EasyChair Preprint

№ 5270

Cyber-Victimological Problems in the Context of Information Security of Ukraine

Tatiana Voropayeva and Nina Averianova

April 1, 2021

Cyber-victimological problems in the context of information security of Ukraine

Tatiana Voropayeva[1][0000-0001-8388-7169] and Nina Averianova[2][0000-0002-1088-2372]

[1] Kyiv

[2] Taras Shevchenko National University of Kyiv

Tatiana Voropayeva, Candidate of psychological sciences, Associate Professor, Faculty of Philosophy, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine, ORCID: 0000-0001-8388-7169 voropayeva-tania@ukr.net

Nina Averianova, PhD., Faculty of Philosophy, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine, ORCID: 0000-0002-1088-2372 aver_n@ukr.net

Abstract. The article considers cyber-victimological problems that arise as a result of information violence perpetrated by some political parties and anti-Ukrainian organizations with the help of certain TV and radio companies, as well as the information and telecommunication Internet network. In the information society, information violence is able to capture broad sections of society and become a whole industry of influencing the mentality, consciousness and behavior of people. The most subtle variant of information violence is information terrorism, the purpose of which is to weaken and shake the constitutional order of a certain state, as well as the information war against that state. The methodological basis of our study is an integrative approach. We use the concept of cyber-victimization as a heuristic research tool. The study revealed the main manifestations of cyber-victimization of certain groups of Ukrainian citizens, in which purposefully form not only contempt for Ukraine and Ukrainians, but also uncriticalness, indifference, passivity, increased anxiety, inability to defend their rights, reduced motivation to achieves, strong fears, feelings of annoyance and envy, unwillingness to take responsibility, justifying negative and aggressive behavior of others, etc. The article identifies the social consequences of the process of cyber-victimization. It has been proven that people with high and medium competence in the fields of cybersecurity and Ukrainian studies can best resist the destructive information and psychological influences. Constructive cooperation of cybersecurity specialists, lawyers and psychologists will allow to develop effective methods of cyber-victimization prevention and reliable means providing of information security in Ukraine.

Keywords: Author keywords: Information security. Information violence. Cyber-victimization. ICT-sphere. Citizens of Ukraine.

1 Introduction

On February 2, 2021, President of Ukraine Volodymyr Zelensky signed the decision of the National Security and Defense Council of Ukraine "On the Application of Personal Special Economic and Other Restrictive Measures (Sanctions)" [31]. It was this decision that imposed sanctions against people's deputy of Ukraine Taras Kozak ("Opposition Platform – For Life" political party at the Verkhovna Rada of Ukraine), as well as against eight companies that formally belong to him and broadcast under the logos of NewsOne, 112 Ukraine and ZIK. Both journalists, citizens of Ukraine, and experts call these TV channels "Medvedchuk's TV". Thus, Taras Kozak, who is a close associate of Viktor Medvedchuk, was banned from using his property for 5 years, and his channels were banned from producing content.

Most experts and journalists regarded this decision of the National Security and Defense Council of Ukraine as an important step aimed at protecting the Ukraine's information space, as well as at stopping the broadcast of Kremlin propaganda in Ukraine. The experts also spoke and wrote that over the past 5 years many people have been aware of the mechanism for financing "Medvedchuk's TV channels", but for some reason the decision was enacted only in February 2021. In particular, "Ukrayinska Pravda" wrote about the involvement of Taras Kozak in the supply of coal from the temporarily occupied territories as far back as 2016 [27]. In 2021, the Anti-Corruption Action Center conducted a study on the involvement of Taras Kozak's offshore companies in coal trade with the occupied territories. The researchers claim that Taras Kozak has been making money on this trade since 2014 [27].

Now interestingly, the document itself, which was voted for at a meeting of the National Security and Defense Council of Ukraine on February 2, 2021, had been submitted for consideration since 2018, when Petro Poroshenko was still President of Ukraine. In the decree signed by Volodymyr Zelensky, both the proposals of the Verkhovna Rada of Ukraine dated 2018 and the "recommendations of the SSU" were mentioned, which became an important ground for the introduction of these sanctions. Ukrainian Interior Minister Arsen Avakov stated that by 2018, the SSU had already had enough evidence to impose sanctions, but then, according to him, "there was a little lack of political will" [26, 27]. At the same time, a law was applied, according to which sanctions can be imposed against Ukrainian citizens whom the state considers terrorists or against those who finance terrorism [26, 27].

On February 12, 2021, it became known that the SSU initiated two proceedings regarding Medvedchuk's TV channels as early as July 2019. But the articles under which proceedings have been opened have nothing to do with terrorism. One of these is about preparing for high treason, the others are about seizing the corporate rights of legal entities in order to create a media resource and about legalizing illicit proceeds [27]. President of Ukraine Volodymyr Zelensky in his television addresses quoted the

decision of the National Security and Defense Council of Ukraine on imposing these sanctions and referred to the data of the special services which “cannot yet be disclosed” and stressed: “that’s what is the main reason for the termination of broadcasting, but not some criticism of me” [27]. “The trinity of channels supported a whole army of "talking heads" who professionally deceived and zombified Ukrainians”, Volodymyr Zelensky stressed [27]. It is known that after his election, Volodymyr Zelensky promised to “deal” with Medvedchuk’s “information monopoly” back in July 2019, and in August 2019 he stressed that the history of the Opposition Platform – For Life party and its funded channels “is not going to end well” [27].

Some politicians and experts reproach Vladimir Zelensky for why the “Nash” (“Our”) TV channel has not yet been closed; they doubt whether the SSU will have enough evidence of Taras Kozak’s involvement in terrorist activities; and how international courts will welcome this evidence. Naturally, the two following questions arose: 1) when will the procedural and regulatory decisions of the relevant state authorities be enacted? [26], 2) when will the law on transparency of ownership and financing of media be adopted? [26].

So, eight weeks have passed since the removal of Medvedchuk’s TV channels from the media landscape of Ukraine. During this period, after the cessation of satellite, cable and terrestrial broadcasting, Medvedchuk’s TV channels merged their broadcast streams on YouTube, and there were also attempts to launch a new Medvedchuk’s TV channel called the “Pershyi Nezalezhnyi (First Independent)”, but on February 26, 2021, this TV channel went off the air an hour after the start of broadcasting. In February 2021, the theam of V. Medvedchuk filed 10 lawsuits trying to appeal against the Decree of Volodymyr Zelensky, but the Supreme Court of Ukraine has already dismissed two claims, and the rest will be heard in late March and early April.

