Journal of Information Technology Management

Print ISSN: 2008-5893

Online ISSN: 2423-5059

The Legal Mechanisms for Information Security in the context of Digitalization

Svitlana Bondarenko*

*Corresponding Author, Department of Journalism, National Aviation University, Kyiv, Ukraine. E-mail: lana.bond@ukr.net

Olena Makeieva

Department of Theory and History of State and Law, National Aviation University, Kyiv, Ukraine. E-mail: maklena72@ukr.net

Oleksandr Usachenko

Department of Public Administration, Interregional Academy of Personnel Management, Kyiv, Ukraine. E-mail: vsanucha@gmail.com

Vladyslav Veklych

Department of Theory of State and Law and Constitutional Law, Interregional Academy of Personnel Management, Kyiv, Ukraine. E-mail: v1777@online.ua

Tetiana Arifkhodzhaieva

Educational-Scientific Institute of Law named after Volodymyr the Great, Interregional Academy of Personnel Management, Kyiv, Ukraine. E-mail: profmaup@gmail.com

Svitlana Lernyk

Department of Economics and Business Administration, Interregional Academi of Personnel Management, Kyiv, Ukraine. E-mail: svitlanalernyk@gmail.com

Abstract

As a result of the introduction of digital technologies in all spheres of society, various latest technologically conditioned risks and threats have become various. It requires the formation and implementation of a legal mechanism for further development and operation of the system ensuring information security, taking into account the effects of digitalization and transformation of society. The purpose of this study is development of scientifically substantiated proposals and recommendations for implementation legal mechanisms for information security in the context of digitalization. The relevance of this study is due to the needlegal regulation of relations in the information sphere, formation of a system of

protection and counteraction to cybercrime. To achieve the goal of the study, methodological principles and approaches of legal science were used. The results of the analysis showed that the most significant mutual influence is demonstrated by a group of indicators of the state's institutional capacity and a group of indicators of the digital capacity of the national economy and cybersecurity. This study substantiates the main directions of accelerating the optimization of the institutional system of cybersecurity in Ukraine, which provides for two key areas: legal and organizational. The legal mechanisms include further improvement and harmonization of the regulatory framework, the formation of relevant legal norms, state policy in the field of information security. The organizational measures are aimed at improving the efficiency of responsible institutional structures - the subjects of cybersecurity - by increasing their capabilities, eliminating duplication in the exercise of their powers, taking into account the best practices of international and European experience. The core of the integrated information security system is the National Cyber Security Coordination Center.

Keywords: Legal mechanisms; Informational security; Cybersecurity; Digitization; Institutional system for cybersecurity.

Journal of Information Technology Management, 2022, Vol. 14, Special Issue, pp. 25-58
Published by University of Tehran, Faculty of Management
doi: https://doi.org/ 10.22059/jitm.2022.88868
Article Type: Research Paper

Received: January 21, 2022
Received in revised form: March 29, 2022
Accepted: July 14, 2022
Published online: September 13, 2022

Introduction

The active introduction of digital technologies has become another challenge for humanity, as the problem of information security has become more acute. According to Gartner analysts, global spending on automated information security systems and integrated risk management (IRM) in 2020 reached $ 133.78 billion, which is 6.4% more than a year earlier. Such market growth rates reflect the continued demand for technology for remote operation and cloud security. There is a tendency of increasing automation and further introduction of machine learning technologies and artificial intelligence. And, therefore, to combat attacks, organizations will expand and standardize the work of identifying threats and responding to them. The studies have shown that the cyber risk management technology segment in 2020 showed steady growth due to the risks associated with the global crisis caused by the COVID-19 coronavirus pandemic. The areas of significant risks that will stimulate further demand are related to the emergence of new digital products and services and their use for health and safety, as well as third-party risks such as risks of leakage of customer data or attacks on supply channels. The serious consequences of such risks lead to an escalation of the current

data leakage crisis and the acceleration of attacks by extortionist viruses. The figure 1 presents statistics on data leakage over the past fifteen years.

Figure 1. The volume of unauthorized data leaks for 2005-2020.

2020 was a record year for the level of unauthorized use of information. Due to the imperfection of protection, there are unauthorized managers of information, whose activities are partly in the illegal area.

With the development of technology, the importance of information as a resource for development has expanded, and the importance of intellectual capabilities of citizens has increased. However, the lack of knowledge and methodological basis for the practical application of digital methods of processing and storage of information can cause serious engineering and humanitarian and educational problems and even disasters. They require scientifically sound approaches to the definition of fundamental concepts in legislative and regulatory documents: "information", "information resource", "information security" and so on.

Unresolved in Ukraine a number of legal issues related to the information and communication sphere, with the advent of digital technologies is becoming a danger. The communication processes become much more complicated, new types of relationships emerge - all this increases risks and threats, changes their quality, which makes it impossible to confront them with the help of current law. A new type of crime is emerging and becoming more complicated - organized cybercrime. Therefore, the main tasks for the prevention of threats in the information and communication sphere are: protection of critical information infrastructure; protection of personal data; security of information and communication ergasystems, state structures; protection of the working environment and technologies.

Therefore, the digitalization of society and the economy, which is based on the network use of digital information and communication technologies, requires adequate legal support. After all, the digital technologies are associated with the emergence of various new technology-driven risks and threats. In addition, digitalisation is the cause of institutional transformation, which should also have a legal basis. All of the above requires the formation and implementation of a legal mechanism for further development and operation of the system ensuring information security, taking into account the effects of digitalization and transformation of society.

The purpose of the study is to develop scientifically sound proposals and recommendations for implementation legal mechanisms for information security in the context of digitalization.

The object of study - there is a process of formation social relations that arise in the implementation of information processes and relations of subjects under the influence of development of new network systems of communication with the rules and requirements.

Subject of study - features of legal regulation in the field ensuring information security in the context of digitalization.

There is a high level of competition between countries for data resources in the world, and the sovereignty of data in the context of digitalization faces serious challenges. Yes, the United States has a liberal policy on cross-border data flows. Such a policy enables companies operating on the Internet (Facebook, Twitter, YouTube, etc.) to have the primary advantage over the flow of data across borders. Instead, very strict regulatory measures (white list, standard contracts) have been introduced in the EU countries. France has already introduced new cybersecurity rules for critical infrastructure operators. In September 2020, the Chinese Ministry of Foreign Affairs published the Global Data Security Initiative. Yes, it is proposed that global digital governance adhere to the principles of multilateralism, security and development, as well as honesty and justice. Some countries (Japan, Singapore) have already passed laws on personal data protection. At the same time, risk management issues for cross-border data flow remain unresolved.

The EU member states, the NATO members, the international corporations and the experts unanimously recognize Russia and its actions in cyberspace as a major threat to international cybersecurity. Active reconnaissance and sabotage in cyberspace is part of Russia's hybrid war against Ukraine. Russia's destructive activity poses a real threat of acts of cyberterrorism and cyber diversion against the national information infrastructure. The situation is geopolitical in nature, the intensity of interstate confrontation and intelligence and subversive activities in cyberspace is projected to increase. The consequence of such processes is the expansion of the circle of states that will try to form their own cyberspace, to master modern technologies of reconnaissance and sabotage in cyberspace. The need for legal

regulation of relations in the information sphere is due to extraterritoriality. Therefore, regulatory mechanisms should be multilevel, given the actual lack of borders for the dissemination of information. An Informatization, the Internet, the digital technologies in public administration have created the latest phenomenon "e-state", "e-government" and so on. This requires appropriate changes in the legal mechanisms of state and legal institutions. Today, information is an important resource of any state on which the national security of the country depends. Adequate and effective legal provision of information security is an urgent need in the conditions of development of Ukraine as a democratic and legal state. The study examines the experience of Ukraine through the prism of world experience of legal mechanisms for information security in the context of digitalization.

Literature Review

The development of information technology is characterized by the expanded and comprehensive use of information technology and systems. The strengthening information security is based on ensuring the reliability, confidentiality, integrity and availability of state information resources, information with limited access, in particular that circulating on the objects of economic information infrastructure in the context of information and hybrid wars (Krasnobayev et al., 2016; 2019). As a result of active implementation technologies in all spheres of life of people and society there are the newest types of interaction of economic agents (virtual or "hybrid world"). Such interactions are the result of a fusion of real and virtual worlds, where it is possible to perform appropriate actions, the consequences of which are felt in the real world through the virtual. Ensuring information security of the national economy, taking into account the processes of digitalization is possible provided that the principles of connectivity, system, synergy, which involves the interaction of security system components at the macro and micro levels (Yanko et al., 2018). As studies show (Kirkham et al., 2013; Yarovenko, 2020; Zavhorodnii et al., 2021) digital transformation affects not only the introduction of digital technologies, but also the transformation of horizontal and vertical business processes, optimization of operating procedures, changes in established models and formats of interaction between participants in the value chain. The latest technological solutions require complementary investment in improving organizational practices, employee competency development, data culture and digital solutions (Iatsyshyn et al., 2020; Romanenko & Chaplay, 2016). New threats and challenges in institutional transformations are emerging, which is a powerful destabilizing factor for the sustainable development of any country. Research identifies a wide range of issues related to information security.

