**Legal support of the state's information security in the context of hybrid threats: challenges and mechanisms of counteraction in Ukraine**

**Irina Aristova**

Department of Administrative and Information Law

Sumy National Agrarian University

40000, 160 Gerasym Kondratiev Str., Sumy, Ukraine

[aristova07@gmail.com](mailto:aristova07@gmail.com)

<https://orcid.org/0000-0001-9211-3464>

**Nataliia Kapitanenko**

Department of Theory of Law, Constitutional Law and Public Administration

Oles Honchar Dnipro National University

49000, 72 Nauky Ave., Dnipro, Ukraine

[kapitanenko.np@gmail.com](mailto:kapitanenko.np@gmail.com)

0000-0002-1475-5784

**Andrii Lyseiuk**

Center for Educational Activities

Academy of the Security Service of Ukraine

03113, 3 Mykola Vasylenko Str., Kyiv, Ukraine

[andrii\_lyseiuk@sci-univ.com](mailto:andrii_lyseiuk@sci-univ.com)

**Ievgenii Kryvolap**

Faculty of Law and International Relations

National Aviation University

03058, 1 Lubomyr Huzar Ave., Kyiv, Ukraine

[krivolap.evgeniy@gmail.com](mailto:krivolap.evgeniy@gmail.com)

<https://orcid.org/0000-0003-2599-2520>

**Oleksii Kharytonov**

Interregional Academy of Personnel Management

03039, 2 Frometivska Str., Kyiv, Ukraine

<https://orcid.org/0009-0001-2460-244X>

[kharytonov7@gmail.com](mailto:kharytonov7@gmail.com)

**Abstract**

The relevance of the research stems from two key factors: the rapid digitalization of society and the current security situation in Ukraine caused by Russian aggression. While technological progress offers societal benefits, it also poses growing risks to data security. Annual increases in data leaks and the advancement of artificial intelligence demand state-level adaptive protection mechanisms and enhanced international cooperation. In Ukraine, the war has evolved into an information confrontation. The aggressor actively employs cyberattacks and disinformation to undermine state structures and society. This underscores the urgent need for a comprehensive information security strategy as a critical element of national sovereignty. The article explores the complex nature of information security, emphasizing that many studies overlook its dual structure—technical and social. The lack of harmonized terminology results in fragmented legislation. The author analyzes Ukraine's legal framework in this field, classifying legal acts by subject and regulatory level. Key shortcomings in national legislation are identified, particularly the absence of alignment with international legal standards. The article argues for the development of a National Strategy of Information Sovereignty, which should consolidate a clear concept of information security and outline practical measures for its implementation. The aim is to assess the legal regulation of information security in light of current threats and to propose improvements. The novelty of the study lies in formulating a comprehensive definition of information security and substantiating the need for a national strategy that would enhance Ukraine’s resilience in the digital sphere.

**Keywords:** information security; cybersecurity; cyber threats; disinformation; propaganda; National Strategy of Information Sovereignty of Ukraine.

1. **Introduction**

The modern world is fully digitalized. The rapid development of information and communication technologies creates new opportunities for people. Technology advances and we become more interconnected (Akello, 2024). At the same time, these same innovations enable an unprecedented spread of cyberattacks and destructive information influence (Mihaela, 2020). The increase in their number can pose significant security threats in many parts of the world. In ancient times, remote areas were considered safe from invaders and disease. Today, however, even the most remote areas cannot be protected because digitalization is everywhere. Crimes and wars have changed their nature by moving into the digital space.

This issue is particularly critical for countries at war. For Ukraine, the issue of information security is particularly relevant in the context of Russian aggression. Since 2014, Russia has been systematically using methods of information influence to weaken national resilience. It has been using propaganda, information fakes, and cyberattacks. In this situation, a comprehensive legal regulation of the information space is an important condition for preserving state sovereignty. For example, according to Microsoft’s 2022 report, 60% of all cyberattacks observed from nation states originated from the Russian Federation. At the same time, attacks by Russian nation state actors are becoming increasingly effective: the successful compromise rate in 2021 was 21%, and in 2022 – 32%. Russian nation state actors are increasingly targeting government agencies for intelligence gathering, which increased from 3% of all targets in 2021 to 53% (Microsoft Digital Defense Report, 2022). These are mainly agencies involved in foreign policy, national security or defense. The top three countries targeted by Russian cyberattacks include the United States, Ukraine and the United Kingdom (Lubenets et al., 2023).

The growing number of cyberattacks on critical information systems poses new challenges for the state to ensure information sovereignty. In particular, the problem of improving national legislation is particularly acute today. Another important issue is the harmonization of Ukrainian legal norms with international cybersecurity standards. Such measures are important for effective counteraction to hybrid threats and are also driven by Ukraine's European integration. Active military operations further actualize this process, because in such circumstances, a data leak can cost thousands of lives. Or even jeopardize the existence of Ukraine.

Modern hybrid threats are characterized by complexity, multilevelness and constant transformation of methods of influence. This requires the creation of a flexible legal framework. Its effectiveness directly depends on the ability to respond quickly to changing threats (Bielov et al., 2019). At the same time, international experience shows that proper legal regulation of the information space is a key factor in building society's resilience to external threats (Kostenko et al., 2024). It is also important to take into account not only current challenges but also trends in the development of information technology. Development will continue to move forward, and threats to information security will grow with it. Therefore, it is necessary to create a legal framework that can adequately respond to the evolution of such threats.

