JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2020 March Volume 9 Number 3
https://doi.org/10.9770/jssi.2020.9.3(8)

Scopus®

STATE INFORMATION SECURITY AS A CHALLENGE OF INFORMATION AND COMPUTER TECHNOLOGY DEVELOPMENT

Kateryna Chyzhmar[1], Oleksii Dniprov[2], Oksana Korotiuk[3], Roman Shapoval[4], Olga Sydorenko[5]

*[1]*Institute of Law and Postgraduate Education of the Ministry of Justice of Ukraine, Sychovych Streltsivtsiv St., 73, Kyiv, 04053, Ukraine*
[2]Head of the Office of the President of Ukraine, st. Bankova, Kyiv, 11, 01220, Ukraine
[3]Dnipropetrovsk State University Interior, Gagarin Avenue, 26, Dnipro, 49005, Ukraine
[4,5]Yaroslav Mudryi National Law University, 77 Pushkinskaya Street, Kharkiv, 61024, Ukraine

*E-mail: [1]*koaduep@gmail.com (Corresponding author)*

Received 10 February 2019; accepted 10 January 2020; published 30 March 2020

Abstract. The article is devoted to study of information security as a challenge of modern development of information and computer technologies. It was found that achievement of a satisfactory level of information security, which is a state of safety of balanced important interests of an individual, society and state against internal and external threats in the information sphere, is possible based on economic, organizational, technical, legal, psychological and other methods. Existing threats to the information security in Ukraine have been identified. The concept and essence of hybrid war as one of the threats to protection of information interests of an individual, society and the state are considered separately. A conclusion was made about the expediency of supplementing the Information Security Doctrine of Ukraine with such a threat as a hybrid war, which actually takes place in the east of the country. A system of information security components in Ukraine has been disclosed, among which a particular attention has been paid to the Ministry of Information Policy of Ukraine and the State Agency for Electronic Governance of Ukraine. In order to improve the mechanism of protection of the information space of Ukraine, it is proposed to differentiate at the legislative level the concepts of "information security" and "cybersecurity", since their understanding is the basis for the formulation and implementation of the state information policy, improve international cooperation between states to exchange experience, as well as to involve general public to protect the information space.

Keywords: information; information system; information space; information and computer technologies; information security; hybrid war.

Reference to this paper should be made as follows: Chyzhmar, K., Dniprov, O., Korotiuk, O., Shapoval, R., Sydorenko, O. 2020. State information security as a challenge of information and computer technology development. *Journal of Security and Sustainability Issues,* 9(3), 819-828. https://doi.org/10.9770/jssi.2020.9.3(8)

JEL Classifications: F35, F42

1. Introduction

Expanding the use of information technologies, being a positive factor for development of the economy and improvement of functioning of civil and governmental institutions, simultaneously creates new challenges and threats to the national security.

For example, the UN in the Agenda for Sustainable Development till 2030 recognizes that the proliferation of information and communication technologies and global interconnection of networks, as well as scientific and technological innovations in such diverse fields as medicine and energy, offer tremendous opportunities for accelerating human progress, bridging the digital gap and shaping a knowledge-based society, as well as for development. The agenda calls for a significant increase in access to information and communication technolo-

gies and for universal and affordable access to the Internet in the least developed countries by 2020 (UN General Assembly resolution "Transforming our world: the 2030 Agenda for Sustainable Development", 2015).

At the same time, the spread of information technology and access to the Internet create significant threats to the information space of each country in particular and the world at large. So, as of 2015, Ukraine was ranked 5th in the global web-risk ranking, following the attack of Petya virus this year, which affected energy companies, banks, government sites, etc., the anti-rating of our country in cybersecurity issues has significantly increased.

According to official information and the Internet sources, due to "Petya" virus, Ukraine's automotive business alone suffered 20 million euros in damages. As for the whole world, the numbers are no less shocking. According to the International Monetary Fund report as per the expert estimates, economic losses from the attack of the virus "NotPetya" amounted to $850 million, and losses from all global cyberattacks amount to $53 billion.

