UDC 35.01; 23.04.44
DOI: https://doi.org/10.32689/2617-2224-2019-4(19)-222-234

Prav Roman Yuriyovych,
postgraduate student, Interregional Academy of Personnel Management, 04071, Kiev, Str. Pochayinskaya, 25/49, 14, tel.: 067-471-15-55, e-mail: romaprav@gmail.com
ORCID: 0000-0001-8064-2836

Прав Роман Юрійович,
аспірант, Міжрегіональна Академія управління персоналом, 04071, м. Київ, вул. Почайнинська, 25/49, кв. 14, тел.: 067-471-15-55, e-mail: romaprav@gmail.com
ORCID: 0000-0001-8064-2836

Прав Роман Юрьевич,
аспирант, Межрегиональная Академия управления персоналом, 04071, г. Киев, ул. Почайнинская, 25/49, кв. 14, тел.: 067-471-15-55, e-mail: romaprav@gmail.com
ORCID: 0000-0001-8064-2836

REGULATORY AND LEGAL BASES FOR FORMATION AND IMPLEMENTATION OF THE STATE SECURITY POLICY IN THE INFORMATIONAL SPHERE

Abstract. The article emphasizes that the issue of information security of Ukraine is complicated by the lack of an appropriate strategy.

Important strategic documents in the field of information policy and state security also include: "Strategy for the development of the information society in Ukraine" (2013), which defines the priorities of activities in the field of information security; "Cyber security Strategy of Ukraine" (2016). The purpose of this strategy is to create conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and the state. The threats of cybersecurity, the national system of cybersecurity, the main subjects of cybersecurity, priorities and directions of ensuring cyber security of Ukraine and the like are defined. Legislative and regulatory acts on state security in the information sphere can be divided into four blocks according to the level of generalization and concretization. The 1st block consists of conceptual, doctrinal, strategic acts, which are the basis of information security. The 2nd block consists of the laws of Ukraine,

directly or indirectly related to security in the information sphere. The 3rd block consists of subordinate normative acts of the Verkhovna Rada and the Cabinet of Ministers of Ukraine and normative acts of ministries and other executive authorities on security in the information sphere. We have identified the 4th block of regulations; they relate to the occupied Ukrainian territories. It is, first and foremost, the strategy on the information the reintegration of occupied territories of Donetsk and Luhansk areas, the Crimea. We believe that it is necessary to form a separate information policy for the occupied and nearby regions, and for other territory of Ukraine.

The informational component also includes normative-legal acts on ensuring the rights and freedoms of the population of the occupied territories: the Law of Ukraine "On ensuring rights and freedoms of citizens and legal regime on the temporarily occupied territory of Ukraine" (2014), the decision of Parliament "On the Statement of the Verkhovna Rada of Ukraine on guarantees of the rights of the Crimean Tatar people within the Ukrainian State" (2014), the NSDC decision "On urgent measures for the protection of national interests in the South and East of Ukraine, in the Black and Azov seas and the Kerch Strait" (2018).

The article highlights the problems of regulation in the field of information security of Ukraine: the declarative nature of many rules, the lack of legislative authority of the responsible authorities and mechanisms of coordination of activities and the like.

Keywords: state security in the information sphere, the legal basis of information security, the Doctrine of information security, generalization and specification of the principles of state information security.

НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ФОРМУВАННЯ І РЕАЛІЗАЦІЇ ПОЛІТИКИ ДЕРЖАВНОЇ БЕЗПЕКИ У ІНФОРМАЦІЙНІЙ СФЕРІ

Анотація. Акцентовано увагу на питанні інформаційної безпеки України, що ускладнене відсутністю відповідної стратегії.