Of course, there is an active scientific search for ways to regulate the development of the economy in the information society, the legal aspects of information security, standardization and development of strategic documents in this area. The need to use standardization to improve information security is emphasized Topa & Karyda (2019). He systematizes cybersecurity strategies in Latin America in his study Kosevich (2020), author considers the

impact of information security on the development of countries. The ways of counteracting information threats and risks of different countries are formed in different ways. Influential factor of differences Dincelli (2018) highlights the features of national culture and the confidentiality of people's behavior, which determines the character strategies to combat information threats. External information has a negative impact on the country's information environment, especially under the influenceforeign policy conflicts (Kirilenko & Alexeyev, 2018; Marhasova et al., 2020). Thus, the issue of information space is complex.

The information space of the country is a structurally-segmented complex of communication-content dimension of the life of the country, which consists of different in scale and nature of interaction of different elements. The main elements of the information space of the country are presented in Figure 2.

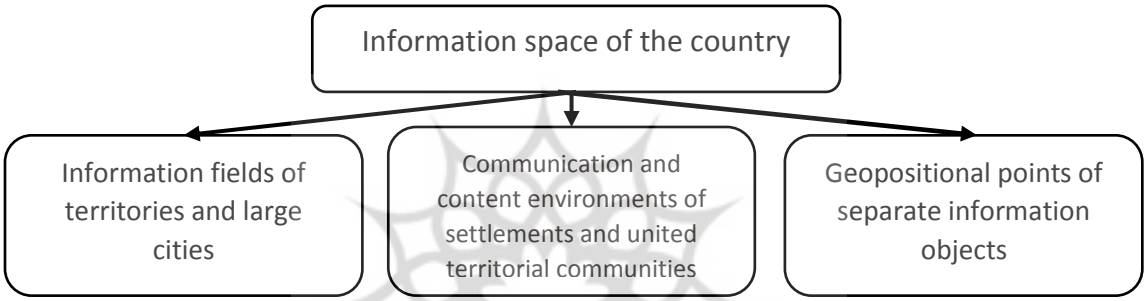


Figure 2. Components of the information space of the country

The information space of the country is formed by information fields, information environments and geopositional points of separate information objects:

1. Information fields of territories and large cities are local mass media, mass media and a number of social networks. That is, it is the whole segment that is present in a given area and interacts with each other.

2. Communication and content environments of settlements and united territorial communities. This is a fairly new phenomenon that has not yet been fully formed. The communities are gradually becoming the center of life. It's only a matter of time.

3. Geopositional points of individual information objects. When a resonant event in a particular point or locality becomes very popular. Such points will always be. We can mention, for example, the Kerch Strait in 2018.

The information coming into the national information space must be safe for this space.

The information security is a state in which, in the conditions of real and potential threats, self-preservation, sustainable and progressive development of the information sphere is

ensured. And this level of security, its criteria for ensuring national interests and inviolability of values, must be enshrined in law and regulated.

The scientific interest in digitalization technologies is represented by research related to the introduction of legal protection in economics, finance and management of blockchain technologies, artificial intelligence, cryptography, cloud technologies, knowledge management, etc.

Klyaus & Gatchin (2020) developed a mathematical model of information protection by means of control of optimization and evaluation of information, ensuring the effectiveness of the security system using the gradient method. Apply the method of fuzzy logic to protect personal data is proposed Dorosh et al. (2019). Blockchain technologies are considered to be promising methods of information protection (Warkentin & Orgeron, 2020). Brozhova et al. (2016) consider qualitative and quantitative data of the network process, options for network development decisions.

Issues of information security relate to information, the phenomenon of cybercrime and the prevention of cyber threats, risks, research on information security issues at the level of society, the state of the individual.

In his scientific research Li et al. (2021), Kuznetsov et al. (2019) provide a methodology for identifying risk areas and classifying the level of risk to support early warning decisions. D'elia (2018) suggested that in order to improve the mechanism of cybersecurity, industrial policy should take into account market-oriented goals and no less important tasks related to data protection and technological independence.

The success factors of information security management are investigated in accordance with the security of business activities, support of senior management, security control and organizational awareness (Ključnikov et al., 2019; Singh & Gupta, 2019). An effective means of information security management in the enterprise is to build an automated security information system (Bekmuratov et al., 2020; Klochanet al., 2021). An important aspect is the legal provision of information security of man, society, state (Hubanovaet al., 2021; Bondarenko et al., 2021).

There are enough laws and regulations on information security and data security in the world.

The legal regulation of information security is a form of authoritative legal influence on public information relations, which has carried out by the state in order to organize, consolidate and ensure them.

However, as practice shows, in general, such laws and regulations are not yet fully developed, which reveals problems such as the lack of comprehensive legislation and further

interpretation, as well as inadequate coordination between protection and development. The legislation has limited territorially through different laws on different continents (Sagan et al., 2020; Bondarenko et al., 2021). In addition, the internationalization of data circulation, possession of personal data exacerbates the need for a legal framework with international standards to resolve data issues and resolve disputes between countries.

Thus, the literature review showed the main directions of scientific research to ensure information security by legal mechanisms:

1) the legal regulation of information security of the country is determined by the degree of regulation by national legislation and norms of international law of public relations in the field of combating threats to national interests in the information sphere. A national data protection strategy needs to be developed. That is, the issue of ensuring information security by means of strengthening the coordination of the information security strategy with the national security strategy and national strategic resources is actualized.

2) The cyber influence is carried out in the information space via the Internet, so, in our opinion, it is necessary to include cybersecurity in the information security of the country.

3) The regulatory policies for the cross-border flow of critical data and user information in key areas such as communications and finance need to be further improved. The assessment of cross-border data flows should be strengthened and appropriate international standards and regulations established.

4) The legal regulation of information security of the country - a single system of legal support of public relations in the field of countering threats to national interests. Therefore, it is important to promote the rule of law in the field of information security and data confidentiality. Implementation rules for existing laws and regulations need to be refined. The scope for adjusting existing laws needs to be expanded, and data ownership laws need to be drafted quickly to clarify the extent of big data ownership. At the present stage, the state information policy should envisage and solve tasks related to the harmonious provision of information security of the individual, society and the state.

5) The issue of improving the classification of data and the system of hierarchical supervision of information is relevant. The system of management and protection of information and data will help to maximize the detection of data value, while protecting data security and personal confidentiality. The data classification system should be started in terms of improving the effectiveness of supervision and adopt different regulatory measures and legal requirements for data of different classification units. At the business level, it is advisable to develop a classification and evaluation system based on industry practices of data protection, data flow and data compliance.

Methodology

The basis of this study were the methodological principles and approaches of legal science, which were used to solve problems. The work used a comprehensive analysis of legal mechanisms, measures and results of information security of Ukraine. The analysis was performed using general scientific methods - description, analysis, synthesis, induction, deduction, abstraction, classification. The method of induction, which consists in the generalization and systematization of empirical material, was used to conduct a comprehensive analysis of information securityas an important component of national security. The interrelations of the main components of information security of the state are clarified, justified interdependence of the state of information legislation and legal support of information security of Ukraine.

The conceptual scheme of information security of the country has presented in Figure 3.

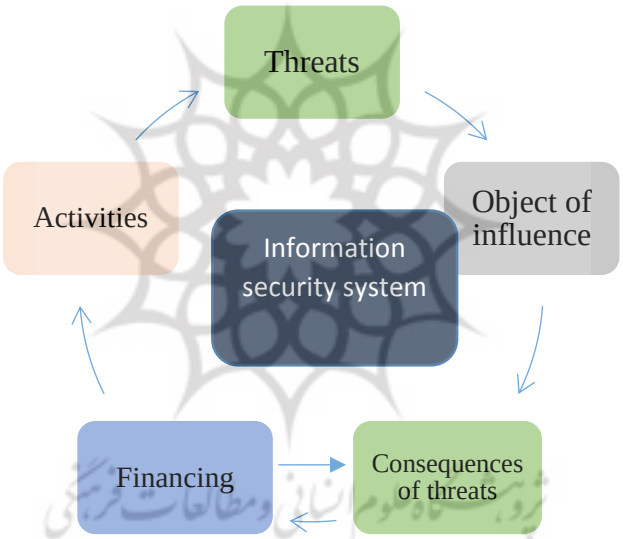


Figure 3. Conceptual scheme of information security

The system approach allowed approaching the consideration of the structural components of the information security system of Ukraine. The Figure 4 shows the main features of information security. The system approach acts not only as a determinant and "measurer" of the system of the subject, but also a kind of breeder in choosing the necessary legal regulators (Anderson & Moore, 2006; Babenko, 2020). In this study, the systems approach is reflected in the consideration of information security as a system of public relations, as well as in the proposals formulated on its basis for systematization of legislation and activities of the national cybersecurity system aimed at protecting information security. The structural and functional political analysis allowed to clarify the roles and functionality of structural units that provide information security, functioning of subjects of information security of the state, established collegial advisory bodies for information protection at the executive bodies of state power.

On the basis of the structural-functional method, the activity of ensuring information security by the executive bodies of state power of Ukraine was considered, the conformity of normative-legal acts with which the modern system of legal provision of information security of the state has associated with real public relations in this sphere and international standards is determined. The institutional method allowed analyzing the activities of public authorities that make up the system of information security of Ukraine.