All this is a clear testimony that the existing on national and international levels tools for protection of the information space from contemporary threats need to be updated, and the policies of all countries need to be consolidating towards development of quality standards for information space security, software that should be used by government structures, establishment of appropriate government agencies responsible for policy formulation and implementation in this field. Given the large number of issues that exist today and the magnitude of economic losses from cyberattacks, it is obvious that studying information security of a country as a challenge for the development of information and computer technologies is quite relevant (Korauš, et. Al., 2019).

2. Literature Survey

Before starting to address issues of information security, it is worth noting that, despite the demand for the problem in sociopolitical discourse, many authors point out that it is poorly highlighted in the scientific literature. While a great deal of attention has been paid to information security in the technical and economic disciplines in recent years, there is a lack of relevant research in the social sciences and humanities (Durmanov et. al., 2019 a,b).

Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri define information security as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction to ensure confidentiality, integrity and accessibility. Accordingly, information by scientists is facts or ideas that can be presented (coded) in the form of various forms of data; knowledge (e.g. data, instructions) on any medium or in any form that may be communication between the entities of the system (Nieles, Dempsey, Pillitteri, 2017).

It should be agreed with Alhassan Mohammed and Adjei-Quaye Alexander that information security is of great importance today and is of interest to everyone in the world of technology, be it mobile or PC users, which is why information security is important in our daily lives and in IT industry. The range of issues that information security entails, respectively, necessitates demand for professionals with knowledge of information security. For example, a cyber-security analyst, a forensic analyst, network administrators, system administrators, software developers, and these are only part of those professionals who are in constant demand with the IT development. In this case, lack of knowledge in the field of information security and competent specialists will more likely lead to insecurity of information from unauthorized penetration of attackers (Mohammed, Adjei-Quaye, Alexander, 2017).

Today, as Awad Ali points out, information security includes the use of authentication and authorization, network security, hardware, secure software, data cryptography, etc. Moreover, information security is a crucial component in the protection of almost all information transactions, and recently, with spread of information and communication technologies, information security has also begun to embrace new areas of increasing demand, including cloud computing, smart cities, telemedicine, wireless sensor networks (Ali, 2018; Sitdikova & Starodumova, 2019).

The need for information security has also arisen in the field of the introduction of such a tool as electronic declaration (Reznik, et.al., 2019). Leonov S., Yarovenko H., Boiko A., Dotsenko T. emphasize the necessity of introduction of financial monitoring information system, which will increase efficiency of the bank operation by studying all banking operations without exception, accelerate detection of suspicious activities, which will give the bank management an opportunity to reduce reputational risk and minimize losses associated with payment of a fine imposed by regulatory authorities (Leonov, et.al., 2019).

The opinion of Mykola Syomych, Iryna Markina and Dmytro Diachkov is also of interest, that there is currently a sharp rise in information security incidents that are widespread and are of significant threat to a wide range of private, corporate and public interests. The main trends in the development of the above-mentioned threats, as noted by scientists, are the following:

(1) increase in the number of cyberattacks, many of which lead to significant losses;

(2) increasing complexity of cyberattacks, which may include several steps using special methods of protection against possible countermeasures;

(3) impact of cyberattacks on most electronic (digital) devices;

(4) increasing the number of cyberattacks on information infrastructure of large corporations, important industrial sites and even governmental structures;

(5) use of different tools and methods of cyberattacks on the most advanced countries in the field of computer technology (Syomych, Markina, Diachkov, 2018).

Pelevina E.S. notes that the problem of information security is closely linked to the concepts of "international security" and "economic globalization". Thus, a key need of the state system is the need to provide conditions necessary for its functioning and development. The rapid proliferation of weapons of mass destruction puts the world community at risk of securing and maintaining peace. The system of international law thus legally enshrined the need for peace as a global fundamental interest and placed a legal obligation on countries to uphold the idea of peace between different countries (Pelevina, 2017).

International information security, in accordance with the United Nations terminology, means protection of the global information system against terrorist, criminal and military-political threats. The discussion of this issue, raised at the Information Community and Development Conference held in Midrand (South Africa) from 13 to 15 May 1996, led to the adoption in 1998 of Resolution 53/70 at the 53rd session of the United Nations General Assembly "Advances in Information and Telecommunications in the Context of International Security". This resolution acknowledged for the first time at the highest international level the possibility of the negative consequences of the spread and use of information technologies and tools. In this context, concerns were also raised that such technologies and facilities could be used for purposes incompatible with international security and stability. Later, similar resolutions were adopted by the UN General Assembly within several years (Pelevina, 2017).

