ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Information Sovereignty under Fire: Legal Challenges for Ukraine

Irina Aristova | Department of Administrative and Information Law, Sumy National Agrarian University, Sumy, Sumy Oblast, Ukraine | ORCID: 0000-0001-9211-3464

Nataliia Kapitanenko | Department of Theory of Law, Constitutional Law and Public Administration, Oles Honchar Dnipro National University, Dnipro, Dnipropetrovsk Oblast, Ukraine | ORCID: 0000-0002-1475-5784

Andrii Lyseiuk | Centre for Organising Educational Activities, National Academy of the Security Service of Ukraine, Kyiv, Ukraine | ORCID: 0000-0002-9026-118

Ievgenii Kryvolap | Faculty of Law and International Relations, National Aviation University, Kyiv, Ukraine | ORCID: 0000-0003-2599-2520

Oleksii Kharytonov | Department of Law, Interregional Academy of Personnel Management, Kyiv, Ukraine | ORCID: 0009-0001-2460-244X

Abstract

The rapid digitalisation of society and the escalation of Russian hybrid aggression have made information security a central component of Ukraine's national sovereignty. Hybrid threats, combining cyberattacks with disinformation campaigns, expose critical gaps in the country's fragmented legal framework. This study aims to analyse Ukraine's legal regulation of information security, identify shortcomings, and propose directions for its harmonisation with international standards, particularly those of the EU and NATO. The research applies structured content analysis of Ukrainian legislation and international documents, comparative legal analysis with European and global practices, and a systemic approach integrating technical and social dimensions of information security. Findings reveal that Ukrainian legislation lacks unified

Received: 26.06.2025

Accepted: 28.08.2025

Published: 22.10.2025

Cite this article as:
I. Aristova, N. Kapitanenko, A. Lyseiuk, I. Kryvolap, O. Kharytonov, "Information sovereignty under fire: Legal challenges for Ukraine," ACIG, vol. 4, no. 1, 2025, doi: 10.60097/ACIG/209993

Corresponding author:
Andrii Lyseiuk, Centre for Organising Educational Activities, National Academy of the Security Service of Ukraine, Kyiv, Ukraine; E-mails: andrii_lyseiuk@sci-univ.com; luseyuk@gmail.com
0000-0002-9026-118

terminology, contains overlapping or vague competences among state institutions, and only partially aligns with international standards, such as ISO/IEC 27001, NIS2, and the General Data Protection Regulation (GDPR). While progress has been made through the adoption of cybersecurity laws and strategies, insufficient coordination and underdeveloped interagency mechanisms undermine effective implementation. Importantly, most legal approaches focus either on cybersecurity or on countering disinformation, neglecting their interdependence. The study concludes that Ukraine requires a National Strategy of Information Sovereignty that integrates both technical and social dimensions, ensures harmonisation with European norms, and strengthens institutional cooperation. Such a strategy should unify terminology, establish clear interagency coordination, incorporate international standards, and include measures for digital literacy and resilience. Addressing these gaps will enhance Ukraine's ability to counter hybrid threats and consolidate its information sovereignty.

Keywords

information security, cybersecurity, cyber threats, disinformation, propaganda, National Strategy of Information Sovereignty of Ukraine

1. Introduction

The modern world is fully digitalised. The rapid development of information and communication technologies creates new opportunities for people. Technology advances and we become more interconnected [1]. At the same time, these same innovations enable an unprecedented spread of cyberattacks and destructive information influence [2]. 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 digitalisation 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 [3], 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% [3]. These are mainly agencies involved in foreign policy, national security, or defence. The top three countries targeted by Russian cyberattacks include the United States, Ukraine, and the United Kingdom [4].

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 harmonisation of Ukrainian legal norms with international cybersecurity standards. Such measures are important for effective counteraction to hybrid threats and are driven by Ukraine's European integration. Active military operations further actualise this process, because in such circumstances, a data leak can cost thousands of lives, or even jeopardise the existence of Ukraine.

Modern hybrid threats are characterised by complexity 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 [5]. 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 [6]. 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.

Undoubtedly, in wartime, the technical elements of information security are of paramount importance. They are the ones that allow us to respond quickly to attacks and mitigate their consequences. At the same time, technical solutions cannot be effective without an appropriate legal basis. The law defines responsible entities, establishes standards, regulates the exchange of information and coordination of actions [7]. This is what gives technical specialists clear rules and the ability to act quickly. In this work, we deliberately

focus on the legal aspect, since it is the framework that allows technical means to work in a coordinated and effective manner.

Despite the adoption of a number of basic laws in the field of cybersecurity, national legislation remains fragmented and insufficiently coordinated. In the context of hybrid aggression, which combines cyberattacks with disinformation campaigns, such gaps directly weaken the resilience of the state [8]. At the same time, the scientific literature still lacks comprehensive legal studies that integrate the technical and social dimensions of information security. The vast majority of publications focus either on the problem of cyber defence or on countering disinformation [9]. The works ignore their interdependence in the legal dimension. This article seeks to fill this gap. Its task is to analyse the legal foundations of Ukraine's information security in the light of hybrid threats, identify key problems of the current legislation, and determine the directions of its harmonisation with international and, above all, European standards.

