Artículo de investigación

Information security and means of its legal support

Seguridad de la información y medios de apoyo legal

Segurança da informação e meio de seu suporte jurídico

Recibido: 26 de febrero de 2019. Aceptado: 5 de abril de 2019

Written by:
Evgen Kharytonov[83]
https://orcid.org/0000-0001-5521-0839
Olena Kharytonova[84]
https://orcid.org/0000-0002-9681-9605
Yuliia Tolmachevska[85]
https://orcid.org/0000-0002-7964-8875
Bondan Fasii[86]
https://orcid.org/0000-0002-8715-930X
Maxym Tkalych[87]
https://orcid.org/0000-0003-4224-7231

Abstract

The article is devoted to the consideration of the problem of legal regulation of relations on the provision of information security in the world. The author also raises questions of informational propaganda. The article introduces the author's concept of information hygiene. As a result of the research carried out, the author came to the conclusion that it is necessary to introduce legal regulation of information relations both at the international and national levels.

Keywords: Security, information security, IT sphere, legal regulation, information hygiene, civil society, legal norm.

Resumen

El artículo está dedicado a la consideración del problema de la regulación legal de las relaciones en la provisión de seguridad de la información en el mundo. El autor también plantea cuestiones de propaganda informativa. El artículo introduce el concepto del autor de higiene de la información. Como resultado de la investigación realizada, el autor llegó a la conclusión de que es necesario introducir una regulación legal de las relaciones de información tanto a nivel internacional como nacional.

Palabras claves: Seguridad, seguridad de la información, ámbito de TI, regulación legal, higiene de la información, sociedad civil, norma legal.

Resumo

O artigo é dedicado à consideração do problema da regulação legal das relações sobre a prestação de segurança da informação no mundo. O autor também levanta questões de propaganda informacional. O artigo introduz o conceito de higiene da informação do autor. Como resultado da pesquisa realizada, o autor chegou à conclusão de que é necessário introduzir uma regulação legal das relações de informação tanto no nível internacional quanto nacional.

[83] Doctor of Law Science - Professor of Civil Law Department National University «Odesa Law Academy»- Corresponding Member National Academy of Law Sciences of Ukraine - Honored Science and Technology Worker of Ukraine- Head of Civil Law Department National University «Odesa Law Academy» Ukraine, Odesa.
[84] Doctor of Law Science - Professor of Intellectual Property and Corporate Law Department National University «Odesa Law Academy» - Corresponding Member National Academy of Law Sciences of Ukraine- Honored Science and Technology Worker of Ukraine- Head of Intellectual Property and Corporate Law Department National University «Odesa Law Academy» Ukraine, Odesa
[85] Master of Law (National University «Odesa Law Academy») Ukraine, Odesa, Academicheskaya
[86] PhD. Assistant professor of Civil Law Department National University «Odesa Law Academy». Ukraine, Odesa.
[87] PhD. Assistant professor of Civil Law Department Zaporizhzhia National University (Ukraine, Zaporizhzhia)

Palavras-chave: Segurança, segurança da informação, esfera de TI, regulação legal, higiene da informação, sociedade civil, norma jurídica.

Introduction

Information security threats can be created by using IT for espionage (Ukrainian Week, 2015), as well as through malicious use of social networks by foreign intelligence agencies.

Some of these threats are aimed at harming the fundamentals of national security, since administrators of such communities sometimes act on the instructions of curators from foreign intelligence agencies, disseminate information calling for the overthrow of the constitutional order, changing the borders of Ukraine, and promoting terrorist organizations. In addition, threats arise as a result of recruiting people through social networks, where recruiters study a person by the profile in a social network: they learn about her views, values, psychological peculiarities, and then, having analyzed them, they use it when recruiting Information security threats should also include offenses (first of all, crimes) in the Network committed with the use of information technology or having objects of intrusion into the system, theft of information (information, data, etc.).

Methodology

The social and legal nature of information security was considered on the basis of the laws and special and scientific literature analysis. Social relations arose in the sphere of information security were material for study.

In the process of research, general scientific and special methods were used. Methodological basis for study was a dialectical method that allowed to review the issues in their development and interconnection. Methods of analysis and synthesis were used to determine the nature of information security as an object of civil legal relations.

The formal and logical method was used to formulate the definition of information security. Using the structural and functional approach, the functions of information security were determined. Experience of providing information security in different legal systems was reviewed using comparative and legal method. Historical method used in historical aspects study related to information security appearance and formation.

Analysis of recent research and publications

There are many publications, touching upon different aspects of information security nowadays. We can mention the ground research of Mica R. Endsley named «Combating Information Attacks in the Age of the Internet: New Challenges for Cognitive Engineering». This article provides an overview of the characteristics of misinformation and information attack and their effects on the perceptions of the public, with the objective of outlining potential solutions and needed research for countering this growing problem (Endsley, 2018).