3. Methods

Given the above, it is difficult to identify one of the methods of protecting the information space of the country. However, there should be a comprehensive approach that will include economic, legal, organizational, technical and psychological methods:

(1) the essence of economic methods lies in the understanding that information is a resource that ensures development of the society and the state, and therefore the priority of the state in the direction of information space security is to finance innovation in the control of information flows and protect information from distortion or destruction;

(2) software is developed, maintained and updated by organizational and technical methods;

(3) legal methods are aimed at normative provision of information security while maintaining the balance between state control over protection of classified information and freedom of speech, free information to citizens, respect for human and citizen's rights and freedoms during military operations;

(4) psychological methods are used to counteract information and psychological aggression in the early stages of information warfare, prevention and prediction of cases of information and psychological aggression.

4. Results

The state information security provides protection of information and information systems from inappropriate and unauthorized activities. Therefore, it is advisable to note that the provisions of the national laws, in particular the Law of Ukraine "On Information" of 1992, which divides information depending on its content into the following types: (1) personal information; (2) reference and encyclopedic information; (3) environmental information (information on ecology); (4) product information (work, service); (5) scientific and technical information; (6) tax-related information; (7) legal information; (8) statistical information; (9) sociological information; (10) other types of information (Law of Ukraine on Information, 1992).

Based on this understanding of types of information, another legal act - the Law of Ukraine "On Basic Principles of Information Society Development in Ukraine for 2007-2015" of 2007 is the only normative act that contains the following definition of information security: "it is a state of protection of vital interests a person, society and the state, in order to prevent damage caused by incomplete, untimely and unreliable information used; negative information impact; negative consequences of the use of information technologies; unauthorized dissemination, use, breach of integrity, confidentiality and accessibility of information "(Law of Ukraine on Basic Principles of Information Society Development in Ukraine for 2007-2015, 2007).

Although Ukrainian legislation contains a definition of "information security", it is appropriate to note that in most post-Soviet and European countries its understanding is somewhat narrower, though similar. For example, the definition of information security in the Republic of Belarus is given in Article 4 of the National Security Concept adopted November 9, 2010 as a state of protection of balanced interests of the individual, society and the State against internal and external threats in the information sphere (National Security Concept of the Republic of Belarus, 2010).

In addition to the concept of "information security", the Doctrine of Information Security of Ukraine of 2017 relates the following to the current threats to the national interests and national security of Ukraine in the information sphere: (1) conducting special information operations aimed at undermining defensive potential, demoralization of the armed forces of Ukraine and other military units, provoking extremist manifestations, fueling panic moods, exacerbating and destabilizing socio-political and socio-economic situation, fueling ethnic and inter-religious conflicts in Ukraine; (2) conducting special information operations in other countries by the aggressor state in order to create a negative image of Ukraine in the world; (3) information expansion of the aggressor state and its controlled entities, in particular by expanding its own information infrastructure on the territory of Ukraine and in other countries; (4) information domination of the aggressor state on the temporarily occupied territories; (5) insufficient development of the national information infrastructure, which limits Ukraine's ability to counteract information aggression effectively and proactively perform in the information sphere to realize Ukraine's national interests; (6) inefficiency of the state information policy, imperfection of legislation regarding regulation of public relations in the information sphere, uncertainty of strategic narrative, (7) insufficient level of media culture of the society; (8) proliferation of calls for radical action, promotion of isolationist and autonomous concepts of coexistence of regions in Ukraine (Doctrine of Information Security of Ukraine, 2017).

At the same time, the place of Ukraine in the regional and world rankings indicates that the above threats do have a negative impact on the information space in the country. Thus, according to the World Cyber Security

Index 2017, Ukraine is not in the last place among the post-Soviet states, however, it is also difficult to state the level of information security in the country (Table 1).