In this regard, this study aims to analyse Ukraine's legal regulation of information security, identify shortcomings, and propose directions for its harmonisation with international standards, particularly those of the European Union (EU) and North Atlantic Treaty Organization (NATO). Therefore, the contribution of the work lies in two dimensions. First, it offers a comprehensive overview of the legal framework for information security, integrating technical and social aspects into a single framework. Second, the work forms practical guidelines for state policy. This allows us to consider the results of the study as a contribution to the development of practical solutions to strengthen the resilience of the state in war conditions.

2. Literature Review

The issue of information security as a component of national security is widely presented in scientific research. At the same time, a significant part of the work remains one-sided. Thus, researchers tend to consider mainly either the technical or the social dimension. Several key directions can be distinguished in this discourse.

The first direction treats information security primarily as a technical category. Researchers emphasise the prevalence of cyberattacks, the rapid development of technologies, and the inadequacy of legal mechanisms to respond to new challenges. Mihaela [2] emphasises the global nature of cyber threats, while Akello [1] analyses the constant clash of organisations with new types of malware and sophisticated methods of intrusion. Fidler [10] argues that fragmented

legislative updates do not guarantee cyber resilience, and the international community still does not have sufficiently effective tools to respond to the rapid development of threats.

The second direction emphasises the social dimension of information security, in particular the issues of disinformation, propaganda, and social engineering. Mazurenko [11] emphasises that the spread of fake news provokes political and social turbulence. Mujinga et al. [12] demonstrate how social engineering exploits human vulnerabilities. Zalevska and Udrenas [13], analysing Russian aggression, show that manipulative narratives significantly complicate the introduction of stable legal mechanisms for protecting the information space.

The third cluster of studies is devoted to legal and organisational aspects. Bohomia and Halunko [9] analyse Ukraine's progress in approximating legislation to global standards. At the same time, the authors emphasise the incompleteness of this process, especially in the area of critical infrastructure protection. Dykyi et al. [14] emphasise the need for constant monitoring of new threats, while Alieksieieva [15] examines in detail the legal framework for protecting critical facilities. These works demonstrate the gap between declared goals and real capabilities.

A separate layer of literature concerns international standards and coordination. Shevchuk [16] and Tychna [17] call for the implementation of international norms into national legislation, while Lubenets et al. [4] emphasise that without international coordination and unification of legislative approaches, effective counteraction to hybrid threats is impossible.

Thus, the scientific discussion demonstrates the diversity of approaches, but also reveals a significant gap between technical and social interpretations of information security. There is a lack of comprehensive studies that would integrate these dimensions into a holistic legal framework. In this sense, the Ukrainian context is particularly valuable for comparative studies. This makes the presented study relevant not only for Ukrainian legal science, but also for the broader body of literature on international and European security [18–20].

3. Materials and Methods

The study is based on a structured analysis of the content of regulatory legal acts of Ukraine and international documents

in the field of information security. The sample includes the Constitution of Ukraine, basic and special laws, and bylaws regulating certain aspects of information security. Additionally, international standards and analytical reports were involved. The inclusion criteria were: (1) relevance to the field of information security; (2) the presence of legal norms that define subjects, mechanisms, and tools for ensuring protection; and (3) relevance in view of the military context of Ukraine. Acts that are purely declarative in nature without regulatory content were excluded.

The research methodology combines several complementary approaches. First, a structured content analysis of legal texts was applied: for each act, key categories were studied (terminology, subject of regulation, institutional competences, procedural mechanisms, and compliance with international standards). This made it possible to identify the presence or absence of definitions, conflicts in norms, and the level of detail of regulatory provisions. Second, the method of comparative legal analysis was used, which made it possible to compare Ukrainian legislation with international standards and EU practice. Third, the method of analysis and synthesis was applied, thanks to which the results were generalised in the form of a classification of acts by their subject and significance for ensuring information security. An important tool of the research was a systemic approach, which provided for the consideration of the legal support of information security as a holistic system, which includes constitutional guarantees, international obligations, special legislation, and the practice of its application. This approach allowed us to distinguish the technical and social dimensions of information security and explore their interaction.

Thus, the results of the study are based on a phased analysis of legal sources, inductive generalisation of their provisions, and comparison with international practices. This provided an opportunity to identify gaps in the current legislation of Ukraine, outline the risks of its fragmentation, and formulate directions for modernisation, which can become the basis for the development of the National Strategy of Information Sovereignty.

4. Results

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

The consideration of the problem of information security should begin with a clarification of key terminology. One of the

most widely used but insufficiently defined concepts is the hybrid threat. NATO documents describe it as a combination of military and non-military, overt and covert means, including disinformation, cyberattacks, and economic pressure [21]. Similarly, the European Council defines them as malicious, coordinated actions that include information manipulation, cyberattacks, economic pressure, political maneuvers, and even threats of force [22].