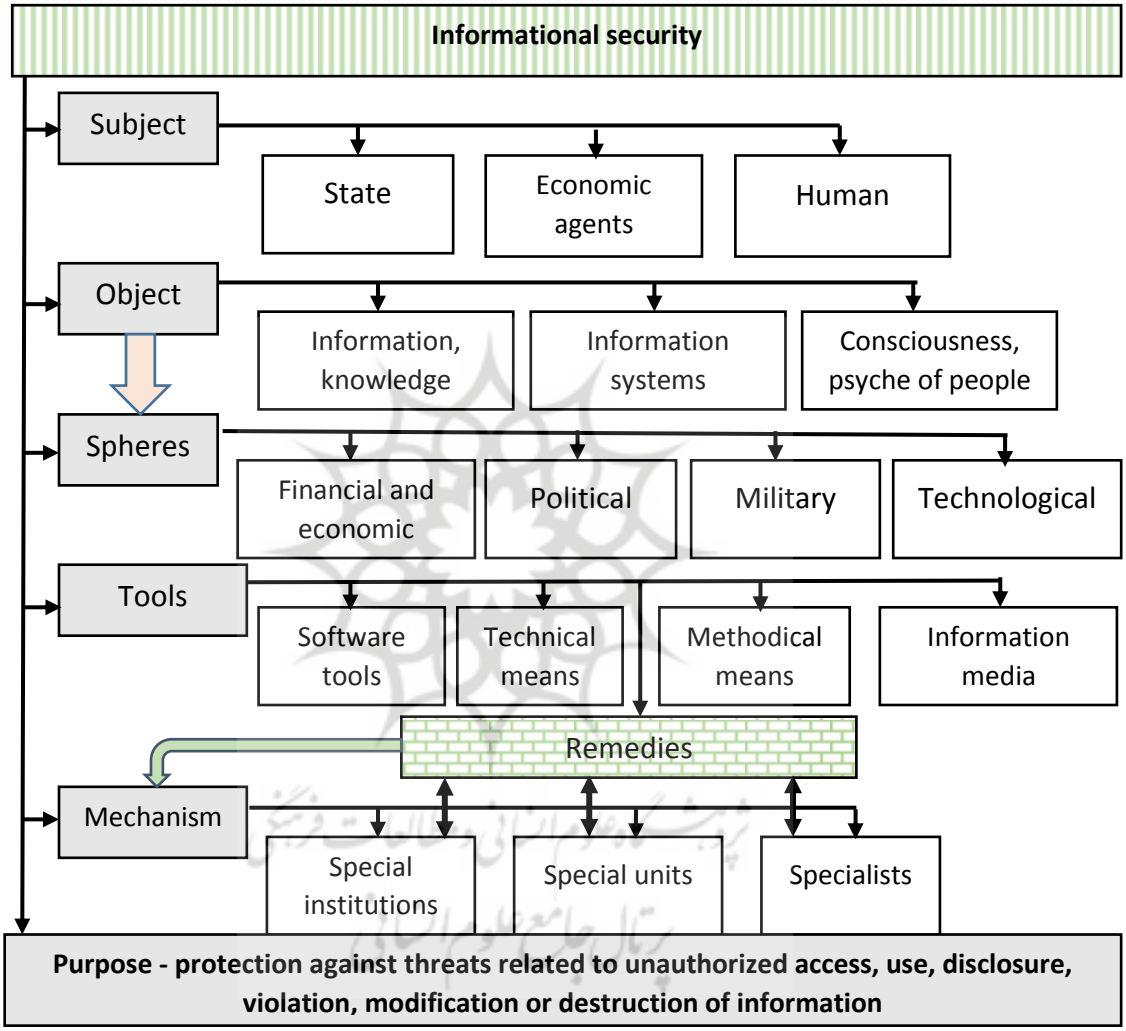


Figure 4. Key components of information security

The comparative legal methodis the basis of a study of international experience in the legal provision of information security of the state. To understand the evolution of the concepts of information society, as well as concepts for the organization of public administration, which are associated with rethinking the role of the state in society in the context of digitalization, used historical-descriptive method of historical knowledge. The analysis of statistical data, qualitative analysis of the documents used in research was carried out. The methods used together allowed to identify priority legal mechanisms and develop recommendations for optimizing the activities of the national cybersecurity system to ensure

information security. The information and factual basis of the study was formed by the laws of Ukraine, decrees of the President of Ukraine, the regulatory framework of relevant ministries and departments, reporting and analytical information of the State Statistics Service of Ukraine; data from the World Bank, Eurostat, Global Web Statistics "Statoperator"; analytical reviews of international rating agencies Deloitte, IBM, e-Governance Academy, International Telecommunication Union, Ponemon Institute, etc .; internal documentation of banks and enterprises; research results.

Results

Current state of information security, index analysis

The digital business has created a new ecosystem in which partners add new business opportunities and new security threats. CISOs must strike a balance between what is needed in cybersecurity and the risks that each participant must take in order to be able to develop, with proper cybersecurity management (Burke et al., 2019). The input data that characterize the interdependence of the following factors were selected for the study:

- the level of information security of the country;

- the level of development of the country.

Stage 1. Let's define the indicators used to determine the level of information security of the country. To this end, a study of official sources in the field of information security and the results of scientific achievements of modern researchers in the field of information security (Yunis & Koong, 2015; Jazri et al., 2018; Yarovenko, 2020; Warkentin, & Orgeron, 2020; Bondarenko et al., 2021). As a result of the study, five indicators have been identified that characterize the individual components of information security, but together they can become the basis for identifying key issues and areas of information security - Fig. 5.

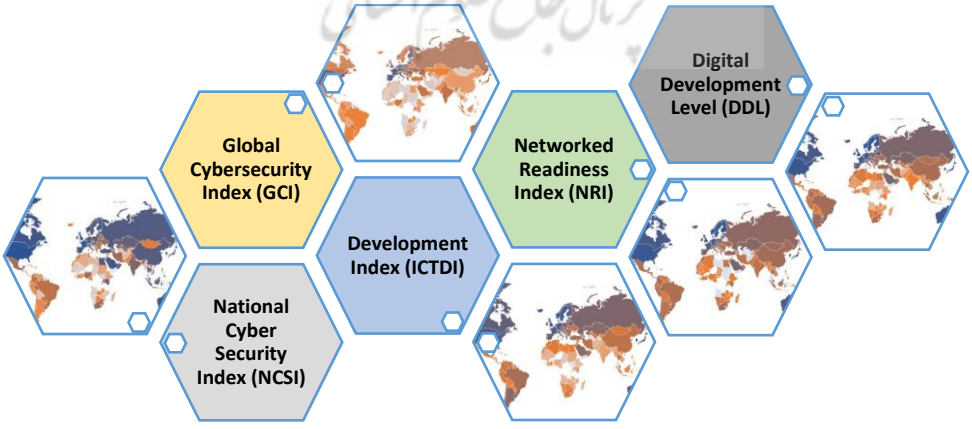


Figure 5. Information security indicators

Indicators that determine the state and prospects of information security at the macro level are as follows:

- The Global Cybersecurity Index (GCI) - characterizes the level of cybersecurity for member countries of the International Telecommunication Union;
- The National Cyber Security Index (NCSI) - determines the level of readiness of the country to counter cyber threats;
- ICT Development Index (ICTDI) - measures the level of information technology development in the country;
- Networked Readiness Index (NRI) - determines the degree of technological readiness of the country for the application of the latest information and communication technologies in various fields;
- Digital Development Level (DDL) - characterizes the level of digitalization of the country.

We propose to call the group of selected indicators that measure information security indicators of the country's digital capability and cybersecurity.

Stage 2. Let's consider each of the selected indicators - to identify problematic aspects of information security.

1) The Global Cybersecurity Index (GCI) measures the level of cybersecurity of states, as well as their readiness to prevent cyber attacks and cybercrime in five areas - technical measures, legal measures, organizational measures, capacity building, cooperation (GCI, 2020). According to the report, the top five included Britain, the United States, France, Lithuania and Estonia. The index indicators of these countries, as well as Ukraine, are presented in Figure 6.

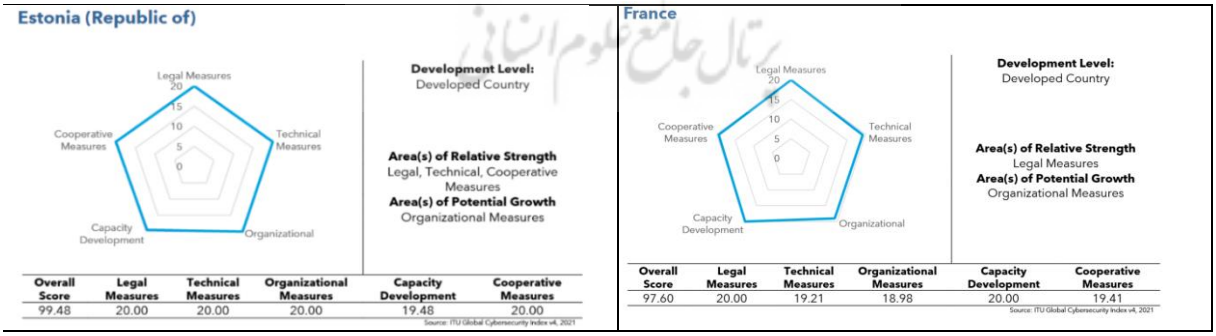
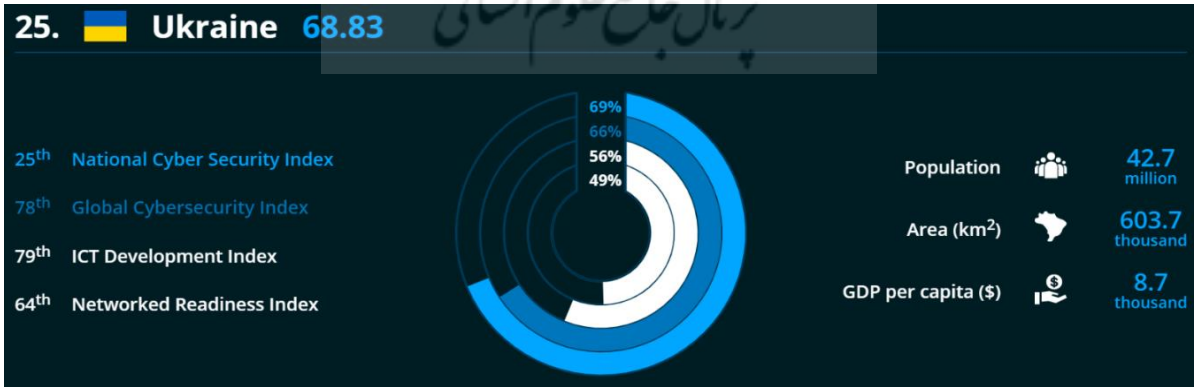


