https://doi.org/10.33271/nvngu/2025-5/132

O. Ilyushyk[1],
orcid.org/0000-0002-4619-5785,
R. Skrynkovskyy[*2],
orcid.org/0000-0002-2180-8055,
A. Dutko[3],
orcid.org/0000-0002-5062-6947,
I. Prots[3],
orcid.org/0000-0002-6483-0121,
M. Kropyvnytskyi[4],
orcid.org/0000-0003-0981-0774

1 – Danylo Halytsky Lviv National Medical University, Lviv, Ukraine
2 – Lviv University of Business and Law, Lviv, Ukraine
3 – Lviv State University of Internal Affairs, Lviv, Ukraine
4 – Private Entrepreneur, Lviv, Ukraine
* Corresponding author e-mail: uan_lviv@ukr.net

LEGAL ASPECTS OF INFORMATION SECURITY IN UKRAINE IN THE CONDITIONS OF EUROPEAN INTEGRATION AND WAR

Purpose. To propose improvements in legal norms in the field of information security (IS). To substantiate the need to improve the legal categories IS. To establish the need to coordinate the course towards European integration in the field of information law in wartime conditions, provide legal substantiation for punishment for participation in information warfare on the side of the aggressor.

Methodology. The method of induction and deduction made it possible to indicate that information warfare (IW) necessitates the need to expand the concept of IS and the interpretation of "cybersecurity" as its subcategory. The hermeneutic method allowed proposing the definition of legal categories in the field of IS. The method of comparative analysis allowed proposing improvements in the norms of information law and providing legal substantiation for punishment for participation in information warfare on the side of the aggressor.

Findings. It is indicated that IW necessitates the need to expand the interpretation of the IS category. Security of information, "cybersecurity" should be defined as a component of IS. It is noted that IS is implemented as a balance in the conditions of constant active counteraction, one of the aspects of which is legal counteraction to information aggression. Not only the absence of a holistic national IS-system is indicated, but also the insufficiency of its systemic support. It is noted that the uncertainty of legal norms causes an increase in the discretionary powers of the judicial branch of government in the field of protecting the human right to information, which increases the responsibility for the democracy level in the country.

Originality. The legal expansion of the definition of information as an object of protection to its definition as an instrument of harm is substantiated. It is indicated that the process of integration of legal norms of the EU and Ukraine necessitates the need for counter changes in EU legislation taking into account Ukraine's experience in countering IW. The definition of legal categories of IS provided.

Practical value. The proposed changes to legal norms and improvement of legal categories will contribute to reducing the level of uncertainty in the field IS.

Keywords: *national security, information security, European integration, protection of the right to information*

Introduction. Information security determines the level of protection of a citizen and the state in terms of national security components: political, social, economic, military, etc. The close relationship between information and national security determines the need for certain restrictions on the right to information in wartime, the introduction of stricter norms in the handling of information, the application of preventive measures to counter information tools of hybrid warfare to stop "controlled information chaos".

This leads to certain discrepancies in the legislation of Ukraine and other states, in particular, the countries of the European Union, which operate in peacetime. This creates the basis for a legal dichotomy between the need for legal protection of national interests in the face of significant external threats and Ukraine's legally approved path to European integration and the development of an open information society.

The poly-interpretability of the concept of "information security" in the European Union law also leads to discrepancies, which has caused a certain instability of this category in the national law.

The significant dynamics of changes necessitates the need for constant improvement of the terminological apparatus in this area. The imperfection and uncertainty of legal terminology complicates the judicial process, imposes on the courts the obligation to interpret vague legal norms and increases their role as a regulator of human rights in the information sphere. This is particularly due to the introduction of restrictions on the human right to information during martial law. This necessitates the need to ensure the functioning of the legal mechanism for balancing citizen rights and public interests in the field of information security, which in turn increases the responsibility of the judicial branch of government in this aspect.

The connection of information security with national security necessitates the complex interdisciplinary nature of its legal support. This, in turn, leads to differences in the interpretation of punishments for offenders in the field of information security.

The dynamism of external influences requires an urgent review of established scientific approaches in the field of information law and, accordingly, the substanti-

ation for the need to introduce changes to the legislation to ensure the proper effectiveness of legal instruments in this area.

Literature review. Scientists point to significant differences even in the interpretation of the main legal categories in the field of information law [1]. In scientific works, in particular, there are statements that information security is a "holistic social system" with the allocation of subsystems for the protection of the individual, the state, and society [2]. In our opinion, such an approach is a simplification of the interpretation of the specified category.

The article by Shemchuk [3] indicates that even threats to information security are interpreted differently in different legislative acts, and the separation of powers regarding the implementation of national security tasks is unclear in the Legislation of Ukraine.

Also, according to experts, a significant level of fragmentation of legal regulation in the field of information security is still a problematic issue [4]. A significant obstacle to determining liability in legal proceedings on information security issues is the high probability of counter forensics [4]. This leads to the vulnerability of evidence in legal proceedings regarding offenses in this area, especially when the aggressor state with wide access to the latest technologies is behind the crime.

Scientists note that a significant number of institutional structures, whose responsibilities in the field of information security protection overlap, the lack of a holistic methodology and criteria for assessing the level of information threat, result in arbitrary interpretation of legal norms and ineffectiveness of the legal measures used to combat crimes [5]. Therefore, in the article by Pilipchuk [6], based on the analysis of legal norms, the need for a "radical change" of Ukrainian legislation in the field of information security is indicated, taking into account the level of challenges of hybrid warfare.

The fact that in war conditions, not only the issues of protecting information resources and networks, but also legal counteraction to information and psychological tools of influence become significant for national security is indicated in the article by Miniailuk [7]. At the same time, scientists mainly consider the use of information tools for "implementation of acts of aggression" [8] as a threat to information security in war conditions. This contradicts the concept of "information war", in which an act of aggression is only part of the general tactical or strategic plan for conducting combat operations. This, in legal terms, leads to disproportionate punishment for participation in the information war against Ukraine.