Thus, the removal of Medvedchuk’s TV channels from the media landscape of Ukraine on February 2, 2021 is associated with both the financing of terrorist organizations and disinformation, or information violence, which was proved not only by our theoretical and empirical studies [2-6], but also by many studies of “Detector media” [14]. EU Foreign Affairs and Security Policy Spokesman Peter Stano said that Ukraine “has a legitimate right to fight disinformation, but at the same time there are certain limits to this fight”, and that the EU is “closely monitoring” developments regarding sanctions [26, 27]. Head of the Ukrainian Mission to the EU Mykola Tochytskyi stated that the EU, although unofficially, is favorable to sanctions. The United States, Great Britain, Estonia and Latvia supported the decision of the National Security and Defense Council of Ukraine with official statements. It is known that there were no mass protests in support of Medvedchuk’s TV channels, and sanctions against these channels and V. Medvedchuk’s wife is approved by 58% of Ukrainians [26, 27]. At the Verkhovna Rada, People’s Deputy of Ukraine Vadym Rabynovych accused the current Ukrainian government of “green fascism”, an attack on freedom of speech, and called the National Security and Defense Council of Ukraine “devils striking at night”, and also called the President and the Sluha Narodu (Servant of the People) party “fascist devils” and then he sang “Arise, Great Country!” He also said that the Opposition platform – For Life party initiates impeachment of the President.

However, the impeachment procedure has never got started, and without a powerful media resource, status of V. Medvedchuk as the main representative of Russia and distributor of Russian money in Ukraine was under threat [27].

So, outright anti-Ukrainian rhetoric was inherent in 2000 – 2013 for the TV channels, such as "Inter", "Kyivska Rus (Kievan Rus)", "ICTV" (first of all and especially, in the shows of Dmitry Kiselyov, who for several years was the editor-in-chief of the Information Service of the "ICTV" TV company, and in May 2014, after the overthrow of Ukraine's President Victor Yanukovych, Kiselyov said that "there is no Ukraine. Now it is a virtual concept, virtual country" and "a failed state"). Later, these channels were joined by Medvedchuk's TV channels, such as "Nash" ("Our") TV channel (which, despite openly anti-Ukrainian rhetoric, the authorities do not plan to close). Specialists emphasize that after the ban on Medvedchuk's TV channels, the intensity of pro-Russian propaganda of the "Inter" TV channel significantly decreased [27].

All these TV channels can be called Ukrainian TV channels producing anti-Ukrainian content. However, unfortunately, there is no legislation in Ukraine that would allow closing TV channels for disinformation, information sabotage and information terrorism. The rapid development of information and communication technologies causes a systematic increase in cyber threats and dangerous consequences of information and psychological impacts on a person and society. The article considers cyber-victimological problems that arise as a result of information violence perpetrated by some political parties and anti-Ukrainian organizations with the help of certain TV and radio companies, as well as the information and telecommunication Internet network.

2 The methodological foundations of the research

It is known that information (derived from Latin "information" – familiarization, explanation, presentation) is data (messages) transmitted from one subject to another in the process of interpersonal communication or through various channels of mass communication in order to form, expand, or change the people's perceptions about and orientations in the events and phenomena of the surrounding world. The concept of "information" has been known since ancient times, and the initial understanding of information as a certain amount of data was preserved until the middle of the XX century, but from the second half of the XX it acquired a new, broader meaning. In 1948, the American mathematician N. Wiener laid the foundation of the concept of "information vision" of many phenomena and processes in the world. And in 1962 – 1963, the American F. Machlup and the Japanese T. Umesao began to develop the concept of "information society" according to which information becomes one of the main resources. The main feature of the information society is the production and dissemination of Information, its transformation into a commodity, a type of service, and even into power (see the works of S. Huntington, Y. Masudi, A. Toffler) [4]. A. Bard, D. Gilmore, M. McLuhan, M. Poster, A. Schütz and other scientists have proved that the main features of the information society is computerized, the information revolution, transformation of information and informatization into a decisive

factor in the life of society, intellectualization of human activity, decentralization and de-bureaucratization, individualization and democratization. Today, information is a multi-level set of knowledge, data and messages that are disseminated and used in society in order to regulate social interaction and relations between person, society and the state. Various types of information (social, economic, political, legal, ideological, socio-cultural, historical, environmental, etc.) define the essence of various social phenomena and processes, circulating through various channels and means of its storage and dissemination. Mass communication is playing an increasingly important role in the dissemination of information, and the power of the Internet has significantly increased the amount of information disseminated in the world [4].

Every day, our world is increasingly informatized and immersed in new technologies; real events are reflected in virtual space. An information resource is an extremely powerful tool of influence, which is why it is used so actively in the course of modern hybrid wars [2-4]. 2014 was marked by dramatic changes in the European space. The destabilization of the internal political situation in Ukraine and the Russian armed aggression have led to a radical change in the current geopolitical situation not only in Europe, but also around the world. The existing security system, which had guaranteed relative stability on the European continent, was completely destroyed. New geopolitical conditions have aggravated old conflicts and activated new ones, which has significantly affected the actualization of the problem of ensuring information security in many modern states [4].

The issues of politicization of mass information processes and the influence of mass media on the mentality, consciousness and behavior of people were studied by D. Bell, J. Baudrillard, M. Castells, K. Cross, N. Luhmann, H. McLuhan, R. Mills, E. Noel-Neumann, A. Touraine, E. Toffler, M. Foucault, S. Huntington and other scientists. Daniel Bell rightly noted that information and theoretical knowledge are becoming strategic resources of modern post-industrial society [8]. Alvin Toffler stressed that the information society challenges man, his ability to live in a completely new social environment, his creative and moral forces, and his ability to adapt to a new type of social communication, and generates various forms of self-government [30]. Michel Foucault noted that in the information society, the concept of discourse fixes the continuity of Text, Technology and Power [16]. In modern society, the special status of mass communication media is reflected in the well-known characteristic called “the Fourth Estate (fourth power)”. Such a state of affairs is confirmed by many facts: manipulative electoral technologies, biased coverage of various conflicts, creating a positive image of incompetent authorities, and other strategies that are intensively utilized in the context of information warfare. So, modern society is characterized by a total increase in the influence of the information component on human existence, society and civilization [4].

Currently, given the growing information confrontation in the world, the issue of information security in many states of the world is becoming increasingly important. Different aspects of information security are studied by D. Ageev, A. Dobrodeev, S. Zephirov, T. Radivilova and other scientists [1, 9, 10, 13, 17, 20, 22, 24, 25, 28, 31-33, 37, 38].