The article «Information security conscious care behaviour formation in organizations» by Nader Sohrabi Safaa, Mehdi Sookhaka, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani, Tutut Herawan deals with the problem of users' behavior in the internet. The authors claim, that hackers use different methods to change confidentiality, integrity, and the availability of information in line with their benefits, while users intentionally or through negligence are a great threat for The results of structural equation modelling (SEM) showed that Information Security Awareness, Information Security Organization Policy, Information Security Experience and Involvement, Attitude towards information security, Subjective Norms, Threat Appraisal, and Information Security Self-efficacy have a positive effect on users' behaviour. However, Perceived Behavioural Control does not affect their behaviour significantly. The Protection Motivation Theory and Theory of Planned Behaviour were applied as the backbone of the research model. information security (Safa, Sookhaka, Solms, Furnell, Ghani & Herawan, 2015).

The research «Collective Data-Sanitization for Preventing Sensitive Information Inference Attacks in Social Networks», fulfilled by Zhipeng Cai, Zaobo He, Xin Guan, Yingshu Li, deals with the problem of releasing of private data in social networks. In this paper, the authors explore how to launch an inference attack exploiting social networks with a mixture of non-sensitive attributes and social relationships. To protect against such attacks, the authors propose a data sanitization method collectively

manipulating user profile and friendship relations (Cai, He, Guan & Li, 2018).

Presentation of key research findings

To begin with, without stopping at the numerous theories and concepts of the information society (Pilipchuk & Dzoban, 2014), we note that it is understood in narrow and wide meanings.

In the narrow meaning, the information society – is: 1) a society in which the production, distribution, and consumption of information is the main area of activity; 2) a new type of society, formed as a result of the explosive development and convergence of information and communication technologies, in which the main condition of well-being is knowledge, the unrestricted access to information and the ability to work with it a global society in which the exchange of information has no limits; which promotes interpenetration of cultures, at the same time giving each community new opportunities for self-identification; 3) the type of post-industrial society, the condition of formation of which are high-tech global information networks, where information is considered as a commodity, the main social value.

In a wide meaning, the information society – is a component of a civil society that functions within a single information and communication space, which is dominated by new technological patterns based on the massive use of information technologies, computer technology and telecommunications, and created a qualitatively new knowledge market. and information as the determinants of the production of information resources and their transformation into real resources of socio-economic development, as well as meeting the needs of society and the individual in information products, services, etc. (Popova & Lipkan, 2016).

For practical reasons, one can restrict itself to a brief definition of the information society as a phase of the evolutionary development of civilization, in which information, and knowledge are produced by using information and communication technologies in a single information space.

In any way, the keywords of the concept of "information society" are: "information" and "society".

At the same time, it should be noted that, although the information field, according to Krifa Koch, is not unique to biological organisms, but exists generally in the universe as such (God is everywhere, n.d.), but with the current level of knowledge, the influence on this field with a view to its ordering is really possible only in part of its biologically (human) substrate.

It is important not only to define "information", "information technology", etc., but an "information society" (which, in particular, was reflected in the UN General Assembly resolution of March 27, 2006, proclaimed May 17 as the International Day for the Information Society). These circumstances are due to the task of studying information asecuration in the information society.

Considering information as a concept inherent in modern information (post-industrial) society, one can not overlook its relationship with another popular concept - "civil society", whose development in Ukraine in today's conditions has become one of the real factors behind the emergence of a difficult situation that has developed.

At the same time, we must take into account that modern civil society is created with the help of certain forms of self-constitution and self-mobilization. It is institutionalized and generalized through the mediation of laws and, in particular, the consolidation of subjective rights that stabilize social differentiation. Self-creation (independent activity) and institutionalization do not necessarily involve each other. But being independent, separated, in the long run, both these processes constitute an indispensable condition for the reproduction of civil society (Koen & Arato, 2003). In civil society, citizens are not the subjects of political-power relations and public law, but private individuals with their interests, subjects of private law, participants in civil-legal relations.

At the same time, we should also speak about the emergence of a new type of person, the existence of high requirements of civil society for its citizens, which distinguish them among people... The basis of civil society is law-conscious citizens and their voluntary associations, the existence of which is regulated not by political power, but by self-government, free expression of citizens and legal law. Civil society has a complex and fluid-structure: it is a complex of social groups, individuals, their associations and institutions (family, school, church, voluntary associations, clubs, unions, public organizations, movements, political parties), whose cooperation is regulated by law (BIlenchuk, Gvozdetskiy & Slivka, 1999).