Table 1. Post-Soviet states in the Global Cybersecurity Index, 2017

Country	Index	World rating
Georgia	0.819	8
Russia	0.788	10
Belarus	0.592	39
Azerbaijan	0.599	48
Ukraine	0.501	59
Moldova	0.418	73
Kazakhstan	0.352	83
Tajikistan	0.292	91
Uzbekistan	0.277	93
Kirgizstan	0.270	97
Armenia	0.196	111
Turkmenistan	0.133	132

At the same time, the list of threats to the state's information security, as set out in the Doctrine of Information Security of Ukraine of 2017, is not exhaustive. In particular, the by-law does not take into account such threat to the national security in the sphere of information interests as the information expansion of the aggressor state and its controlled structures. Such threat is now defined by the term "hybrid war", which is actually used to characterize the current state of information security in eastern Ukraine.

The term "hybrid war" was first coined by Frank G. Hoffman, who used this term to characterize international conflicts that did not fit the traditional notion of waging a war. He also noted that hybrid threats are a combination of traditional and irregular tactics and strategies for warfare; involve non-governmental actors along with the use of simple and sophisticated technologies. The traditional forms of war are mixed with cyberwarfare, organized crime, irregular conflicts, terrorism.

We can also find other definitions of hybrid war in scientific literature: (a) it is an irregular war that allows use of different methods of combat at the same time and involves adaptation of the armed forces to new conditions; (b) it is a military strategy which, in addition to the conventional war, includes cyber war and involves use of nuclear, biological and chemical weapons, improvised explosive devices and information warfare; (c) it is a deliberate process of establishing external control by one entity over another, establishing total control over the area of management where information plays a crucial role (Antonyuk & Malskyy, 2016).

Speaking about hybrid war, one should agree with Anzhela Parulu that in the context of hybrid wars, all the basic information methods and tools of conventional wars are used. Hybrid war contains both military and civilian components. Certainly, the emergence of hybrid war as a new form of conflict fundamentally alters the established security architecture and casts doubt on the possibilities of existing security guarantees (Parulua, 2018).

Presently, hybrid war actually takes place in the temporarily occupied territories in Donetsk and Luhansk regions, and therefore the legislator has made an attempt to normatively regulate the specifics of state policy for securing state sovereignty in these territories by adopting the relevant law in 2018. According to this law, to ensure national security, in particular state, economic, informational, humanitarian and environmental in the Donetsk and Luhansk regions, the security and defense sector bodies, other state bodies of Ukraine, their officials take measures to restore territorial integrity of Ukraine, and provide comprehensive development of secure, economic, information-telecommunication, social and humanitarian infrastructure in the territories adjacent to the temporarily occupied territories in Donetsk and in the Luhansk regions, implement, in accordance

with the strategic defense planning documents, measures to strengthen the defense and security capabilities of Ukraine (Law of Ukraine on Features of State Policy for Ensuring the State Sovereignty of Ukraine in the Temporarily Occupied Territories in Donetsk and Luhansk Regions, 2018).

This regulatory act raises several questions, although some of them answers in part. First, it is still unclear why the legislator still does not include in the list of threats to information security the hybrid war in eastern Ukraine, and secondly, which subjects the legislator meant by pointing to the security and defense sector, other Ukrainian state authorities and their officials. Considering the above mentioned when considering information security of the state and the national and globalization aspects it is necessary to pay attention also to the subjects responsible for ensuring information security.

So, the decision of the National Security and Defense Council of Ukraine "On measures to improve formation and implementation of the state policy in the field of information security of Ukraine" of 2014 gives grounds to conclude that the subjects of information security in Ukraine are: (a) the Cabinet of Ministers of Ukraine; (b) the Security Service of Ukraine; (c) the State Special Communications and Information Protection Service of Ukraine; (d) Ministry of Foreign Affairs of Ukraine; (e) State Border Guard Service of Ukraine; (f) State Migration Service of Ukraine.

Without going into a detailed analysis of the role of each of these entities in protecting the information space from inappropriate and unauthorized activities, we suggest to emphasize only some of them. In particular, presently in Ukraine an important part of the tasks in the domain of protection of the state interests in the information sphere is entrusted to the Ministry of Information Policy of Ukraine, which, in accordance with the provision approved by the resolution of the Cabinet of Ministers of Ukraine of 2015, is responsible for:

(1) ensuring formation and implementation of the state policy in the areas of information sovereignty of Ukraine and information security of the state, in particular on issues of dissemination of socially important information in Ukraine and abroad;

(2) ensuring formation and implementation of the state policy in the field of state foreign language broadcasting;

(3) ensuring development of a system of the state strategic communications in Ukraine;

(4) ensuring implementation of mass media reforms in Ukraine on the dissemination of socially important information (Regulation on the Ministry of Information Policy of Ukraine, 2015).