Studies of information security issues indicate a shift in emphasis from human rights protection during a large-scale war [9] to the implementation of national security tasks in the information sphere and the need to ensure the stability of society. Therefore, some scholars consider the legal category of "information security" mainly from the point of view of restricting the right to information in order to ensure national security tasks, and for this purpose the category of "state information policy" is used [10]. This, in our opinion, is a somewhat narrow understanding of the concept of "information security".

Also, scholars often identify cybersecurity and information security, as evidenced, for example, by the focus of the legal mechanism of information protection exclusively on cyber threats or the identification in the legal field of cyberspace with information space as a sphere of confrontation in hybrid warfare [11].

Scholars note that the state of information security corresponds to the balance of security and democracy [12]. In their opinion, the specified balance should be formed by regulatory legal methods without the formation of a single institutional structure that takes care of the specified sphere [12].

Scientific works consider the application of the norms of the Criminal Code of Ukraine (CCU) or the Code of Ukraine on Administrative Offenses (COA) in case of information security violations [13], which is indirect evidence of the insufficiency of the level of imperativeness of Ukrainian legislation in information law. The article by Kunev [14] even introduces the concept of "information-administrative law", which somewhat limits the application of criminal law norms in case of crimes in the field of information security that are directly related to national security issues.

In the article by Voitsikhovskyi [15] the use of the legal experience of leading states in the field of information security by Ukrainian legislators is investigated, in particular in view of the declared course of European integration. This is certainly important, but contradicting this thesis is the statement [15] about the inconsistency of this experience, for example, due to the lack of development of interstate cooperation and the absence of a single strategic approach in the field of information security, the absence of direct regulation and determination of the level of severity of crimes in European Union law [4].

In the study of the evolution of EU law in the field of information security, the article by Oliinyk and Petroie [16] indicated key standards of the European Union in the specified field: protection of personal data, network security, strategic management of cybersecurity. This thesis indicates the key issues of cybersecurity and not information security. This confirms the need for a clear distinction between these legal categories.

A review of scientific literature sources indicated that hybrid warfare determines not only the need to improve the norms of information law in the field of information security, but even the need to revise the main legal categories in this area. Also, the experience gained by Ukraine in information warfare requires a change in emphasis in the integration of national legislation and EU law.

The purpose of the article is to propose improvements in legal norms in the field of information security.

The tasks are to substantiate the need to improve the legal categories of information security; to establish the need to coordinate the course for European integration in the field of information law under war conditions; to provide a legal justification for punishment for participation in information warfare on the side of the aggressor.

Methods. The study used general scientific and special methods of scientific knowledge. The induction and deduction method allowed indicating that information warfare necessitates the expansion of the concept of "information security" and the interpretation of "cybersecurity" as its subcategory. The hermeneutic method allowed proposing the definition of legal categories in the field of information security. The method of compara-

tive analysis of current legal norms, judicial practice and modern threats to information security made it possible to propose improvements to the norms of information law and provide legal substantiation for punishment for participation in information warfare on the side of the aggressor. The generalization and formalization method allowed establishing that the uncertainty of legal norms in the field of information law leads to an increase in the discretionary powers of the judicial branch of government in the field of protecting the human right to information, which places responsibility for the level of democracy in the country on this branch of government. The abstraction method indicated that even the courts of the first instance, due to the implicit nature of the norms of information law, acquire the level of guarantors of the constitutional human right to information, which goes beyond the limits of "legal guarantees".

Results. In the context of both significant technological changes in information and communication technologies and significant threats, the problem of information security acquires special importance.

The concept of "information security" in the context of significant targeted external threats goes beyond the information and communication relations of legal entities. With the spread of information technologies to all spheres of society, "information security" becomes not only a legal category but also a social phenomenon, which, in particular, requires citizens to distinguish information from disinformation and psychological manipulation, not to take direct part in the mass process of provoked misinformation. The above-mentioned interpretation of the specified sphere of security multiplicatively increases the significance of "information security" as a component of national security for both branches of law and society.

Changes in Ukrainian legislation in the field of "information security", which are due to the experience of information and psychological warfare, also create the prerequisites for objective differences in this area between Ukrainian legislation and the norms of laws of other countries, in particular the European Union countries, which operate in peacetime.

The lack of efficiency in improving EU legislation in the field of information security is evidenced, for example, by the directions of the main EU legal documents: EU Regulation No. 526/2013 on cybersecurity; NIS Directive of 06.07.16; EU Regulation 2016/679 on the information protection of individuals, etc.

This creates certain complications in the implementation of Ukraine's declared goal of bringing its own legislation into line with EU legislation. To a certain extent, Ukraine's legal experience in the field of "information security" also necessitates the need for counterchanges in European Union law, primarily in relation to countering the coordinated use of information tools of hybrid warfare for criminal purposes.

The dynamism of external influences on all areas of Ukraine's security also does not allow one properly not only to fully implement the establishment of the information law sector in the field of information security, as evidenced by, in particular, the introduction of a full-fledged conceptual and categorical apparatus and the formalization of structural and functional relationships of legal categories [17], but even to properly ensure the integrity of information policy, as indicated in paragraph 20 of the "National Security Strategy" approved by the Decree of the President of Ukraine dated September 14, 2020 No. 392/2020 as amended on January 7, 2025.

This indicates not only the absence of a holistic information security system, but also the insufficiency of its systemic support.

The speed of changes in external influences leads to a certain time lag between the detection of information threats, awareness of their consequences and the implementation of legislative norms to prevent or neutralize them. In particular, in some Laws of Ukraine, the concepts of "information security" and "cybersecurity" are still directly or indirectly identified. Therefore, the importance of an integrated, comprehensive legal approach to information security problems in the national security polysystem is increasing, the first step of which is the "National Security Strategy" approved by the Decree of the President of Ukraine dated September 14, 2020 No. 392/2020.

This is inherent not only to the legislation of Ukraine but also to the legislation of other countries that have not gained experience in confronting information and psychological tools of hybrid warfare [18]. Thus, the US laws "On Information Security Management" of 2002 and "On Information Protection" of 1998, Directive 95/46 of the European Parliament and the Council of the EU indirectly define the category of "information security" as "cybersecurity", which narrows the possibilities of neutralizing significant information threats.

