurity.

Ukraine faces numerous cyber threats, in particular due to the ongoing hybrid war with Russia, which has increased the need to create a comprehensive cybersecurity system. One of the main steps in this direction was the adoption of the Law of Ukraine «On the Basic Principles of Cybersecurity of Ukraine» in 2017. The related legislation act [1] defined the key tasks and subjects of national cybersecurity, which allowed to streamline the processes of threat management in cyberspace.

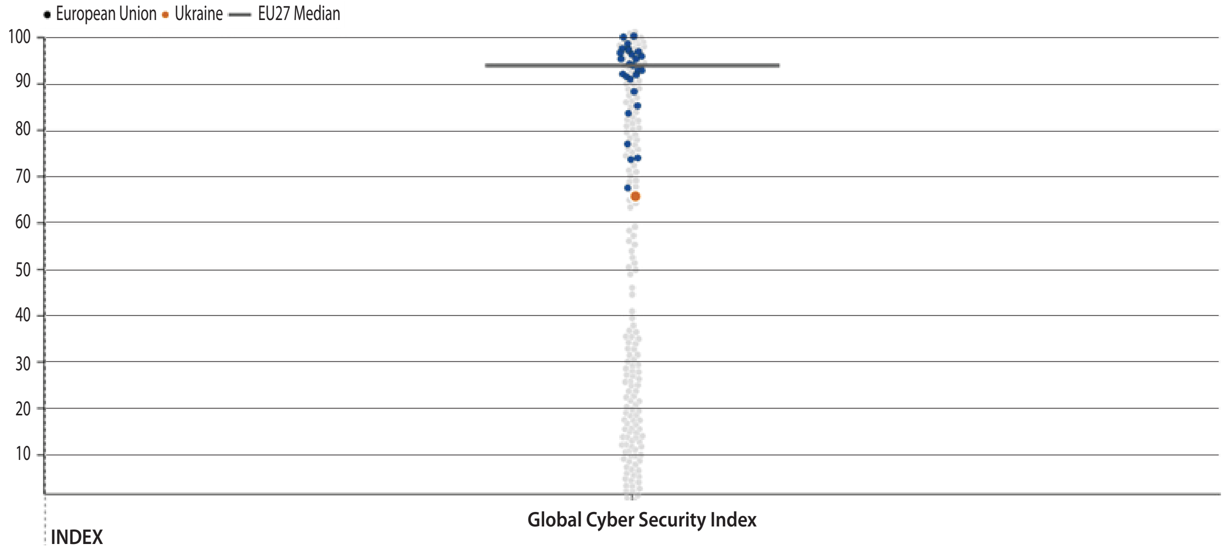

Fig. 1. Comparison of the EU and Ukraine (International Cybersecurity Index [7])

Table 2

Comparative analysis of key documents regulating the functioning of EU cybersecurity

Parameter	NIS Directive [4]	Cybersecurity Act [5]
Objective	Protection of critical systems	Certification and risk management
Coordination	CSIRT	ENISA
Flexibility	Medium	High
Relevance (year of last update)	2016	2019
Coverage	Limited to critical sectors	Pan-European
Certification mechanisms	Implemented through ENISA	

In the context of cybersecurity, the National Security and Defense Council of Ukraine (NSDC) plays an important role in coordinating State policy in the field of cybersecurity. In 2022, the NSDC approved the "Implementation Plan for the Cybersecurity Strategy of Ukraine" [8], which became a key document for the further development of the cybersecurity system. The Implementation Plan covers such areas as national cyber preparedness, ensuring cyber protection of critical infrastructure, development of mechanisms for responding to cyber incidents, and international cooperation in the field of cybersecurity.

One of the main goals of this plan is to increase national cyber preparedness, which includes the development of cyber defense infrastructure, improvement of incident management procedures, and raising the level of technical training. The NSDC decision emphasizes the need to improve coordination between government agencies, the private sector, and international partners. For example, paragraph 36 of the Plan emphasizes strengthening cooperation with international organizations, such as NATO and the EU, to integrate Ukraine into the global cybersecurity system.