Figure 6. The Global Cybersecurity Index (GCI) of the countries with the highest level of cybersecurity, as well as Ukraine (GCI, 2020)

The experts have referred Ukraine to the group of countries that are "maturing" in the cybersecurity sector. The analysis of the data presented in the table confirms the existence of unresolved problems in Ukraine on cyber security and the need to improve both organizational, legislative and technical measures that have already been implemented in leading countries and have achieved high global index.

2) The National Cyber Security Index (NCSI) 2020 has identified Ukraine as the 25th largest country in the world (Fig. 7).



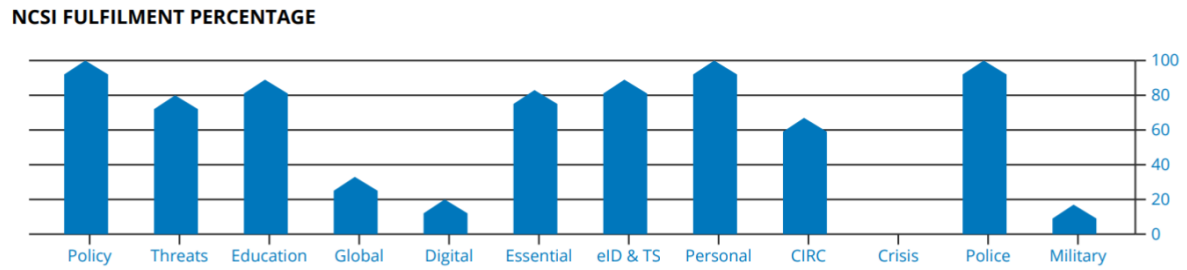


Figure 7. The National Cyber Security Index, Ukraine (NCSI, 2020)

The main problems of Ukraine in the field of security National Cyber Security is:

- weak protection of digital services;
- lack of a comprehensive cyber crisis management system.

The information security threats:

- dissemination of unreliable information;
- external influences on public consciousness;
- informational influences on immunity;
- uncontrolled activity of some mass media, etc.

If we compare the ratings of the countries on the Global Cybersecurity Index (GCI) and the National Cyber Security Index (NCSI), the data show that the GCI index of most countries has ratings above average, while NCSI - the vast majority have average values. So, obviously, the problems are related to the ability of the tools used by a particular country to overcome all kinds of cyber threats. Studies have shown that in general the general state of the national cybersecurity system is fully consistent with the level of economic development of the country. That is, there is a direct impact of the level of development on the state of information security of the country.

3) ICT Development Index (ICTDI) - an integrated indicator, calculated since 2009 on the basis of 11 indicators, which are grouped into sub-indices for three groups of processes: access to ICT, use of ICT and ICT skills. In 2018, the index was supplemented by three new indicators: subscriptions to mobile broadband Internet traffic, the percentage of mobile phone owners and the percentage of people with information and communication technology skills.

The index brings these indicators together as a single criterion that serves to compare the achievements of countries in the development of ICT and can be used as a tool for comparative analysis at the global, regional and national levels. The main goals of IDI are to measure:

- the level and evolution over time of ICT development in countries and the experience of these countries;
- progress in ICT development in both developed and developing countries;
- digital divide, ie differences between countries in terms of their level of ICT development;
- The potential for ICT development and the extent to which countries can use it to enhance growth and development in the context of existing opportunities and skills.

The process of ICT development in conjunction with the evolution of the country on the formation of the information society is a three-stage model (Fig. 8).

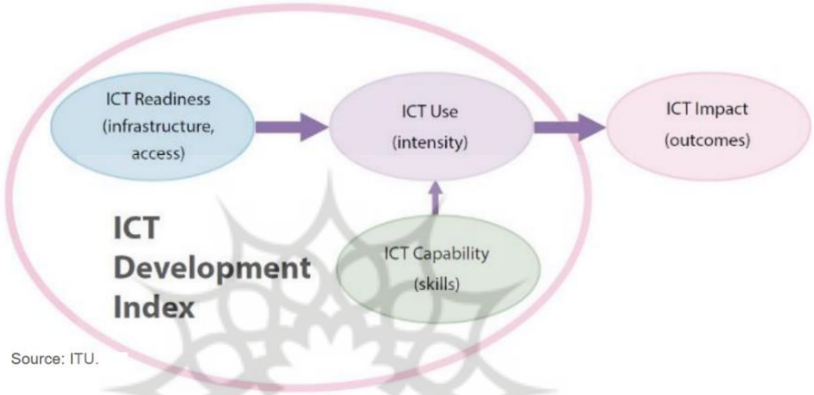


Figure 8. The model of evolution of the country - the formation of the information society

According to the presented model, the formation of the information society includes the following stages:

Stage 1: ICT readiness - reflects the level of network infrastructure and access to ICT;

Stage 2: ICT intensity - reflects the level of ICT use in society;

Stage 3: Impact of ICT - reflects the effects / results of more efficient and effective use of ICT.

Studies show that mobile and broadband Internet traffic services are available in most European countries (Figure 9).

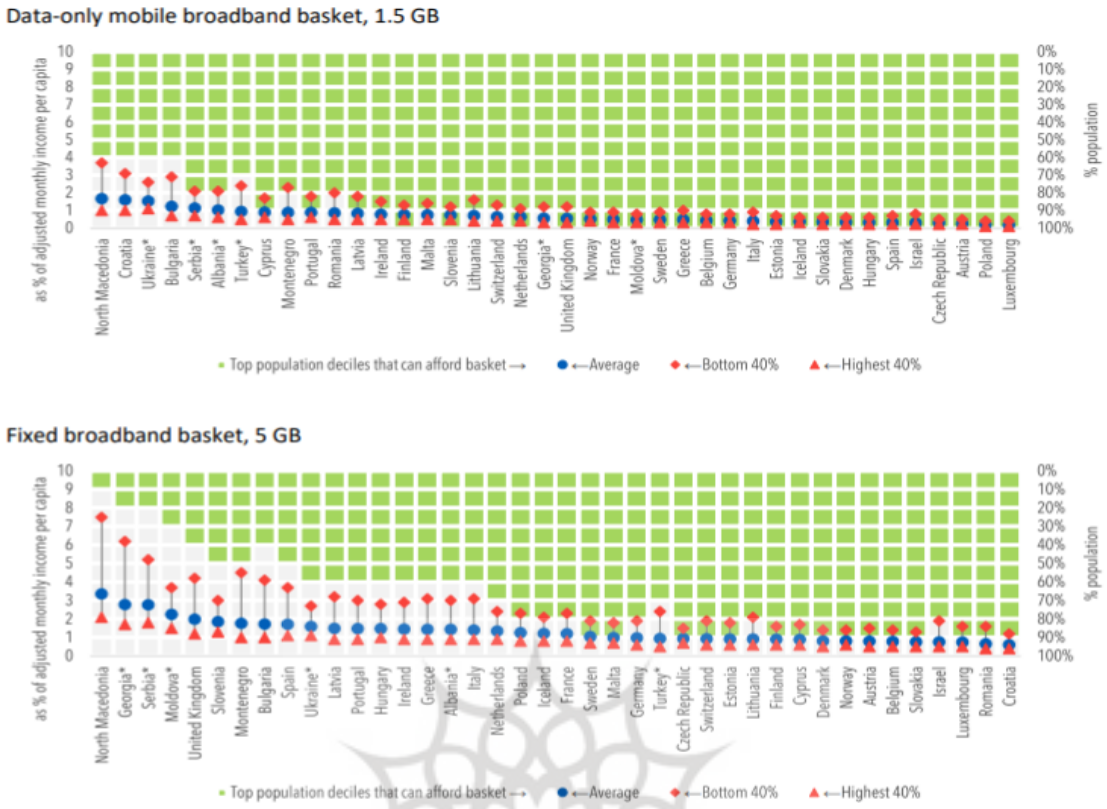


Figure 9. Availability of mobile and broadband Internet traffic services - by income level in Europe, 2020

Note: The prices in terms of adjusted monthly income per capita for the average, bottom 40 per cent and highest 40 per cent consumers are shown on the left vertical axis; every green square indicates a population decile that can afford a basket (price relative to adjusted monthly income is 2 per cent or less), conversely, every gray square indicates a population decile that cannot afford a basket.

* Data for Albania, Georgia, Moldova, Ukraine, Serbia and Turkey are based on consumption distribution.