The above-mentioned discrepancy is exacerbated by the fact that the phrase "information security" in English can mean both "information security" and "security of information", which is not identical, since the second interpretation semantically corresponds to the category of "cybersecurity". This is evidenced, in particular, by the context of the document of the Commission of the European Communities dated 06.06.2001 "Network and Information Security".

This leads to legal uncertainty of the norms of the legislation of English-speaking countries and complicates the process of bringing them into line with the specified norms of the legislation of Ukraine.

This also gives grounds to indicate that "information security" has moved from defining information as an object of protection to what is indicated in a number of laws of Ukraine, in particular in Clause 1 of Article 9 of the Law of Ukraine No. 2657-XII "On Information", to protecting individuals, communities, and the state from information as a tool for causing harm. This was caused by the aggressor's use of a wide range of tools in the information war to manipulate public consciousness and even distort the understanding of the national identity of Ukrainians.

This leads to the emergence of another dimension of information security – as a condition for ensuring social security in all its aspects – psychological, emotional, value orientations of communities, etc., which requires institutional structures to form the information stability of society. Hybrid war, an integral part of which is informational and psychological warfare, which is waged continuously and each act of informational aggression is part of a complex operational plan, determines another

feature of information security at this time. This feature is that informational security is implemented as a balance in the conditions of constant active counteraction, one of the aspects of which is legal counteraction.

This necessitates the need, for the assessment of informational security as a scientific category, to legally expand the consideration of informational relationships in the triad individual-society-state, defined by legislation, by including the element of the "aggressor state", in particular for the legal justification of punishment for participation in informational warfare on the side of the aggressor.

The above does not contradict Clause 3, Article 3, Law of Ukraine No. 2469-VIII as amended on 09.08.24 "On National Security of Ukraine" regarding the fact that information security is a component of national security, but only expands its interpretation given that state security and public security are interconnected.

Under this approach, information security, "cybersecurity", should be defined as an integral component of information security, but only as a component of it. The set of elements of the complex concept of information security are in complex multi-level technological and social relations, which should be reflected in legal categories [19]. Crimes in the field of information security can have much more serious consequences than offenses in the field of cybersecurity. Therefore, determining responsibility for these crimes may require, contrary to the claims of some scholars [20], the application of not only the norms of administrative law, but also criminal and international law in the case of the intentional use of information tools for criminal purposes, which led to particularly serious consequences or has the characteristics of a crime against humanity.

Accordingly, this requires a review of information security policy and the introduction of more stringent imperative state activity, the use of not only soft law norms and norms aimed at self-regulation of legal relations, but also norms-principles.

The above does not exclude the use of cybersecurity tools to protect information security. An example is the use of artificial intelligence to detect information threats of hybrid warfare. This, accordingly, necessitates the need for a normative and procedural definition of an artificial intelligence tool, in particular, for use as evidence in court proceedings. This is part of a larger problem – the legal definition of digital evidence created by information systems in an autonomous mode.

An obstacle in this process may be the probable compromise of evidence for the use of digital technologies by one of the parties to the court proceedings. This is also related to the normative definition of liability for an error of an automated system or analytical materials provided by it, the conclusions based on which allow for incorrect interpretation, that is, are actually manipulative. Resolving these issues will allow Ukraine to join the AI Act of the European Union [21].

The lack of a strategic communications system, as indicated in the "Information Security Strategy" approved by the Decree of the President of Ukraine dated 28.12.21 No. 685/2021, also does not contribute to the proper counteraction to information threats.

In these conditions, the norms of the Laws of Ukraine, aimed at creating the prerequisites for information security of individuals and legal entities, human communities and the state, need to be improved. But these dynamic changes require a revision of the traditional presentation of information security as a stable state or level and its interpretation through other norms not specified in the Legislation of Ukraine, for example, "security" [22]. It also requires the legal separation of the "information protection" subsystem in the information security system, paying attention to the issues of information influence, disinformation, etc.

The sphere of information security is distinguished from other legal spheres by the deep integration of legal norms and categories with the ultramodern direction of scientific and technological progress. The sphere of information security is also distinguished from other legal spheres by the possibility of directing digital technologies to such goals as forecasting, identifying and monitoring the directions of action of information threats, developing measures to neutralize them, etc.

This requires strengthening the legal responsibility of institutional structures defined in the legislation for the level of achievement of the specified goals or improper fulfillment of management tasks in the information sphere in all its aspects – from the information and communication direction to the implementation of human rights even in conditions of hybrid war. The importance of the above is evidenced by the introduction of the legal category "information measures of state defense" by the Decree of the President of Ukraine No. 685/2021 of 28.12.21 and the specification of these measures.

When applying a comparative approach, there is a certain dichotomy in the regulation of certain categories of information security in Ukraine and the countries of the European Union, the integration of which is determined by the Law of Ukraine 1629-IV of 18.03.2004 as amended on 04.11.2018.

This primarily concerns the sphere of human rights, in particular the right to information [22]. This right under the norms of the European Union is not subject to restriction and at the same time there are certain legal restrictions on the person regarding the methods and tools of the information activity of the specified person.

In Ukrainian legislation, the specified right may be restricted in cases stipulated by law, in particular, Clause 5 of Article 2 of the Law of Ukraine No. 2657-XII as amended on 14.06.2025 "On Information", and in order to achieve the goal established in the specified clause of the Law of Ukraine.

The conflict of differences between national legislation and EU law is detailed in cases No. 40238/02 "Bucur and Toma v. Romania", No. 10465/83 "Olsson v. Sweden" and No. 48135/06 "Youth Initiative for Human Rights v. Serbia" considered by the European Court of Human Rights (ECHR). Thus, in the decision in case No. 40238/02 "Bucur and Toma v. Romania", the ECHR upheld the claim on the grounds of insufficient precision and predictability of the Romanian legislation in the specified area, non-compliance with the declared goal of protecting the right to information by the government and taking into account the public importance of the information disclosed by the Plaintiff. According to Clause 29, Part 3, Article 30 of the Law of Ukraine No. 2657-XII "On Information", it is determined which information may be a subject of public interest.