Another important component is to support the activities of the government's Computer Emergency Response Team (CERT-UA) [9], which monitors and responds to incidents. CERT-UA actively cooperates with other countries, in particular within the framework of international organizations such as the Forum of Incident Response and Security Teams (FIRST), which allows Ukraine to share information about threats faster and increase its cyber resilience. In particular, this body liaises with international partners, including CSIRT (EU) and US-CERT (US), which facilitates the rapid exchange of threat information.

The legal framework of Ukraine also includes a number of resolutions of the Cabinet of Ministers of Ukraine that define mechanisms for responding to cyber threats. For example, CMU Resolution No. 1295 of 2020 [10] approves the procedure for the functioning of the system for identifying vulnerabilities and responding to cyber incidents. It regulates the stages of detecting and eliminating cyber threats, and defines procedures for cooperation between various cybersecurity actors.

To improve the effectiveness of cyber incident response, CMU Resolution No. 299 of 2023 [11] defines six stages of incident response: preparation, detection and analysis, containment, elimination, recovery, and evaluation of the effectiveness of actions. These stages provide a comprehensive approach to responding to cyber incidents and help establish clear coordination between different cybersecurity actors. *Fig. 2* shows the structure of Ukraine's regulatory framework in the field of cybersecurity, which includes legislative acts, NSDC decisions, and bylaws of the Cabinet of Ministers.

Thus, despite the achievements in building a cybersecurity system, Ukraine needs to continue to improve its regulatory framework, in particular, to integrate it with European standards such as [4–6]. This will ensure a higher level of critical infrastructure protection and better integration into the global cyber defense system (*Tbl. 3*).

An examination of the approaches to cybersecurity in the United States, the European Union, and Ukraine has shown that each of these countries or associations has its own specifics in developing cybersecurity regulations and response mechanisms.

Ukraine has made significant progress in developing a national regulatory framework, but continues to work on integration with international standards and coordination at the State level. The establishment of CERT-UA and support through NSDC decisions provide a framework for cybersecurity, but there is

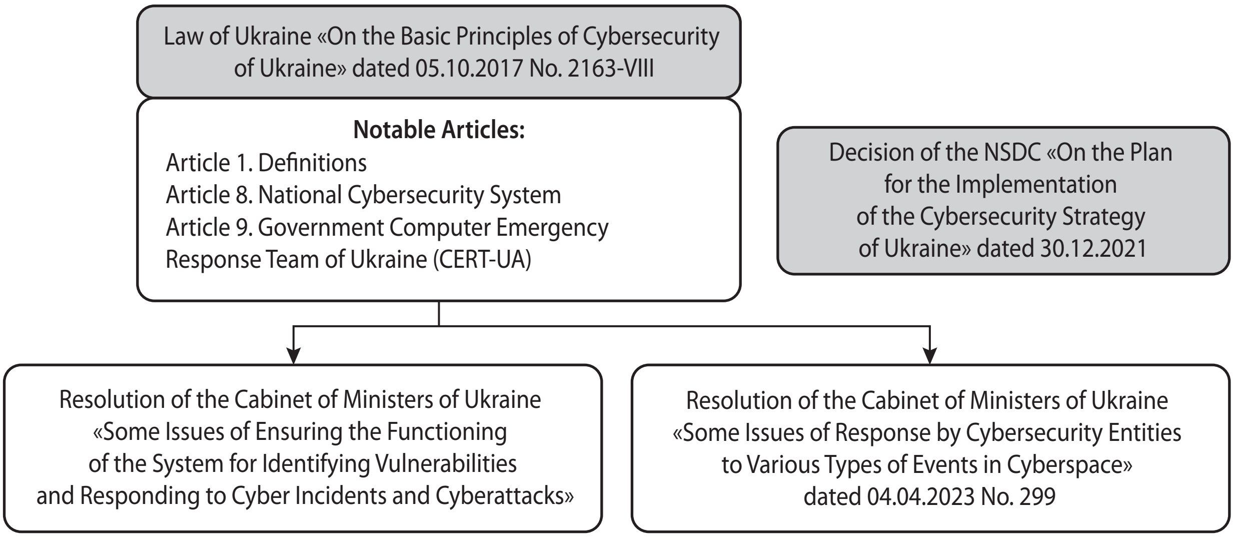
Law of Ukraine «On the Basic Principles of Cybersecurity of Ukraine» dated 05.10.2017 No. 2163-VIII
Notable Articles:
Article 1. Definitions
Article 8. National Cybersecurity System
Article 9. Government Computer Emergency Response Team of Ukraine (CERT-UA)
Decision of the NSDC «On the Plan for the Implementation of the Cybersecurity Strategy of Ukraine» dated 30.12.2021
Resolution of the Cabinet of Ministers of Ukraine «Some Issues of Ensuring the Functioning of the System for Identifying Vulnerabilities and Responding to Cyber Incidents and Cyberattacks»
Resolution of the Cabinet of Ministers of Ukraine «Some Issues of Response by Cybersecurity Entities to Various Types of Events in Cyberspace» dated 04.04.2023 No. 299