До важливих стратегічних документів у сфері інформаційної політики та державної безпеки відносяться "Стратегія розвитку інформаційного суспільства в Україні" (2013), у якій визначено пріоритети діяльності в галузі забезпечення інформаційної безпеки, "Стратегія кібербезпеки України" (2016). Метою цієї стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Визначено загрози кібербезпеці, національну систему кібербезпеки, основних суб'єктів забезпечення кібербезпеки, пріоритети та напрями забезпечення кібербезпеки України тощо. Законодавчо-нормативні акти щодо державної безпеки в інформаційній сфері можна поділити на чотири блоки за рівнем узагальнення і конкретизації: 1-й блок складають концептуальні, доктринальні, стратегічні акти, які є основою забезпечення інформаційної безпеки; 2-й блок — закони України, що безпосередньо або опосередковано стосуються безпеки в інформаційній сфері; 3-й блок — підзаконні нормативні акти Верховної Ради і Кабінету Міністрів Украї-

ни і нормативні акти міністерств, інших органів виконавчої влади щодо безпеки в інформаційній сфері; виділено 4-й блок нормативних актів, які стосуються окупованих українських територій. Це, насамперед, стратегії щодо інформаційної реінтеграції окупованих територій — Донецької і Луганської областей, Криму. Ми вважаємо, слід формувати окрему інформаційну політику для окупованих та прилеглих регіонів і для іншої території України.

Інформаційну складову включають також нормативно-правові акти щодо забезпечення прав, свобод населення окупованих територій: Закон України "Про забезпечення прав і свобод громадян та правовий режим на тимчасово окупованій території України" (2014), постанова ВРУ "Про Заяву Верховної Ради України щодо гарантії прав кримськотатарського народу у складі Української Держави" (2014), рішення РНБО "Про невідкладні заходи щодо захисту національних інтересів на Півдні та Сході України, у Чорному та Азовському морях і Керченській протоці" (2018).

У статті виділено проблеми регулювання у сфері інформаційної безпеки України: декларативність багатьох норм, відсутність законодавчо наданих повноважень відповідальних органів і механізмів координації діяльності тощо.

Ключові слова: державна безпека в інформаційній сфері, правові засади інформаційної безпеки, Доктрина інформаційної безпеки, узагальнення і конкретизація засад державної інформаційної безпеки.

НОРМАТИВНО-ПРАВОВЫЕ ОСНОВЫ ФОРМИРОВАНИЯ И РЕАЛИЗАЦИИ ПОЛИТИКИ ГОСУДАРСТВЕННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СФЕРЕ

Аннотация. Акцентировано внимание на вопросе информационной безопасности Украины, что затруднено отсутствием соответствующей стратегии.

К важным стратегическим документам в сфере информационной политики и государственной безопасности относятся "Стратегия развития информационного общества в Украине" (2013), в которой определены приоритеты деятельности в области обеспечения информационной безопасности, "Стратегия кибербезопасности Украины" (2016). Целью этой стратегии является создание условий для безопасного функционирования киберпространства, его использование в интересах личности, общества и государства. Определены угрозы кибербезопасности, национальную систему кибербезопасности, основных субъектов обеспечения кибербезопасности, приоритеты и направления обеспечения кибербезопасности Украины и др. Законодательно-нормативные акты по государственной безопасности в информационной сфере можно разделить на четыре блока по уровню обобщения и конкретизации: 1-й блок составляют концептуальные, доктринальные, стратегические акты, которые являются основой обеспечения информационной безопасности; 2-й блок — законы Украины, непосредственно или косвенно касающиеся

безопасности в информационной сфере; 3-й блок составляют подзаконные нормативные акты Верховной Рады и Кабинета Министров Украины и нормативные акты министерств, других органов исполнительной власти, безопасности в информационной сфере; выделено 4-й блок нормативных актов, которые касаются оккупированных украинских территорий. Это, в первую очередь, стратегии по информационной реинтеграции оккупированных территорий — Донецкой и Луганской областей, Крыма. Мы считаем, следует формировать отдельную информационную политику для оккупированных и прилегающих регионов, и для другой территории Украины.

Информационную составляющую включают также нормативно-правовые акты по обеспечению прав, свобод населения оккупированных территорий: Закон Украины "Об обеспечении прав и свобод граждан и правовой режим на временно оккупированной территории Украины" (2014), постановление ВРУ "О Заявлении Верховной Рады Украины относительно гарантии прав крымскотатарского народа в составе Украинского государства" (2014), решение СНБО "О неотложных мерах по защите национальных интересов на Юге и Востоке Украины, в Черном и Азовском морях и Керченском проливе" (2018).