The ECHR Decision in Case No. 10465/83 "Olsson v. Sweden" explicitly states that a norm cannot be interpreted as legal if it does not meet the requirements of sufficient and necessary precision, which is a complication for the national judicial system due to the uncertainty of concepts in the Legislation of Ukraine.

The ECHR Decision in Case No. 48135/06 "Youth Initiative for Human Rights v. Serbia" states that in the event of inconsistency of national legislation in the field of the right to information, the law by which this right is determined takes precedence over other legislative acts in the specified area. This decision also states the requirement for urgent changes to national legislation in accordance with international standards in this area.

These ECHR decisions should become a precedent for all countries that have recognized the validity of the ECHR, in particular Ukraine.

This leads to the fact that the level of satisfaction of the right to information becomes an indicator of the state as a legal institution and an indicator of the level of democracy of the country, which is extremely important for Ukraine even in times of war.

This is due, in particular, to the requirement of the "European Convention for the Protection of Human Rights and Fundamental Freedoms" (abbreviation, English, ECHR) ratified by the Law of Ukraine No. 475/97-VR, in that restrictions on any human rights under national legislation will have legal grounds only in a state that is recognized as democratic in the world. This is confirmed in the Decision of the ECHR in case No. 34725/08 "Savin v. Ukraine" which states the illegality of a violation of a human right if it is not "necessary in a democratic society".

This is also confirmed in the Separate Opinion of the Judge of the Constitutional Court of Ukraine (CCU) V. V. Lemak regarding the Opinion of the CCU No. 5-v/2019 [23], according to which the restriction of the right to information even in view of national security needs, is implicit in the lack of identity between human rights and the legal categories listed in Section II of the Constitution of Ukraine. The indicated implicitness is also characteristic of a certain part of the legal norms regarding information security.

Failure to comply with the requirement of clarity of legislative norms in accordance with the provisions of Article 8 of the ECHR leads to the possibility for representatives of institutional structures to interpret their duties in the implementation of citizens' rights to information as discretionary powers. By definition, discretionary powers can substantiate the choice of "to act – not to act", or to choose at their discretion options for actions that do not directly contradict the law (Resolution of the Cassation Administrative Court of the Supreme Court in case No. 1840/2970/18). Given the implicit nature of the judiciary in assessing such actions by representatives of institutional structures, this may lead to legal conflicts.

Since the conditions of war led to the need to restrict the right to information regarding the dissemination of confidential information about a person and the right to freely disseminate information at one's own discretion, this also complicated the practice of judicial proceedings due to the need to interpret Clause 1 of Article 29 of the Law of Ukraine "On Information", which states the need to reconcile the potential harm of the dissemination of confidential information and the benefits to society from its disclosure.

The above is complicated by the lack of legal methodology for determining the level of materiality of harm and the level of public benefit, the vagueness of the so-called "right to cause harm", the lack of recognition of the limits of proportionality of restrictions on the right to information under *stricto iuris* norms.

The above requires attention in judicial practice, since it is the requirement of proportionality of interference with human rights that the European Court of Human Rights prioritizes, which was confirmed in the Decision of the ECHR in cases No. 30562/04 and No. 30566/04 "S. and Marper v. the United Kingdom". Therefore, the above places the responsibility on judges for: the implementation of the right granted to citizens by the Constitution, the level of citizens' trust in the justice of the domestic judicial system and, even, the level of democracy in the country.

It is also important that the Courts acquire the level of guarantors of constitutional human rights, in particular the right of citizens to information, which goes beyond the so-called "legal guarantees". This increases the importance of the judicial branch of power, but also increases its responsibility in this area.

This becomes more complicated in times of war, when institutions responsible for national security can, without additional substantiation, close access to information by giving it a conference, official, or even secret status.

At the same time, a negative attitude towards restricting the right to information, even in times of war, and the related right to freedom of speech is evidenced by Ukraine in the section "National Challenges and Threats" of the "National Security Strategy" as amended on 07.01.25. The date of this document confirms the relevance of the issue. Also, the citizen's right to information is regulated as the "fourth strategic goal of the "Information Security Strategy" approved by Decree of the President of Ukraine No. 685/2021.

This is confirmed by the decision of the Lviv District Administrative Court in case No. 380/2525/20 regarding the provision of information by a military unit even in wartime at the request of an individual, if this request meets the requirements of the three-component test, in particular in terms of the priority of the public interest over the harm from the disclosure of information. It should be noted that the "three-component test" is mandatory when the question of satisfying a citizen's right to information that is classified as "for official use", arises. The above decision of the Lviv District Administrative Court is also indicative of the imposition of liability for the inaction of representatives of official structures in satisfying the right to information.

The above indicates not only the instability of the institutional (functional) legal approach to ensuring national security and its component – information security, but also its significant differences with the comprehensive legal approach [24].

The functional approach is indirectly regulated by determining specific areas of threat action, in particular, cyber threats, for example, in Clause 21 of Article 1, Section I and Clause 5 of Article 3, Section II of the Law

of Ukraine No. 2469-VIII", which, due to their long-term presence, have even displaced information threats from consideration.

A comprehensive legal approach to security issues is approved in: Article 17 of the Constitution of Ukraine, which specifies the areas of security and, in particular, specifies the area of information security; Part 5, 8, Article 1, Section I of the Law of Ukraine No. 2469-VIII, which states the need for a comprehensive approach; Part 4, Article 3, Section II; Part 3, Article 19, Section IV of the Law of Ukraine No. 2469-VIII emphasizes the importance of information security, which also indirectly approves a comprehensive legal approach.

In Part 10, Article 1, Section I of the Law of Ukraine No. 2469-VIII, the objects of protection are indicated – a person, society and the state. However, in the specified Law in particular and in the Legislation of Ukraine in general, the categories "information security of a citizen", "information security of the state" and "information security of society" are not distinguished.