Problems with the issue of information security begin 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. For example, in February 2022, the Computer Emergency Response Team of Ukraine (CERT-UA) warned of large-scale cyberattacks being prepared against the country's state, banking, and defence sectors. However, due to the ambiguous legislative definition of concepts, different authorities could interpret this challenge differently. This created gaps in operational response and communication [23].

It is worth noting that the information security of the state includes many elements that, in fact, form it. Therefore, let's consider a number of scientific views on the relevant issue. As defined in the literature [14], information security is a form of protection of the most important interests of citizens, the state, and society, which helps to prevent damage to information, its poor quality, and unfair and untimely dissemination. We believe that the definition is too narrow. It reduces the problem only to the quality and timeliness of information. However, the definition provided does not take into account technological and social aspects. Tsymbaliuk [24] believes that information security of Ukraine is a state of protection of state interests in the field of information. Here, a certain flaw is the author's focus exclusively on the interests of the state. He does not mention the lack of the rights of citizens and the needs of society. This allows us to call this definition one-sided. Bondar [25] proposes to define information security as the functioning of a system of means that ensure the security of information systems. In this definition, information security is effectively reduced to cybersecurity and ignores the social dimension.

According to Kochubey [26], information security characterises the state of protection of vital interests, information armament of the state, society, and individual. Despite the broader approach, the definition remains declarative and does not indicate by what means

this protection is ensured. Mazurenko [11] 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 the development and use of the information environment in the interests of each individual; and protection from threats. The author emphasises information culture and protection against threats. However, the concept of 'information culture' is too general, and the definition has no practical focus. Zalevska and Udrenas [13] 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. The mentioned authors [13] emphasise the need to counter the aggressor's special information operations. However, it also has a certain drawback. The authors emphasise only the military-information aspect, without forming a holistic concept of information security [13].

Tychna [17] 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; and dynamic, as a set of practical actions aimed at protecting data from unauthorised access or alteration, both during storage and transmission. Although an interesting distinction is proposed, it again focuses mainly on technical aspects, without taking into account the social component. Shevchuk [16] 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. The author emphasised the functions of state bodies, but lacks systematic coverage of technical and social components.

However, most of these studies give a very vague definition of information security, which includes ensuring the interests of the state/society/individual [16, 24, 26] or consider it in the context of ensuring counteraction to the spread of disinformation [11, 14, 27]. There are also a number of approaches that define the concept under study through data security [17, 25]. 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 the 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. Thus, most existing definitions suffer from vague wording and lack of a systemic vision. They are either too general and declarative, or focus only on a single aspect. This complicates the development of a coherent conceptual framework and creates terminological gaps.

Information security contains technical and social elements [28]. 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 [29], 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, and prevention and neutralisation 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 unauthorised access, hacking, cyberattacks, data leaks, etc. In this aspect, technical means of monitoring and analysing 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. [8].

The social dimension of information security focuses on protecting the information environment from destructive influence [12]. 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 [13]. 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 [11].

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	IPO
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

A common feature of all components of the information space is information that requires protection from internal and external threats [14]. Thus, the information security of the state is formed at the intersection of the following 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, and psychological operations aimed at manipulating public opinion and destabilising society.

In modern security debates, the concept of 'information sovereignty' is interpreted as the ability of a state to control its own information space, including independence in the regulation of data, infrastructure, standards, and legal norms. In the EU context, this resonates with the idea of digital sovereignty, which implies strategic autonomy [30]. In international law, the essence of information sovereignty is associated with the principle of inviolability of the cyberspace of the state. In other words, when cyber infrastructure, data, and decisions are not subject to external interference. This is emphasised in the concept of cyber-sovereignty, set

out in the Tallinn Manual 2.0. It states that the state has sovereign rights over cyber infrastructure, jurisdiction, protection, and judicial control [31].

The distinction between the technical and social dimensions of information sovereignty allows us to combine two key dimensions. The first includes cybersecurity, standards, and infrastructure. The second includes the cultural and legal context – media literacy, trust in state institutions, and the right to information security. This approach corresponds to the discussion of digital sovereignty, which includes technical, legal, and democratic aspects. This helps to transform a personal strategy into a significant theoretical contribution to the field of security sciences and international law [32].

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 [33]. 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 multicomponent 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 a 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. Unlike previous approaches, it avoids ambiguity by specifically defining the components. The definition combines two dimensions at once – technical and social, and also forms a systemic vision. Such a vision is suitable

for both theoretical analysis and practical application in the field of legislation and public policy.

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. Analysing 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 [34]. 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 [35], 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 [29]. It provides for the formation of a cyber defence system based on multisubjectivity. It defines the main tasks for countering cyber threats and procedures for interaction between authorised bodies. However, we noted the need for additional bylaws. For example, the law does not unify the procedure for exchanging data on incidents.