В статье выделены проблемы регулирования в сфере информационной безопасности Украины: декларативность многих норм, отсутствие законодательно предоставленных полномочий ответственных органов и механизмов координации деятельности и тому подобное.

Ключевые слова: государственная безопасность в информационной сфере, правовые основы информационной безопасности, Доктрина информационной безопасности, обобщение и конкретизация принципов государственной информационной безопасности.

Problem statement. In an era of constant acceleration of development, we treat information as something that we unconditionally deserve, it is a decisive factor for success in all spheres of activity.

In Ukraine "the right to information is protected by law. The state guarantees all subjects of information relations equal rights and access to information. No one may restrict the rights of a person to choose the forms and sources of information, except as provided by law". "Everyone has the right to information, providing for the possibility of free receipt, use, distribution, storage and protection of information necessary for the realization of their rights, freedoms and legitimate interests" (law "On information") [1]. Also, the law "On information" contains provisions on the inadmissibility of abuse of the right to information: "Information can not be used to call for the overthrow of the constitutional system, violation of the territorial integrity of Ukraine, propaganda of war, violence, cruelty, incitement to ethnic, racial, religious hatred, terrorist acts, violation of human rights and freedoms" [1].

So, information is a benefit that needs to be protected in a certain way, especially when it comes to information in the defense of the state or other areas where disclosure threatened strategic interests. The harmonization of these two aspects (free access to information and its protection) is not straightforward, since the concept of security in the information sphere equally concerns the state as an institution, society and the individual citizens who form them.

Our country does not have a strategy of state information security, at the same time its elements can be found in various sources. An urgent task is to analyze the array of legal acts in this area.

State security in the information sphere can be viewed from several sides: on the one hand, as protection of citizens' rights to free access to information and freedom of speech, on the other — as protection of citizens from the influence of distorted, incomplete, false information, manipulative information impact, on the other — as protection of private or public important information from unlawful attacks by people, public or private structures, including foreign.

Analysis of recent research and publications. Among the latest studies, we would like to pay attention to the publication of Ya. Malyk (2015), in which the author considers the state and prospects of development of information security of Ukraine [2]. V. Savytskyi (2017) explores information security in the national security system of Ukraine [3].

Formulation of the objectives (goals) of the article: to analyze the legal basis for the formation and implementation of the policy of state security of Ukraine in the information sphere, to try to structure the legal acts of this sphere in a certain system, identified shortcomings and problems.

Presentation of the main material. In the development of mankind, information has always played an important role, but recently its importance has increased incredibly. It is access to and the ability to use information that currently determines the opportunities for success in many industries. Today, information resources are considered as no less important than demographic, raw materials or energy resources, and are the basis for the functioning of many human activities, such as governance, economy, politics, social and cultural spheres, national security, defense and international relations.

However, the information ceases to be valuable if it can't be saved, selected, allocated, transmitted, distributed and understood. That is why information becomes valuable only when it is available to people who need it and in the right place. Otherwise, it can be not only useless, but also dangerous.

Useful information is valuable, that is, the information that objectively or subjectively increases the level of human knowledge in a certain area (increases knowledge). Also, the actual usefulness of the information is determined by its accuracy, completeness and timeliness, that is, its arrival to the recipient at the right time and in the right amounts, which will allow the recepient to make the right decision. In addition, the information should be real (reliable), accessible, free from distortion and uncertainty.

The rights of access to information, its collection and dissemination are

now regarded as one of the fundamental human and civil rights, an integral part of it, confirms the dignity of the human person as a subject of civil society and forms the basis of democracy. It can even be argued that a state that does not guarantee its citizens free access to information will sooner or later be degraded, thereby abandoning the principles of pluralism, tolerance and openness, without which a democratic society cannot be imagined.