Fig. 2. A generalized structure of the regulatory framework on cybersecurity in Ukraine

Table 3

Comparison of approaches to cybersecurity: USA, EU and Ukraine

Parameter	USA	EU	Ukraine
Key regulatory documents	NIST SP 800-61, CSF 2.0	NIS (NIS 2) Directive, Cybersecurity Act	The Law of Ukraine 'On Cybersecurity', NSDC resolution [8]
Coordination authorities	US-CERT	ENISA, CSIRT	CERT-UA
Focus on certification	None	High (certification system through ENISA)	Implemented on the basis of international standards
International cooperation	Extensive cooperation with partners, including NATO and other countries	Cooperation within the EU and with other global partners	Active cooperation with the EU, NATO, FIRST
Integration of standards	Own standards (NIST)	Pan-European standards	Harmonization with international and European standards
Scope of application	Nationwide, all sectors	Operators of critical services and digital services	Operators of critical infrastructure, government agencies

a need for further improvement and harmonization with the EU legislation.

Systematizing the political aspects of improving cybersecurity mechanisms at the national level allows to strategically determine the trajectory of the national security development of the State.

International cooperation is a key aspect in improving Ukraine's cybersecurity mechanisms. In particular, integration with the European Union (EU) and NATO plays a crucial role in strengthening the country's cyber defense. For effective integration and cooperation, the following steps and decisions should be followed.

Harmonization of legislation with the EU regulatory framework is a priority for Ukraine. This implies the development and adoption of a new version of the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" taking into account the requirements of Directive NIS2 (EU) 2022/2555 [12]. The new law should include risk assessment and incident reporting mechanisms for operators of essential services and digital service providers, similar to the requirements of Article 20 of the NIS2 Directive. To coordinate this process, it is advisable to create an interagency working group that will include representatives of the NSDC, the State Service for Special Communications, the SSU, and other relevant agencies. This group will ensure a comprehensive approach to harmonizing legislation and taking into account the interests of all stakeholders.

Integration into European cybersecurity structures is the next important step. Ukraine should apply for observer status in ENISA in accordance with Article 42 of Regulation (EU) 2019/881 [5], which will allow Ukrainian experts to participate in ENISA Board meetings and gain access to key information on cyber threats. In addition, a cooperation agreement should be concluded between CERT-UA and CERT-EU to ensure the rapid exchange of information on cyber incidents and threats. Such cooperation will allow Ukraine to integrate into the European cybersecurity system.