The disadvantage of this law is the unclear delimitation of competences between state bodies. This leads to duplication of functions or, conversely, gaps in the response to cyber incidents. In particular, in cases of large-scale attacks, it is unclear which body has priority powers, and which reduces the effectiveness of the response. The corresponding gap has its consequences in a practical dimension. For example, in the second quarter of 2023, the number of critical information security events increased by 38.1%, and incidents with malicious software – by more than 95% [36]. These indicators demonstrate that the situation in the cyber dimension is worsening. This is especially important in the context of threats from Russia [37]. In such conditions, legislative ambiguity regarding

who exactly is responsible for protection, monitoring, and initial response seriously slows down the response process. As a result, this creates risks for critical infrastructure.

The Law of Ukraine on Protection of Information in Information and Telecommunication Systems [38] 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, National Institute of Standards and Technology [NIST], etc.) [9]. This means that business entities operating in Ukraine are forced to focus simultaneously on both international requirements and domestic regulations. The provisions of the Law of Ukraine on Personal Data Protection [39] 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 harmonisation with the European General Data Protection Regulation (GDPR), which complicates integration with the EU's digital single market. In practical terms, this means that multinational companies are wary of cooperating with Ukrainian partners, as the level of legal data protection in national legislation is considered lower than European standards.

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 [40, 41]. It outlines strategic directions for countering propaganda and destructive influence. However, it should be noted that its provisions are rather conceptual. They only outline strategic directions but do not contain clear mechanisms for implementation or control. The lack of specific procedures makes it impossible to respond promptly to information threats, as responsibility for implementation is vaguely distributed between different institutions.

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 [15]. 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 harmonisation 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 [9].

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) [34]
	Law of Ukraine on Information [35]
	Law of Ukraine on Access to Public Information [42]
	Law of Ukraine on Media [43]
	Law of Ukraine on Public Media of Ukraine [44]
National security	Law of Ukraine on National Security of Ukraine [41]
	Law of Ukraine on Defense of Ukraine [45]
	Law of Ukraine on State Secrets [40]
	Law of Ukraine on the Security Service of Ukraine [46]
	Law of Ukraine on Intelligence [47]
General information issues	Law of Ukraine on the Basic Principles of Ensuring Cybersecurity of Ukraine [29]
	Law of Ukraine on Protection of Information in Information and Telecommunication Systems [38]
	Law of Ukraine on Personal Data Protection [39]
	Law of Ukraine on Electronic Communications [48]
Other related issues	Law of Ukraine on Sanctions [49]
	Law of Ukraine on Electronic Identification and Electronic Trust Services [50]

To summarise, 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 harmonising it with international treaties, which we will discuss later in the paper.

4.3. Harmonisation 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 [10]. 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 (ISMS) in any organisation. This systematic approach involves a comprehensive consideration of technical, organisational, and human security factors. This comprehensiveness helps to identify and minimise specific risks and continuously improve data protection procedures [51].

The National Institute of Standards and Technology Cybersecurity Framework (hereinafter referred to as NIST CSF) (2025) is important [52]. 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 [53] 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 defence centres. 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 the best practices between state institutions. Long-term cooperation in combating information threats is a key. Given the constant growth of threats in the information security sector, national governments are increasingly turning to the norms and recommendations of international organisations [8].

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 [29] 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 [39] 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 bylaws. Their provisions should focus on detailed regulation of actions when detecting cyber threats.

In 2021, the Cybersecurity Strategy of Ukraine for 2021–2025 was also adopted. This legal act is directly oriented towards the principles of ISO/IEC 27001 and NIST CSF. It defines tasks for state bodies

in the field of cyber risk management and incident response [54]. As part of the harmonisation, the Law of Ukraine 'On Critical Infrastructure' was also adopted [55]. The relevant legal act establishes mechanisms for identifying and protecting critical infrastructure facilities in accordance with NIS2 standards. The Resolution of the Cabinet of Ministers of Ukraine 'On Approval of the Procedure for Ensuring Cybersecurity of Critical Information Infrastructure Facilities' [56] also brings Ukraine's requirements closer to ISO/IEC 27001. This is the implementation of ISMS. In addition, the document provides for security planning, auditing, and reporting. These mechanisms are similar to international ones.

Therefore, the prospects for adapting Ukrainian legislation to international standards lie in the consistent updating of relevant laws and bylaws in close coordination with international partners. In general, Ukraine needs a comprehensive document that would include the full range of regulation of relevant issue, starting with the correct definition of terminology and components. The harmonisation of Ukrainian legislation with EU standards is already underway, but is fragmentary. The next step should be the comprehensive implementation of NIS2 requirements into national law. In addition, it seems advisable to harmonise data protection provisions with the GDPR. Such an approach will ensure compliance with the European legal space, which is a key condition for integration.

Harmonisation of Ukrainian legislation with international information security standards has obvious advantages, but the process faces a number of obstacles. First of all, it is about limited resources. The introduction of ISO/IEC 27001 or NIS2 requirements requires significant financial costs for technical upgrades, system certification, and personnel training. For many institutions, such costs are excessive. An additional problem is the shortage of qualified specialists, which limits the ability of the state and business to maintain an adequate level of compliance with international practices [20].