In the information society, information violence is able to capture broad sections of society and become a whole industry of influencing the mentality, consciousness and behavior of people. The most subtle variant of information violence is information terrorism, the purpose of which is to weaken and shake the constitutional order of a certain state, as well as the information war against that state.

The methodological basis of our study is an integrative approach. The integrative approach helps to find methods that are adequate to the phenomenon under study, taking into account all the features and levels of its development. The methodological basis of the integrative approach is the philosophical idea of human integrity. Modern American philosopher and writer Ken Wilber was the founder of the integral metatheory, designed to combine into one dialectical whole the science of the world and of a human, the traditions of Eastern mysticism and Western rationalism, external experience and internal mental states. Ken Wilber, by developing the ideas of Immanuel Kant, Franz Brentano, Wilhelm Dilthey and Carl Jung, created a complete picture of the human consciousness evolution and described a multi-level spectrum of psychic reality. atheory, designed to combine into one dialectical whole the science of the world and of a human, the traditions of Eastern mysticism and Western rationalism, external experience and internal mental states. Ken Wilber, by developing the ideas of Immanuel Kant, Franz Brentano, Wilhelm Dilthey and Carl Jung, created a complete picture of the human consciousness evolution and described a multi-level spectrum of psychic reality. The concept of “integrative approach” means combining methods and theories into a single complex model that have proven to be correct in certain contexts, rejecting reductionism.

For Ukraine, the issue of information security is of the most critical importance. The most relevant threats to the information security of Ukraine are represented not only by the natural threats arising due to natural events and phenomena that are beyond reasonable control of a person or society. Artificially created threats, which can be accidental or intentional, are very dangerous too. The said threats are directly caused by society and can manifest themselves through mistakes, carelessness, negligence, or they can also be intentionally created. These threats include: 1) inappropriate content (these are dangerous and malicious applications, mailings, web pages that are prohibited by law, and materials that do not meet age restrictions); 2) unauthorized access (a phenomenon when an unauthorized employee gets access to the hidden data by violating its official duties); 3) information leaks (which can be accidental or intentional); 4) data loss (can be triggered either by hardware malfunction, or by malicious events caused by users (accidentally or intentionally); 5) fraud (information fraud, malicious operations with bank cards, online banking hacking, cryptomining, etc.); 6) information terrorism; 7) information wars. It is known that the breach of information security of any organization depends on many factors, and can also be due to the planned actions of intruders or lack of skilled personnel. It is also important to remember about employees who can sell information to other organizations. It is known that there are a number of protective software shells, the databases of which need to be updated daily (protection against inappropriate content (antivirus, antispam, web filters, antispyware), data encryption, backup, etc.). In this paper the issues of information terrorism and information warfare against Ukraine are analyzed.

We use the concept of cyber-victimization as a heuristic research tool. In the absence of a system with appropriate means of ensuring information and psychological security of children, adolescents and citizens of many countries of the world, scientists have laid the foundations of a new science – cyber victimology – a branch of victimology that studies the causes and psychological mechanisms of cyber victimization (the process and result of turning people into victims of information violence and information terrorism). The object of cyber victimology research is cyber victims (that is, individuals or groups of people who have suffered harm or damage as a result of negative information and psychological impact caused by the use of certain information technologies (internet space, cell phones, various digital devices and gadgets, etc.). The scope of cyber victimology research is the socio-psychological determinants and mechanisms of cyber victimization of people, as well as the directions and methods of its prevention [7, 21, 34]. Olga Bovt emphasizes that the socio-psychological mechanisms of victimogenic information and communication impact on people have their own specifics and should be studied within the framework of a specific specialized field of scientific knowledge – cyber victimology [11, 12]. Modern researchers try to establish the scientific rationale for cyber victimology, its scientific and theoretical basis, main vectors and prospects of development, theoretical and methodological foundations for ensuring cybersecurity and cyber victimological prevention [11, 12]. The institutionalization and development of cyber victimology is carried out "at the intersection" of several scientific disciplines: victimology, criminology, deviance studies, social psychology, sociology, pedagogy, and others. The study of cyber threats and cybercrimes and their prevention, as well as the need to develop means and methods for ensuring information security of children, adolescents and adults are priority areas for the development of modern cyber victimology. The practicality of specialized professional training in the field of cyber victimology is considered as one of the most effective and promising areas of tackling information violence, cybercrime, and information terrorism.

Victimity is considered as a set of human traits arising from a complex of social, psychological and biophysical conditions that contribute to the maladaptive mode of response of a person, leading to harm to its physical or emotional and mental health [11, 12]. Victimity – is the potential or actual ability of a person individually or collectively to become a victim of a socially dangerous manifestation. At the same time, this ability can be considered both as the ability to become a victim of a crime under certain circumstances and as the inability to avoid criminal encroachment in situations where it is objectively possible [7, 15, 21, 32, 34]. Personal victimity is associated with a vulnerability to critical and destructive social situations. Victimity, as a psychological trait of personality, is developed through defects in interactive communication. At the same time, a personality becomes subject to frustration arising from influences, including sociogenic ones, and compensates for its inherent defects through various forms of deviant behaviour. Olga Bovt focuses on the forms of behavioural disorders in which a victim's maladaptation is manifested. She notes that a personality can become a victim of unfavorable subjective and objective factors of socialization [11, 12].

3 Theoretical and empirical studies of information security

Among the most common facts of cyber victimology are the facts of inciting minors to suicidal behaviour using the information and telecommunications network of the Internet, namely, driving minors to suicide by involving them in the so-called "death groups". With the social networks and messengers that are used in the information and telecommunications network of the Internet, the organizers of life-threatening games, such as "Blue Whale Challenge", "Wake me up at 4.20", "A Silent House", "Run or Die", "A Fire Fairy", offered children "exciting quests" and other "adventures" (for example, they wanted them to unexpectedly run across the roadway in front of a car approaching, to play with household gas, to ride on the outside of the moving vehicles, that is so-called "vehicle surfing", to get to the roofs of tall buildings and structures, i.e. so-called "roofing", etc.) which actually contained an open or veiled call to risk their lives, including to commit suicide. Especially widespread was the game challenge called "Blue Whale" containing 50 "game" tasks and due to which the organizers suppressed the will of children and adolescents and inculcated an idea of the need to commit suicide upon them [15].

Today, cyber victimological research in the context of information security of Ukraine (in the context of information violence, information terrorism and information war) is one of the most priority, urgently needed and promising.