Source: Price data from ITU and A4AI; income and consumption expenditure data from World Bank PovcalNet

As can be seen from Figure 8, the unavailability of services - due to low incomes - has already led to significant digital gaps, which inevitably affects the ability of countries to ensure their information security.

The reference mobile broadband basket was available to the entire population in 22 of the 40 countries covered. Despite the generally good state of communication in Europe, a large part of the population cannot afford broadband Internet traffic in the Eastern part of Europe: in Bulgaria and Northern Macedonia (40 percent of the population).

In Ukraine, about 30 percent of the population cannot afford any of the baskets.

4) the Networked Readiness Index (NRI) - is a comprehensive indicator that measures the level of development of ICT and digital economy in the world by 62 main parameters, which are grouped into four main groups:

A. A technologies - the level of information and communication technologies, which are a prerequisite for the country's participation in the world economy, has assessed. Namely: access opportunities (fundamental level of ICT in countries, including communication infrastructure and accessibility), content (type of digital technology produced in countries, as well as content / applications that can be deployed locally) and readiness for future technologies (countries' readiness for the future in the digital economy and new technological trends such as artificial intelligence (AI) and the Internet of Things (IoT).

B. A people - assess the willingness of citizens, business and government to use ICT (have access, resources and skills for their productive use in the economy).

C. The management - assesses the level of control over the process of transforming the economy into digital. Namely: the level of trust (cybersecurity, security and confidentiality issues), regulation (facilitating government regulation of the digital economy) and connectivity (digital divide within the country and managing to address issues such as gender inequality, disability and socio-economic status).

D. The impact - the impact of the development of ICT and digital economy on the growth of the socio-economic condition of the country and the welfare of the population has assessed. Namely, the economy (economic effect of participation in the development of the digital economy), quality of life (impact of the digital economy on the social sphere) and the country's contribution to achieving the goals of sustainable development (hereinafter - CSD) are assessed and indicators such as health, education and the environment.

The 2020 study made methodological changes to two subcomponents: trust (conceptually and significantly enhanced by the inclusion of indicators related to two aspects of digital trust: trust, environment and behavior) and the contribution to the CSR (redesigned so that each indicator was clearly tied to the specific task of the CSW: good health and well-being; quality education; gender equality; available and clean energy; sustainable cities and communities).

A significant feature of the top 10 countries (2020) is that they are successful in most NRI parameters (Table 1).

Table 1. Leading countries in terms of NRI, top 10, 2020 (NRI, 2020)

Country	NRI Rank	NRI Score	Technology	People	Governance	Impact
Sweden	1	82.75	2	4	4	3
Denmark	2	82.19	5	1	2	5
Singapore	3	81.39	10	5	13	1
Netherlands	4	81.37	3	9	3	4
Switzerland	5	80.41	1	13	10	2
Finland	6	80.16	9	3	5	9
Norway	7	79.39	11	8	1	6
United States	8	78.91	4	7	8	14
Germany	9	77.48	7	12	12	7
United Kingdom	10	76.27	8	14	14	10

In Western Europe, there is a dominance in the ranking of countries that are in the top ten ranking of countries with the most developed ICT and digital economy. Signs that distinguish the indicators of the economy with the highest rating:

- development of ICT infrastructure;
- introduction of digital innovative technologies;
- readiness of citizens, businesses and government agencies to use ICT;
- sufficiently high level of knowledge and beginners in the development of digital technologies;
- high quality of digital services;
- approaches of states in the part concerning ensuring wide access to ICT or regulation in this sphere of economic activity;
- high level of implementation of innovative technologies, such as artificial intelligence, robotics, Internet of Things, 5G, and the amount of investment directed at them.

Ukraine continues to be an outsider in the European region (+3 positions, 64th place out of 134 countries analyzed, or 49.43 points, while the average number of points in the European region is 64.21 points) (Fig. 10).

Figure 10. The Network Readiness Index, Ukraine, 2020 (NRI, 2020)

Ukraine is classified as a low-income country.

In four main groups, according to which the analysis of countries was conducted, Ukraine took:

- 62nd place or 41.51 points - in the group "Technology" (European average - 59.93 points);
- 65th place or 48.87 points - in the group "People" (European average - 59.89 points);
- 58th place or 58.19 points - in the group "Management" (European average - 72.98 points);
- 79th place or 49.16 points - in the group "Influence" (European average - 64.04 points).

According to the level of achievement of the UN Sustainable Development Goals - Ukraine ranks 91st. The weaknesses of Ukraine include:

- quality of legislation (87th place or 46.57 points), including the regulation of ICT activities (75th place or 41.66 points);
- 4G mobile coverage (129th place or 3 points);
- number of mobile broadband subscribers (102 place or 17.56 points);
- availability of clean energy (128th place or 23.7 points);
- cost of mobile phones (113 place or 21.72 points);
- low level of well-being and opportunities to freely choose the path of implementation (109 and 105 place respectively or 57.88 points);
- potential life expectancy (86th place or 58.97 points);
- low ability to use digital platforms in rural areas (93rd place or 53.97 points).

The strengths of the country include:

- the level of literacy of the adult population and legislation in the field of e-commerce (1 place or 100 points);
- number of subscribers with a speed of fixed Internet connections of 10 Mbps (16th place or 95.72 points);
- international Internet bandwidth per user (50th place or 70.28 points);
- the possibility of adapting the legal framework to new technologies (43rd place or 50.29 points);
- affordability of mobile services (46th place or 70.14 points);
- provision of primary school with the Internet (40th place or 57.79 points);
- Web services for IT hosting (34th place);
- opportunity to start a business, e-democracy, availability of innovative technologies (49th place or 53 points);
- the number of patent applications in the field of ICT (45th place);
- the level of transformation into the digital economy (36th place or 60.68 points);
- ensuring gender equality (24th place or 83.72 points);
- use of big data and professional level involved in business (31st place);
- population and the number of enrolled in higher education (14th place or 60.28 points);
- quality of education (42 place or 48.07 points).

Thus, the indicators in the NRI (2020) are directly related to the level of income. Thus, the thesis of the direct dependence of the country's ability to ensure the appropriate level of information security and the level of economic development of the country has confirmed.

5) the Digital Development Level (DDL) characterizes the level of digitalization of the country. This index has calculated as the average percentage that the country received from the maximum value of the "ICT Development Index" and the "Network Readiness Index". The comparison of countries by DDL and NCSI allows to determine the degree of digitalization of the country corresponds to the level of its cybersecurity, which contributes to the formation of recommendations for adjusting the cybersecurity program (Fig. 11).

Figure 11. The Digital Development Level (DDL), Ukraine, 2020

The results of DDL analysis indicate the following:

- developed countries are characterized by a high level of digital development;
- for most developing countries - average and above average;
- the least developed countries have a low level of digitalization.

Stage 3. Forming recommendations for adjusting the cybersecurity program.

The analysis showed a direct dependence of the country's development and its ability to ensure an adequate level of information security.

The crisis of the "digital divide" between countries deepening in the world,the threat to Internet security is growing. Thus, the “digital divide” that existed before the current global crisis, as a result of the COVID-19 pandemic, has exacerbated inequalities and drawn additional attention to the challenges of digital infrastructure, digital skills, security and safety in digital networks.

Ukraine is in dire need of systematic measures to transform the Ukrainian economy and effectively use the country's potential to increase the competitiveness of the economy and the welfare of the population.

Ukraine's weaknesses include: the quality of state institutions, political instability, imperfect legislation, including in the part related to the regulation of ICT activities, the low level of the internal market and the welfare of the population, which form the delayed demand for goods and services, including ICT services, as well as insufficient branching and innovation of telecommunication infrastructure, high cost of mobile phones compared to the income of the population, low possibility of using digital platforms in rural areas, etc.

Ukraine's strengths still remain the level of education of the population, namely: adult literacy, the percentage of those with higher education, the quality of education and the professional level of those involved in business; creativity and innovation; as well as e-commerce legislation, the possibility of adapting the legal framework to new technologies, ensuring gender equality, affordability of mobile services, ease of starting a business, e-democracy, the availability of innovative technologies and the number of patent applications in the field of ICT, the possibility of using large data, etc.

Thus, the main recommendations for Ukraine are:

1) modernization of infrastructure, acceleration of the transition to alternative energy, expansion of access to energy resources and ICT;

2) pursue a state regulatory policy in the field of ICT, which would promote digital transformation in the country, create a competitive environment for telecommunications services, including broadband throughout the country at affordable prices;

3) promote digital innovation by preserving intellectual property rights;

4) to ensure the increase of digital potential and skills of the population, as well as small business, public sector in terms of using the opportunities of digital technologies;

5) to improve the legislation in the field of rail technologies and to improve the formation of state policy in terms of the activities of the Internet of Things and the smart city;

6) ensure the protection and security of Internet connections, as well as take care of the security of users, especially children - on the Internet, detect and stop any types of abuse (which are classified as criminal activity);

7) ensure the protection of personal data from misuse by both the state and the private sector;

8) ensure systematic monitoring and collection of accurate and up-to-date data on ICT activities.

The analysis revealed the existence of potential opportunities for Ukraine to develop various components of its information security.

The digitalization is a stimulating driver for the development of the national economy, and the formation of comprehensive mechanisms for information security will have a positive impact on national security in general.

The legal bases information security in the context of digitalization

The specific features of digital transformations of technological processes in the conditions of digitalization to ensure the legal basis of information security have presented in table 2.