Another factor is political and legal difficulties. In war conditions, state priorities are aimed at an operational response, rather than systemic harmonisation. The difference in legal traditions also complicates the adaptation of the EU acquis. Some provisions may contradict the existing Ukrainian norms or require long-term implementation. This leads to fragmentation and delays in reforming the legal framework. No less important is the social aspect of harmonisation, which remains ignored. Legislation focuses mainly on technical standards and control mechanisms. At the same time, issues of digital literacy, the formation of a culture of security, and trust

in institutions are practically not considered. Ignoring this dimension reduces the effectiveness of harmonisation because technical solutions will not provide results without public support and proper behavioural adaptation of users.

The implementation of international standards is critically important for Ukraine today. The Report of the State Centre for Cyber Defence for the second quarter of 2023 noted that using the tools of the system for detecting vulnerabilities and responding to cyber incidents and cyber-attacks, 122 million suspicious information security events were detected (during primary analysis) and 55,000 critical information security events were processed (potential cyber incidents detected by filtering suspicious information security events and secondary analysis). At the same time, 191 cyber incidents were recorded and processed directly by security analysts [57]. The reports emphasise that the state is actively implementing lessons from military cyberattacks. However, the application of international standards is not always legally formalised. As a result, state and private institutions improvise security measures.

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 [9]. All this should be standardised in the provisions of the strategy. A unified approach is necessary to ensure effective coordination of measures in various departments.

It is important to emphasise 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. Legal field: It 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 IPO.
7. Educational component: This contains programmes 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.

In this context, it is important to define clearly the institutions responsible for implementing the strategy. Coordination should be provided by the National Security and Defence Council of Ukraine. It is the body that forms strategic security priorities. Executive functions can be distributed among several departments. The Ministry of Digital Transformation is responsible for the development of information infrastructure. The Security Service of Ukraine is responsible for countering cyber threats and information attacks. The Ministry of Education and Science is responsible for the educational component. Finally, the Ministry of Defence is responsible for the military sphere. Such a division of responsibilities ensures the comprehensiveness and practical effectiveness of the strategy.

It is worth emphasising that the National Strategy for Information Sovereignty is not a declarative idea. Its emergence is due to a

specific political impulse. Ukraine is an EU candidate country and a NATO partner. It has already undertaken a number of obligations in the field of information and cybersecurity. Therefore, taking into account EU, NATO, and Organisation for Security and Cooperation in Europe (OSCE) standards opens the way for international cooperation in the fight against disinformation. Equally important is the harmonisation of the new document with the existing acts in the field of national security. These are the National Security Strategy, the Information Security Doctrine, and the Concept of Digital Economy Development. The proposed strategy should be their logical continuation and deepening.

An important principle in preparing a strategy should be to focus on the development of technologies in advance. Therefore, it is worth planning the 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 protect effectively its information sovereignty.

5. 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 specialised bylaws have been developed. At the same time, the current norms are not always synchronised with each other, and their implementation is significantly complicated due to the lack of resources and incoherence of interagency interaction [58].

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 [5].

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 cover fully the tools used by the Russian Federation remains open. It is important to prevent such threats, and not just respond to them promptly [6]. 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 practical consequences of the identified gaps are especially noticeable in the context of a full-scale invasion. The vagueness of legal norms and the lack of unified terminology create vulnerabilities in the information space. This is manifested in delays in data exchange between authorities, fragmented response, and contradictory communications with society. As a result, cyberattacks against critical infrastructure facilities can not only cause technical failures but also serve as an intelligence tool for identifying strategically important targets. Thus, legal shortcomings directly affect

the stability of the state, reducing its ability to counteract promptly complex threats during martial law.

The alignment of the Ukrainian legal framework with European standards is of strategic importance. It ensures integration into the EU's single digital market. Harmonisation not only unifies technical requirements. Globally, it strengthens the trust of international partners in Ukraine's ability to adhere to high standards of cyber resilience. In today's conditions, this is an important political signal about the state's readiness to be part of the European security space [53]. At the same time, it is worth considering that in recent years, the EU's security policy has shifted its emphasis from a narrow understanding of 'information security' to the broader concept of foreign malignant interference. This framework encompasses more than just cyber defence. Among other things, it also includes countering disinformation, protecting electoral processes, democratic institutions, and critical infrastructure [59]. Ukraine systematically faces Russia's multifaceted information operations. Its integration into this broader paradigm is the key. It allows us to move from a fragmented response to individual cyberattacks to a systematic counteraction to hybrid threats across their entire spectrum.

The international comparative context deserves additional attention. For example, Estonia implemented a comprehensive cyber resilience system after the 2007 attacks. This made it a leader in cyber defence within NATO [19]. Poland created legal mechanisms to implement the requirements of NIS and NIS2, in particular regarding mandatory reporting by critical infrastructure operators [18]. Involving this experience allows Ukraine to adapt proven international models and take into account the best practices for its own conditions.

6. Conclusions

Thus, based on the research conducted by the authors, shortcomings were identified in the formation of conceptual terminology. Information security is defined as a multicomponent 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 harmonisation with international standards. At the same time, the practical implementation of the 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 the following: 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; and educational measures. Taking into account the prospects of technological development in advance will allow creating a proactive concept of actions.