The right to information was already formulated in 1948 in the Declaration of human rights adopted by the UN General Assembly. More broadly, the idea of the right to communication arising from other human rights was first formulated in conjunction with the Concept of civil society. Its creator was Jean d'arcy, Director of the UN Information office. The International Covenant on civil and political rights, ratified by Ukraine in 1973, also includes the right to have and express one's own views and to collect, receive and disseminate information. This right may be restricted only by law. Provision for access to information can also be found in other acts of international law, such as the European Convention on Human rights or the Charter of fundamental rights of the European Union. In the 1990s, the principles of openness, transparency and access to documents were incorporated into existing EU decisions.

In domestic legislation, the right to information, especially on the activities of public authorities, as well as any other, is provided by the Constitution. Thus, part 1 of article 34 of the Basic law states "Everyone is guaranteed the right to freedom of thought and speech, to freedom of expression of their views and beliefs". Part 2 of article 34 provides for the right of everyone to freely collect, store, use and disseminate information orally, in writing or otherwise [4]. The exercise of these rights may be restricted by law in the interests of national security, territorial integrity or public order, for the prevention of disorder or crime, for public health, for the protection of the reputation or rights of others, for the prevention of disclosure of information received confidentially, or for the maintenance of the authority and impartiality of justice [4].

Also, article 32 of the Constitution provides for the right of citizens to get acquainted with information about themselves, which is not a state secret or other information protected by law, in public authorities, local self-government bodies, institutions and organizations [4].

The development of these rights is contained in the legislative acts of Ukraine, in particular in the law "On access to public information", which regulates the subjective and objective scope and method of obtaining information on the activities of state bodies (2011, new edition 2015) [5], and the new version of the law "On information" has fixed the "right of everyone to information", "ensuring everyone's access to information", the principle of maximum openness of information, except for information with limited access [1]. In addition, the Law "On information" contains other provisions important for the implementation of the right of access to information, namely: 1) permission to disseminate information with limited access, if it is socially necessary, that is, is the subject of pub-

lic interest; 2) the right of the public to know this information is dominated by the potential harm from its dissemination (part 1. 29) [1]. These laws, as amended, no longer establish, as in the past, the erroneous concept of ownership of information in general and of the state's ownership of information in particular.

International norms on freedom of speech and press are reflected in article 15 of the Constitution of Ukraine — "Censorship is prohibited" [4]. In turn, we find the expansion of the constitutional principle of freedom of speech and expression in the law "On the print media (press) in Ukraine" [5].

Although the right to information is considered to be a fundamental human right, it may be restricted, for example, for the purpose of ensuring public order, security, morals, combating slander, fraud, manipulation, protection of other rights. No matter what the reasons are, these restrictions always cause controversy or resistance, because many people perceive it as interference with fundamental civil rights and freedoms.

Restrictions on the right to information arise primarily due to the risks associated with the misuse of information or its use by unauthorized persons. Given the importance of information to modern people, societies, states and the international community, it is undeniable that, in addition to the obvious benefits that information can bring, it can also be exposed to threats that arise from various factors.

Threats in the information sphere: the unauthorized disclosure, asymmetries in international exchange of information, espionage, karpasiana, cybercrime, lack of information, "information chaos", disinformation, information warfare (war), manipulation of information. Manipulation of information is also the provision of false information, and reducing the importance of information, biased selectivity of information, its ambiguity, and excess, causing "information chaos".

From the point of view of state security, information wars are considered to be the greatest threat in the field of information. We perceive them as threats, conflicts in which information is both a resource, an object of attack, and weapons, and physical destruction of information infrastructure is not excluded, carried out by the enemy. This fight can have two purposes: destruction of information resources of the opponent and ensuring own safety. This is usually done through the following tools: influence on political and cultural processes; information and psychological campaigns; misinformation and influence on the media; diplomacy; penetration into computer networks and databases.