Table 2. The digitization of processes of providing legal bases of information security in the country

Processes, their properties	**Transformation in the context of digitalization**	**The level of legal support**
Degree of integration of processes and data	Availability of a single information space for continuous data exchange between different areas of activity, the use of Big-Data technologies and artificial intelligence	Provisions of the Doctrine of Information Security. The document defines the national interests of the country in the information sphere.
Process virtualization	Creating electronic duplicates	**Concept** information security of Ukraine**.** National Security Strategy of Ukraine. Information security strategy.
Data management	Continuous management of data about objects, throughout their life cycle, including automatic collection, accumulation, modification and analysis of information, as well as the generation of similar data	The concept of information security of public administration. Development and implementation of a coordinated information policy of public authorities.
Process management	Continuous accumulation and big data analysis (Data), including with the help of machine learning algorithms (Machine Learning), digitization makes possible advanced management	Ministries and other central executive bodies develop state target programs and other programs on the basis of sectoral strategies for the implementation of state policy in the areas of national security and defense in the manner prescribed by law.
Flexibility processes	Operational interaction geographically distributed entities via the Internet	Ensuring compliance with the Law of Ukraine "On National Security of Ukraine" regulations of ministries and other central executive bodies

The legal basis of information security of the country includes the following components, according to the levels of legal regulation:

1. The doctrine of information security is a doctrine, scientific or philosophical theory, political system, guiding theoretical or political principle, or normative formula of regulatory and normative-legal influence on the level of information security. It should usually be taken for up to 20 years of implementation.

2. The concept - system of views, one or another understanding of phenomena and processes; the only, defining idea of information security. The concept is a surrogate form of theory, the purpose of which is the integration of a certain body of knowledge, in an effort to use it to explain, search for patterns of information security and the process of ensuring the appropriate level. It must be approved by a Resolution of the Verkhovna Rada of Ukraine for a period of 10 years.

3. The strategy information security - a general, non-detailed plan of a particular activity, which covers a long period, a way to achieve a complex goal. Approved by the Decree of the President of Ukraine and, as evidenced by international practice, for the period of his tenure as President.

4. A program- pre-approved (defined) action. Approved by decisions of central executive bodies for 1 year with certain tactical methods of its implementation.

5. A tactics - a conceptual action that has carried out in the form of one or more specific tasks.

Thus, the basis of ensuring the information security of the country is the formed information security policy. Such a policy has based on theoretically applied and scientifically sound theories of its provision, of which there are currently many. The government adopts legal provisions on the basis of their theoretical justification, which leads to the emergence of relevant ministries and eclectic regulations.

The information security, as defined in the draft Information Security Strategy, is an integral part of Ukraine's national security, the state of protection of vital interests of man, society and the state, which establishes an effective system of protection and combating harm through the spread of negative information influences, including coordinated dissemination.

The legal basis for ensuring information freedom is informational legal relations. This isregulated by law social relations arising in the process of interaction of subjects, on the implementation of their goals to meet the interests of having the necessary information, to transfer some available information to other entities, as well as to preserve such information and protect it from unauthorized influence of others parties.

To realize the interests of the subjects of public relations, the object of which is information, a necessary condition is a stable and secure functioning of the information infrastructure of society. The composition of the information infrastructure and the content of social relations that arise in connection with its use have determined by the level of development of society, its economic capacity to implement the results of scientific and technological progress. The Figure 12 shows the components of the information infrastructure.

Figure 12. The components of the information infrastructure in the information security system

The modern information infrastructure includes the following components:

1) organizational and managerial:

- bodies and services - ensure the functioning of technological and information elements of the infrastructure;
- media - for transmitting information to large groups of people, reaching out to a mass audience, accessibility to many people, dissemination of information;
- organizations that provide information services - intermediaries to meet the information needs of consumers interested in specific information;

2) technological

- networks and objects of communication, telecommunications;
- means of automation of management of social and technological processes, automation of data processing, computer networks and systems;

3) information

- information systems, including in the form of library, archival and museum funds;
- websites, Internet resources.

The legal aspects of such relations are due, on the one hand, the significant social importance of interactions, and on the other - the difficulty of achieving the desired social result without the state. The information legal relations are directly related to the object of information security (Fig. 13).

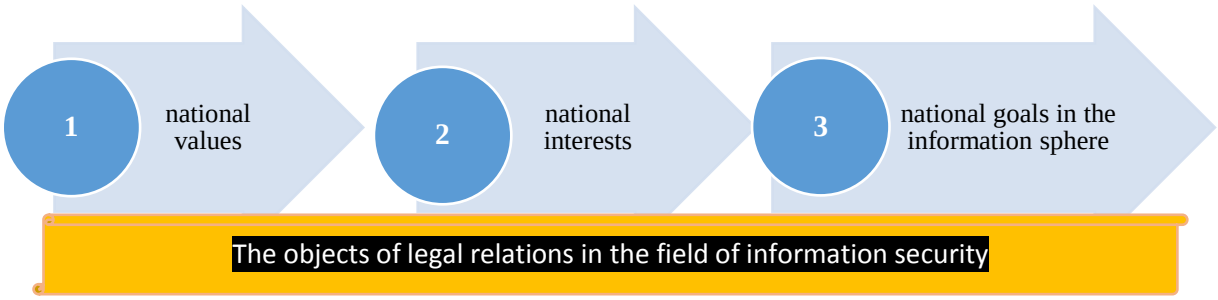


Figure 13. The objects of legal relations in the field of information security

Thus, the objects of legal relations in the field of information security are: national values, national interests, national goals in the information sphere - the content of each of the selected objects is enshrined in legislation.

The legal basis of relations in the field of information security is the Constitution of Ukraine, the laws of Ukraine, the National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine of September 14, 2020 № 392/2020 "On the decision of the National Security and Defense Council of Ukraine of September 14, 2020."

On the National Security Strategy of Ukraine ", the Cyber Security Strategy of Ukraine was approved, as well as international agreements, the binding nature of which was approved by the Verkhovna Rada of Ukraine. At present, the Information Security Strategy has not been approved in Ukraine.

According to the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" (№ 2163), strategic management and coordination of cybersecurity agencies is entrusted to the National Security and Defense Council of Ukraine, which reports to the Center for Cyber Threat Response in the State Special Service. The latter should develop a comprehensive system of cybersecurity of strategic objects and monitor the activities of companies that audit such strategic objects.

The State Center for Cyber Attack Response is subordinated to the State Special Communications Service, and its unit, CERTUA, monitors and identifies potential cyber threats. The Cyber Police of Ukraine is responsible for the prevention and investigation of cybercrime. The Ministry of Defense and the General Staff provide protection for military facilities and critical infrastructure during war and emergency. The SBU prevents terrorist attacks in cyberspace and has the right to inspect critical infrastructure. The list of facilities belonging to the critical infrastructure has determined by the Cabinet of the Ministers of Ukraine, and cybersecurity in the banking sector is taken care of by the National Bank of Ukraine. However, the law does not define the areas of responsibility between the various state and law enforcement agencies.

Despite Ukraine's relatively high NCSI rating, the National Security and Defense Council of Ukraine (NSDC) reported that as of August 2020, there were approximately 1 million cyber threats, including network attacks, network scan attempts, WEB-attack attempts, phishing, and widespread denial attacks in the maintenance ('DDoS') and distribution of malicious software.

It is advisable to consider the experience of the most successful countries in the world in the field of information security. The foreign experience shows that the institutional and functional support of cybersecurity involves two main areas: the formation of cyberpolice units, expanding their competence and the establishment of the National Cybersecurity Centers. The organizational measures to ensure information security, which were carried out in economically developed countries include:

- formation of a cybersecurity system;
- creation of cyber command and cyber troops;
- creation of a system of training highly qualified specialists in the field of cybersecurity;
- organizational, legislative and technical support for the actions of cyber units;
- scientific support, development and implementation of the latest technological developments;
- strengthening control over the national cyberspace, increasing the number of cyberspace units.

The technical measures include:

- conducting cyber exercises;
- research and development of new types of offensive, defensive and reconnaissance cyber weapons.

To ensure cybersecurity, the International Telecommunication Union (INU) has developed a global cybersecurity program. According to this program, each state cooperating with INU must have a national computer incident response team - CERT.

Today there are 305 CERT teams in 66 countries. For example, in the USA - 72 teams, in Japan and Germany 23 teams each in Lithuania - 5, in Russia and Poland 2 teams each. They coordinate the actions of state computer security units of state authorities, telecom operators, as well as other subjects of information infrastructure to stop violations related to unauthorized interference in the work of information, telecommunications and information and telecommunications systems and networks. Let's analyze the formation of a cybersecurity system in the leading countries of the world (table 3).