It is known that information security is a condition of vital interests of a person, society and the state being protected, which prevents damage due to: a) incompleteness, untimeliness and unreliability of the information used; b) negative information impact, negative consequences of the use of Information technologies; c) unauthorized dissemination and use of Information; d) violation of the integrity, confidentiality and availability of information [4]. It is also known that researchers distinguish two types of information security – information-technical and information-psychological, but today the technical and technological aspects of information security are comprehensively studied and almost no attention is paid to its socio-humanitarian aspects, i.e. the information-psychological security of Ukrainian society. This is a negative trend, because the object of information and psychological influence is the mentality, consciousness and behavior of the population and military personnel, the system of forming public opinion and making socially important decisions [4].

Taking into account the socio-humanitarian aspects of information security implies the state of protection of a person, family, ethnic group, nation, as well as their traditions, customs, rights, way of life, life ideals, priorities and values, regardless of race, gender, age, religious-confessional and language characteristics. At the same time, it is also necessary to take into account the protection of a person's physical and mental health, free choice, free self-identification of subjects at the individual, group and social levels, and free development of a person, family, community, society, and the state. The concepts of humanitarian security in many countries of the world coincide in a certain way with the concept of sustainable development proposed by the UN. In the context of new civilizational challenges, doctrines of "new wars" of the Third Millennium, aimed at deforming the collective identity, mentality, self-consciousness, worldview and behavior of citizens of those States that some aggressor States consid-

er their enemies, the issue of ensuring information security of Ukrainian citizens is very urgent [4].

The famous phrase “who owns the information, he owns the world” has long been popular, but it is necessary to remember the important remark of the “father of cybernetics” N. Wiener says that the basis for the survival of any System is an accurate information picture. Today, these phrases are becoming even more important, since information is not only the foundation of various communications, but also the conceptual basis of all relations in society (and this conceptual basis can be both adequate and deformed). Therefore, the ability of our state to defend its own information space in the context of globalization and Russian aggression is becoming existential issue of modern Ukrainian society [4].

In the context of the international Russo-Ukrainian armed conflict, which, unfortunately, has been going on in Ukraine for seven years, it is very difficult to ensure humanitarian, information and psychological security of citizens. However, comprehensive consideration of the semantic dimension of information security will allow us to adequately counteract destructive information impacts on Ukrainian citizens not only by preventing the destabilization of the functioning of state institutions, political, legal, energy and socio-economic spheres of Ukrainian society, but also by professional counteraction to long-standing attempts to reduce the togetherness of Ukrainian citizens, undermine the sovereignty and territorial integrity of the state. This approach would make it possible to consolidate Ukrainian society, strengthen the state's defense capacity and organize ideological mobilization of Ukrainian citizens [4].

During 1991 – 2021, we studied the condition of information security in Ukraine using content and intent analysis methods. It was found out that in the course of information war waged against Ukraine and the Ukrainian people (which began immediately after the collapse of the USSR in 1991, escalated several times (in 1994 – 1995, 2000 – 2001, 2003, 2004 – 2006, 2010 – 2011, and 2013 – 2021) and naturally developed into the current Russo-Ukrainian armed conflict), various information resources are used: the press, radio, television, Internet, hacker attacks, etc. Russian media use the methods of “focusing attention”, “labeling”, “hoaxes”, “throwing in disinformation”, “transferring negative images”, “least evil”, “affirmative statements”, “simplifying the problem”, “ignoring”, “distracting propaganda”, “preventive propaganda”, “replicating horror stories”, “exploiting opinion leaders and groups of influence”, “disrupting logical and temporal connections between events”, “selective compilation of information”, “replacing sources of communication”, “destruction of cultural archetypes and basic values”, methods of blocking and distorting information flows and decision-making processes. The rumors, speculation, “fakes”, “vocabulary of hate”, “hate speech”, myths and stereotypes etc. are also used [4].

Since modern scientists believe that information warfare by its nature occupies an intermediate position between the “cold” war (which also includes economic wars) and real military operations involving the armed forces, many real actions of the Russian Federation (in particular, several local economic wars against Ukraine), as well as statements of famous political and public figures of Russia fully confirm this point. For example, A. Gubarev emphasized in his dissertation called “Information Warfare as an Object of Political Research” (2005) that information wars are a means of im-

plementing a “new colonization” policy [18]. D. Rogozin stated in his interview with Rossiyskaya Gazeta (published on June 28, 2013) that “now information technologies are considered as a weapon of the first strike”, and when “the state, which is the victim of aggression becomes almost paralyzed, it is struck by classical military means” [19]. The Russian-Ukrainian armed conflict on the territory of Ukraine confirmed these aggressive intentions of the Russian Federation (the armed conflict on the territory of Ukraine is considered as an interstate armed conflict of a neocolonial type [2-6, 35, 36]).

It is worth giving at least a few examples of destructive statements that were broadcast in the Ukrainian media during 1991 – 2021: “crafty khokhols (Ukranians)... you're nothing but babblers... you always need a foreign swineherd!”; “Ukraine? There is no such state! This is an illegitimate child”; “Ukraine is doomed to be interested in Russia”; “Ukraine does not even exist without Russia”; “civil war may become a reality of our days”; “Ukraine will be dismembered”; “destroying Ukrainians on the Internet – there is such a job!”; “Crimea is a special region of Russia”; “Russia should rent Crimea”; “Around Donbass, there is Russia which shares the same religion, blood, and spirit’; ‘let’s solve the issue of autonomy of the Donetsk region”; “Ukraine will be a federal state”; “the South-East of Ukraine wants to be with Russia”; “the country will fall into the abyss”; “Ukraine is falling apart before our eyes”; “Ukraine is a failed state, and Ukrainians aren’t a state-forming people!”; “we are nothing without Russia”; “stop pretending to be shamans and shout: "We have only one Ukraine!"... , if need be, there will be 2 Ukraines, or 5-6 Ukraines...”. We emphasize that these messages were broadcast on national radio and TV channels of Ukraine.

Our scientific publications on violations of information security in the Ukrainian mass media, as well as written appeals on this issue to representatives of all branches of government in Ukraine dated 1994, 1999, 2003 – 2005, 2010, 2012, 2014 have not receive an adequate response from the authorities [4, 35, 36]. Despite the fact that they were given specific examples: 1) manipulation of public opinion, 2) destructive ideological influence, 3) undermining the international image of Ukraine, 4) discrediting public opinion leaders, 5) provoking inter-ethnic and inter-confessional conflicts, 6) discrediting the basic values of the population, 7) destabilizing the situation in the country, 8) undermining the morale of the population, etc. [4].