Strengthening cooperation with NATO is critical for improving Ukraine's defense capabilities in cyberspace. A road-map should be developed for Ukraine to achieve full interoperability with NATO cyber defense systems. Such a road-map should cover technical, organizational, and legal aspects of integration. An important step would be to establish a joint NATO-Ukraine Cyber Defense Center of Excellence at a Ukrainian university, similar to the NATO Tallinn Cyber Defense Center of Excellence [13]. Such a center could become a platform for experience exchange, research, and training of cybersecurity professionals. Additionally, an exchange program between Ukrainian cybersecurity structures and the relevant authorities of the NATO Member States should be introduced to facilitate the exchange of best practices and improve the skills of Ukrainian specialists.

Participation in international exercises and trainings is an important aspect of improving Ukraine's readiness to counter cyber threats. The solution is Ukraine's annual participation in NATO's Cyber Coalition and Locked Shields exercises [13] with an expanded list of participants from various government agencies and the private sector.

The development of public-private partnerships in the field of cybersecurity is necessary to ensure an integrated approach to cybersecurity, and, accordingly, it is necessary to develop tactical and strategic measures in the main functional areas of improving the State instruments for ensuring cybersecurity in Ukraine (*Tbl. 4*).

It is proposed to create a National Cyber Security Alliance involving the State, business and academic institutions, similar to the National Cyber Security Alliance in the United States [14]. Such an alliance could become a platform for coordinating the efforts of various sectors in the field of cybersecurity and facilitate the exchange of information and resources.

Implementation of these measures will allow Ukraine to significantly increase the level of integration into European and Euro-Atlantic cybersecurity structures, ensure effective exchange of information and best practices, and strengthen the national cyber defense system in accordance with international standards. It is important to emphasize that successful international integration and cooperation in the field of cybersecurity requires a systematic approach, constant updating of strategies and Ukraine's active participation in global initiatives to counter cyber threats.

Effective cybersecurity administration and management is critical to ensuring the resilience of the national information infrastructure. In this section, we will consider key administrative aspects of improving cybersecurity mechanisms in Ukraine.

Optimization of national cybersecurity structures is an important step to improve the effectiveness of response to cyber threats. The existing system, which includes the State Service for Special Communications and Information Protection of Ukraine (SSSCIP), the Security Service of Ukraine (SSU) and other agencies, needs to be improved to eliminate duplication of functions and increase the efficiency of response to cyber incidents.

In the context of the study, it is reasonable to state that the solution is to create a single National Cybersecurity Center (NCC) as the main coordinating body that will combine the functions of existing

Table 4

Tactical and strategic measures in the main functional areas of improvement of State-based cybersecurity instruments in Ukraine

Area	Proposed steps
Harmonization of legislation	1. New version of the Law [1]. 2. Implementation of risk assessment mechanisms. 3. Establishment of an interagency working group
Integration into the EU structures	1. Obtaining observer status in ENISA. 2. Agreement on cooperation between CERT-UA and CERT-EU. 3. Organization of joint exercises with the EU
Cooperation with NATO	1. Development of an interoperability road-map. 2. Specialist exchange program. 3. Participation in NATO exercises
Public-private partnership	1. Establishment of the National Cyber Security Alliance

structures. The model of such a center can be based on the experience of the National Cyber Security Center of the United Kingdom, which successfully integrates various aspects of cyber defense under a single leadership [15]. The NCC can become a central hub for exchanging information on cyber threats, coordinating incident response [16], and developing a national cybersecurity strategy.

An important aspect of optimization is the introduction of a system of key performance indicators (KPIs) to assess the performance of cybersecurity structures. Such KPIs should include such metrics as incident response time, number of successfully prevented attacks, and the level of preparedness of critical infrastructure against cyber threats. Implementation of such a system will allow for an objective assessment of the performance of various departments and the necessary adjustments to their activities.

Effective cooperation between the public and private sectors is a key factor in countering cyber threats. To improve this interaction, it is proposed to create a National Cyber Threat Information Sharing Platform (NCTISP), which will operate on the principle of public-private partnerships discussed in the previous section.