In practical terms, such a strategy should include several key components. First, it should unify the main concepts, in particular, hybrid threat or information and psychological operation, which remain inconsistent in the current legislation. Second, it is necessary to establish clear procedures for interdepartmental coordination, which will ensure effective interaction between CERT-UA, the Security Service of Ukraine, and other institutions. Third, the strategy should provide for regular updating of technical regulations in accordance with ISO/IEC and NIST standards. This will reduce the gap between law and practice. Fourth, full harmonisation with EU acts is a necessary condition for integration into the European digital security space. Finally, the strategy should combine technical resilience with social measures. Taken together, these elements transform the strategy from a declarative vision into an effective instrument of state policy. 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.

The results obtained have important implications for science and practice. They show that the legal framework for information security in Ukraine remains fragmented. This requires further interdisciplinary research. The future work may focus on comparing Ukrainian approaches with EU and NATO practices. Such research will help to develop specific recommendations for the legislator. The practical significance lies in the possibility of using the findings to develop a National Strategy for Information Sovereignty. The identified legal gaps may become the basis for new legislative initiatives. This will contribute to harmonisation with international standards and increase the state's resilience to cyber threats and disinformation.

The results are also useful for practitioners. They can be used by state bodies, educational institutions, and international partners. Thus, the work creates a basis for further research and has applied significance for security policy. 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 make it impossible to conduct a deep analysis of internal departmental documents and real law enforcement mechanisms. Therefore, further interdisciplinary research should be conducted to reveal the problem comprehensively.

References

[1] B.O. Akello, "Organizational information security threats: Status and challenges," *World Journal of Advanced Engineering Technology and Sciences*, vol. 11, no. 1, pp. 148–162, 2024, doi: 10.30574/wjaets.2024.11.1.0152.

[2] C.L. Mihaela, "Current security threats in the national and international context," *Journal of Accounting and Management Information Systems,* vol. 19, no. 2, pp. 351–378, 2020, doi: 10.24818/jamis.2020.02007.

[3] Microsoft Digital Defense Report. [Online]. Available: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report?rtc=1 [Accessed: 11 Sept. 2025].

[4] S. Lubenets, I. Harchenko, Y. Pavlenko, "Current problems of international information security," *The Journal of V.N. Karazin Kharkiv National University*, vol. 17, pp. 42–48, 2023, doi: 10.26565/2310-9513-2023-17-04.

[5] D. Bielov, I. Aristova, M. Hromovchuk, "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*, vol. 16, pp. 265–273, 2019.

[6] O.M. Kostenko, K.I. Bieliakov, V. Tykhomyrov, I. Aristova, "Legal personality" of artificial intelligence: Methodological problems of scientific reasoning by Ukrainian and EU experts," *AI & Society*, vol. 39, pp. 1683–1693, 2024, doi: 10.1007/s00146-023-01641-0.

[7] C. Luidold, C. Jungbauer, "Cybersecurity policy framework requirements for the establishment of highly interoperable and interconnected health data spaces," *Frontiers in Medicine,* vol. 11, 2024, doi: 10.3389/fmed.2024.1379852.

[8] M. Syrovatchenko, "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,* vol. 1, no. 41, pp. 314–320, 2024, doi: 10.23939/law2024.41.314.

[9] V. Bohomia, V. Halunko, "Legal regulation of cybersecurity in the context of critical infrastructure protection," *Information Technology: Computer Science, Software Engineering and Cyber Security*, vol. 4, pp. 35–42, 2024, doi: 10.32782/IT/2024-4-5.

[10] D. Fidler, "Whither the web? International law, cybersecurity, and critical infrastructure protection," *Georgetown Journal of International Affairs,* vol. 16, no. 8, pp. 8–20, 2015.

[11] M. Mazurenko, "Information security in the terms the Russian-Ukrainian war: Challenges and threats," *The Journal of V.N. Karazin Kharkiv National University*, vol. 42, pp. 50–57, 2022.

[12] M. Mujinga, M. Eloff, J.H. Kroeze, "A socio-technical approach to information security," *Twenty-third Americas Conference on Information Systems*, 2017. [Online]. Available: https://www.researchgate.net/publication/320288245_A_socio-technical_approach_to_information_security [Accessed: 11 Sep. 2025].

[13] I.I. Zalevska, H.I. Udrenas, "Information security of Ukraine in the conditions of the Russian military aggression," *South Ukrainian Law Journal*, vol. 1–2, pp. 20–26, 2022.

[14] A. Dykyi, K. Naumchuk, T. Trosteniuk, "Analysis of current threats to the information security of the state," *Economic Space,* vol. 176, pp. 155–158, 2021.

[15] O.A. Alieksieieva, "Legal support for cybersecurity of critical infrastructure facilities," *Information and Law,* vol. 4, no. 47, pp. 168–176, 2023, doi: 10.37750/2616-6798.2023.4(47).291633.

[16] M.O. Shevchuk, "On the question of the genesis of the concept of information security as a component of national security," *Scientific Bulletin of Uzhhorod National University*, vol. 78, no. 2, pp. 134–139, 2023.