In 1991 – 2021, our research group monitored the constructive and destructive influence of Ukrainian and foreign media on the development of collective (religious, regional, ethnic, national, civilizational) identity of Ukrainian citizens. This monitoring was carried out within the framework of several international research projects of the Center of Ukrainian Studies of the Department of Philosophy (until September 2000, it was the Institute of Ukrainian Studies) of Taras Shevchenko National University of Kyiv which were supported by the Renaissance Foundation, the Friedrich Ebert Foundation, the Foundation for Fundamental Research of the Ministry of Education and Science of Ukraine, as well as the Association of Ukrainian Banks. The students and postgraduates of 3 universities of the city of Kyiv actively participated in these projects (including students and postgraduates of the departments of psychology, sociology, philosophy, geology and mechanics and mathematics, as well as cadets

of the Military Institute of Taras Shevchenko National University of Kyiv). The students, cadets, and postgraduates worked as interviewers, processed data, and performed other types of work. A total of 50,000 respondents aged 18 to 89 were surveyed. The surveys were conducted in all regions of Ukraine using the method of individual interviews at the place of residence. The sample is representative in terms of the main socio-demographic indicators. The statistical error does not exceed 2.9%. Methods of content analysis, intent analysis, M. Kuhn-T. McPartland "Who-am-I" technique, M. Sinerella's adapted technique of "Identity measurment scale", and other methods were used. In our research, 2 groups were identified – Group A (whose members prefer TV channels with pro-Ukrainian content) and Group B (whose members prefer TV channels with anti-Ukrainian content). The study showed that the civil-political and European civilizational identity experiences the greatest deformations among those respondents who belong to Group B (86% of respondents mainly watch TV channels with anti-Ukrainian content) [3].

For a full-fledged formation of national identity, semantic connections are needed (specific dynamic formations) that not only "sew" together the personality and its national community, combining the value-semantic sphere of the personality and the value-semantic universe of the national culture, but also act as a bridge between the social and cultural and fundamental spiritual and ideological basis for the formation of any collective identity. The ideological systems of the Ukrainian people (mythological, religious, scientific and philosophical) represent not only different semantic stratifications in Ukrainian spirituality, but also the semantic content of Ukrainian life. The actualization of the ideological, imaginative and semantic content of culture greatly accelerates the process of crystallization of worldview. So, for the formation of national identity, the semantic links between the individual and his national community, as well as a clearly structured semantic field of Ukrainian identity, are extremely necessary.

It is known that any political, economic, historical, ethno-cultural information requires semantic processing while it is being assimilated. After all, meaning is a "unit" of the inner world of a person (Alexey Leontiev), and «striving for meaning» is one of the main motivational tendencies of a person, however, life senselessness causes people to experience such conditions as existential vacuum, detachment, depression, loss of faith, etc. (Viktor Emil Frankl). The semantic content can become a determinant of the ideological design of the semantic field of Ukrainian identity (both individual and collective). So, objects that contain sensitive information and use various forms (landmark, symbolic, figurative, axiological, etc.) of semantic content representation can become not only a source of Ukrainian academic competence, but also a system-forming factor of the worldview centering of the semantic field of Ukrainian identity. It is in the adequate informational formalization of such a semantic field that the possibility of the rapid spread of joint identities and corresponding identification practices (conservative-retrospective, constructive-perspective, desacralizing, etc.) are embedded. But the information and psychological war (which has been waged against the Ukrainian people for many years) distorts not only the internal structure of the identification matrices of the citizens of Ukraine, but also the meaningful content of these matrices, causing semantic destruction and semantic differences in the under-

standing of Ukrainian history, Ukrainian national interests, activities of prominent Ukrainian figures, fighters for freedom and independence, by the citizens. In this regard, it is very important to study the systemic role of the noetic (semantic) dimension of identifying subjects (both individual and collective).

The manifestations of information terrorism and the information and psychological war of the Russian Federation against Ukraine can be compared with the activities of the Rwandan radio station called "Free Radio and Television of the Thousand Hills" (Radio Télévision Libre des Mille Collines), which was broadcast from July 8, 1993 to July 31, 1994 and played a significant role in the genocide in Rwanda during April-July 1994. The station's name derived from the description of Rwanda as "Land of a Thousand Hills". It received support from government-controlled Radio Rwanda. The radio station, which was quite popular among the entire population, spread racist propaganda directed against Tutsis, moderate Hutus, Belgians and the United Nations mission. According to many Rwandans (as also recognized by the UN war crimes tribunal), it played a crucial role in creating an atmosphere of strong racial hostility in the country, which made genocide possible. Studies indicate that approximately 51,000 deaths were caused by the broadcasting of this radio station. The Hutu and Tutsi peoples, who lived side by side for several centuries, spoke the same language and adhered to the same traditions, turned into deadly enemies under the influence of the mass media. The rate of murder exceeded five times that in German concentration camps during World War II. It was the mass media that played a crucial role in the mass murder of the Rwandan population. Mass media representatives purposefully incited tribalism and openly called for violence and mass murder. The Rwandan government purposefully used the mass media as a weapon of mass destruction. The Hutus received clear instructions and recommendations on how to destroy the Tutsis, as well as approval for such actions. Jean Kambanda, the Prime Minister, Ferdinand Nahimana, a founder and a director of "Radio and Television of the Thousand Hills", and Hassan Ngeze, an editor of "Kangur" newspaper were given life sentences for inciting hatred through the mass media. Georges Ruggiu, a radio host who gave voice to calls for killing Tutsis, whom he called "cockroaches", was sentenced to 12 years in prison.

Tatiana Popova notes that Russian journalists, editors, directors and mass media owners who are waging an information war against Ukraine should remember the sad experience of their colleagues from Rwanda [23]. The heads of propaganda TV channels, news anchors of TV channels of Russia and unrecognized DPR and LPR, apparently, naively believe that they will be able to avoid punishment for purposefully inciting ethnic hatred [23]. Some of the stories of these TV channels contain open calls for violence, and they are even ahead of the "creations" of their colleagues from Rwanda in terms of the amount of false information. The Russian authorities have chosen Russian TV channels as weapons of mass destruction. Tatiana Popova emphasizes that in the struggle for information security of our country, a number of measures have already been taken: disconnecting Russian TV channels from broadcasting cable networks, monitoring Russian and regional media for separatist sentiments, informing the population about disinformation and preparing facts of violations regarding the veracity of information and inciting ethnic hatred. Russian TV

channels are full of edited stories calling for the arrival of volunteers from Russia to "protect the Russian-speaking population". Tatiana Popova states that almost every Russian journalist who was "awarded" the Kremlin Order "For Merit to the Fatherland" II class, in fact, continues to destroy the lives of thousands of innocent people with impunity – both Russians, residents of certain areas of Donetsk and Luhansk oblasts (regions), ordinary civilians of Ukraine, and the Ukrainian military defending their homeland. The situation of Rwanda is revealing. Tetiana Popova notes that Russian media specialists should remember that information does not disappear anywhere, on the contrary, it is collected, verified and evaluated. And not a single mass crime against humanity has gone unpunished [23].