Information war does not necessarily mean that the country is in a state of actual war, such activities occur in peacetime. Actions are used not only to obtain information, but also to cause unrest, government crises. As a substitute for open aggression, they can compromise a state or its authority in the international arena, undermine its political authority or discredit it in the economic sphere. This struggle concerns not only the military sphere, but also in the civil one. It is conducted in an open or secret way, it is an armed struggle, but in extreme cases it can lead to physical destruction of the object. This is a universal struggle that it is carried out in all spheres of the state, not only in the

military. It can take the form of political, military and economic pressure, as well as intimidation. It is carried out not only in the field of cybernetic impact on databases of digital encrypted data, but also, first of all, through the wide dissemination of negative real or false information, for example, to create specific social attitudes. These events, often unconsciously, involve the mass media, which are making public sensations, are currently the most effective tool in the information struggle. Al this arsenal that we bmentioned above is used by Russia in the war against Ukraine.

Article 17 of the Constitution states: "Protection of sovereignty and territorial integrity of Ukraine, ensuring its economic and information security are the most important functions of the state, the business of the Ukrainian people" [4]. Thus, the state considers not only an opportunity, but also its duty to protect the citizens of Ukraine from information threats.

Given the current military and political situation of Ukraine, which is in a hybrid war with Russia, also expecting future threats from the aggressor, it is important to create a system of state security in the information sphere, which would provide reliable protection of the state and the people.

The approved "Doctrine of information security of Ukraine" is a response to modern threats to national security. "The purpose of the doctrine is to clarify the basics of the formation and implementation of the state information policy, primarily to counter the destructive information influence of the Russian Federation in the conditions of its unleashed hybrid war" [5]. The Doctrine defines national interests (individuals, society and the state) in the information sphere, actual threats to national interests and national security of Ukraine, priorities of state policy in the information sphere and the mechanism of implementation of the Doctrine.

As we can see, the Doctrine sets out only the conceptual foundations of information security. The issue of implementation of information security of Ukraine is complicated by the lack of an appropriate strategy. The information security strategy is considered within the framework of the national security Strategy of Ukraine [5]. Despite the fact that there is no direct definition of the concept of security in the information sphere in the legislative acts of Ukraine, it can be perceived as a state that is achieved after certain conditions are met. These conditions are defined in the national security Strategy of Ukraine. Therefore, the state of information security should be considered as a state when:

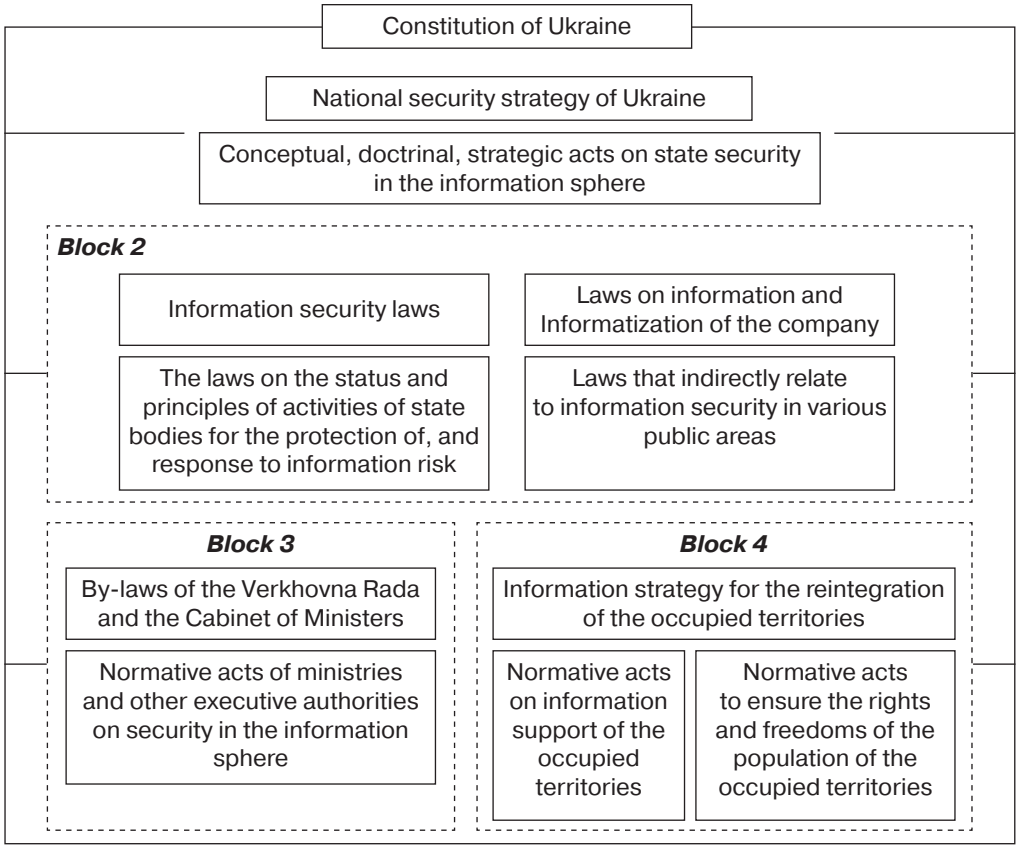
- measures of information security policy on the basis of asymmetric actions against all forms and manifestations of information aggression are provided;
- an integrated system of information threats assessment and rapid response to them has been created;
- there is a resistance to information operations against Ukraine, manipulation of public consciousness and dissemination of distorted information, protection of national values and strengthening the unity of Ukrainian society;
- coordinated information policy of public authorities has been developed and implemented;