[17] B. Tychyna, "Information security as the basis of information activity of the Armed Forces of Ukraine," *Legal Bulletin*, vol. 2, no. 55, pp. 108–113, 2020, doi: 10.18372/2307-9061.55.14782.

[18] F.J. Egloff, *Cybersecurity and the age of privateering.* Washington, D.C.: Georgetown University Press, 2020.

[19] A. Kozłowski, "Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan," *European Scientific Journal,* vol. 3, pp. 1–14, 2020, doi: 10.19044/esj.2014.v10n7p%25p.

[20] F. Teichmann, "Cybersecurity of critical infrastructure in Europe: the NIS2 directive in focus," *International Cybersecurity Law Review*, vol. 6, pp. 207–220, 2025, doi: 10.1365/s43439-025-00154-4.

[21] NATO. *Countering hybrid threats*, 2024. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_156338.htm [Accessed: 11 Sep. 2025].

[22] European Council. Hybrid threats, 2025. [Online]. Available: https://www.consilium.europa.eu/en/policies/hybrid-threats/? [Accessed: 11 Sep. 2025].

[23] I. Saric, (2022). Ukraine warns of cyberattacks on government and agencies. *Axios*. [Online]. Available: https://www.axios.com/2022/02/21/ukraine-warning-cyberattack [Accessed: 11 Sep. 2025].

[24] V.S. Tsymbalyuk, "Legal regulation of information security in Ukraine: problems of theory and practice," *Administrative Law and Process*, vol. 2, no. 8, pp. 22–30, 2014.

[25] I.R. Bondar, "Information security as the basis of national security," *Mechanism of Economic Regulation*, vol. 1, pp. 68–75, 2014.

[26] L.O. Kochubey, "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*, vol. 3, pp. 220–237, 2015.

[27] I. Kalina, V. Khurdei, V. Shevchuk, T. Vlasiuk, I. Leonidov, "Introduction of a corporate security risk management system: The experience of Poland," *Journal of Risk and Financial Management,* vol. 15, no. 8, article number 335, 2022, doi: 10.3390/jrfm15080335.

[28] F. Basholli, R. Mezini, A. Basholli, "Security in the components of information ystems," *Advanced Engineering Days*, vol. 7, pp. 185–187, 2023.

[29] Verkhovna Rada of Ukraine. Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring Cybersecurity of Ukraine". 2017. [Online]. Available: https://zakon.rada.gov.ua/laws/show/2163-19#Text [Accessed: 11 Sep. 2025].

[30] G. Hulkó, J. Kalman, A. Lapsánszky, "The politics of digital sovereignty and the European Union's legislation: navigating crises", *Frontiers in Political Science,* vol. 7, article number 1548562, 2025, doi: 10.3389/fpos.2025.1548562.

[31] M.N. Schmitt, "Sovereignty," in *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, M.N. Schmitt, Ed. Cambridge: Cambridge University Press, 2017, pp. 11–29.

[32] R. Baldoni, G. Di Luna, "Sovereignty in the digital era: the quest for continuous access to dependable technological capabilities," *IEEE Security & Privacy,* vol. 23, no. 1, pp. 91–96, 2025, doi: 10.1109/MSEC.2024.3500192.

[33] N. Lytvyn, H. Andrushchenko, Y.V. Zozulya, O.V. Nikanorova, L.M. Rusal, "Enforcement of court decisions as a social guarantee of protection of citizens' rights and freedoms," *Prawo i Wiez,* vol. 39, no. 1, pp. 80–102, 2022, doi: 10.36128/priw.vi39.351.

[34] Verkhovna Rada of Ukraine. Constitution of Ukraine, 1996. [Online]. Available: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text [Accessed: 11 Sep. 2025].

[35] Verkhovna Rada of Ukraine. Law of Ukraine No. 2657-XII "On Information," 1992. [Online]. Available: https://zakon.rada.gov.ua/laws/show/2657-12#Text [Accessed: 11 Sep. 2025].

[36] A. Greenberg, Russia's sandworm hackers attempted a third blackout in Ukraine. *Wired*, 2022. [Online]. Available: https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/ [Accessed: 11 Sep. 2025].

[37] Verkhovna Rada of Ukraine. Law of Ukraine No. 80/94-VR "On the Protection of Information in Information and Communication Systems," 1994. [Online]. Available: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text [Accessed: 11 Sep. 2025].

[38] Verkhovna Rada of Ukraine. Law of Ukraine No. 2297-VI "On the Protection of Personal Data," 2010. [Online]. Available: https://zakon.rada.gov.ua/laws/show/2297-17#Text [Accessed: 11 Sep. 2025].

[39] Verkhovna Rada of Ukraine. Law of Ukraine No. 2469-VIII "On National Security of Ukraine," 2018. [Online]. Available: https://zakon.rada.gov.ua/laws/show/2469-19#Text [Accessed: 11 Sep. 2025].