In our research, 2 groups were identified – Group A, 400 respondents (whose members prefer TV channels with pro-Ukrainian content) and Group B, 400 respondents (whose members prefer TV channels with anti-Ukrainian content). Group A and Group B respondents were found to have the following characteristics (the first digit represents Group A data, and the second one represents Group B data, respectively): submissiveness (27% and 68%), credulity (23% and 76%), frivolity (14% and 55%), inability to defend their rights (18% and 62%), lack of subjectivity and critical approach (21% and 75%), unwillingness to take responsibility (19% and 59%), inability to correctly assess life situations (16% and 58%), passivity (20% and 83%), indifference (14% and 62%), non critical thinking (16% and 73%), strong suggestibility (25% and 57%), justification of negative and aggressive behaviour of others (11% and 82%), tendency toward dependent and helpless behaviour (10% and 67%), increased anxiety (31 and 64%), suspiciousness (11% and 58%), strong manifestations of fear (13% and 61%), resentment towards the world (33% and 54%), sense of misunderstanding and isolation from the world (10% and 56%), reduced achievement motivation (12% and 76%), high vulnerability (15% and 72%), tendency toward self-destructive behaviour (9% and 57%), desire for aggressive (31% and 61%), rash actions of a spontaneous nature (12% and 69%), sense of frustration (14% and 65%), envy (32% and 69%), tendency toward risk-taking and reckless behaviour (26% and 69%), antisocial behaviour (8% and 49%), tendency toward violation of social norms, rules and moral and ethical values (10% and 44%), undifferentiated sociability (22% and 81%), etc.

Unfortunately, even in the context of the Russo-Ukrainian armed conflict in Ukraine, no serious organizational and managerial decisions were made to create a complete system for countering Russian information aggression. Not everyone has yet understood that information weapons have a cross-border striking power, and that in current conditions, the defense capability of Ukraine largely depends not only on the professional activities of its Armed Forces, but also on the effective protection of its own information space, as well as on the ability to deter and prevent both external and internal information aggression. Regrettably, in the context of the information warfare, the formation of the Ukrainian political nation is significantly slowed down.

The fatal blow of information assassins is aimed at undermining the following main nation-building foundations: 1) at weakening the Ukrainian ethnic nation (which is the "core" of political one); 2) at destroying the Ukrainian national culture; 3) at eliminating civil society and collective identity (primarily national and European

civilizational one); 4) at disrupting the Ukrainian information space; 5) at weakening the Ukrainian state (through regional segmentation, separatization and federalization, etc.). Destructive influence on the consciousness and subconscious sphere of Ukrainian citizens can destroy any basis for the consolidation of Ukrainian society, deform the positive image of Ukraine, and drive a wedge between the West and East of Ukraine. Simultaneously, the opinions are most consistently spread that Ukrainian culture is undeveloped, flawed, unprofitable, backward and low-grade, that the Ukrainian language is a dialect of Russian, that Ukrainians and Russians are one people, but Ukrainians are underdeveloped Russians [4]. That is why the citizens of Ukraine (including the current political elite, party leaders, as well as Ukrainian oligarchs) should understand that without completing the processes of nation-building, without preserving own national identity and without stopping information aggression and "hybrid" war, Ukraine could not be a competitive state of the world.

Psychological and spiritual-ideological influence (that is, influence on individual and mass consciousness, on the collective unconscious, world perception, on value orientations and collective representations of the population in order to deform motivation, mentality, identity, worldview, and behavior of an individual and society) is a threat not only to national interests, but also to society and the state as a whole, since it belongs to the so-called mental-ideological aggression which contributes to the complete spiritual subjection to an opponent in the information war.

Any information aggression is associated with a destructive impact on military personnel and civilians, with the spread of disinformation, with manipulation of information, with intimidation, with the penetration of destructive information flows into the territory of a sovereign state, with the destruction of information communication between the state (which has become the object of aggression) and society, with a decrease in the effectiveness of the functioning of state authority, with an increase in psychological pressure on the civilian population, with the imposition of false goals and assessments, with the spread of rumors and panic, with demoralization, with the development of defeatism, with the presentation of any information to the advantage of an aggressor. It is known that negative information-psychological influences can lead not only to deformations of a person's perception of the world, serious violations of mental and physical health of an individual, emotional-volitional and behavioral disorders, but also to distortions of group and mass consciousness, destructive collective actions, serious consequences in the spiritual and socio-political life of society, public organizations and government institutions. All this contributes to distorting the true pattern of events in the eyes of the civilian population, possible defecting to the enemy's side and stopping any resistance to external aggression.

4 Conclusion

Today, cyber victimological research is not only extremely relevant, but also one of the most priority, urgently needed and promising. The rapid development of information and communication technologies causes a systematic increase in cyber threats and dangerous consequences of information and psychological impacts on a person and society.

Unfortunately, in Ukraine, the issue of humanitarian and information-psychological security has long been simply ignored. In particular, more attention was paid, first of all, to the information-technical "dimension" of information security (i.e., the security of computer and technical means, software, means and mode of protection against unauthorized information leakage), and not to the political-psychological and spiritual-ideological aspects of Information security. But it is the comprehensive consideration of these two dimensions of information security that would allow to adequately counteract destructive information influences on the citizens of Ukraine.

The study revealed the main manifestations of cyber-victimization of certain groups of Ukrainian citizens, in which purposefully form not only contempt for Ukraine and Ukrainians, but also uncriticalness, indifference, passivity, increased anxiety, inability to defend their rights, reduced motivation to achieves, strong fears, feelings of annoyance and envy, unwillingness to take responsibility, justifying negative and aggressive behavior of others, etc. The article identifies the social consequences of the process of cyber-victimization. Based on the results of our study, two main fields of prevention of cyber-victim behaviour of Ukrainian citizens are identified: information-technological and socio-psychological. It has been proven that people with high and medium competence in the fields of cybersecurity and Ukrainian studies can best resist the destructive information and psychological influences.