• the entities of the Ukrainian information space used by Russia to information warfare against Ukraine have been identified, and their subversive activities and so on have been eliminated [5].

Important strategic documents in the field of information policy and state security also include: "Strategy for the development of the information society in Ukraine" (2013), which defines the priorities of activities in the field of information security; "Cyber security Strategy of Ukraine" (2016). The purpose of this strategy is to create conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and the state. It identified the threats to cybersecurity, the national cyber security system, the main subjects of cyber security, priorities and directions of cyber security of Ukraine, etc. [5].

In general, the legislative and regulatory acts on state security in the information sphere on the level of generalization and specification of the principles defined in them can be divided into four blocks (Figure).

The 1st block consists of conceptual, doctrinal, strategic acts, which are the basis of information security. These



Structuring of legislative and regulatory acts on the level of generalization and specification of the bases of state security in the information sphere defined in them
Created by author.

include “Strategy of national security of Ukraine”, “Doctrine of information security of Ukraine”, “Cyber security Strategy of Ukraine”, “Strategy of development of information society in Ukraine”, “National strategy in the sphere of human rights” (2015), also “Concept of the National program of Informatization” (last edition of 2013), “Military doctrine of Ukraine” (new edition of 2015) [5].

The 2nd block includes the laws of Ukraine and can be divided into four groups:

The laws that specifically relate to security in the information sphere: “On information security of Ukraine”, “On information protection in information and communications systems”, “On basic principles of ensuring cyber security of Ukraine”, the laws “On fundamentals of national security of Ukraine”, “On nonstate ensuring of national security of Ukraine”. We believe that the law “On ensuring the functioning of the Ukrainian language as the state language” adopted by the Verkhovna Rada of Ukraine on April 25, 2019 can be rightfully attributed to this block;

• Laws concerning freedom of information and Informatization of the society: “On information”, “On access to public information”, “On the basic principles of development of the information society in Ukraine for 2007–2015”, “On Public television and radio broadcasting of Ukraine” (2014), “On printed media (press) in Ukraine”, “On the National program of Informatization” (last edition of 2016);

• Laws on the status and principles of activity of state bodies on protection and counteraction of information danger: “On the security Service of Ukraine”, “On the national security and defense Council of Ukraine”, “On the state service of special communication and information protection of Ukraine” (2015), “On the intelligence agencies of Ukraine”, “On the National police” (2015). This also include “Regulations on the Ministry of defense of Ukraine”, approved by the Cabinet of Ministers (2014);

• Laws indirectly relate to information security in various public areas: “On the basics of domestic and foreign policy” (2010), “On state secrets”, “On sanctions” (2014), “On combating terrorism”, “On counterintelligence activities”, “On defense of Ukraine”, “On state protection of state authorities of Ukraine and officials” (1998). Criminal, Civil and other codes of Ukraine related to the regulation of relations in the field of national security, and therefore information.