An analysis of current Ukrainian legislation shows that a basic legal framework is in place. The legislator has adopted a number of laws regulating cybersecurity and related issues. At the same time, the dynamic development of technologies complicates the process of updating legal norms. This results in a fragmented and inconsistent legal framework. Researchers identify gaps and contradictions that need to be addressed (Bohomia & Halunko, 2024). In some cases, the legislation does not contain exhaustive definitions of key concepts. This leads to discrepancies in law enforcement practice and complicates coordination of efforts between government agencies involved in countering various types of information attacks (Syrovatchenko, 2024). In addition, even if relevant legislation is in place, the implementation of its provisions is often hampered by a lack of sufficient resources. As a result, this reduces the overall effect of the adoption of laws and makes it difficult to counter real threats. Therefore, a comprehensive improvement of legislation is needed to strengthen Ukraine's ability to effectively counter modern information challenges.

1. **Literature Review**

The issue of information security as a separate component of national security has been reflected in the works of many scholars. However, a significant part of the academic discourse focuses on the one-sided nature of information security, which does not take into account its duality. However, Basholli (Basholli et al., 2023) draw attention to the fact that an integrated approach to the security of information systems is crucial. Based on the analysis of all the research, the author concluded that information security consists of a technical and social component.

Many professional publications emphasize the dynamic nature of modern threats. Thus, Mihaela (2020) notes that cyberattacks have become widespread as a result of the rapid development of technologies. Therefore, today they pose a significant threat to global stability. Similarly, Akello (2024) points to the constant clash of organizations with the latest types of malicious software and advanced methods of intrusion. Fidler (2015) emphasizes that the global community still does not have sufficiently effective mechanisms to keep up with the rapid pace of new threats. Therefore, there is a need for comprehensive international legal instruments. Such remarks are consistent with the view that fragmentary legislative updates do not guarantee proper cyber resilience. A significant amount of research concerns the socio-political aspects of information security, especially in the context of countering disinformation and propaganda. Thus, Mazurenko (2022) emphasizes that the spread of fake news creates political and social turbulence. In turn, Mujinga (Mujinga et al., 2017) prove that social engineering exploits human vulnerabilities. Therefore, the technical vector of information security is insufficient. An analysis of the experience of Russian military aggression conducted by Zalevska and Udrenas (2022) demonstrates how propaganda and manipulative narratives significantly complicate the implementation of stable legal mechanisms for protecting the information space.

Research on the interaction between technology and legal regulation occupies a prominent place in the literature. In the works of Bohomia and Halunko (2024) it is emphasized that, although Ukraine has made certain steps in bringing its legislation closer to global standards, this process is still far from complete - in particular, in the area of critical infrastructure protection. Dykyi (Dykyi et al., 2021) emphasize the need for constant monitoring of emerging threats. Alieksieieva (2023) examines the security of critical infrastructure facilities in detail. These works prove that there is a significant gap between declared threats and real challenges.

Researchers also note the undeniable importance of international standards in building comprehensive information security systems. Many scholars (Shevchuk, 2023; Tychna, 2020) call for the implementation of international standards at the national level. This factor is superimposed on the argument of Lubenets (Lubenets et al., 2023), who argue that without close international coordination and unification of legislative approaches, successful counteraction to modern hybrid threats becomes difficult. As a result, scientists are inclined to believe that for Ukraine, the issue of ensuring information security is a matter of survival and state stability.

1. **Materials and Methods**

The study is based on a comprehensive approach that takes into account the multifactorial nature of this problem. The choice of methodology is due to the need to simultaneously take into account a wide range of legal acts and the dynamics of changes associated with the war. The use of analysis and synthesis methods made it possible to isolate individual components of the legal field and clarify the content and direction of each of them. In addition, this method was used to combine the results of the article into a holistic picture of the legal support of information security. Among other things, this is reflected in the conclusions to the work. The use of the analysis and synthesis method made it possible to consider key provisions of laws and identify existing gaps. The results of the stage of analytical differentiation of different categories of threats (technical and social) were the basis for forming a definition of the concept of *information security*. The author used a systemic approach, which required considering the legal support of information security as a system of interconnected components: from constitutional guarantees and international obligations to special sectoral laws and by-laws. The application of this approach ensured the classification of legislative acts in the field of information security into separate categories according to their subject.

The application of the legalistic method was focused on a thorough textual analysis of national legislation and international legal acts. This method provides an opportunity to explore formal and legal aspects. The analysis of the provisions of the Laws of Ukraine provided a holistic view of the legal field of information security. At the same time, the fragmentation of legal acts and certain gaps were identified. It is recommended to harmonize legal acts with international information security standards. Considerable attention was paid during the study to the correlation between theoretical conclusions and practical challenges.

The study also envisaged the simultaneous use of analysis and synthesis together with systemic and legalistic methods at each stage. Such a combination allowed to “layer” the array of legal documents and identify their imperfections. At the same time, this allowed us to identify promising ways of modernization that can be used as the basis for the concept of a national strategy for information sovereignty.

Thus, the selected research methods allowed us to obtain a holistic view of the state of legal regulation of information security in Ukraine, identify problems and propose constructive directions for their solution. The results obtained can serve as a basis for further scientific research.