[40] Verkhovna Rada of Ukraine. Law of Ukraine No. 3855-XII "On State Secrets," 1994. [Online]. Available: https://zakon.rada.gov.ua/laws/show/3855-12#Text [Accessed: 11 Sep. 2025].

[41] Verkhovna Rada of Ukraine. Law of Ukraine No. 2939-VI "On Access to Public Information," 1996. [Online]. Available: https://zakon.rada.gov.ua/laws/show/2939-17#Text [Accessed: 11 Sep. 2025].

[42] Verkhovna Rada of Ukraine. Law of Ukraine No. 2849-IX "On Media," 2023. [Online]. Available: https://zakon.rada.gov.ua/laws/show/2849-20#Text [Accessed: 11 Sep. 2025].

[43] Verkhovna Rada of Ukraine. Law of Ukraine No. 1227-VII "On Public Media of Ukraine," 2014. [Online]. Available: https://zakon.rada.gov.ua/laws/show/1227-18#Text [Accessed: 11 Sep. 2025].

[44] Verkhovna Rada of Ukraine. Law of Ukraine No. 1932-XII "On the Defence of Ukraine," 1992. [Online]. Available: https://zakon.rada.gov.ua/laws/show/1932-12#Text [Accessed: 11 Sep. 2025].

[45] Verkhovna Rada of Ukraine. Law of Ukraine No. 2229-XII "On the Security Service of Ukraine," 1992. [Online]. Available: https://zakon.rada.gov.ua/laws/show/2229-12#Text [Accessed: 11 Sep. 2025].

[46] Verkhovna Rada of Ukraine. Law of Ukraine No. 912-IX "On Intelligence," 2020. [Online]. Available: https://zakon.rada.gov.ua/laws/show/912-20#Text [Accessed: 11 Sep. 2025].

[47] State Service of Special Communication and Information Protection in Ukraine. The CERT-UA Team has processed 2,543 cyber incidents over 2023, 2024. [Online]. Available: https://cip.gov.ua/en/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti [Accessed: 11 Sep. 2025].

[48] Verkhovna Rada of Ukraine. Law of Ukraine No. 1089-IX "On Electronic Communications," 2020. [Online]. Available: https://zakon.rada.gov.ua/laws/show/1089-20#Text [Accessed: 11 Sep. 20255].

[49] Verkhovna Rada of Ukraine. Law of Ukraine No. 1644-VII "On Sanctions," 2014. [Online]. Available: https://zakon.rada.gov.ua/laws/show/1644-18#Text [Accessed: 11 Sep. 2025].

[50] Verkhovna Rada of Ukraine. Law of Ukraine No. 2155-VIII "On Electronic Identification and Electronic Trust Services," 2017. [Online]. Available: https://zakon.rada.gov.ua/laws/show/2155-19#Text [Accessed: 11 Sep. 2025].

[51] International Organization for Standardization. (2023). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. [Online]. Available: https://www.iso.org/ru/standard/73906.html [Accessed: 11 Sep. 2025].

[52] National Institute of Standards and Technology Cybersecurity Framework. (2025). *NIST cybersecurity framework 2.0: Cybersecurity, enterprise risk management, and workforce management quick start guide.* [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1308.ipd.pdf [Accessed: 11 Sep. 2025].

[53] European Union. A Strategic Compass for Security and Defence, 2020. [Online]. Available: https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf [Accessed: 11 Sep. 2025].

[54] Verkhovna Rada of Ukraine. Law of Ukraine No. 1882-IX "On Critical Infrastructure," 2021. [Online]. Available: https://zakon.rada.gov.ua/laws/show/1882-20#Text [Accessed: 11 Sep. 2025].

[55] President of Ukraine. Decree of the President of Ukraine No. 447/2021 "On the Decision of the National Security and Defence Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine," 2021. [Online]. Available: https://zakon.rada.gov.ua/laws/show/447/2021#Text [Accessed: Sep. 11, 2025].

[56] Verkhovna Rada of Ukraine. Resolution of the Cabinet of Ministers of Ukraine No. 518 "On Approval of the Procedure for Ensuring Cyber Protection of Critical Information Infrastructure Facilities," 2019. [Online]. Available: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text [Accessed: 11 Sep. 2025].

[57] State Center for Cyber Defense. Report for the second quarter of 2023, 2023. [Online]. Available: https://scpc.gov.ua/uk/articles/318 [Accessed: 11 Sep. 2025].

[58] O.S. Oliinyk, R.M. Shestopalov, V.O. Zarosylo, M.I. Stankovic, S.G. Golubitsky, "Economic security through criminal policies: A comparative study of Western and European approaches," *Revista Cientifica General Jose Maria Cordova,* vol. 20, no. 38, pp. 265–285, 2022.

[59] D. Bielov, I. Aristova, M. Hromovchuk, "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*, vol. 16, pp. 265–273, 2019.

[60] D. Fried, A. Poliakova, "Democratic Defense against Disinformation," 2018. [Online]. Available: https://www.atlanticcouncil.org/wp-content/uploads/2018/03/Democratic_Defense_Against_Disinformation_FINAL.pdf [Accessed: 11 Sep. 2025].