The 3rd block includes subordinate normative acts of the Verkhovna Rada and the Cabinet of Ministers (resolutions, decrees, orders). As for security in the information sphere, these are: resolutions of the Verkhovna Rada “Recommendations of parliamentary hearings on the topic: “Reforms in the field of information and communication technologies and the development of the information space of Ukraine” (2016), “Recommendations of parliamentary hearings on the topic: “Legislative support for the development of the information society in Ukraine” (2014); decrees of the President of Ukraine “On measures to improve the formation and implementation of state policy in the field of information security of Ukraine” (2014), “On promoting the development of civil society in

Ukraine" (2016), "Concept of development of the security and defense sector of Ukraine" (2016), "On measures to develop the national component of the global information network internet and support" (2000); Resolutions of the Cabinet of Ministers "On approval of the Regulations on the unified information system of the Ministry of internal Affairs and the list of its priority information resources" (2018), "On approval of the Order of formation of the list of information and telecommunication systems of critical infrastructure of the state" (2016).

We also refer to the 3rd block regulatory legal acts of ministries and other executive bodies, which, on the basis of the current legislation and within their competence, issue departmental regulatory acts on security in the information sphere (orders, decisions, instructions, regulations, resolutions, programs). For example, the decision of the Council of national security and defense of Ukraine "On measures to improve the formation and implementation of state policy in the sphere of information security of Ukraine" (2014) and "On improvement of measures to ensure the protection of critical infrastructure" (2016) the order of the security Service of Ukraine "On approval of the collection of information constituting a state secret" (2005), the decision of the national Council of television and radio broadcasting "On approval of the development plan, the national TV and radio informational space" (2010, as amended by 2018), orders of the Ministry of defense "Concept of strategic communications of the Ministry of defense of Ukraine and the Armed Forces of Ukraine" (2017) and "Register of electronic information resources of the Ministry of defense of Ukraine" (2015).

We have also identified the 4th block of legal acts relating to the occupied Ukrainian territories. These are, first of all, strategies for information reintegration of the occupied territories. In July 2018, the "Strategy of information reintegration of Donetsk and Luhansk regions" was approved. The purpose of the Strategy is the implementation of information rights and freedoms of man and citizen, increasing the level of support of citizens of Ukraine state policy in the field of information reintegration of temporarily occupied territories in Donetsk and Luhansk regions; introduction of an effective mechanism to ensure access of Ukrainian citizens living in temporarily occupied territories in Donetsk and Luhansk regions, as well as adjacent territories, to the all-Ukrainian information space [5].

The implementation of the Strategy is planned for the period up to 2020. Achieving the objectives of the Strategy requires the following tasks: countering the use of information technologies by the Russian Federation aimed at inciting national and religious hatred, propaganda of war, violent change of the constitutional system, violation of the territorial integrity and sovereignty of Ukraine; strengthening the sense of community between citizens of Ukraine who live in the temporarily occupied territories in Donetsk and Luhansk regions, adjacent territories, as well as citizens of Ukraine who live in other regions of Ukraine; creating conditions to meet the needs of the population of the temporarily occupied territories in objective, timely and reliable information [5].

In December 2018, the strategy of information reintegration of the Autonomous Republic of Crimea and Sevastopol was approved. The purpose of this strategy is to provide information reintegration of the occupied territory of Ukraine (Autonomous Republic of Crimea and the city of Sevastopol), creation of information tools prerequisites for the restoration of territorial integrity and sovereignty of Ukraine. Implementation of the Strategy involves the implementation of such tasks: the implementation of the state information policy of the Crimea and Sevastopol on the principle of "one voice"; approval in the Ukrainian and international information space of strategic narratives of mandatory restoration of the territorial integrity of Ukraine; implementation of constant monitoring of the information space of the occupied territory of Ukraine, collection, accumulation, systematization, analysis, evaluation of the information received and exchange it for the purpose of rapid response by the relevant authorities to the actions of the Russian Federation; informing citizens of Ukraine, foreigners about the situation in the Crimea; refutation by ideologues of the Russian propaganda concerning the past and modern Crimea, which are spread in the Ukrainian and foreign mass media; mobilization by information tools of the international support of restoration of territorial integrity of Ukraine and others [5]

In addition, other normative acts on information support of the occupied territories were adopted. These are, in particular, the decision of the National Council of broadcasting "On broadcasting of TV and radio organizations in the territory of the antiterrorist operation" (2014), the order of the state television and radio of Ukraine "On measures to preserve broadcasting by state television and radio companies to meet the information needs of national minorities and persons living in the temporarily occupied territories" (2015).