**4. Results**

*4.1. Theoretical foundations of information security and its role in national security ensuring*

Problems with the issue of information security begin already at the stage of defining its terminology. Domestic legislation does not contain a single definition of the concept of *information security*. This creates fragmentation of legal acts devoted to various aspects of countering information threats. Moreover, this applies to both information security and its constituent elements. It is worth noting that the information security of the state includes many elements that, in fact, form it. So, let's consider a number of scientific views on the relevant issue. As defined by Dykyi, Naumchuk and Trosteniuk (2021), information security is a form of protection of the most important interests of citizens, the state and society, which helps prevent damage to information, its poor quality, unfair and untimely dissemination. Tsymbaliuk (2014) believes that information security of Ukraine is a state of protection of state interests in the field of information. Bondar (2014) proposes to define information security as the functioning of a system of means that ensure the security of information systems.

According to Kochubey (2015), information security characterizes the state of protection of vital interests, information armament of the state, society, and individual. Mazurenko (2022) notes that information security includes a sufficient level of information culture of the individual; the ability of the state to create conditions for the normal development and satisfaction of human needs for information, while avoiding information threats; guarantees of the development and use of the information environment in the interests of each individual; protection from threats. Zalevska and Udrenas (2022) do not provide a direct definition of the concept under study, but note that information security regulates the need to counteract *special information operations of the aggressor state*.

Tychna (2020) proposes to consider information security in two planes: static, as the protection of the individual, society and the state from destructive and other negative influences in the information space; dynamic, as a set of practical actions aimed at protecting data from unauthorized access or alteration, both during storage and transmission. Shevchuk (2023) defines information security as a permanent process of activity of competent authorities aimed at preventing and counteracting threats in the information sphere through the use of active measures of information influence, as well as a set of conditions for such activities that can be implemented and monitored over time.

However, most of these studies give a very vague definition of information security, which includes *ensuring the interests of the state/society/individual* (Tsymbaliuk, 2014; Kochubey, 2015; Shevchuk, 2023) or consider it in the context of ensuring counteraction to the spread of disinformation (Dykyi et al., 2021; Mazurenko, 2022; Kalina et al., 2022). There are also a number of approaches that define the concept under study through data security (Bondar, 2014; Tychyna, 2020). However, we have found almost no approaches to identifying the key components of information security around which its definition should be built. Most scholars consider *information security* in only one of two ways: either ensuring data protection or countering disinformation. In our opinion, this concept should combine both elements, and their inclusion is critical to understanding this concept.

Information security contains technical and social elements (Basholli et al., 2023). The technical component of information security can be called *cybersecurity*. It concerns the issue of implementing technical measures to protect information. According to the Law of Ukraine *On the Basic Principles of Ensuring Cybersecurity of Ukraine* (Verkhovna Rada of Ukraine, 2017b), *cybersecurity is the protection of the vital interests of a person and a citizen, society and the state when using cyberspace, which ensures the sustainable development of the information society and the digital communicative environment, timely detection, prevention and neutralization of real and potential threats to the national security of Ukraine in cyberspace*. In other words, the technical component covers the protection of information and telecommunication systems from unauthorized access, hacking, cyberattacks, data leaks, etc. In this aspect, technical means of monitoring and analyzing threats play a key role. In addition, intrusion detection and prevention systems are important. In general, the technical element of information security includes all technical elements of its functioning. It is the technical component that determines the state's ability to respond to cyberattacks. The main types of cybersecurity threats are malware, ransomware, phishing, insider threats, distributed denial of service (ddos) attacks, botnets, cloud exploits, etc. (Syrovatchenko, 2024).

The social dimension of information security focuses on protecting the information environment from destructive influence (Mujinga, 2017). It includes such elements of influence as propaganda, disinformation, or information and psychological operations (hereinafter – IPO). Given the current security situation in Ukraine, it is of particular importance to study the methods and channels of spreading false information and forming negative narratives in public opinion. The hybrid nature of modern threats means that purely technical counteraction does not solve the entire problem. After all, the aggressor's goal may be to undermine trust in state institutions, manipulate public sentiment, and increase internal instability (Zalevska & Udrenas, 2022). In recent years, social networks have been saturated with information flows. Today, there is virtually no scientific empirical and social management experience in responding to such waves of information (Mazurenko, 2022).

A common feature of all components of the information space is information that requires protection from internal and external threats (Dykyi et al., 2021). Thus, the information security of the state is formed at the intersection of two spheres:

1) Cybersecurity (technical dimension) provides for the protection of information systems and networks from any external or internal interference aimed at violating the integrity, availability or confidentiality of data.

2) Information influence (social dimension) covers the issues of countering disinformation, propaganda, psychological operations aimed at manipulating public opinion and destabilizing society.