The essence of civil society is that it is the result of reconciling the interests and relationships that are formed between private individuals and their established associations that exist and operate in a market environment.

Civil society is characterized by the following: 1) it is the result of a contract (consensus) between private individuals; 2) it arises and exists on the basis of liberalism; 3) it exists in the conditions of a developed civilized market; 4) it adheres to the formula of freedom expressed as the social imperatives of democracy; 5) it is the basis of the relationship between people's activity of a democratic and liberal nature; 6) it is considered primarily as a phenomenon of behavioral and institutional; 7) it is not an object of public administration, claiming, on the contrary, to provide the state with the conditions for its functioning and life.

One can agree with the understanding of civil society as a whole sphere of public life, relatively independent from state institutions and from the mechanism of state power. Civil society – is a unique system of interaction between social individuals, social groups, layers and strata, which balances the vectors of its components, виявляючи рівнодіючу безлічі індивідуальних і групових прагнень та сподівань. The social system, by its operation, objectively reproduces social imperatives in the political system, simultaneously precipitating the formation of such state forms that would be able to respond adequately to the objective interests of society (Pasko, I.T. & Pasko, Ya.I., 1999).

Information society plays an important role in information and communication technologies that allow collecting, processing, receiving and transmitting information at the local, national and international levels. The leading place among such technologies is the Internet - the global telecommunication network, which appeared in 1969 and actively develops, starting with the 80s of the XX century. The main purpose of the Internet is to disseminate information among users, sharing such information. It is a unique means of communication that does not know the temporal and spatial boundaries because the exchange of information occurs lightning and regardless of distance and boundaries. The World Wide Web has undergone three stages in its development.

The first phase is associated with Web 1.0, functionally limited to giving users the ability to read information and buy things.

The onset of the second phase (Web 2.0) dates back to the early 2000s when more powerful websites and more reliable web infrastructures appeared due to IT development, which allowed users not only to consume information from the Internet but also to publish it. At this stage, the Network has become something bigger than a giant shopping mall and online encyclopedia, turning into a place where people could do a variety of activities (Shmidt & Rozenberg, 2016).

With this stage, we can associate the formation of an interactive civil society, which is understood as the system of interaction of free citizens and their voluntary associations through the Internet, in which information is the main factor of socialization, in order to create a mechanism for the implementation and protection of fundamental human rights and freedoms, satisfaction of individual and group aspirations and expectations, influence on the power state institutions, direction of state development in general.

The categories «information society», «information», «information security» and «IT sphere» are correlated to each other, that is, inextricably linked concepts, where each change in one of them leads to a change in another. This necessitates considering them in terms of communication and interaction, which we will do next.

Let's start with the fact that the term «information» affects many phenomena (sometimes related to each other, and sometimes related only to the appearance) that exist in various fields and are accompanied by interpretations and estimates from different angles of view. This makes it virtually impossible for a single approach to its characteristics, which is drawn attention in reference and educational publications (Kormich, 2011).

Therefore, for practical reasons, we restrict ourselves to the simplified basic definition of «information», considering further its properties from the angle of view of the peculiarities of legal regulation of its relations.

However, it should be noted that there were two approaches to understanding information: 1) distributing and 2) narrowing (qualifying).
The first of these is based on the widest possible understanding of information. So, according to Art. 1 of the Law of Ukraine of October 2, 1992

«On Information», information is any information and/or data that can be stored on physical media or displayed in an electronic form.

An example of a «narrowing (qualifying) approach» may be the understanding of information as new information, taken, understood and rated by the user as useful. In other words, the knowledge received by the consumer (subject) as a result of the perception and processing of certain information (https://uk.m.wikipedia.org/wiki/інформація).
In domestic law, this approach was reflected in the original wording of Art. 200 of the Civil Code of Ukraine in 2003, where it was determined that the information is documented or publicly disclosed information about events that have or have occurred in society, the country, and the environment. Under the implication of this norm was the assumption that it refers to information that constitutes real or potential «personal» (as information about a person) or «commercial» value (as information about the property status of a person).

Such an approach significantly narrowed the notion of information, since it could only be regarded as such if there were a number of features specified in the law (Article 226 of the Civil Code of Ukraine).

However, recently the «distribution» approach prevails, as a result of which the vision of the essence of information is significantly liberalized.

In particular, the transformation of the vision of the essence of information as an object of civil rights reflected in the modernization of Art. 200 of the Civil Code of Ukraine, which now, in the wording of the Law of January 13, 2011, states that the information contains any information and/or data that can be stored on tangible media or displayed electronically.

Thus, in order for the information to be an object of law at the moment, no novelty, value or relevance, nor a special content nor a special form is required of it.