The informational component also includes normative-legal acts on ensuring the rights and freedoms of the population of the occupied territories: the Law of Ukraine "On ensuring rights and freedoms of citizens and legal regime on the temporarily occupied territory of Ukraine" (2014), the decision of Parliament "On the Statement of the Verkhovna Rada of Ukraine on guarantees of the rights of the Crimean Tatar people within the Ukrainian State" (2014), the NSDC decision "On urgent measures for the protection of national interests in the South and East of Ukraine, in the Black and Azov seas and the Kerch Strait" (2018).

We believe that it is necessary to form at the state level a special information policy for the occupied and nearby regions, and for other territory of Ukraine. It is necessary to start from those accents which are important for the population of concrete territories. For residents of Donbass it is one accent, for Crimeans it is another one. It is necessary to formulate goals, objectives, resources and tools to achieve these goals and objectives.

Conclusions and prospects for further research. The analysis showed that the legal framework of the sphere of state information security is quite large and extensive, but it has significant problems. The problem of regulation in the field of information security of Ukraine, as well as other areas of state

regulation, is the discrepancy between the legal framework and the practical implementation of certain steps, the declarative nature of many norms. The bodies that are determined to be responsible for the implementation of the state security policy in the information sphere also have legislative powers and coordination mechanisms. This applies primarily to the National Security and Defence Council of Ukraine and the Ministry of Information Policy, as well as other bodies.

Another aspect that requires further research is the feasibility of separating cybernetic security from information security in legal acts. It is also necessary to coordinate the activities of state and public structures in the field of information security of Ukraine, especially those that are already in force ("Academy of national security", "Stop-fake", "Information resistance", "Informanapalm", "Razom" and the like).

REFERENCES

1. VRU (1992) Pro informaciju. [About the information], Zakon Ukrajiny 02.10.1992 № 2657-XII, redakcija 01.01.2017 URL: https://zakon.rada.gov.ua/laws/main/2657-12
2. Malyk Ja. (2015). Informacijna bezpeka Ukrajiny: stan ta perspektyvy rozvytku [Information security of Ukraine: the state and prospects of development]. *Zbirnyk naukovykh pracj "Efektyvnistj derzhavnogho upravlinnja" — Collection of scientific works "Efficiency of Public Administration"*, 44, 13–20 [in Ukrainian].
3. Savycjkyj V. T. (2017). Informacijna bezpeka v systemi nacionaljnoji bezpeky Ukrajiny [Information security in the system of national security of Ukraine]. *Universytetsjki naukovi zapysky – University scientific notes*, 62, 195–207 [in Ukrainian].
4. Konstytucija Ukrajiny [Constitution of Ukraine] 28.06.1996 № 254к/96-ВР. URL : https://zakon.rada.gov.ua/laws/main/254к/96-вр
5. Zakonodavstvo Ukrajiny. Verkhovna Rada Ukrajiny [Legislation of Ukraine. Verkhovna Rada of Ukraine]. URL : https://zakon.rada.gov.ua/laws/

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про інформацію. Закон України від 02.10.1992 № 2657-XII, поточна редакція від 01.01.2017. URL : https://zakon.rada.gov.ua/laws/main/2657-12
2. *Малик Я.* Інформаційна безпека України: стан та перспективи розвитку // Збірник наукових праць. 2015. Вип. 44 "Ефективність державного управління". С. 13–20.
3. *Савицький В. Т.* Інформаційна безпека в системі національної безпеки України // Університетські наук. записки. 2017. № 62. С. 195–207.
4. Конституція України: від 28.06.1996 № 254к/96-ВР. URL : https://zakon.rada.gov.ua/laws/main/254к/96-вр
5. Законодавство України. Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/