However, other central executive authorities responsible for formation and implementation in other spheres also have powers in the area of information space protection. First of all, it should be noted that the State Border Service of Ukraine and the State Migration Service of Ukraine are taking measures to protect the national security of Ukraine in the information sphere when addressing issues related to residency in the territory of Ukraine of foreigners and stateless persons (journalists, cameramen, other media workers). In its turn the Ministry of Foreign Affairs of Ukraine takes measures to establish international cooperation on counteracting negative information-psychological influences and cybercrime (Decision of the National Security and Defense Council of Ukraine on measures to improve formation and implementation of the state policy in the field of information security of Ukraine, 2014).

The State Agency for Electronic Governance of Ukraine is also tasked with counteracting information threats and ensuring information security in the country. According to the Regulations on the State Agency for Informatization, approved by the Cabinet of Ministers of Ukraine in 2014, the agency:

(a) conducts digital expertise and prepares conclusions for draft regulatory acts on informatization, formation and use of national electronic information resources, development of information society, e-democracy, provision of administrative services, digital development;

(b) carries out activities, within the powers provided for by the law, related to information system of electronic interaction of state electronic information resources;

(c) informs the public about the state of development of the information society and promotes its benefits (Regulation on the State Agency for Informatization, 2014).

That is, the analysis of the above allows to conclude that Ukraine is making steps towards creating conditions for proper protection of the information space of the state, specialized normative legal acts are adopted, entities responsible for formulating and implementing state policy in the information sphere, etc. are in place, but not all scientists agree that it is sufficient.

Thus, Mykola Buchyn and Yuliia Kurus point out that despite Ukraine's significant steps towards counteracting the country's information security threats, it still lags in this direction. Accordingly, the scientists propose to build the information security strategy in several levels.

Therefore, the first level should cover the following information policy tools:

(1) Involvement of the world community and world public opinion to identify the aggressor and its devastating consequences;

(2) informing the world community about enemy attacks and the objective situation in own country;

(3) strengthening counter-propaganda, national information space and formation of the operational information centers;

(4) ban on mass media in the territory belonging to the aggressor's information space in order to avoid propaganda and destructive influence on citizens;

(5) maintaining a stable state of information security and a positive image of the country;

(6) collaboration and exchange of experience with international organizations on combating cyberattacks and information threats.

The second level, in turn, is quite extensive and combines the system of public administration and national information infrastructure, the country's overall defense capability, its ability to withstand aggressive attacks and maintain information, territorial, economic, socio-political, cultural integrity of the country. With regard to the third level, the involvement of the public in supporting stability of socio-political development and consolidation of citizens in general is essential here. An important role at this level also belongs to the media, which have all the tools to protect information and counteract the information war on Ukraine (Buchyn & Kurus, 2018).

5. Discussion

In today's globalization, the issue of counteracting cyberattacks as a threat to information security has become extremely acute. Indeed, cyberattacks today are capable of causing significant damage and destabilizing information space of the country. All this led to highlight the concept of "cybersecurity". At the same time, some scientists believe that cybersecurity is a component of information security, which only relates to counteracting malicious activity in electronic networks, while others give a broader definition to the concept of cyber security, such that is identical with the concept of information security.

To substantiate their opinion, G.V. Foros and K.S. Kondrashev point out that cybersecurity is first and foremost the security of information and information infrastructure in the digital environment, while information security is ensuring confidentiality, integrity of information and a number of related information processes (Foros

& Kondrasheva, 2016).

Also interesting is the position of Rossouw von Solms and Johan van Niekerk, who also differentiate between cybersecurity and information security, emphasizing that cybersecurity is the protection of cyberspace, electronic information, information-computer technologies which support cyberspace and human user of the cyberspace. While information security is protection of any information and taking measures to ensure compliance with the rules for obtaining, using and disclosing restricted information, secret information, etc. This leads to the conclusion that the term "cyber security" is different in its meaning from the definition of "information security" (Solms & Niekerk, 2013).