The decisive thing is that it is:

1) any information and/or data, that is, information as such;
2) this information and/or data may be recorded in any way. In this case, there is an important mention of «electronic display», which, in fact, serves as a reference to the IT sphere.

Such a concept of information, as an object of civil rights, deprives the need for its special characteristics in terms of civilization. However, as noted by experts, in relation to certain industries, it requires special consideration. Problems that arise in connection with the lack of a unified approach were drawn attention in the literature (Pylypchuk & Tsymbaliuk, 2016).

However, from the practical point of view, for the legal regulation of relations in the IT-sphere, the above-mentioned vision of the notion and essence of information is quite suitable. In addition, it is flexible enough to adapt to possible changes in the technological aspects of the information society. (Except for the fact that the mention of fixation in «electronic form» looks too «concrete», as other forms of display of information and/or data may soon appear, which will necessitate a widespread interpretation of this expression).

At the same time, it should be noted, that such an approach, being acceptable for legal regulation of «normal» relations in the IT-sphere, complicates the characterization of information security requirements, since the «subject of security/protection» is understood too widely.

Just as «information», «information security» is a multi-valued notion (Popova & Lipkan, 2016).

For practical reasons, without analyzing existing approaches to its characteristics and understanding of the essence, let's take as a basis the definition contained in par. 2 chapters 13 of the Law of Ukraine dated January 9, 2007 «On the Basic Principles of the Development of the Information Society in Ukraine for 2007-2015»: «Information security - a state of protection of vital interests of a person, society and the country, in which the harm is prevented due to: incompleteness, timelessness and the unlikelihood of the information used; negative information influence; negative consequences of the use of information technology; unauthorized distribution, use and violation of integrity, confidentiality and availability of information». (It should be noted that many criticisms may be made on this definition. At the same time, since there are divergences on this issue, and consensus has not yet been achieved, it seems justified to use it as a benchmark in determining the directions of legal regulation in this area).

So, as follows from the above definition of information security, its features are:

1) the existence of certain stable conditions, circumstances (more precisely, it would probably be to speak about the «situation», not «state») in which the society is. It should be noted that in the IT-field, the term «state» (State) denotes a design pattern, refers to the class «behavior patterns». However, in the mentioned Law, as follows from the systematic interpretation of its provisions, it is precisely the conditions, circumstances in which the society is located;
2) the protection of vital interests of human being, society and state;
3) the intention to prevent damage to these interests;
4) the recognition of the existence of differences in the interests of people, society and the state;
5) the recognition of the mutual connection of the interests of man, society and state in terms of the need to prevent the task of harm to them;
6) the achievement of the goal on the basis of recognition of the harmony of the interests of man, society and the state without favoring any of them;
7) «information security» is a generic term and covers such varieties as «cybersecurity», «media security in real terms», and so on.

Beginning to consider information security issues, it is worth mentioning that in English the notion of IT-security has two meanings:

1) functional safety (safety) means that the system realizes correctly and in full implements those and only those goals that correspond to the intentions of its owner, that is, operates in accordance with existing requirements;
2) the actual information security (security) - concerns the safety of the process of technical information processing and is the property of a functionally secure system. Such a system should prevent unauthorized access to data and prevent their loss in the event of a malfunction (https://uk.m.wikipedia.org/wiki/).

In domestic law, this was reflected in the proposal that information security should take into account not only the threat of information but also the threats that come directly from the information itself, its technologies and products. This reference is based on the thesis that informational relationships may arise: threats associated with encroachment upon their information resources (mainly those that have limited access) and the threats that arise during the formation of the environment, the conditions of activity of such subjects. In the first case, information acts as an object of threats, and in the second - an instrument for their implementation (Zubok, 2015).

The conclusion about the dual nature of «threats» seems appropriate, although it needs to be clarified. In particular, it should be noted that not only information itself can be the object and tool of threats (and the result of the threat implementation in cases where its damage occurs), but information technologies as such may be a special object and threat tool.

«Information security - a state of protection of vital interests of a person, society and the country, in which the harm is prevented due to: incompleteness, timelessness and the unlikelihood of the information used; negative information influence; negative consequences of the use of information technology; unauthorized distribution, use and violation of integrity, confidentiality and availability of information» (par. 2 chapters 13 of the Law of Ukraine dated January 9, 2007 «On the Basic Principles of the Development of the Information Society in Ukraine for 2007-2015»).

Let's also pay attention to the practical significance of the distinction between «threat to information» and «threat from information».

In terms of civilization, it means that in the first case, the requirement of «information security» means the need to protect «information» as an object of civil rights. In this case, it is about prevention and liquidation of the consequences of active illegal actions of persons who encroach on information, try to distort information, destroy it, etc.