The ability of citizens to resist information and psychological warfare is of great importance in ensuring the defense capacity of any modern state. Our research has shown that respondents with a low level of national and European civilizational identity have the lowest level of Ukraine-specific cultural competence, and also receive the information they need mainly from those media outlets that systematically violate the information and psychological security of Ukrainian citizens.

Constructive cooperation of cybersecurity specialists, lawyers and psychologists will allow to develop effective methods of cyber-victimization prevention and reliable means providing of information security in Ukraine.

In this regard, it is necessary: 1) to develop a modern doctrine of information security of Ukraine; 2) to ensure a more prompt response of the National Security Council and Defense, the SSU and relevant public organizations to the facts of information aggression from other states; 3) to develop an information security culture of an individual and the skills of "information hygiene" since school; 4) to unite the efforts of all information security specialists (both the representatives of the technological field and the representatives of the socio-humanitarian field) in the protection of the information component of national security of Ukraine; 5) to stop broadcasting movies and shows that include anti-Ukrainian content, humiliate national feelings and dignity of the Ukrainian people; to ensure timely professional response to those media outlets, which have become the mouthpiece for anti-Ukrainian propaganda, discredit Ukrainians and try to destabilize the political, legal and socio-economic situation in Ukraine; 6) to legally govern the use of a powerful resource of mass media by the ruling parties, financial and political group, and to protect citizens of Ukraine from the destructive influence of those mass media that broadcast anti-Ukrainian, antisocial and immoral ideas, messages, thoughts and spread anti-Ukrainian sentiments, escalate fear,

anxiety, apathy, and the like; 7) to strengthen socio-humanitarian component of Ukraine's domestic policy, to develop and implement a comprehensive system of socio-humanitarian technologies in order to form and maintain a sense of collective national self-esteem of Ukrainian citizens, to develop their personal agency, patriotism, subjectity, critical thinking, and competence of Ukrainian studies, which are an important basis for the constituting of a positive national identity.

References

1. Ageyev D, Bondarenko O, Alfroukh W, Radivilova T (2018) Provision security in SDN/NFV. In: 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET). IEEE, pp 506–509. DOI: https://doi.org/10.1109/tcset.2018.8336252
2. Averianova NM (2017) Gibrydna vijna: rosijsko-ukrayinske protystoyannya [Hybrid warfare: The Russian-Ukrainian confrontation]. Molodyj vchenyj 3(43): 30–34 (in Ukrainian)
3. Averianova N, Voropaieva T (2020) Transformation of the Collective Identity of Ukrainian Citizens after the Revolution of Dignity (2014–2019). Kyiv-Mohyla Humanities Journal 7: 45–71
4. Averianova N, Voropayeva T (2020) Information security of Ukraine: social and humanitarian aspects. Paper presented at the International Conference «Problems of Infocommunications. Science and Technology» (PIC S & T-2020), Kharkiv, 6-9 October 2020
5. Averianova NM, Voropayeva TS (2020) Information and psychological security of Ukraine. In: International scientific integration ‘2020. Conference proceeding. November 9-10, 2020. KindleDP, Seattle, Washington, pp 515–518. DOI: 10.30888/2709-2267.2020-4
6. Averianova NM, Voropayeva TS (2020) Features of settlement of modern armed conflicts: integrative approach. In: Organization of scientific research in modern conditions ‘2020: conference proceedings. KindleD, Seattle, pp 477–481. DOI: 10.30888/979-865-1656-02-8.0
7. Becker K, Schmidt MH (2004) Internet chat rooms and suicide. Journal of the American Academy of Child. Adolescent Psychiatry 43(3): 246–247. DOI: 10.1097/00004583-200403000-00002
8. Bell D (1999) The Coming of Post-Industrial Society. Basic Books, New York
9. Bondarev V (2016) Vvedenie v informaczionnuyu bezopasnost avtomatizirovannykh sistem [Introduction to information security of automated systems. MGTU Baumana, Moscow (in Russian)
10. Borodakiy YV, Dobrodeev AY, Butusov IV (2013) Kiberbezopasnost kak osnovnoy faktor natsionalnoy i mezhdunarodnoy bezopasnosti XXI veka (Chast 1) [Cybersecurity as the main factor of national and international security of the XXI century (Part 1)]. Voprosy kiberbezopasnosti 1(1): 2–9 (in Russian)
11. Bovt OV (2014) Issledovanie psikhologicheskikh determinant viktimnogo povedeniya podrostkov [Research on the psychological determinants of victim behavior in adolescents]. Problemi suchasnoyi psikhologiyi 25: 45–59 (in Russian)
12. Bovt OV (2018) Kiberviktimologiya [Cybervictimology]. Akademiya Estestvoznaniya, Moscow (in Russian)