**Table 1.** Components of information security

|  |  |
| --- | --- |
| **Informational security** | |
| **Technical**  **(counteracting the phenomena below)** | **Social**  **(counteracting the phenomena below)** |
| malware | propaganda |
| ransomware | disinformation |
| phishing | fake news |
| insider threats | information and psychological operations |
| distributed denial of service attacks | deepfakes |
| botnets | targeted manipulations in social networks |
| cloud exploits | social engineering |
| supply chain attacks | astrosurfing |
| DNS hijacking | hate speech |
|  | creation of manipulative groups and channels |
|  | imitation of authoritative sources |

Thus, we have determined that information security is a multicomponent concept. It includes many aspects of information protection. On the one hand, technical measures to counter threats must be implemented. They provide the technical component of information security. On the other hand, social attitudes are also important, because undermining society from within through disinformation and propaganda poses no lesser threats to information security. Both elements are extremely important. However, in academic circles, these elements are often separated, as we have already seen from the definitions above. Very few academic papers talk about multicomponentism (Lytvyn et al., 2022). Most either equate information security with cybersecurity or refer to it exclusively as countering disinformation. The lack of a unified scientific approach is the basis for further problems that can be found in domestic legislation. And they have become especially evident since the beginning of the full-scale invasion. Due to the lack of definition, we observe fragmentation of legislation. Therefore, the definition of terminology is a key initial step towards creating a comprehensive legal framework. Based on our research, we define information security as a multi-component state of protection of the digital and communication space from technical and social threats, which ensures the integrity and confidentiality of information, as well as the resilience of society to external and internal destructive influences. This element is key to the development of a national concept of information sovereignty, which will include a comprehensive system for ensuring state security in the event of a full-scale invasion and in peacetime.

*4.2. Legal aspects of ensuring information security in Ukraine*

As we have already noted, Ukrainian legislation is rather fragmented. Nevertheless, we cannot ignore the existing legal acts. Analyzing them will help to identify their advantages and disadvantages and will be useful for developing practical recommendations. The analysis should probably start with the main legal act – the Constitution of Ukraine (Verkhovna Rada of Ukraine, 1996a). According to the provisions of Article 17, *...ensuring information security is one of the most important functions of the state*. The provisions of Article 32 guarantee the right to inviolability of personal information. And Article 34 states that *everyone has the right to freely collect, store, use and disseminate information*. According to the Law of Ukraine *On Information* (Verkhovna Rada of Ukraine, 1992c), *information means any information and/or data that can be stored on material carriers or displayed electronically.* Article 6 of this Law ensures the right to information. However, it also states that this right may be limited by law in the interests of national security.

We have reviewed these legal acts for a general understanding of the regulation of *information* and the right to information. Next, we will focus in more detail on information security legislation. And in this context, we will draw attention to the Law of Ukraine *On the Basic Principles of Ensuring Cybersecurity of Ukraine* (Verkhovna Rada of Ukraine, 2017b). It provides for the formation of a cyber defense system based on multisubjectivity. It defines the main tasks for countering cyber threats and procedures for interaction between authorized bodies. However, we noted the need for additional bylaws. For example, the law does not unify the procedure for exchanging data on incidents. In addition, its provisions do not always clearly define the limits of competence of various government agencies, which is especially noticeable when investigating large-scale cyberattacks.

The Law of Ukraine *On Protection of Information in Information and Telecommunication Systems* (Verkhovna Rada of Ukraine, 1994b) also regulates the issue of technical protection of information. It sets out requirements for maintaining the confidentiality and integrity of data and defines approaches to cryptographic and technical protection. At the same time, a number of its provisions, in particular, regarding security levels and responsibilities of business entities, need to be clarified or updated in accordance with modern international standards (ISO/IEC 27000, NIST, etc.) (Bohomia & Halunko, 2024). The provisions of the Law of Ukraine *On Personal Data Protection* (Verkhovna Rada of Ukraine, 2010) should also be taken into account, which is designed to regulate the processing of personal information and ensure the rights of citizens in the digital environment. There is still a problem of full harmonization with the European GDPR, which complicates integration with the EU's digital single market.

From the legal point of view, information security is closely related to national security in general. The Laws of Ukraine *On National Security of Ukraine* and *On State Secrets* define key aspects of protection of information constituting a state secret. At the same time, they include general provisions on ensuring security in the information sphere (Verkhovna Rada of Ukraine, 2018; Verkhovna Rada of Ukraine, 1994a). It outlines strategic directions for countering propaganda and destructive influence. However, it should be noted that its provisions are rather conceptual. With this in mind, we believe it is necessary to develop detailed implementation plans and control mechanisms.

Despite the existing legislation, they identified certain gaps that negatively affect the effectiveness of regulation. First of all, there is a lack of unified terminology: the concepts of *hybrid threat*, *disinformation* or *information and psychological operation* often do not have a single definition in different legal documents. This is similar to the issue of defining information security. Such shortcomings give rise to conflicts. In addition, some legislation related to the distribution of powers and responsibilities for cyber incidents remains unclear. We also note underdeveloped mechanisms for interagency coordination. They can complicate the rapid response to information attacks (Alieksieieva, 2023). At the same time, technical regulations governing the security of IT systems are often not updated in time and lag behind modern challenges. A separate gap is the lack of harmonization with EU legislation, for example, on personal data protection and the implementation of the NIS2 Directive, which sets out requirements for the cyber resilience of critical information infrastructures (Bohomia & Halunko, 2024).

Of course, we will not describe all legal acts in detail. We have focused only on those that were important to us for understanding the key aspects and problematic issues in the context of information security. However, after conducting a detailed analysis of all legal acts that directly or indirectly relate to the issue of information and information space, we classified them as shown in Table 2.