Instead, in the second case, the center of gravity shifts to preventing damage and eliminating the damage that arose as a result of the threat posed by improper use of information and information and communication technologies. Since the information for the offender is a means of implementing his plans, an instrument of unlawful actions, it would be more accurate to speak not about «information security», but about «information danger».

Now, let's touch on the legal basis for establishing a basic list of possible threats to information security.
Actually, already in the definition of the concept of «information security» in par. 2 chapters 13 of the Law of Ukraine (January 9, 2007) contains not only its characteristics but also an indication of what threats to information security are legal and should be warned (eliminated).

Such threats include, in particular:

1) incompleteness, timeliness and unlikelihood of the information used;
2) negative information influence;
3) the negative effects of the use of information technology;
4) unauthorized distribution, use and violation of the integrity, confidentiality, and availability of information.

The first question that arises in connection with the proposed list is to find out whether this list is exhaustive or indicative.

We must proceed from the assumption that threats to information security may have legal value, and in cases where they actually occur, although they are not mentioned in legislative acts.

Thus, significant information security threats create an «information war», which is described as «the fourth generation war - the war of cultures», which absorbs not only resources but also intelligence, using all the new methods and tools that can be used for combat operations. At the Munich Conference on Safety in 2017, we talked about such a toolkit of this war as «a post-truth». The concept of the latter was formed when, with the help of the Internet, our mind began to find the set of things that could not have been imagined before. Thousands of sources work, there is no censorship - all of this makes the information flow much firmer than before.

Therefore, there is such a concept as a fake, which is a distortion of the truth. It differs from PR or propaganda, which nevertheless must be based on the truth, possibly hyperbolizing it. Fake does not want to be true, it is more important for him to achieve his own goals, rather than informing the person. Fake is a deliberate distortion of the information, but this is done so that the consumer does not notice this information. Theoretically, an event that the fake tells could be, but in reality it was not. After the fake, propaganda can replicate it, because its toolkit is just a false generalization, when a single fact is presented as a regularity. That is, propaganda violates the rules twice, when on the basis of fake is drawn artificial world (Pocheptsov, 2017).

Cyber attacks are a serious threat to the information security.

In particular, according to Rob Wainwright, Director of the European Union Police Service (Europol), on Sunday, May 14, broadcast on the British television channel ITV, mass cyber attacks hit at least 150 countries, whereas a whole more than 200 thousand computers were affected. «Many of the victims - business representatives, including huge corporations ... I'm afraid that the number of victims will increase when people on Monday come to work and turn on their computers», – Wainwright said. Earlier it was reported that the global cyber attack, which struck many companies and institutions since Friday, May 12, 2017, has already affected 104 countries. The Telegraph reported that the large-scale attack of the worm-emitter virus WannaCryptor, which hit tens of thousands of computers, was followed by a cybergroup associated with Russia (Over 200,000 computers in 150 countries were hit.., n.d.)

Massive cyber attacks hit the Ukrainian economy. So, on June 27, 2017, many Ukrainian agencies, public and private companies were hit by hackers, as a result a normal rhythm of work was violated and the victims suffered losses. The virus for some time paralyzed the work of the Cabinet of Ministers of Ukraine, New Post, Alfa Insurance, Kyivenergo, Ukrtelecom, media holding TRK Lux, Kyivenergo, Boryspil Airport, Kyiv State Administration, PJSC «Ukrgazvydobuvannya», Savings Bank, Chains of gas stations «Klo», Kyiv Metro, Toskombank, Bank «Pivdenny» and others. Answering the questions of the lead «112 channel» (112.UA) on June 29, 2017: «Who is behind the PETYA virus?», a well-known IT specialist, the founder of one of the American companies of the Silicon Valley, which deals with cyber attacks – Mykola Bilogorsky, a defense against cyber attacks, argued that the purpose of creating the virus was precisely the task of harming the country in the information sphere. Although, supposedly, there was a squandering of funds from attacked entities, the requirements for transferring money were only the «cover». In fact, this virus (which, according to the expert, required 5-10 different specialists with different skills during the month) was technically adapted to the conditions of Ukraine: it was launched through the system of

the accounting report « M.E.Doc», which applies only in our country. In addition, the purpose was to damage and destroy information (data), since, even after the payment of money to victims, the possibility of recovery of the loss did not occur. Later, with the help of this virus, computer systems were attacked in other countries, although the motives for the attack remained unclear («Investigation of cyber attack. », n.d.). In any case, according to Oleg Derevyanko, the head of Information System Security Partners, this was a clearing of traces of previous attacks, a demonstration of cyber-attacks, and the development of a large-scale coordinated attack, including the ability to mislead the enemy, issuing one type of attack for another, preparing for the next attacks, testing of cybersecurity capabilities, especially attack speed and system recovery (Demonstration of power, n.d.).