Also, the Ukrainian legislation does not include the category of "international information security", which has become extremely relevant due to the use of information tools in hybrid warfare aimed at undermining international information security.

Since the responsibility of the Ukrainian state should extend to the security of cross-border information flows and the threat to national security may be posed by these flows, it is proposed to include them in the objects of protection in Clause 10 of Article 1, Section I of the Law of Ukraine No. 2469-VIII, and the interpretation of the legal categories of "international information security", other objects of protection should be provided in Clause 1 of Article 1, Section I of the Law of Ukraine No. 2657-XII "On Information". Also, given the information component of hybrid warfare, it is proposed to begin work in international structures on recognizing the falsification of digital evidence of war crimes as complicity in them.

Problems in the judicial process are caused by the uncertainty of categories regarding information security even in criminal and administrative law, which contradicts the principles of negotia *stricti iuris*, in particular, Articles. 109, 110, 111, 114 of the Criminal Code of Ukraine, although they indicate the punishment for committing a violation of information security, but the specified articles do not directly contain the category of "information". The category of "information security" in the specified articles is also absent.

The complication of the application of the norms of criminal and administrative law in this area is caused by the uncertainty, for example, in Article 111-2 of the Criminal Code of Ukraine, of the significance, along with material ones, of information resources, which sometimes represent much greater value and their loss can pose a danger to individuals and legal entities and even to the state.

At the same time, it is necessary to note a certain continuity of terminological unregulation of the Legislation of Ukraine when cybersecurity is considered separately from information security as an equivalent component of national security (Part 3, Article 19, Section IV of the Law of Ukraine No. 2469-VIII), and not, which is more legitimate – as a component of information security. Therefore, the specified norms of the Laws of Ukraine must be coordinated with article 17 of the Constitution of Ukraine, where among the most important functions of the state is indicated "ensuring... economic and information security" but there is no category of "cybersecurity".

Also, according to Article 22 of the Law of Ukraine No. 2469-VIII, according to which information security is entrusted to the special communications service, the protection of information security is directed only to the cyber protection of critical information infrastructure, which creates a legal contradiction with Clause 3, Article 19, Section IV of the Law of Ukraine No. 2469-VIII; regulated institutional information resources; protection of information with limited access (Article 21 of the Law of Ukraine No. 2657-XII), use of radio frequencies and telecommunications resources.

A significant problem in the practice of legal proceedings is the discrepancy between the norms of laws aimed at ensuring the right of citizens to receive and, even, disseminate information, including information with limited access and national security needs. In particular, Article 302 of the Civil Code of Ukraine (CCU) regulates the right of a citizen to collect, store and publish information while verifying its authenticity. But the rules for such verification and determining the level of authenticity are not provided by the said law. Also, the use of Clause 3 of Article 30 of the Law of Ukraine No. 2657-XII exempts from liability for the disclosure of information even with limited access, if the need for this information for society is established in the judicial process. This reduces the possibilities of fulfilling one of the main functions of law – preventing crimes when the offender is aware of the inevitability of punishment. But information law does not provide for proper mandatory liability, sometimes even for the use of other areas of law, even for actions in the field of information security that have led to significant negative consequences. Thus, under the rules of administrative law in accordance with Article 212-3 of the Code of Administrative Offenses "Violation of the Right to Information and the Right to Appeal" and Article 212-6 of the Code of Administrative Offenses, which regulates violations of cybersecurity norms, only a fine is imposed, which does not always correspond to the consequences of the offense, especially in conditions of progressive inflation and non-increase in the non-taxable minimum income of citizens.

Even the judicial practice of qualifying most crimes in the information sphere under civil law norms with the imposition of obligations to compensate for the damage caused is limited. This is particularly facilitated by the uncertainty of legal norms in this area.

Thus, under Clause 3, Clause 2, Article 11 of the Code of Civil Procedure, there are only two grounds for the emergence of civil law obligations to compensate for damage: property (material) losses and moral damage, which are combined in the specified article of the Code of Civil Procedure, but the consequences of information damage can be loss of health and even life.

Thus, liability for violations of information security in most cases can be qualified as tort liability, although in judicial practice there are no accusations of violations of information security norms caused by the inaction of a person.

Therefore, even the category of tort liability in the field of information law requires regulation. This also reinforces the need to introduce a distinction between crimes and torts in the field of information security without the possibility of double interpretation of these categories. In particular, it is proposed to regulate the category of "signs of information tort". The publication of one's own photo or video from a military plant or training ground with geolocation data, which provoked the aggressor to launch a missile and bomb strike could be an example of the significance of such an offense. Obviously, this is a violation of information security, which led to serious consequences. But the legal qualification of such an offense is problematic due to the uncertainty of the legislation.

The legal aspects of information security in the entire scope of its impacts have long been considered using the mechanism of indirect legal definition. Only the use of information tools and methods in hybrid warfare to such an extent that they can be defined as the category of "information warfare" has led to an understanding of the need for legal countermeasures, but a significant number of legislative norms on information security lead, first of all, to achieving tactical goals without taking into account the strategic consequences of the aforementioned legal norms.

Also, the categories of "disinformation" and "information manipulation" have not yet been legally formalized. Although the legislation provides for the legal consequences of the dissemination of false and unreliable information, there are no legal means of distinguishing purposeful, organizationally and resourcefully provided disinformation and misinformation, i.e. they do not contribute to the distinction in practice of legal proceedings between the conscious use of false, deliberately corrected or irrelevant information with the aim of causing harm from the unconscious dissemination of such information. Therefore, the following definitions are proposed:

1. Disinformation – the purposeful dissemination of inaccurate or incomplete information, with the aim of causing harm to a person, society or the state.

2. Misinformation – the dissemination of inaccurate or incomplete information, without the aim of misleading a person, society or the state.

The absence of the aim of misleading does not mean the absence of consequences of misinformation, which in the legal sphere can be interpreted as unintentional harm (Article 192 of the Criminal Code of Ukraine "in the absence of signs of fraud").