**Table 2.** Classification of the main legal acts of Ukraine in the context of information security and related issues

|  |  |
| --- | --- |
| **Regulated issues** | **Legal acts** |
| Freedom of speech and the right to information | Constitution of Ukraine (1996) |
| Law of Ukraine *On Information* (Verkhovna Rada of Ukraine, 1992c) |
| Law of Ukraine *On Access to Public Information* (Verkhovna Rada of Ukraine, 1996b) |
| Law of Ukraine *On Media* (Verkhovna Rada of Ukraine, 2023) |
| Law of Ukraine *On Public Media of Ukraine* (Verkhovna Rada of Ukraine, 2014a) |
| National security | Law of Ukraine *On National Security of Ukraine* (Verkhovna Rada of Ukraine, 2018) |
| Law of Ukraine *On Defense of Ukraine* (Verkhovna Rada of Ukraine, 1992a) |
| Law of Ukraine *On State Secrets* (Verkhovna Rada of Ukraine, 1994a) |
| Law of Ukraine *On the Security Service of Ukraine* (Verkhovna Rada of Ukraine, 1992b) |
| Law of Ukraine *On Intelligence* (Verkhovna Rada of Ukraine, 2020b) |
| Decree of the President of Ukraine *On the Doctrine of Information Security of Ukraine* (2017) |
| General information issues | Law of Ukraine *On the Basic Principles of Ensuring Cybersecurity of Ukraine* (Verkhovna Rada of Ukraine, 2017b) |
| Law of Ukraine *On Protection of Information in Information and Telecommunication Systems* (1994) |
| Law of Ukraine *On Personal Data Protection* (2010) |
| Law of Ukraine *On Electronic Communications* (Verkhovna Rada of Ukraine, 2020a) |
| Other related issues | Law of Ukraine *On Sanctions* (Verkhovna Rada of Ukraine, 2014b) |
| Law of Ukraine *On Electronic Identification and Electronic Trust Services* (Verkhovna Rada of Ukraine, 2017a) |

To summarize, we can note the multisectoral nature of information security legislation. It covers a wide range of issues, from protecting freedom of speech and countering cyber threats to regulating media activities. Although the legal framework is broad enough, it remains fragmented and requires clearer interaction between acts of different levels. In addition, the effectiveness of the legislation could be enhanced by harmonizing it with international treaties, which we will discuss later in the paper.

*4.3. Harmonization of Ukrainian legislation with international information security standards*

International standards in the field of cybersecurity play a fundamental role in the formation of a comprehensive system of information resources protection/ Such standards are developed on the basis of many years of experience and are constantly updated in accordance with the development of technologies and new threats (Fidler, 2015). Their implementation is intended to improve the overall level of information protection in countries. In addition, it contributes to the unification of approaches to security at the international level, which is becoming a crucial factor for effective international cooperation in countering cyberattacks.

One of the most famous groups of standards that have gained worldwide recognition is ISO/IEC 27000. It contains a number of documents that describe requirements and best practices for information security management. The key standard here is ISO/IEC 27001, which defines the process of maintaining an Information Security Management System (hereinafter – ISMS) in any organization. This systematic approach involves a comprehensive consideration of technical, organizational and human security factors. This comprehensiveness helps to identify and minimize specific risks and continuously improve data protection procedures (International Organization for Standardization, 2023).

The National Institute of Standards and Technology Cybersecurity Framework (hereinafter referred to as NIST CSF) (2025) is important. This document proposes a risk management framework that focuses on vulnerability identification. Its main advantage is flexibility, as its provisions can be applied selectively according to the needs of the person applying them. Within the EU, the Directive on the Security of Network and Information Systems (European Union, 2016) is of great importance, or rather, the new version, 2022, which replaced the NIS Directive, known as the NIS2 Directive. The relevant Directive establishes legal obligations for Member States to increase the level of cyber resilience and improve coordination in responding to cyberattacks. A particularly important aspect is the requirement for providers of critical infrastructure and digital services. According to the provisions of the Directive, they are obliged to comply with basic security measures, report incidents in a timely manner and cooperate with national cyber defense centers. Thanks to this approach, EU Member States strive to form a single standard for protecting key industries.

In general, the role of international standards is primarily to increase the overall level of preparedness for threats and rapid response to incidents. The use of universal norms allows for unified requirements for security procedures. In addition, they ensure the exchange of best practices between state institutions. Long-term cooperation in combating information threats is key. Given the constant growth of threats in the information security sector, national governments are increasingly turning to the norms and recommendations of international organizations (Syrovatchenko, 2024).

In today's circumstances, for Ukraine, compliance with international security standards in the information space is an additional guarantee of increasing the stability of critical information systems, and therefore, national stability. In the process of ensuring national security, international standards are considered an effective tool for achieving strategic goals in the field of information space protection.

The European vector of Ukraine’s development also necessitates the incorporation of international information standards. Ukraine has taken a number of steps in this direction, in particular, the Law of Ukraine *On the Basic Principles of Ensuring Cybersecurity of Ukraine* (Verkhovna Rada of Ukraine, 2017b) was adopted. Despite this, there are still a number of areas that require deeper reforms. First, the implementation of NIS2 can improve the regulatory framework for the protection of critical infrastructure. In particular, the directive focuses on the operational exchange of information on cyber incidents.