The analysis of statistical crimes (those for which citizens are turning for help to law enforcement agencies) indicates that about 65% of all crimes in the Network are fraud. But, in addition, a significant array of so-called «actual crimes» are: blocking computers, various devices, theft of data, including banking, etc (Gor, n.d.). Although the latter cannot be quantified, it is possible to determine the directions and means of dealing with them.

Summarizing the statement in this section, it should be noted that, depending on their sources of origin (those who create threats in the IT sphere), it is appropriate to distinguish between public and private threats to information security.

The first is from the subjects of public relations - the states and their faces. Often, they take place in the process of using various forms of information warfare, operations of special services of foreign states, and etc.

The second ones are the source of illegal activity of private individuals, who in the current conditions are often hackers, pirates, fraudsters of different kinds, the «field of activity» of which is the IT-sphere.
We note that recent events, in particular, the activation of cyber attacks, indicate the failure of the idea of self-regulation of the IT sphere at the present stage of its development.

So, threats to information security cannot be overcome only with the help of technical means, since the latter can affect only on the technical component of the IT sphere, leaving out the attention of the «social element», which are participants in the relations arising in the IT sphere (including, programmers, providers, users, etc.). This cannot be considered justified, because at this stage of development of IT, the social element is the main factor of the violation of information security, and the person is called among the Top 10 digital threats XXI century (Macarevich, 2017). In search of influence on this component of the IT sphere, we must consider the means of influencing the human factor as a source of threats to information security.

Depending on the type and source of cyber threats, various preventive, organizational and legal means can be used to prevent and eliminate the consequences of the state, the normative basis of which is the Doctrine of Information Security of Ukraine, adopted in December 2016 by the National Security and Defense Council and put into force on February 25, 2017 by the Decree of the President of Ukraine. Although some experts believe that the Doctrine is only a declaration (The doctrine of the information security of Ukraine..., n.d.), it should be acknowledged that it establishes sufficiently clear guidelines for activities in this area. Based on the provisions, one can name the main directions of influence.

So, in the context of information warfare, proper anti-propaganda with the use of IT is important. It should reveal false information from the enemy side and, instead, submit own information that corresponds to reality. People have the right to the truth. In its absence, trust in power is constantly decreasing. We lose when we give some facts with delay because the facts are always part of the mass consciousness together with the interpretation. But to get rid of this, even hostile information for us, is difficult, because it entered to the consciousness first. To overcome this first introduced information, much more effort is needed. At the same time, in some cases (such as with Russia) there is an aggressive conflict, and therefore there are specific tasks. In others, to promote the country, its own position is needed all over the world. We have some tasks in Europe, others in the United States. And in Europe, the conversation with the Baltic states and Poland will be different. These are all fundamentally different audiences. So, it is unlikely that it would be true to argue that the information war is being conducted by Ukraine with Poland. Most likely, there is a different interpretation of history, where one can find an understanding and will find it sooner or later. In addition, each country has an expert community that influences on the government and a journalistic community that has an impact on the population. And they too should receive the

messages that are configured on them. The main thing is trust to the information. That is why it is looking for ways to call confidence in your own message. Future propaganda will be much more effective since it will be based on an objective type of toolkit. At the same time, propaganda will be complicated technologically, and the person will remain the same (physiologically, psychologically), which was two thousand and more years ago. The modern toolkit will work against the unchanging brain. In addition, the task is complicated by the fact that, although the problem of information security exists for each country (the information space is largely common, it is difficult to set boundaries), but here there is an asymmetry: we are watching American serials, reading American books, and they do not watch our movies and do not read our books. So your product should become the most interesting for the audience because it reflects your own world picture. Therefore, the state must invest in creating their own bestsellers and blockbusters, and etc (Pocheptsov, 2017).

Information hygiene is an important preventive measure against information threats.

Experts note that the safety of Ukrainians in the information space and the lack of hygiene on the Web kills immunity to cyber threats. In their opinion, society is practically not protected. People think very little about safety. Everyone is reading about cyber attacks and crafty hackers, but at the same time they put primitive passwords simply because they are so convenient and they lay out information about themselves that third parties need not to know. The low culture of security is the factor behind most of the crimes on the Web: people go through unfamiliar links, are fake and become victims - they lose their money, data, and their computers are blocked by criminals.