Disinformation can involve and use misinformation to reach a larger number of people and achieve a multiplier effect of spreading false and/or manipulative information, which accordingly increases the need to implement these categories in judicial practice.

Also, the category of "information-psychological special operation" (IPSO) has not even been legally formalized. Although the term "information-psychological special operation" is used in a number of legal documents, in particular in the "Information Security Strategy" by Decree of the President of Ukraine No. 685/2021 of 15.10.21, its legal interpretation is not provided in these documents. This narrows the possibilities of detecting signs of IPSO in judicial practice and punishing participation in it.

IPSO is a subcategory of psychological operations that can be carried out both to demoralize the enemy's troops and rear within the framework of military operations, dehumanize the enemy's image, and to motivate one's own troops and one's own social communities. This is important to distinguish when implementing the legal category of IPSO.

The following definition is proposed – "information and psychological special operation is a planned set of measures for the use of disinformation and psychological manipulation tools aimed at the target community of citizens to change their behavior for an unlawful purpose".

Since IPSO is a tool of hybrid warfare, it requires the definition of punishment for involvement in it in the Criminal Code of Ukraine. According to Clause 6 of Article 111-prim of the Criminal Code of Ukraine, punishment is provided for information activities in cooperation with the aggressor state, but the purpose of such activities specified in this clause does not include causing information and psychological harm to a citizen or the state. In addition, the activity specified in Clause 6 of Article 111-prim of the Criminal Code of Ukraine must not have signs of treason. And conscious participation in the implementation of an information and psychological special operation against Ukrainian citizens or the state of Ukraine for the purpose of causing harm in the presence of signs of treason must be specified in the Criminal Code of Ukraine.

For this purpose, it is proposed to supplement the Criminal Code of Ukraine with Article 114-3. "Known participation in an information and psychological operation directed against Ukrainian citizens or the state of Ukraine, which had serious consequences for the life and health of people or (or) other serious consequences, is punishable by imprisonment for a term of...." The term under this article should be determined by an expert group of lawyers. In this case, the proposed legal distinction between disinformation and misinformation provides an opportunity to distinguish their legal consequences.

This also indicates the need for a legal definition of the categories of "information and psychological security" of an individual and a community of such individuals, "destructive information and psychological influence", "information space", "information conflicts".

In the field of information law, there is also no regulatory establishment of the categories of "information tort", "obligations of the state regarding information security", etc.

It is also proposed to separate the "State Information Security Service" leaving the responsibility for protecting special communication channels and technical aspects of information protection under the "State Service for Special Communications and Information Protection of Ukraine". This is in line with the regulatory practice of the European Union, since the "European Agency for Network and Information Security" was established by the Decision of the European Parliament and the Council of the EU No. 460/2004 of 4.03.04.

There are still restrictions in court proceedings related to the failure to define information on digital media or in digital networks as a category of evidence. This category is absent even in Clause 1 of Article 27 of the Criminal Procedure Code of Ukraine regarding the

right "to receive both oral and written information in court" and therefore this clause should be amended with the addition of the category "digital".

The results of the study also suggest the following changes to legal norms:

1. In Part 3 and Clause 2 of Article 11 of the Code of Criminal Procedure: "causing property (material), moral damage and (or) harm to the health of another person or community of persons".

2. In Part 21 of Article 1, Section I of the Law of Ukraine No. 2469-VIII "Strategy of Information Security of Ukraine and its Components, Including Cybersecurity..." with the subsequent replacement in this paragraph of the definitions "cybersecurity" and "cyberspace" with the definitions "information security" and information space".

3. In Part 5 of Article 3, Section II of the Law of Ukraine No. 2469-VIII, add "Information Security Strategies".

4. Given the reduced opportunities for citizens to protect information compared to state structures, Clause 10 of Article 1, Section 1 of the Law of Ukraine No. 2657-XII "ensuring equal opportunities for ... protection, protection of information necessary for the exercise of one's rights, freedoms and legitimate interests, and imposing obligations for the protection, protection of information with limited access on state structures determined by the Legislation of Ukraine". This improvement also allows one to eliminate contradictions, in particular with Clause 2, Article 21, Section II of the Law of Ukraine No. 2657-XII.

5. In Article 111-2. CCU regarding aiding the aggressor state in "transfer of material, non-material or information resources".

6. In Article 182. CCU "Collection, storage, use, destruction, dissemination or modification of confidential information with the aim of violating the right of an individual to privacy...".

7. In Article 330 of the Criminal Code of Ukraine "Transmission, dissemination or collection of information constituting official information. In the field of defense and national security of the country" and to supplement Paragraph 1 of this article as follows: "Transmission, dissemination or collection of information for the purpose of disclosure or transmission...".

These changes will allow avoiding some discrepancies in the interpretation of legal norms.

Conclusions. It is indicated that with the spread of information technologies to all spheres of society, "information security" becomes not only a legal category but also a social phenomenon, which, for example, requires citizens to distinguish information from disinformation and psychological manipulation on a daily basis, not to take direct part in the mass process of misinformation.

It is indicated that information warfare, in which the aggressor uses a wide range of tools to manipulate public consciousness, and even to distort the understanding of the national identity of Ukrainians, leads to the need for a significant expansion of the concept of "information security". Today, this concept in the legal sphere has moved from defining information as an object of protection to protecting individuals, communities, and the state from information as an instrument of harm. This leads to the emergence of another dimension of information security – as a condition for ensuring social security in all its aspects – psychological, emotional, value orientations of communities, etc., which requires institutional structures to form the information stability of society. This necessitates the legal expansion of the consideration of informational relationships in the triad individual-society-state by including the element of the "aggressor state" in order to assess information security as a scientific category, in particular to legally substantiate the punishment for participating in information warfare on the side of the aggressor.

The existence of complications in the process of adapting national legislation to EU legal norms in the field of information law, confirmed by Ukraine, is noted. It is indicated that the main focus of EU lawmaking in this area is focused on cybersecurity issues, while Ukraine is gaining experience in information warfare, which is a component of hybrid aggression. It is indicated that this Ukrainian experience necessitates the need for corresponding changes in European Union law.