EU Regulation 2016/679 (GDPR) also cannot be ignored. The Law of Ukraine *On the Protection of Personal Data* (Verkhovna Rada of Ukraine, 2010) was adopted before the GDPR came into force, so it needs to be amended to meet stricter standards for the processing of personal data. Adaptation to the GDPR is designed to increase the legal protection of citizens and facilitate access to the European market. Another important aspect is the need to develop comprehensive by-laws. Their provisions should focus on detailed regulation of actions when detecting cyber threats.

Therefore, the prospects for adapting Ukrainian legislation to international standards lie in the consistent updating of relevant laws and by-laws, in close coordination with international partners. In general, Ukraine needs a comprehensive document that would include the full range of regulation of the relevant issue, starting with the correct definition of terminology and components. We believe that such a document could be the National Strategy of Information Sovereignty, which we will consider further in the work.

*4.4. Conceptual principles for the formation of a national information sovereignty strategy*

The shortcomings that exist in domestic legislation, together with modern military and non-military threats, necessitate the adoption of the National Strategy for Information Sovereignty of Ukraine. Its provisions should take into account the constant threat from the aggressor, as well as the future development of technologies. That is, we believe that such a strategy should be divided into a state of war and the post-war functioning of Ukraine in the context of information threats.

The formation of the Strategy requires comprehensive coordination of efforts. A strategic vision will allow combining the efforts of the state and non-state actors to counteract destructive information influence. One of the key prerequisites for the effectiveness of such a strategy is the clarity of terminology. It is important to clearly and fully define the concept of *information security*. Today, we have identified conceptual inaccuracies and the lack of a clear definition of terms in the current legislation (Bohomia & Halunko, 2024). All this should be standardized in the provisions of the strategy. A unified approach is necessary to ensure effective coordination of measures in various departments.

It is important to emphasize that the strategy should not only unify the norms of national legislation, but also incorporate the provisions of international legal acts. We believe that international cooperation between participants in international relations is the key to building sustainable information security in the world and in each individual country. Based on the research conducted, we want to highlight the structural elements of the national strategy:

1. Terminology. This block should include definitions of all key terms.

2. Analytics. The relevant part of the strategy should contain an assessment of current threats and identify critical areas that require special protection.

3. The legal field should include the need to develop unified legislation, including international standards.

4. Institutional cooperation. This block establishes the structure and powers of competent authorities in the field of ensuring information security (separately – technical and social). In addition, this part should contain a clear description of the procedures for interagency interaction.

5. Technological infrastructure. The corresponding block is aimed at implementing modern security standards.

6. Measures to counter social threats. This part describes the mechanisms for combating information and psychological operations.

7. Educational component contains programs for training and retraining specialists in the field of information security and the formation of information literacy of the population.

8. Forecasting. This part of the strategy should take into account technological trends and possible threats that may arise as a result. That is, ensure the adaptability of the strategy to rapid changes in the digital environment.

An important principle in preparing a strategy should be to focus on the development of technologies in advance. Therefore, it is worth planning measures to counter potential threats in advance. Such an approach will allow the state to be proactive in shaping information security policy. Ukraine will continue to be the object of targeted pressure from the Russian Federation, in particular through various information operations. Their goal is to weaken national stability and undermine trust in state institutions. This nature of the threat dictates the need to take into account the specifics of Russian information aggression, which Ukraine has been facing for years. For more than 10 years, research has been conducted into the aggressor's narratives. This can be collected within the framework of the development and implementation of the national strategy of information sovereignty. In particular, the priority areas should include constant monitoring of propaganda. Only with systemic readiness for Russia's hybrid operations in the digital and media space, Ukraine will be able to effectively protect its information sovereignty.

1. **Discussion**

The issue of legal support for information security in Ukraine is becoming particularly relevant in the face of constant threats. It is necessary to simultaneously take into account the technical aspects of cyber security and social factors of information security. The results of the analysis of Ukrainian legislation indicate that some progress has been achieved. In particular, fundamental laws in the field of cybersecurity and information space have been adopted, and specialized by-laws have been developed. At the same time, the current norms are not always synchronized with each other, and their implementation is significantly complicated due to the lack of resources and incoherence of interagency interaction (Oliinyk et al., 2022).

The problem of the lack of a unified approach to terminology is of considerable interest in the scientific community. In particular, key concepts can be interpreted differently in different regulatory acts. Moreover, there is no definition of "information security", and those provided by the doctrine are not complete. This provokes discrepancies in law enforcement. Therefore, we propose to introduce a single glossary of terms in the Strategy of National Information Sovereignty.

No less acute is the issue of determining the limits of the powers of state bodies in the field of information security. Moreover, we consider international cooperation to be an important element of ensuring information security. At the same time, the legislation of Ukraine has not incorporated many international standards in this area. Often, this complicates international cooperation. Therefore, researchers pay considerable attention to the issue of implementing international standards. Against the background of Ukraine's European integration aspirations, the implementation of the NIS2 directives is of great importance. The adoption of ISO global standards is also important. The role of the state is to create incentives to increase the attractiveness of investments in the field of information security (Bielov et al., 2019).

A separate area of discussion is the problem of persistent pressure from the Russian Federation. The enemy systematically uses cyberattacks and information operations to achieve its political goals. The question of whether national legislation is able to fully cover the tools used by the Russian Federation remains open. It is important to prevent such threats, and not just respond to them promptly (Kostenko et al., 2024).