The state's activities to provide Ukrainians with knowledge about cyber threats are also criticized. It is noted that although the «Cybersecurity Strategy of Ukraine», approved by the National Security and Defense Council of Ukraine, among the priorities of the development of safe esports is called «enhancement of digital literacy of citizens and culture of safe behavior in cyberspace, implementation of state and public projects raising public awareness about cyber threats and cyber defense», however, the creation of the National Cybersecurity Coordination Center under the National Security and Defense Council has not changed the situation so far. Despite the fact that the focal point was established in June 2016, but in December of that year, sites of the Ministry of Finance, the Pension Fund and the State Treasury were paralyzed by hackers because of the absence of any serious counteraction. At the same time, the analysis of the December (2017) attacks showed that the minimum success was achieved by the attackers in the National Bank, where the greatest attention was paid to cybersecurity (Lopaiev & Golub, 2017).

Critics argue that to solve the problem of cybernetic protection of the population such measures as the blocking of dangerous sites, is not enough. In the information age, solving any problems is not prohibitions, it is education and raising the level of literacy of the population. To achieve this goal, literary and cinematic must work in an accessible and popular form and tell people how to act correctly. In this case, instilling information hygiene is necessary at the elementary school and university education (Gor, n.d.).

Recognizing the importance of information hygiene and the appropriateness of criticizing the lack of active state activity in this area, it should be noted that the excessive hopes for the effectiveness of educational and educational activities would be a mistake. First, because it's about a long process of education, whose results will become visible, at best, in a few years, while the current situation in the field of information security needs rapid improvement. Secondly, hopes look naive to a sufficient increase in the level of "informational and security literacy" of the population, starting with "primary school and university education", on the background that in the information society the types and nature of cyber-threats are rapidly changing. However, as a radical change, according to experts, in the IT sphere should be also the nature of the future education itself («Everything crashes in a relatively short period of time…», 2017)What will be taught in the "elementary school" is unlikely to be relevant to solving the problem of cybersecurity legal support at the time of its completion (except when it comes to general principles of cohabitation in society, compliance with general safety rules and information security).

In this regard, it should be more effective to recognize the non-education of «informational and security literacy» of only the «passive» type, and the formation of the psychology of active public response to cyber threats (as is the case with the "hacktivists" who created the Ukrainian Cyberlance - UCA and united Ukrainian

communities in the IT field, whose purpose is to counteract cyber threats to Ukraine's national security).

It should be noted that, it would not be justifiable to transfer on volunteers the duty of the state to ensure the counteraction to cyber threats. Taking into account the above, "information hygiene" should be recognized as a factor in the formation of legal awareness, a condition for the effectiveness of the use of legal means, among which the means of public-law influence occupy an important place (which, let us note, in the context of the need to overcome cyber-threats, are not considered to be human rights violations, even in democratic countries).

Conclusions

Assessing from this standpoint the situation in this area that takes place in our country, we note that solving the problem of legal support requires consideration of two aspects: legislative and law enforcement.

As for the first of them, the most important draft law is the draft law «On countering threats to national security in the information sphere». In addition, experts point out some progress towards the cyber security of the state (a strategy for cyber security has been developed, with the NSDC there is a focal point, etc.), however, they draw attention to the lack of a law on cybersecurity, the lack of a legal basis for public-private partnerships in this area, without which no advanced country can do (Demonstration of power…, n.d.).

Experts point out and the need to pass a law on the responsibility of hackers who now feel safe and practically do not hide (Belogorskiy, 2016).

At the same time, it is worth emphasizing the need for interstate coordination of efforts in this field. Some positive changes have already been made in this area.

So, the ministers of finance of the G7 countries (the Group of Seven (G7) is a group consisting of Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States), at a meeting held in the Italian city of Bari, on May 13, 2017, pledged to combine their efforts to combat international cyber attacks. This is reflected in the draft document, compiled on the basis of their meeting. It recognizes the fact that «cyber incidents are a growing threat to the economy and that the reaction is needed ».

The joint statement of the G7 countries calls for the introduction of a common practice for the rapid detection of vulnerabilities in the global financial system and emphasizes the need for effective measures to assess the cybersecurity of individual financial firms and at the security level. As Italian Minister of Finance Pierre Carlo Padoan said, discussions that were scheduled prior to the May 12 attacks were «unfortunately very timely» (more than 75,000 computers in 99 countries were hit by this virus attack) (The G7 countries will agree on joint measures to combat cyberattacks, n.d.).

At the same time, although the creation of special legislation aimed on the legal support of information security is important but equally important is the efficient application of already existing legislation, the rules of which in many cases allow to protect effectively the rights and interests of participants in IT relations related to information security.

One can agree with the idea that even in the Internet, where there seem to be no borders, the restrictions are introduced quite easily and operate effectively. The main thing is that they bring benefits to the country, and not harm (Kazanskyi, 2017). It should be added that the effectiveness of such measures depends to a large extent on proper legislative support.