The NCTISP should become a centralized mechanism for the exchange of information on cyber threats in real time between government agencies, critical infrastructure operators, and private companies. Such a platform can be developed similarly to the Cyber Security Information Sharing Partnership in the UK [17], but with the specifics of the Ukrainian context in mind. The key components and functions of the NCTISP could include:

- ✦ automated exchange of compromise indicators and technical data on cyber threats;
- ✦ a forum for discussing tactics, techniques and procedures of cybercriminals;
- ✦ an early warning mechanism for new types of cyber threats;
- ✦ a platform for joint analysis of cybersecurity trends.

To ensure the effectiveness of NCTISP, clear information exchange protocols should be developed to guarantee the confidentiality of commercial information of private companies and compliance with personal data protection legislation.

Implementation of the proposed administrative mechanisms will significantly increase the effectiveness of Ukraine's national cybersecurity system. Optimization of structures, improved coordination between the public and private sectors, and the introduction of an adaptive approach to cyber risk management create the basis for building a sustainable system of national cyberspace protection.

In the area of political reforms, the priority task is to establish an Interagency Commission on Cybersecurity under the National Security and Defense Council of Ukraine. This institution should become the central body for coordinating cybersecurity policy, bringing together representatives of key ministries, agencies and the private sector. The Commission should be empowered to develop and implement a national cybersecurity strategy, coordinate the actions of various agencies, and respond quickly to critical cyber threats. In parallel, a cybersecurity certification system for critical infrastructure should be developed and implemented, adapted to national needs but harmonized with European standards, in particular with the provisions of the EU Cybersecurity Law [5].

In the context of administrative changes, the key recommendation is to establish the National Cyber Resilience Center (NCRC) as an operational body for responding to cyber incidents in accordance with the practice of [15]. The NCRC should combine the technical capabilities of CERT-UA, the analytical resources of intelligence agencies, and the operational capabilities of law enforcement agencies. The main functions of the NCRC should include round-the-clock monitoring of cyberspace, coordination of response to large-scale cyber incidents, digital forensics, and technical support to critical infrastructure operators. The main recommendations for improving cybersecurity mechanisms in Ukraine in various areas are presented in *Tbl. 5*.

Implementation of the above recommendations will require considerable effort and resources, but the potential benefits for national security and economic development could be significant.

CONCLUSIONS

The development of the State cyber security mechanisms is critically important for ensuring the national security of Ukraine in the face of modern challenges, in particular the growing number and complexity of cyber threats. The conducted comparative analysis of the approaches of the USA, the European Union, and Ukraine demonstrates that Ukraine has already taken a significant step forward in creating a regulatory framework and cyber defense mechanisms. However, there is a need for further improvement of national mechanisms, in particular through optimization of the administrative structure, coordination between the public and private sectors, and the integration of international experience.

Ukraine needs to continue harmonizing its legislation with European and international standards, such as the NIS Directive and the Cybersecurity Act. In our opinion, this will not only increase the level of protection of national critical infrastructure, but also improve cooperation with international partners, in particular the EU and NATO. The creation of the National Cyber Security Center and the implementation of the system of key performance indicators (KPI) will allow to increase the effectiveness of responding to cyber incidents and preventing threats.

Implementation of the proposed measures will contribute to strengthening the stability of Ukraine's cyberspace, which is important for supporting not only national security, but also economic development and further European integration of the country. ■

BIBLIOGRAPHY

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#n56
2. NIST SP 800-61. NIST. 2021. URL: https://www.nist.gov/privacy-framework/nist-sp-800-61.
3. The NIST Cybersecurity Framework 2.0. *NIST*. 2024. DOI: https://doi.org/10.6028/nist.cswp.29.ipd
4. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning

Table 5

Key recommendations for improving cybersecurity mechanisms in Ukraine in various areas