Table 3. Experience of countries in the formation of cybersecurity

Country	Characteristics of the cybersecurity system
France	Five main directions are introduced in relation to: general stability; fight against cybercrime; cybersecurity issues under the Common Security and Defense Policy; industrial issues; international policy in the field of cyberspace. An in-depth review of its defense and national security policies was conducted in 2008 and 2013 and new priorities were identified: preventing and responding to cyberattacks. In 2009, the French Network and Information Security Agency (ANSSI) and the National Information Security Agency were established as an inter-ministerial agency. This agency is part of the Prime Minister's Office, is a national body for the protection of information systems.
Japan	On June 10, 2013, the Information Security Policy Council adopted the Cyber Security Strategy of Japan. The strategy aims to develop "world-leading", "sustainable" and "dynamic" cyberspace and to transform Japan into a world leader in cybersecurity. The state body that regulates cybersecurity in Japan is the National Center for Information Security (NISC), which develops draft government standards for information security measures, formulates recommendations based on the results of cybersecurity assessments, and promotes cybersecurity measures.
South Korea	Prospects in the system of cyberspace protection in South Korea are: encryption for network access; creation of an intrusion prevention system (IPS); expanding threat resilience (APT); internet security. There are three institutions in South Korea to address cybersecurity issues: the National Cybersecurity Center; Korean Internet Security Agency (KISA); Cyber Terror Response Center of the National Police Agency. These agencies are responsible for detecting, preventing and responding to cyber attacks and security threats. In addition, a school specializing in cyberwarfare and training security experts has been established.
The United Kingdom of Great Britain and Ireland	The United Kingdom is the country with the highest global cybersecurity index. The UK uses two ways to tackle cyberspace vulnerabilities: disclosing the vulnerability so that it can be captured and benefit global technology users; maintain knowledge of this vulnerability and use it in the future for intelligence purposes to disrupt the activities of those seeking damage in the United Kingdom. A board of leading world experts from three agencies (GCHQ, NCSC and the Ministry of Defense) has been established. The UK-established National Center for British Cybersecurity is the most efficient and fifth in the world.
Finland	The cybersecurity strategy was adopted in 2013. The National Cyber Security Center has been operating in Finland since 2014. Activities are aimed at ensuring security in cyberspace, providing guaranteed protection and access to users of information and communication networks of general and special communication, overcoming cyber threats.

The analysis of organizational measures in the world's leading countries on the formation of cybersecurity shows that they implement appropriate cybersecurity measures, have their own strategies, defense and national security policies, created new agencies, national centers, teams to respond to computer incidents. Such organizational structures are able to coordinate the actions of state units of computer security of public authorities, telecom operators, as well as other subjects of information infrastructure and the team to respond to computer incidents - CERT.

For Ukraine, 2020 was a year of active initiation of cybersecurity reform (SSSCIP, 2021). One of the key goals for 2021 is:

- introduction of measures to protect critical infrastructure (IP) and critical information infrastructure (CII);

- introduction of new standards and best world practices in the field of cyber attack prevention and protection of IP & CII;
- conducting protection audits and continuous monitoring of cybersecurity using sensor infrastructure and 24/7 response to cyber incidents.

In October 2020, the Government of Ukraine adopted two key regulations governing IP facilities (№ 1109, 2020) and CII objects (№ 943, 2020). In December 2020, the Government by its resolution (№ 1295,2020) determined the order of functioning of systems for detecting vulnerabilities and responding to cyber incidents and cyber attacks. Basically, this procedure is aimed at establishing a system for responding to cyber incidents at state-owned facilities.With the transfer of banking services to an online format, risks and cyber threats have increased significantly. The response to this situation was the Resolution of the National Bank of Ukraine (№151, 2020), which defines the means of CII in the banking system of Ukraine.

For Ukraine, accelerating the optimization of the institutional system of cybersecurity is an effective tool that provides for two key areas: legal and organizational. The legal - initiative development of the necessary regulatory framework and its continuous improvement in order to form the relevant legal norms, which have reflected in the Cyber Security Strategy and the Law of Ukraine "On the basic principles of cyber security of Ukraine". The organizational - in improving the efficiency of responsible institutional structures - cybersecurity entities, ministries, other central executive bodies and civil society institutions by increasing their capacity, eliminating duplication in the exercise of their powers, joining forces under the auspices of the working body of the National Security and Defense Council of Ukraine - National Coordination Center for Cyber Security, taking into account the best practices of international and European experience in this field.

Conclusion

This study examines the main aspects implementation legal mechanisms for information security in the context of digitalization. It has proved that the problems of ensuring the country's information security have related to the ability of the means used by a particular country to overcome various types of cyber threats. The studies have shown that in general, the general state of the national cybersecurity system is fully consistent with the level of economic development of the country. That is, there is a direct impact of the level of development on the state of information security of the country. The analysis shows that the most significant mutual influence is demonstrated by a group of indicators of the state's institutional capacity and a group of indicators of the digital capacity of the national economy and cybersecurity. A significant obstacle is the low level of information infrastructure of society, which is also due to the level of development of society, its economic capacity to implement the results of scientific and technological progress. The objects of legal relations in

the field of information security are: national values, national interests, national goals in the information sphere - the content of each of the selected objects is enshrined in legislation. An important component of the development of legal and institutional support for cybersecurity in Ukraine is:

- development of new national standards in the field of cybersecurity, in particular the implementation of the international standard ISO 27001;
- development of organizational and technical model of cyber defense;
- planning and ensuring the implementation of measures to implement the Cyber Security Strategy - the National Cyber Security Coordination Center should coordinate their implementation and monitor the implementation and effectiveness;
- constant monitoring and obligatory annual publication of a public report on the status of implementation and implementation of the Cyber Security Strategy according to general estimates;
- introduction of coordinated detection and disclosure of vulnerabilities of information and communication systems;
- unification of information exchange formats and expansion of the information exchange network on cyber attacks, cyber incidents and cyber threat indicators based on the technological platform of the National Cyber Security Coordination Center, with integrated participation of all government agencies and critical infrastructure facilities;
- introduction of mechanisms to encourage the private sector, the scientific community, public organizations and individuals to participate in the formation and implementation of measures to ensure cybersecurity of the state;
- introduction of mandatory provision of real-time information on cyber attacks and cyber incidents by all departmental and sectoral (sectoral) centers to the National Cyber Security Coordination Center;
- introduction of mechanisms for timely identification of cyber threats, detection of cyberattacks for the purpose of operative and adequate response to them and fast restoration of stable work on their consequences;
- introduction of a national program to identify vulnerabilities in information and communication systems;
- conducting on a regular basis an audit of the security of communication and technological systems of critical infrastructure facilities for vulnerabilities, etc.

Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article

References

Anderson, R., Moore, T. (2006). Economics of information security. Science, 314 (5799), 610-613.

Babenko, V. (2020). Enterprise Innovation Management in Industry 4.0: Modeling Aspects. Emerging Extended Reality Technologies for Industry 4.0: Early Experiences with Conception, Design, Implementation, Evaluation and Deployment Collective monograph. Ed. by Jolanda G. Tromp et al. A John Wiley & Sons, Inc., Publication, 1-24. https://doi.org/10.1002/9781119654674.ch9

Bekmuratov, T. F., Ganiev, A. A., & Botirov, F. B. (2020). Concept of establishing multiagent intellectual automatically systems in the enterprise. International Journal of Scientific and Technology Research, 9(4), 347-352. http://www.ijstr.org/paper-references.php?ref=IJSTR-0420-34436.

Bondarenko, S., Halachenko, O., Shmorgun, L., Volokhova, I., Khomutenko, A. & Krainov, V. (2021). The Effectiveness of Network Systems in Providing Project Maturity of Public Management. TEM Journal, 10(1), 358- 367. https://doi.org/10.18421/TEM101-34

Bondarenko, S., Tkachuk, H., Klochan, I., Mokhnenko, A., Liganenko, I., Martynenko, V., (2021). Modeling of economic security of the enterprise at change of investment maintenance. Studies of Applied Economics, 39(7), 1- 19, https://doi.org/10.25115/eea.v39i7.5011.

Bondarenko, S., Rusavska, V., Niziaieva, V., Manushkina, T., Kachanova, T. & Ivaniuk U. (2021). Digital Logistics in Flow Management in Tourism, Journal of Information Technology Management, Special Issue, 1-21. https://10.22059/JITM.2021.80734

Brožova, H., Šup, L., Rydval, J., Sadok, M., & Bednar, P. (2016). Information security management: ANP based approach for risk analysis and decision making. Agris On-line Papers in Economics and Informatics, 8(1), 13-23. Retrieved from https://ideas.repec.org/a/ags/aolpei/233959.html

Burke W., Oseni T., Jolfaei A., Gondal I. (2019). Cybersecurity Indexes for eHealth. In Proceedings of the 2019 Australasian Computer Science Week Multiconference, ACSW 2019 (Australia, Sydney, January, 2019). ACM International Conference Proceeding Series, 17, 1-8. https://dl.acm.org/doi/10.1145/3290688.3290721.

D'elia, D. (2018).Industrial policy: the holy grail of French cybersecurity strategy? Journal of Cyber Policy, 3 (3) , pp. 392-413.

Dincelli, E. (2018). The role of national culture in shaping information security and privacy behaviors. In D. Siegel (Ed.), World Scientific Reference on Innovation: Volume 4: Innovation in Information Security, 47-68. https://doi.org/10.1142/10209

Dorosh, M., Voitsekhovska, M., & Balchenko, I. (2019). Research and Determination of Personal Information Security Culture Level Using Fuzzy Logic Methods. In Proceedings of the 2nd International Conference on Computer Science, Engineering and Education Applications, ICCSEEA 2019 (Ukraine, Kiev, 29 March 2019), Advances in Intelligent Systems and Computing, Volume 938, 503-51). https://doi.org/10.1007/978-3-030-16621-2_47

e-Governance Academy Foundation. (NCSI, 2020). National Cyber Security Index. NCSI : website. URL: https://ncsi.ega.ee/ncsi-index/.

Global Cybersecurity Index (GCI, 2020). International Telecommunication Union : website. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx .

Hrabovskyi, Y., Babenko, V., Al'boschiy, O., Gerasimenko, V. (2020). Development of a Technology for Automation of Work with Sources of Information on the Internet. *WSEAS Transactions on Business and Economics*, 17(25), 231-240. https://doi.org/10.37394/23207.2020.17.25

Hubanova, T., Shchokin, R., Hubanov, O., Antonov, V., Slobodianiuk, P. & Podolyaka, S. (2021). Information technologies in improving crime prevention mechanisms in the border regions of southern Ukraine. Journal of Information Technology Management, Special Issue, 75-90. https://doi.org/10.22059/JITM.2021.80738

Iatsyshyn, A. V., Kovach, V. O., Romanenko, Y. O., Deinega, I. I., Iatsyshyn, A. V., Popov, O. O., . . . Lytvynova, S. H. (2020). Application of augmented reality technologies for preparation of specialists of new technological era. Paper presented at the CEUR Workshop Proceedings, , 2547 181-200.

Jazri H., Zakaria O. & Chikohora E. (2018). Measuring cybersecurity wellness index of critical organisations. 2018 IST-Africa Week Conference, IST-Africa 2018 (Botswana, Gaborone, May 2018). Institute of Electrical and Electronics Engineers Inc., 1-8.

Kirilenko, V. P., & Alexeyev, G. V. (2018). Political technologies and international conflicts in the information space of the Baltic Sea region. Baltic Region, 10(4), 20-38. https://doi.org/10.5922/2079-8555-2018-4-2

Kirkham, T., Winfield, S., Ravet, S., Kellomaki, S. (2013). The personal data store approach to personal data security IEEE Security & Privacy, 11 (5) , 12-19

Ključnikov, A., Mura, L., & Sklenar, D. (2019). Information security management in smes: Factors of success. Entrepreneurship and Sustainability Issues, 6(4), 2081-2094. https://doi.org/10.9770/jesi.2019.6.4(37)

Klochan, V., Piliaiev, I., Sydorenko, T., Khomutenko, V., Solomko, A. & Tkachuk A. (2021). Digital Platforms as a tool for the transformation of strategic Consulting in Public Administration. Journal of Information Technology Management, Special Issue, 42-61. https://doi.org/10.22059/JITM.2021.80736

Klyaus, T. K., & Gatchin, Yu. A. (2020). Mathematical model for information security system effectiveness evaluation against advanced persistent threat attacks. Paper presented at 2020 Wave Electronics and its Application in Information and Telecommunication Systems, WECONF 2020 (Russian Federation, Saint-Petersburg, 1-5 June 2020), Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/WECONF48837.2020.9131540

Kosevich, E. (2020). Estrategias de seguridad cibernetica en los paises de America Latina [Cyber security strategies of Latin America countries]. Iberoamerica, 1, 137-159. (In Spanish). https://doi.org/10.37656/S20768400-2020-1-07

Krasnobayev, V.A., Yanko, A.S., Koshman, S.A. (2016). A Method for Arithmetic Comparison of Data Represented in a Residue Number System. Cybernetics and Systems Analysis, 52(1), 145-150.

Krasnobaev, V., Kuznetsov, A., Babenko, V., Denysenko, M., Zub, M., and Hryhorenko, V. (2019). The Method of Raising Numbers, Represented in the System of Residual Classes to an Arbitrary Power of a Natural Number, 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), July 2-6, Lviv, Ukraine, pp. 1133-1138. https://doi.org/10.1109/UKRCON.2019.8879793

Kuznetsov, A., Shekhanin, K., Kolhatin, A., Kovalchuk, D., Babenko, V., Perevozova, I. (2019). Performance of Hash Algorithms on GPUs for Use in Blockchain. *2019 IEEE International Conference on Advanced Trends in Information Theory*, ATIT 2019 – Proceedings Kyiv, Ukraine, pp. 166-170. https://doi.org/10.1109/atit49449.2019.9030442

Kuznetsov, A., Smirnov, O., Gorbacheva, L., Babenko, V. (2020). Hiding data in images using a pseudo-random sequence. *CEUR Workshop Proceedings*, 2608, pp. 646-660.

Li, J., Shen, S., Sun, X. & Xing, X. (2021). Identification and classification for risk paths in the context of cross-border important data flow. Chinese Journal of Management Science, 29 (3), 90-99.

Marhasova V., Kovalenko Yu., Bereslavska O., Muravskyi O., Fedyshyn M., Kolesnik O. (2020). Instruments of Monetary-and Credit Policy in Terms of Economic Instability. *International Journal of Management*, 11 (5), 43–53 URL: http://surl.li/koqs

On approval of the Procedure for reviewing the state of cyber protection of critical information infrastructure, state information resources and information, the requirement for protection of which is established by law [Pro zatverdzhennia Poriadku provedennia ohliadu stanu kiberzakhystu krytychnoi informatsiinoi infrastruktury, derzhavnykh informatsiinykh resursiv ta informatsii, vymoha shchodo zakhystu yakoi vstanovlena zakonom] (2020). Resolution of the Cabinet of Ministers of Ukraine, 11.11.2020, № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text (in Ukrainian).

On approval of the Regulations on the definition of critical infrastructure in the banking system of Ukraine [Pro zatverdzhennia Polozhennia pro vyznachennia obiektiv krytychnoi infrastruktury v bankivskii systemi Ukrainy] (2020). Resolution of the Board of the National Bank of Ukraine, 30.11.2020, № 151. URL: https://zakon.rada.gov.ua/laws/show/v0151500-20#Text (in Ukrainian).

On the basic principles of cybersecurity in Ukraine: the Law of Ukraine, 05.10.17, № 2163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

Romanenko, Y. O., & Chaplay, I. V. (2016). Marketing communication system within public administration mechanisms. Actual Problems of Economics, 178(4), 69-78.

Sagan, O., Yakovleva, S., Anisimova, E., Balokha, A., & Yeremenko, H. (2020). Digital didactics as a new model in the theory of education. Revista Inclusiones, 7 num Especial, 193-204.

Singh, A. N., & Gupta, M. P. (2019). Information Security Management Practices: Case Studies from India. Global Business Review, 20(1), 253-271. https://doi.org/10.1177/0972150917721836

Some critical infrastructure issues [Deiaki pytannia obiektiv krytychnoi infrastruktury] (2020). Resolution of the Cabinet of Ministers of Ukraine, 9.10.2020, № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text (in Ukrainian).

Some issues of critical information infrastructure [Deiaki pytannia shchodo obiektiv krytychnoi informatsiinoi infrastruktury] (2020). Resolution of the Cabinet of Ministers of Ukraine, 9.10.2020, № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text (in Ukrainian).

Some issues of ensuring the functioning of the system for detecting vulnerabilities and responding to cyber incidents and cyberattacks [Deiaki pytannia zabezpechennia funktsionuvannia systemy vyiavlennia vrazlyvostei i reahuvannia na kiberintsydenty ta kiberataky] (2020). Resolution of the Cabinet of Ministers of Ukraine, 23.12.2020, № 1295. URL: https://www.kmu.gov.ua/npas/deyaki-pitannya-zabezpechennya-funkcionuvannya-sistemi-viyavlennya-vrazlivostej-i-reaguvannya-na-kiberincidenti-ta-kiberataki-i231220-1295 (in Ukrainian).

State Special Communications Service of Ukraine (SSSCIP, 2021). SSSCIP : website. URL: https://cip.gov.ua/en.

THE NETWORK READINESS INDEX 2020 Accelerating Digital Transformation in a post-COVID Global Economy. URL: https://networkreadinessindex.org/wp-content/uploads/2020/10/NRI-2020-Final-Report-October2020.pdf.

Topa, I., & Karyda, M. (2019). From theory to practice: guidelines for enhancing information security management. Information and Computer Security, 27(3), 326-342. https://doi.org/10.1108/ICS-09-2018-0108.

Zavhorodnii, A., Ohiienko, M., Biletska, Y., Bondarenko, S., Duiunova, T. & Bodenchuk, L. (2021). Digitization of agribusiness in the development of foreign economic relations of the region. Journal of Information Technology Management, Special Issue, 123-141. doi: 10.22059/JITM.2021.82613

Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. International Journal of Information Management, 52, 102090. https://doi.org/10.1016/j.ijinfomgt.2020.102090

Yanko, A., Koshman, S., Krasnobayev, V. (2018). Algorithms of data processing in the residual classes system 2017 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2017 – Proceedings 2018-January, 117-121.

Yarovenko, H. (2020). Evaluating the threat to national information security. Problems and Perspectives in Management, 18(3), 195-210. https://doi.org/10.21511/ppm.18(3).2020.17.

Yunis M.M. & Koong K.S. (2015). A conceptual model for the development of a national cybersecurity index: An integrated framework. 21st Americas Conference on Information Systems, AMCIS 2015 (Puerto Rico, El Conquistador Resort and Convention CenterFajardo). AMCIS URL: https://aisel.aisnet.org/amcis2015/ISSecurity/GeneralPresentations/44/.

Bibliographic information of this paper for citing:

Bondarenko, S.; Makeieva, O;, Usachenko, O.; Veklych, V.; Arifkhodzhaieva, T. & Lernyk, S. (2022). The Legal Mechanisms for Information Security in the context of Digitalization. *Journal of Information Technology Management*, 14 (Special Issue), 25-58. https://doi.org/ 10.22059/jitm.2022.88868