It is noted that the dynamism of external influences on all areas of Ukraine's security also does not allow for the proper implementation of the establishment of the field of information law in the field of information security, evidence of which would be, in particular, the introduction of a full-fledged conceptual and categorical apparatus, the formalization of structural and functional relationships of legal categories, and even ensuring the integrity of information policy. This indicates not only the absence of a holistic information security system, but also the insufficiency of its systemic support.

It is noted that the information security sector is distinguished from other legal areas by the deep integration of legal norms and categories with the ultramodern direction of scientific and technological progress and the ability to forecast, identify and monitor areas of danger using digital tools. This provides advantages for the introduction of institutional and legal measures to neutralize dangers.

The level of threats also requires increased legal responsibility of representatives of institutional structures defined in the legislation for the level of achievement of the specified goals or failure to fulfill the tasks of proper management in the information sphere in all its aspects – from the information and communication direction to the implementation of human rights even in conditions of hybrid war. The importance of the above is evidenced by the introduction by the Decree of the President of Ukraine of the legal category "information measures of state defense" and the specification of these measures.

It is indicated that problems in judicial proceedings are caused by the uncertainty of categories regarding information security even in criminal and administrative law, which contradicts the principles of *negotia stricti iuris*. In particular, the complication of the application of criminal and administrative law norms in this area causes uncertainty, the importance of information resources, along with material ones, which sometimes represent much greater value, and their loss can pose a danger to individuals and legal entities and even to the state.

It is noted that the restriction of the right to information, even in view of the needs of national security, is implicit in the lack of identity between human rights and the legal categories listed in Section II of the Constitu-

tion of Ukraine. This implicitness is also characteristic of a certain part of the legal norms regarding information security. Failure to comply with the requirement of clarity of legislative norms in accordance with the provisions of Article 8 of the ECHR leads to the possibility of treating representatives of institutional structures as discretionary powers by representatives of institutional structures. Given the implicitness of the judiciary in assessing such actions of representatives of institutional structures, this may lead to legal conflicts.

The uncertainty of legal norms determines the increase in discretionary powers of the judicial branch of power in the field of protecting the human right to information, which places responsibility for the level of democracy in the country on this branch of power.

It is also important that the Courts acquire the level of guarantors of human rights, in particular the right of citizens to information, which goes beyond the so-called "legal guarantees". This increases the importance of the judicial branch of power, but also increases its responsibility in this area.

Based on the results of the study, definitions of legal categories and improvements to legal norms are proposed.

Further research is expected to include an in-depth study of the legal aspects of Ukraine's information security in the context of European integration and war.

References.

1. Bondarenko, R., & Mykhalchuk, V. (2021). Information security of the state. *Investments: practice and experience*, *5*, 95-101. https://doi.org/10.32702/2306 6814.2021.5.95

2. Horulko, V. V. (2022). The role and place of information security in the overall system of the state's national security. *The Journal of V. N. Karazin Kharkiv National University, Series "Law"*, *34*, 104-109. https://doi.org/10.26565/2075-1834-2022-34-12

3. Shemchuk, V. (2020). Information security threats: problems of determination and troubleshooting. *Expert: paradigms of legal sciences and public administration*, *1*(7), 285-296. https://doi.org/10.32689/2617-9660-2020-1(7)-285-296

4. Nitsenko, V., Mardani, A., Streimikis, J., Ishchenko, M., Chaikovsky, M., Stoyanova-Koval, S., & Arutiunian, R. (2019). Automatic Information System of Risk Assessment for Agricultural Enterprises of Ukraine. *Montenegrin Journal of Economics*, *15*(2), 139-152. https://doi.org/10.14254/1800-5845/2019.15-2.11

5. Onopriienko, S. (2022). Classification of the types of the information security as a legal category. *Newsletter of Taras Shevchenko National University of Kyiv*, *1*(49), 60-62. https://doi.org/10.17721/1728-2217.2022.49.60-62

6. Pilipchuk, V. (2025). Theoretical and legal problems of the development of legislation in the sphere of national and information security of Ukraine. *Information and law*, *2*(53), 9-22. https://doi.org/10.37750/2616-6798.2025.2(53).334015

7. Miniailuk, V. (2024). On the problem of ensuring information security under the conditions of the legal regime of martial law. *Law & Border*, *4*(2), 108-129. https://doi.org/10.32453/law_border/t1b33x66

8. Kaplia, O. M. (2023). Legal regulation of citizen's information security during martial law. *Expert: paradigms of legal sciences and public administration, 6*(24), 16-20. https://doi.org/10.32689/2617-9660-2022-6(24)-16-20

9. Moroz, V. (2021). Features of information security in martial law. *Scientific Works of Kyiv Aviation Institute. Series Law Journal "Air and Space Law"*, *2*(59), 94-101. https://doi.org/10.18372/2307-9061.59.15600

10. Shynkar, T. (2023). Application of the "Necessity" Category in Justifying Restrictions on the Right to Information in the Interests of National Security: General Principles and Practice of the European Court of Human Rights. *Academic Visions. Section "Law"*, *18*. https://doi.org/10.5281/zenodo.8343591

11. Halipchak, V. (2023). State-legal mechanism of information security in Ukraine in the context of Russian aggression. *Scientific journal "Politikus", 5*, 19-24. https://doi.org/10.24195/2414-9616.2023-5.3

12. Koterlin, I. B. (2022). Information security in martial law in terms of ensuring information rights and freedoms. *Actual problems of domestic jurisprudence*, *1*, 150-155. https://doi.org/10.32782/392257

13. Kudinov, S. S., & Shynkar, T. I. (2021). Criminal law mechanisms of limiting information activities characterized by collaboration sign. *South Ukrainian Law Journal*, *2*(3), 23-29. https://doi.org/10.32850/sulj.2021.3.2.4

14. Kunev, Yu. (2021). Legal provision of information security as a subject of legal investigation. *Scientific Works of Kyiv Aviation Institute. Series Law Journal "Air and Space Law"*, *1*(58), 95-102. https://doi.org/10.18372/2307-9061.58.1531