Area	Recommendations	Justification
Political	Establishment of the Interagency Commission on Cybersecurity under the NSDC of Ukraine	Coordination of cybersecurity policy, development of a national strategy, rapid response to threats
	Implementation of a cybersecurity certification system for critical infrastructure harmonized with European standards	Increase the level of protection of critical infrastructure and integration with European practices
Administrative	Establishment of the National Cybersecurity Centre (NCSC)	Optimization of existing structures, coordination of the work of the State Service for Special Communications, the Security Service of Ukraine and other authorities
	Implementation of KPIs for assessing the effectiveness of cybersecurity	Assessment of cybersecurity structures in terms of response time, readiness and number of attacks prevented
	Establishment of the National Cyber Threat Information Sharing Platform (NCTISP)	Ensuring public-private cooperation and real-time exchange of threat information
International	Strengthening cooperation with the EU and NATO in the field of cybersecurity, participation in joint programs	Integration into the global cybersecurity system to obtain advanced technologies and practices
	Harmonization of Ukrainian legislation with the NIS Directive and the EU Cybersecurity Act	Ensuring compliance with international standards and improving cooperation with European partners

measures for a high common level of security of network and information systems across the Union. *EUR-Lex*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148&qid=1707927214161

5. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act) (Text with EEA relevance). *EUR-Lex*. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj
6. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) (Text with EEA relevance). *EUR-Lex*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1972&qid=1707927623379
7. ITU Global Cybersecurity Index (GCI). URL: https://prosperitydata360.worldbank.org/en/indicator/WB+GTMI+I+43
8. План реалізації Стратегії кібербезпеки України : введено в дію рішенням РНБО України від 30.12.2021 р. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#n16
9. CERT-UA. URL: https://cert.gov.ua/
10. Постанова Кабінету Міністрів України «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» від 23.12.2020 р. № 1295. URL: https://zakon.rada.gov.ua/laws/show/1295-2020-п#n11
11. Постанова Кабінету Міністрів України «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» від 04.04.2023 р. № 299. URL: https://zakon.rada.gov.ua/laws/show/299-2023п#Text
12. Directive (EU) 2022/2555 of the European Parliaˀment and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). *EUR-Lex*. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022L2555
13. The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub. *CCDCOE*. URL: https://ccdcoe.org/
14. National Cybersecurity Alliance. URL: https://staysafeonline.org/
15. The National Cyber Security Centre. URL: https://www.ncsc.gov.uk/
16. Categorising UK cyber incidents. *National Cyber Security Centre*. URL: https://www.ncsc.gov.uk/information/categorising-uk-cyber-incidents
17. About CISP. *National Cyber Security Centre*. URL: https://www.ncsc.gov.uk/cisp/home

REFERENCES

"About CISP". National Cyber Security Centre. https://www.ncsc.gov.uk/cisp/home

"Categorising UK cyber incidents". *National Cyber Security Centre*. https://www.ncsc.gov.uk/information/categorising-uk-cyber-incidents

CERT-UA. https://cert.gov.ua/

"Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union". *EUR-Lex*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148&qid=1707927214161

"Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) (Text with EEA relevance)". *EUR-Lex*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1972&qid=1707927623379

"Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)". *EUR-Lex*. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022L2555

ITU Global Cybersecurity Index (GCI). https://prosperitydata360.worldbank.org/en/indicator/WB+GTMI+I+43

[Legal Act of Ukraine] (2017). https://zakon.rada.gov.ua/laws/show/2163-19#n56

[Legal Act of Ukraine] (2020). https://zakon.rada.gov.ua/laws/show/1295-2020-п#n11

[Legal Act of Ukraine] (2021). https://zakon.rada.gov.ua/laws/show/n0087525-21#n16

[Legal Act of Ukraine] (2023). https://zakon.rada.gov.ua/laws/show/299-2023п#Text

"NIST SP 800-61" NIST. 2021. https://www.nist.gov/privacy-framework/nist-sp-800-61

National Cybersecurity Alliance. https://staysafeonline.org/

"Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act) (Text with EEA relevance)". *EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2019/881/oj

The National Cyber Security Centre. https://www.ncsc.gov.uk/

"The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub". *CCDCOE*. https://ccdcoe.org/

"The NIST Cybersecurity Framework 2.0". *NIST* (2024). DOI: https://doi.org/10.6028/nist.cswp.29.ipd