In turn, Rachana Buch, Dhatri Ganda, Pooja Kalola, Nirali Borad also approach cybersecurity as a set of tools, policies, security concepts, security guarantees, guidelines, risk management approaches, actions, best practices, technologies that can be used to protect the cyber environment (Buch, et.al., 2017).

With these considerations, it is necessary to distinguish between cyber security and information security at the legislative level, especially since one of the threats to the information security of the state under the State Information Security Doctrine is the uncertainty of the strategic narrative. According to the above, it is obvious that the proper understanding of these categories by the legislator will become the basis for the development and implementation of the state information security strategy, which in future will allow to minimize threats to the information interests of the country.

Conclusions

Thus, the issue of information security of the country as a state of protection of vital interests of the individual, society and the country, which prevents damage due to incompleteness, untimely and unreliable information used, negative information impact, negative consequences of the use of information technology, unauthorized dissemination, use, violation of integrity, confidentiality and accessibility of information is relevant both in national and globalization aspects.

At the same time, the level of information security in Ukraine cannot yet be considered satisfactory, notwithstanding the availability of relevant legal acts and the emergence of new entities in the system of information space protection of the state, namely the Ministry of Information Policy of Ukraine, the State Agency for Electronic Governance of Ukraine, today there are a number of threats to the information interests of the country. Such threats include information expansion of the aggressor state, insufficient development of the national information infrastructure, inefficiency of the state information policy, imperfection of legislation regarding regulation of public relations in the information sphere, insufficient level of media culture of the society, etc. A significant place in the list of threats belongs directly to the hybrid war, and therefore today the priority of the state is countering the negative tendencies of the hybrid war in the east of Ukraine. Moreover, it is crucial to strengthen international cooperation in this area with the aim of sharing experiences and involving the public in the protection of the information space.

In order to increase the level of information security of the state, the authorized entities should not only use the appropriate information policy tools, but also expand the information infrastructure to increase the state's ability to withstand aggressive attacks, especially in the east of Ukraine, where due to armed conflict information infrastructure is damaged, destroyed or under the authority of the aggressor state, and to involve citizens in maintaining stability of the information space of the country, including media, etc.

References

Alhassan, Mohammed, Adjei-Quaye, Alexander (2017). Information Security in an Organization. *International Journal of Computer (IJC)*. 24(1), 100–116.

Awad, Ali (2018). Introduction to information security foundations and applications. Information Security: *Foundations, Technologies*

and Applications, Edition: First, Chapter: 1, Publisher: The Institution of Engineering and Technology (IET), Editors: Ali Ismail Awad and Michael Fairhurst. http://doi.org/10.1049/PBSE001E_ch

Decision of the National Security and Defense Council of Ukraine "On measures to improve the formation and implementation of state policy in the field of information security of Ukraine" (2014). URL: https://zakon.rada.gov.ua/laws/show/n0004525-14.

Durmanov, A., Bartosova, V., Drobyazko, S., Melnyk, O., Fillipov, V. (2019). Mechanism to ensure sustainable development of enterprises in the information space. *Entrepreneurship and Sustainability Issues*, 7(2), 1377-1386. http://doi.org/10.9770/jesi.2019.7.2(40)

Fopoc G.B. Kondpasheva K.C. (2016). Information Society and Cyber Security. Cybersecurity in Ukraine: legal and organizational issues: materials in Ukraine. bp. conf. 233 c.

Global Cybersecurity Index (2017). URL: https://digital.report/globalnyiy-indeks-kiberbezopasnosti-ot-itu-gruziya-i-rossiya-voshli-v-top-10/#prettyPhoto

Korauš, A., Gombár, M., Kelemen, P., Backa, S. (2019). Using quantitative methods to identify insecurity due to unusual business operations, *Entrepreneurship and Sustainability Issues* 6(3): 1101-1012. http://doi.org/10.9770/jesi.2019.6.3(3)

Law of Ukraine «On Features of State Policy for Ensuring State Sovereignty of Ukraine in Temporarily Occupied Territories in Donetsk and Luhansk Oblasts» (2018). URL: https://zakon.rada.gov.ua/laws/show/2268-19

Law of Ukraine "On Basic Principles of Information Society Development in Ukraine for 2007-2015" (2007).