After all, the importance of interdisciplinary research in the field of information security is steadily growing. Lawyers, together with IT specialists, should develop recommendations. Such research will help form a conceptual basis for further legislative initiatives. In addition, it is important for the implementation of practical measures.

The limitations lie primarily in the dynamism of the Ukrainian regulatory framework, which is in the stage of active reform. In addition, most of the results are based on open sources, which makes it impossible to conduct a deep analysis of internal departmental documents and real law enforcement mechanisms. Therefore, further interdisciplinary research should be conducted to comprehensively reveal the problem.

1. **Conclusion**

Thus, based on the research conducted by the author, shortcomings were identified in the formation of conceptual terminology. Information security is defined as a multi-component state of protection of the digital and communication space from technical and social threats, which ensures the integrity and confidentiality of information, as well as the resilience of society to external and internal destructive influences. The modern development of digital technologies and hybrid threats indicate the priority of ensuring information security. This industry is becoming one of the priority areas of national security. A comprehensive assessment of the legislation of Ukraine revealed a number of problems. They consist in the fragmentation of legal acts and insufficient harmonization with international standards. At the same time, the practical implementation of existing laws is complicated by limited resources and the war in Ukraine.

The analysis showed that effective legal support for information security requires systemic coordination, unification of key concepts and adaptation to advanced global and European approaches. The implementation of international standards can increase the level of Ukraine's overall readiness for information threats. In addition, international cooperation is the key to countering information threats.

Given the hybrid nature of threats, the information security strategy should cover not only the technical dimension (cybersecurity), but also the social one – primarily countering disinformation, propaganda and psychological pressure. At the same time, great importance is attached to the development of institutional potential and the formation of a culture of information hygiene.

The development of the National Strategy for Information Sovereignty is of particular importance. This document provides for: a clear definition of terminology; systematic updating of the regulatory and legal framework; institutional cooperation; the creation of extensive mechanisms for forecasting threats and corresponding proactive measures; educational measures. Taking into account the prospects of technological development in advance will allow creating a proactive concept of actions.

Thus, a comprehensive approach to the legal regulation of information security, integrating technical and social aspects, is crucial for preserving the state sovereignty of Ukraine. The formation of a coordinated system, enshrined in the national strategy, will ensure the further sustainable development of Ukrainian society in the face of security threats.

**References**

Akello, B. O. (2024). Organizational information security threats: Status and challenges. *World Journal of Advanced Engineering Technology and Sciences*, *11*(1), 148–162.

Alieksieieva, O. A. (2023) Legal support for cybersecurity of critical infrastructure facilities. *Information and Law*, *4*(47), 168–176. <https://doi.org/10.37750/2616-6798.2023.4(47).291633>

Basholli, F., Mezini, R., & Basholli, A. (2023). Security in the components of information ystems. *Advanced Engineering Days*, *7*, 185-187.

Bielov, D., Aristova, I., & Hromovchuk, M. (2019). The history of the paradigm of constitutionalism at the present stage of development of the Post-Soviet States (on the example of Ukraine). *Studia Universitatis Cibiniensis, Series Historica*, *16*, 265–273.

Bohomia, V. & Halunko, V. (2024). Legal regulation of cybersecurity in the context of critical infrastructure protection. *Information Technology: Computer Science, Software Engineering and Cyber Security*, *4*, 35–42. https://doi.org/10.32782/IT/2024-4-5

Bondar, I. R. (2014). Information security as the basis of national security. *Mechanism of Economic Regulation*, *1*, 68–75.

Dykyi, A., Naumchuk K., & Trosteniuk T. (2021). Analysis of current threats to the information security of the state. *Economic Space*, *176*, 155-158.

Fidler, D. (2015). Whither the web? International law, cybersecurity, and critical infrastructure protection. *Georgetown Journal of International Affairs,* *16*(8), 8–20.

International Organization for Standardization. (2023). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. <https://www.iso.org/ru/standard/73906.html>

Kalina, I., Khurdei, V., Shevchuk, V., Vlasiuk, T., & Leonidov, I. (2022). Introduction of a corporate security risk management system: The experience of Poland. *Journal of Risk and Financial Management,15*(8), article number 335. <http://doi.org/10.3390/jrfm15080335>

Kochubey, L.O. (2015). Information security of the state։ Instruments of protection of the Ukrainian information field (on the Example of Peculiarities of Information and Communication Technologies in the Modern Donbas). *Scientific Notes of I.F. Kuras Institute of Political and Ethnic Studies*, *3*, 220-237.

Kostenko, O. M., Bieliakov, K.I., Tykhomyrov, V., & Aristova, I. (2024). “Legal personality” of artificial intelligence: Methodological problems of scientific reasoning by Ukrainian and EU experts. *AI & Society*, *39*, 1683–1693.

Lubenets, S., Harchenko, I., & Pavlenko, Y. (2023). Current problems of international information security. *The Journal of V. N. Karazin Kharkiv National University*, *17*, 42-48. http://doi.org/10.26565/2310-9513-2023-17-04

Lytvyn, N., Andrushchenko, H., Zozulya, Y. V., Nikanorova, O. V., & Rusal, L. M. (2022). Enforcement ofcourt decisions as a social guarantee of protection of citizens rights and freedoms. *Prawo i Wiez, 2022*(39), 80-102. http://doi.org/10.36128/priw.vi39.351

Mazurenko, M. (2022). Information security in the terms the Russian-Ukrainian war: Challenges and threats. *The Journal of V. N. Karazin Kharkiv National University*, *42*, 50-57.