13. Darren Death (2017) Information Security Handbook: Develop a threat model and incident response strategy to build a strong information security framework. Packt Publishing Ltd
14. Dovzhenko O (2020) Sauron i Saruman prorosiiskoi propahandy. Pidsumky monitorynhu dezinformatsiinykh naratyviv pid chas mistsevykh vyboriv 2020 [Sauron and Saruman of pro-Russian propaganda. Results of monitoring of disinformation narratives during the 2020 local elections]. https://detector.media/propahanda_vplyvy/article/182872/2020-11-27-sauron-i-saruman-prorosiyskoi-propagandy-pidsumky-monitoryngu-dezinformatsiynykh-naratyviv-pid-chas-mistsevykh-vyboriv-2020/. Accessed 20 Feb 2021 (in Ukrainian)
15. Ferguson A, Swenson K (2017) Texas family says teen killed himself in macabre 'Blue-Whale' online challenge that's alarming schools. The Washington Post, July 11
16. Foucault M (1965) Madness and Civilization: A History of Insanity in the Age of Reason. Vintage, New York
17. Grachkov IA (2018) Informaczionnaya bezopasnost ASU TP: vozmozhnye vektora ataki i metody zashhity [Information security of APCS: possible attack vectors and protection methods]. Bezopasnost informaczionnykh tekhnologij 1: 90–98 (in Russian)
18. Gubarev AB (2005) Informacionnye vojny kak obekt politologicheskogo issledovaniya: avtoref. dis. na soisk. uchen. step. kand. polit. nauk: 23.00.02 [Information wars as an object of political science research: abstract of the thesis for the degree of candidate of political sciences: 23.00.02]. Ussuriysk (in Russian)
19. Informacionnaya vojna [The information war] (2013). In: Sovremennaya armiya. http://www.modernarmy.ru/article/282/informacionnaya-voina. Accessed 20 Feb 2021 (in Russian)
20. Kalinichenko IA (2017) Praktiko-orientirovannyj podkhod k podgotovke speczialistov v oblasti kiberbezopasnosti [Practice-oriented approach to training specialists in the field of cybersecurity]. Voprosy kiberbezopasnosti 2 (20): 3–6 (in Russian)
21. Lyubov EB, Antochin EY, Palaeva RA (2016) A comment two-faced web: Werther vs Papageno. Suicidology vol 7, 4(25): 41–51 (in Russian)
22. Pompon R (2016) IT Security Risk Control Management: An Audit Preparation Plan. Apress
23. Popova T (2014) Uroki «Radio Ruandy» dlya Ukrainy i rossijskikh SMI [Lessons from "Radio Rwanda" for Ukraine and Russian media]. In: Ukrainskaya pravda. https://www.pravda.com.ua/rus/columns/2014/07/15/7031973/. Accessed 10 March 2021(in Russian)
24. Radivilova T, Ageyev D, Kryvinska N (2020) Data-Centric Business and Applications: ICT Systems-Theory, Radio-Electronics, Information Technologies and Cybersecurity, vol 5. Springer Nature
25. Saveliev AG, Karasev PA (2018) Perspektivy regulirovaniya i sokrashcheniye voyennoy kiberugrozy [Prospects for the regulation and reduction of the military cyberthreat]. Vestnik Moskovskogo universiteta. Seriya 12. Politicheskiye nauki 5: 47–61 (in Russian)
26. **Sklyarevskaya G (2021) «Na viini yak na viini». Sotsmerezhi – pro vymknennia kanaliv ZIk, NewsOne ta «112 Ukraina» [«In war as in war». Social networks – about disconnection of ZIk, NewsOne and «112 Ukraine» channels].** https://ms.detector.media/sotsmerezhi/post/26551/2021-02-03-na-viyni-yak-na-viyni-sotsmerezhi-pro-vymknennya-kanaliv-zik-newsone-ta-112-ukraina/. Accessed 10 March 2021 (in Ukrainian)

27. Sklyarevskaya G (2021) Yak zhe my bez kanaliv Medvedchuka? Khronolohiia podii i poperedni vysnovky [How are we without Medvedchuk's channels? Chronology of events and preliminary conclusions] https://ms.detector.media/trendi/post/26871/2021-03-17-yak-zhe-my-bez-kanaliv-medvedchuka-khronologiya-podiy-i-poperedni-vysnovky/. Accessed 17 March 2021 (in Ukrainian)
28. Stitilis D, Klisauskas V (2018) Osobennosti pravovogo regulirovaniya kiberbezopasnosti v natsional'nykh zakonakh Litvy, Rossii i USA: strategii kiberbezopasnosti [Peculiarities of the legal regulation of cybersecurity in the National Laws of Lithuania, Russia and the USA: cybersecurity strategies]. Voprosy rossiyskogo i mezhdunarodnogo prava 7–8: 80–100 (in Russian)
29. Stoletov OV (2018) Problema pravovogo regulirovaniya mezhdunarodnoy informatsionnoyi kiberbezopasnosti v sovremennoy mirovoy politike [The Problem of Legal Regulation of International Information and Cybersecurity in Modern World Politics]. Rossiyskiy zhurnal pravovykh issledovaniy 5(1): 66–72. https://doi.org/10.17816/RJLS.71 (in Russian)
30. Toffler A (1980) The Third Wave. William Morrow, United States
31. Ukaz Prezydenta Ukrainy №43/2021 Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 2 liutoho 2021 roku «Pro zastosuvannia personalnykh spetsialnykh ekonomichnykh ta inshykh obmezhuvalnykh zakhodiv (sanktsii)» [Decree of the President of Ukraine №43/2021 On the decision of the National Security and Defense Council of Ukraine of February 2, 2021 «On the application of personal special economic and other restrictive measures (sanctions)»] (2021). https://www.president.gov.ua/documents/432021-36441. Accessed Feb 2021 (in Ukrainian)
32. Uslinsky FA (2014) Kiberterrorizm v Rossii: ego svojstva i osobennosti [Cyberterrorism in Russia: Its Properties and Features]. Pravo i kiberbezopasnost 1: 6–11 (in Russian)
33. Vacca J (ed) (2016) Network and System Security, 2nd Edn. Kindle Edition.
34. Vlasova SV, Nametkin DV (2019) K voprosu o vyyavlenii, raskrytii i rassledovanii prestuplenij v sfere skloneniya nesovershennoletnikh k suiczidalnomu povedeniyu posredstvom informaczionno-telekommunikaczionnoj seti Internet [On the issue of the identification, disclosure and investigation of crimes in the sphere of vulnerabilities to the suicidal behavior by means of the information-telecommunication network Internet]. Vestnik Voronezhskogo instituta MVD Rossii 3: 180–186 (in Russian)
35. Voropayeva TS (2011) Formuvannya nacionalnoyi identychnosti gromadyan Ukrayiny ta problemy informacijnoyi bezpeky [Formation of national identity of citizens of Ukraine and problems of information security]. Naukovyj visnyk Volynskogo nacionalnogo universytetu imeni Lesi Ukrayinky. Seriya Filosofski nauky 24(221): 78–85 (in Ukrainian).
36. Voropayeva TS (2016) Gumanitarna j informacijno-psyhologichna bezpeka yak chynnyk zmicznennya oboronozdatnosti Ukrayiny [Humanitarian, information and psychological security as a factor in strengthening Ukraine's defense capabilities]. In Komunikacijno-kontentna bezpeka v umovax gibrydno-mesianskyx agresij Putinskoyi Rosiyi. Kyiv: VIKNU, pp 63–67 (in Ukrainian)
37. Whitman ME, Mattord HJ (2014) Principles of Information Security. Cengage Learning, Australia, Brazil, Japan, Korea, Mexico, Singapore, Spain, United Kingdom,United States
38. Zefirov SL, Shcherbakova AY (2020) Oczenka informaczionnoj bezopasnosti obekta pri provedenii audita informaczionnoj bezopasnosti [Information security assessment of the object during information security audit]. In: Informaczionnye sistemy i tekhnologii IST-

2020. Sbornik materialov XXVI Mezhdunarodnoj nauchno-tekhnicheskoj konferenczii. Nizhny Novgorod State Technical University R.E. Alekseeva, pp 517–522 (in Russian)

39.