Law of Ukraine "On Information" (2014). URL: https://zakon.rada.gov.ua/laws/show/2657-12

Leonov, S., Yarovenko, H., Boiko, A., Dotsenko, T. (2019). Information system for monitoring banking transactions related to money laundering. *CEUR Workshop Proceedings*, 2422, pp. 297-307.

Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri (2017). An Introduction to Information Security. *NIST Special Publication.* DOI: https://doi.org/10.6028/NIST.SP.800-12r1

Mykola Buchyn, Yuliia Kurus (2018). Russian Information War against Ukraine: Peculiarities and Mechanisms Of Countering. *Political Science*, 4(1), 55-62 https://doi.org/10.23939/shv2018.01.055

Natalya Antonyuk, Markiyan Malskyy (2016). Russia's Hybrid Warfare Against Ukraine In The Context Of European Security. *Visnyk of the Lviv University. Series International Relations,* 38, 23–42.

National Security Concept of the Republic of Belarus (2010) URL: http://mvd.gov.by/en/main.aspx?guid=14961

Parulua, A. (2018). Hybrid Warfare – Contemporary Concept in Georgia's External Security. URL: https://pdfs.semanticscholar.org/8960/ce273c800c7f5bdf6e2ab96579ffc5905bb5.pdf

Pelevina E.S. (2017). Political problems of international relations, global and regional development. *Theories and Problems of Political Studies*, 6(1A), 194–205.

Presidential Decree No. 47/2017 "On the Decision of the National Security and Defense Council of Ukraine of December 29, 2016" On the Doctrine of Information Security of Ukraine "(2017). URL: https://www.president.gov.ua/documents/472017-21374

Rachana Buch, Dhatri Ganda, Pooja Kalola, Nirali Borad (2017). World of Cyber Security and Cybercrime. *Recent Trends in Programming Languages* 4(2), 18–23.

Resolution of the Cabinet of Ministers of Ukraine "Issues of activity of the Ministry of Information Policy of Ukraine" (2015).

Resolution of the Cabinet of Ministers of Ukraine "On Approval of the Regulations on the State Information Agency" (2014). URL: https://zakon.rada.gov.ua/laws/show/492-2014-%D0%BF

Reznik, O.M., Shendryk, V., Zapototska, O., Popovich, E., Pochtovyi, M. (2019). The features of e-declaration as an effective tool to prevent corruption. *Journal of Legal, Ethical and Regulatory Issues*, 22 (Special Issue 2), 6 p.

Rossouw von Solms, Johan van Niekerk (2013). From information security to cyber security. *Computer and Security,* 38, 97–103.

Syomych, M., Markina, I., Diachkov, D. (2018). Cybercrime as a leading threat to information security in the countries with transitional economy. *Advances in Social Science, Education and Humanities Research.* 2nd International Conference on Social, economic, and academic leadership, 217, 342–350.

UN General Assembly Resolution on Transforming Our World: A Sustainable Development Agenda for 2030 (2015). URL: https://daccessods.un.org/TMP/931266.397237778.html

URL: https://zakon.rada.gov.ua/laws/show/2-2015-%D0%BF

URL: https://zakon.rada.gov.ua/laws/show/537-16

Kateryna CHYZHMAR, Doctor of Juridical Sciences, Associate Professor, Institute of Law and Postgraduate Education of the Ministry of Justice of Ukraine
ORCID ID: orcid.org/0000-0003-4569-8863

Oleksii DNIPROV, Head of the Office of the President of Ukraine
ORCID ID: orcid.org/0000-0003-2587-4412

Oksana KOROTIUK, Candidate of Juridical Sciences , Dnipropetrovsk State University Interior
ORCID ID: orcid.org/0000-0001-5471-6432

Roman SHAPOVAL, Doctor of Jurisprudence, Professor, Yaroslav Mudryi National Law University
ORCID ID: orcid.org/0000-0002-4312-7826

Olga SYDORENKO, Candidate of Juridical Sciences ,Yaroslav Mudryi National Law University
ORCID ID: orcid.org/0000-0002-0282-2775