References

Belogorskiy, N. (2016). Silicon Mountains and Valleys. New country time, № 48, 56-58.
Bilenchuk P.D., Gvozdetskiy V.D., Slivka S.S. (1999). Philosophy of Law. Kiyv: AtIka.
Cai, Z., He, Z., Guan, X., & Li, Y. (2018). Collective Data-Sanitization for Preventing Sensitive Information Inference Attacks in Social Networks. IEEE Transactions on Dependable and Secure Computing, 15(4), 577-590. Retrieved February 01, 2019, from https://ieeexplore.ieee.org/abstract/document/7576667.
Demonstration of power. Oleg Derevianko about the key goals of the latest cyber attack. (n.d.). Retrieved January 12, 2019 from http://vlasti.net/news/263539
E. Macarevich, (2017) Top 10 digital threats of the XXI century. Focus, № 27, 20-23.
Endsley, M. R. (2018). Combating Information Attacks in the Age of the Internet: New Challenges for Cognitive Engineering. PubMed, 60(8), 1081-1094. Retrieved January 12, 2019, from https://www.ncbi.nlm.nih.gov/pubmed/30376429.

Espionage for a new era. (2015). Ukrainian Week, № 31, 34-36.
Everything crashes in a relatively short period of time. Interview with IT expert Igor Novikov. (2017, June 15). Kraina, 20.
God is everywhere. A physicist from the United States put forward the theory that the universe has consciousness. (n.d.). Retrieved February 25, 2019, from http://nv.ua/techno/science/bog-povsjudu-amerikanskij-fizik-vydvinul-teoriju-o-tom-chto-vselennaja-obladaet-soznaniem-1546675.html
Gor, A. Vkontakte has been banned, threats have remained: how Ukrainians are deceived in the network (n.d.). Retrieved January 8, 2019 from https://apostrophe.ua/ua/article/society/2017-06-01/vkontakte-zapretili-ugrozyi-ostalis-kak-ukraintsev-obmanyivayut-i-verbuyut-v-seti/12599
Investigation of cyber attack. Police "disturbed" the company M.E.Doc. (n.d.). Retrieved December 15, 2018 from http://glavnoe.ua/news/n312705-rassledovanie_kiberataki._policija_potrevozhila_kompaniju_m.e.doc_
Kazanskyi, D. (2017). Non-virtual effect. Ukrainian Week, 23, 8-16.
Koen, D. L., Arato, E. (2003). Civil society and political theory. Moscow: Ves Mir.
Kormich B.A. (2011). .Information law. Kharkiv: BURUN i K.
Lopaiev Yu., Golub A., (2017) Another front, Ukrainian Week, № 3, 20-23.
Pasko, I.T., Pasko, Ya.I. (1999). Civil society and national idea. (Ukraine against the backdrop of European processes, comparative essays). Donetsk: TsGO NAN Ukrayni.
Pilipchuk, V.G., Dzoban, O.P. (2014). Information Society: Philosophical and Legal Dimension. Uzhgorod: TOV «IVA».
Pocheptsov, H. (2017, March 9). Interview Mariya Boyko. Vgolos. Retrieved January 1, 2019, from http://www.ji-magazine.lviv.ua/2017/Pocheptsov_Vijna_4_pokolinnya.htm Over 200,000 computers in 150 countries were hit by mass hacking attacks. (n.d.). Retrieved December 21, 2018, from https://www.rbc.ua/ukr/news/massovyh-hakerskih-atak-postradali-200-tysyach-1494761345.html
Popova. T.V., Lipkan, V.A. (2016). Strategic Communications. Kiyv: FOP O.S. Lipkan.
Pylypchuk, V., & Tsymbaliuk, V. (2016). GtHistorical and legal problems of formation and development of information sphere and information law in Ukraine (end of XX - beginning of XXI century). Bulletin of the National Academy of Legal Sciences of Ukraine, 4, 39-42.
Safa, N. S., Sookhaka, M., Solms, R., Furnell, S., Ghani, N.A., Herawan, T. (2015). Information security conscious care behaviour formation in organizations. Computers & Security, 53, 65-48. Retrieved January 15, 2019, from https://www.sciencedirect.com/science/article/pii/S0167404815000863.
Shmidt E., Rozenberg Dzh. (2016). How Google works. Kiyv: Vidavnicha grupa KM-BUKS.
The doctrine of the information security of Ukraine is only a declaration - experts (n.d.). Retrieved December 15, 2018 from https://www.radiosvoboda.org/a/28336852.html
The G7 countries will agree on joint measures to combat cyberattacks. (n.d.). Retrieved January 10, 2019 from http://www.eurointegration.com.ua/news/2017/05/13/7065662/
Zubok, M. (2015). Information security in entrepreneurial activity. Kiyv: HNOZIS.