Microsoft Digital Defense Report (2022). Retrieved from <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report?rtc=1>

Mihaela, C. L. (2020). Current security threats in the national and international context. *Journal of Accounting and Management Information Systems,* *19*(2), 351-378. http://doi.org/10.24818/jamis.2020.02007.

Mujinga, M., Eloff, M., & Kroeze, J. H. (2017). A socio-technical approach to information security. *Twenty-third Americas Conference on Information Systems*. Retrieved from <https://www.researchgate.net/publication/320288245_A_socio-technical_approach_to_information_security>

National Institute of Standards and Technology Cybersecurity Framework. (2025). *NIST cybersecurity framework 2.0: Cybersecurity, enterprise risk management, and workforce management quick start guide.* Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1308.ipd.pdf>

Oliinyk, O.S., Shestopalov, R.M., Zarosylo, V.O., Stankovic, M.I., & Golubitsky, S.G. (2022). Economic security through criminal policies: A comparative study of Western and European approaches. *Revista Cientifica General Jose Maria Cordova, 20*(38), 265-285.

Shevchuk, М.О. (2023). On the question of the genesis of the concept of information security as a component of national security. *Scientific Bulletin of Uzhhorod National University*, *78*(2), 134-139.

Syrovatchenko, M. (2024). Legal aspects of cybersecurity in Ukraine: Current challenges and the role of national legislation. *Bulletin of the National University of Lviv Polytechnic. Series: Legal Sciences,* *1*(41), 314-320. <http://doi.org/10.23939/law2024.41.314>

Tsymbalyuk, V. S. (2014). Legal regulation of information security in Ukraine։ problems of theory and practice. *Administrative Law and Process*, *2*(8), 22-30.

Tychna, B. (2020). Information security as the basis of information activity of the Armed Forces of Ukraine. *Legal Bulletin*, *2*(55), 108-113.

Verkhovna Rada of Ukraine. (1992a). Law of Ukraine No. 1932-XII “On the Defense of Ukraine” Retrieved from <https://zakon.rada.gov.ua/laws/show/1932-12#Text>

Verkhovna Rada of Ukraine. (1992b). Law of Ukraine No. 2229-XII “On the Security Service of Ukraine”. Retrieved from <https://zakon.rada.gov.ua/laws/show/2229-12#Text>

Verkhovna Rada of Ukraine. (1992c). Law of Ukraine No. 2657-XII “On Information”. Retrieved from <https://zakon.rada.gov.ua/laws/show/2657-12#Text>

Verkhovna Rada of Ukraine. (1994a). Law of Ukraine No. 3855-XII “On State Secrets”. Retrieved from <https://zakon.rada.gov.ua/laws/show/3855-12#Text>

Verkhovna Rada of Ukraine. (1994b). Law of Ukraine No. 80/94-VR “On the Protection of Information in Information and Communication Systems”. Retrieved from <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>

Verkhovna Rada of Ukraine. (1996a). Constitution of Ukraine. Retrieved from <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

Verkhovna Rada of Ukraine. (1996b). Law of Ukraine No. 2939-VI “On Access to Public Information”. Retrieved from <https://zakon.rada.gov.ua/laws/show/2939-17#Text>

Verkhovna Rada of Ukraine. (2010). Law of Ukraine No. 2297-VI “On the Protection of Personal Data”. Retrieved from <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

Verkhovna Rada of Ukraine. (2014a). Law of Ukraine No. 1227-VII “On Public Media of Ukraine”. Retrieved from <https://zakon.rada.gov.ua/laws/show/1227-18#Text>

Verkhovna Rada of Ukraine. (2014b). Law of Ukraine No. 1644-VII “On Sanctions”. Retrieved from <https://zakon.rada.gov.ua/laws/show/1644-18#Text>

Verkhovna Rada of Ukraine. (2017a). Law of Ukraine No. 2155-VIII “On Electronic Identification and Electronic Trust Services”. Retrieved from <https://zakon.rada.gov.ua/laws/show/2155-19#Text>

Verkhovna Rada of Ukraine. (2017b). Law of Ukraine No. 2163-VIII “On the Basic Principles of Ensuring Cybersecurity of Ukraine”. Retrieved from <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

Verkhovna Rada of Ukraine. (2018). Law of Ukraine No. 2469-VIII “On National Security of Ukraine”. Retrieved from <https://zakon.rada.gov.ua/laws/show/2469-19#Text>

Verkhovna Rada of Ukraine. (2020a). Law of Ukraine No. 1089-IX “On Electronic Communications”. Retrieved from <https://zakon.rada.gov.ua/laws/show/1089-20#Text>

Verkhovna Rada of Ukraine. (2020b). Law of Ukraine No. 912-IX “On Intelligence”. Retrieved from <https://zakon.rada.gov.ua/laws/show/912-20#Text>

Verkhovna Rada of Ukraine. (2023). Law of Ukraine No. 2849-IX “On Media”. Retrieved from <https://zakon.rada.gov.ua/laws/show/2849-20#Text>

Zalevska, I. I. & Udrenas, H. I. (2022). Information security of Ukraine in the conditions of the Russian military aggression. *South Ukrainian Law Journal*, *1-2*, 20-26.