15. Voitsikhovskyi, A. (2020). Information security as component national security systems (international and foreign experience). *The Journal of V. N. Karazin Kharkiv National University. Series Law*, *29*, 281-288. https://doi.org/10.26565/2075-1834-2020-29-38

16. Oliinyk, N., & Petroie, I. (2025). Volution of European legal standards and mechanisms for information security governance in public authorities amidst digital tranformations. *Bulletin of Postgraduate education: Ser. "Social and Behavioral Sciences; Management and Administration". Updated*, *32*(61), 328-346. https://doi.org/10.58442/3041-1858-2025-32(61)-328-346

17. Skrynkovskyy, R., Petkov, S., Koretskyi, O., Hudyma, V., Koziar, R., Chorniy, B., ..., & Chubenko, A. (2024). Interaction between the Armed Forces of Ukraine, other components of the defense forces and representatives of the mass media under martial law. *International scientific journal "Internauka". Series: "Legal Sciences"*, *3*(73), 130-143. https://doi.org/10.25313/2520-2308-2024-3-9682

18. Yarema, O. G., & Ilyushyk, O. M. (2022). System of legal remedies for ensuring information security. *Analytical and Comparative Law*, *1*, 237-241. https://doi.org/10.24144/2788-6018.2022.04.43

19. Prots, I. (2023). Legal regulation of information security in public administration. *Information and analytical support for the activities of the security and defense sector bodies of Ukraine: materials of the Scientific and Practical Conference*. (Lviv, December 22, 2023. Lviv: Lviv State University of Internal Affairs). Retrieved from https://dspace.lvduvs.edu.ua/bitstream/1234567890/6900/1/22_12_2023.pdf#page=138

20. Perun, T. S. (2018). Ways to improve cooperation between Ukraine and the EU in the field of information security. *Scientific Papers of the Legislation Institute of the Verkhovna Rada of Ukraine, 1*(5), 26-31. Retrieved from https://www.researchgate.net/publication/329604665_Slahi_pokrasenna_vzaemodii_miz_Ukrainou_ta_ES_u_sferi_zabezpecenna_informacijnoi_bezpeki

21. European Parliament (2024). *Artificial intelligence act*. Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

22. Kelman, M. S., Tokarska, A. S., Yarmol, L. V., Tsebenko, S. B., & Dutko, A. O. (2020). *Modern mechanisms for the protection of human rights: a collective monograph*. Lviv: Galician Publishing Union. Retrieved from https://lpnu.ua/sites/default/files/2023/6/19/paragraphs/50930/monografiyakelmantokarskayarmolcebenko.pdf

23. Constitutional Court of Ukraine (2019). *Separate opinion of the judge of the Constitutional Court of Ukraine Lemak Vasyl Vasyliovych regarding the Opinion of the Constitutional Court of Ukraine dated November 13, 2019 No. 5-в/2019 dated 11/13/2019*. Retrieved from https://zakon.rada.gov.ua/laws/show/nd05d710-19#Text

24. Horielova, V. Y., & Vikhryst, S. M. (2024). Legal support and prospects for the development of state policy in the field of information security. *Legal Bulletin*, *13*, 79-85. https://doi.org/10.31732/2708-339X-2024-13-A11

Правові аспекти інформаційної безпеки України в умовах Євроінтеграції та війни

О. М. Ілюшик[1], *Р. М. Скриньковський*[*2], *А. О. Дутко*[3], *І. М. Проць*[3], *М. О. Кропивницький*[4]

1 – Львівський національний медичний університет імені Данила Галицького, м. Львів, Україна

2 – Львівський університет бізнесу та права, м. Львів, Україна

3 – Львівський державний університет внутрішніх справ, м. Львів, Україна

4 – Приватний підприємець, м. Львів, Україна

* Автор-кореспондент e-mail: uan_lviv@ukr.net

Мета. Запропонувати вдосконалення правових норм у сфері інформаційної безпеки. Обґрунтувати необхідність удосконалення правових категорій інформаційної безпеки. Встановити необхідність узгодження курсу на Євроінтеграцію у сфері інформаційного права за умов війни, надати правове обґрунтування покарання за участь у інформаційній війні на боці агресора.

Методика. Метод індукції й дедукції дозволив показати, що інформаційна війна зумовлює потребу розширення поняття «інформаційна безпека» та трактування «кібербезпеки» як її субкатегорії. Герменевтичний метод дозволив запропонувати визначення правових категорій у царині інформаційної безпеки. Метод компаративного аналізу надав можливість запропонувати вдосконалення норм інформаційного права й надати правове обґрунтування покарання за участь у інформаційній війні на боці агресора.

Результати. Показано що інформаційна війна обумовлює потребу розширення трактування категорії «інформаційна безпека». Безпека інформації, «кібербезпека», має визначатися як складова інформаційної безпеки. Зазначено, що інформаційна безпека реалізується як баланс в умовах ведення постійних активних контрдій, одним із аспектів яких є правова протидія інформаційній агресії. Указано не лише на відсутність цілісної національної системи інформаційної безпеки, але й на недостатність її системного забезпечення. Зазначено, що невизначеність правових норм обумовлює зростання дискреційних повноважень судової гілки влади у сфері захисту права людини на інформацію, що збільшує її відповідальність за рівень демократії у країні.

Наукова новизна. Обґрунтоване правове розширення означення інформації як об'єкту захисту до її визначення також як інструменту нанесення шкоди. Показано, що процес інтеграції правових норм ЄС і України обумовлює необхідність зустрічних змін у законодавстві ЄС за урахування досвіду України у протидії інформаційній війні. Надане визначення правових категорій інформаційної безпеки.

Практична значимість. Запропоновані зміни правових норм і вдосконалення правових категорій сприятимуть зменшенню рівня невизначеності у сфері інформаційної безпеки.

Ключові слова: *національна безпека, інформаційна безпека, Євроінтеграція, захист права на інформацію*

The manuscript was submitted 05.04.25.