advancing technology generally, and those of the assemblage of integrated persons and integrated good in particular. Exactly what the shape of the law should be in this respect remains to be explored and debated. Nevertheless, it is only by confronting everyday cyborgs and their technologies head-on that we can better understand the challenges for the law and, more importantly, begin to imagine alternative legal futures for dealing with them[489].

Conclusions. Based on the results of our own research we represented a conceptual-attributive understanding of *a new world's order* as a state and differently-directed functionality of the modern world in transhumanistic conditions of human's morphological freedom implementation under pandemic and post-pandemic reality, including its digitalized component.

Also, within our research, we determined attributes and defined *information security* as a state of safety under the permanent control of vulnerabilities on an acceptable level. Attributes of information security vary depending on an information security type.

We made a conclusion that a category of *a person* in modern reality may be understood not just as a natural person or a legal entity but including a human with integrated implants, who may be called a cyber-human. In conditions of transhumanism within the morphological freedom implementation, they have to acquire "a human right on own body techno-modification".

Finally, on the basis of the mentioned above, we have represented our own understanding of ***a person's information security*** in new world order conditions as a state of personal safety within his/her country and even the whole world under the permanent control of threats and vulnerabilities on an acceptable level.

The prospects for its development and improvement are directed to reveal the legal status of humans with integrated implants, make an appropriate legal regulation of their rights, freedoms and duties, and sufficient measures for their protection in glocal conditions of the digitalized world under its new order.

[489] Quigley M., Ayihongbe S. Everyday Cyborgs: On Integrated Persons and Integrated Goods. *Medical Law Review*. 2018. 26. P. 307-308. DOI:10.1093/medlaw/ fwy003

Chapter XIII
INFORMATION PROTECTION OF A PERSON AS A COMPONENT OF INFORMATION SECURITY OF THE STATE

Human security is the security of the country[490].

Man, his life and health, honor and dignity, inviolability and security – the highest social value in Ukraine. Implementation of this norm of the Constitution of Ukraine is the main goal of the state policy of national security[491]. The Human Development Strategy of June 2, 2021 stipulates that significant challenges to the socio-economic situation in the country as a whole and its regions in recent years are challenges such as the armed aggression of the Russian Federation against Ukraine and the temporary occupation of its territory, demographic crisis, epidemic situation related to the spread of acute respiratory disease COVID-19 caused by coronavirus SARS-CoV-2, problems in medicine, education, science, culture, physical culture and sports, social support, national and patriotic education[492].

At the same time, ensuring the security of man (citizen) and society presupposes the existence and development of social institutions (including civil society institutions), developed forms of public consciousness, current legislation guaranteeing the realization of legitimate interests, protection of rights and freedoms of every member of society.

The level (degree, measure) of security of society always depends on the political regime, the state of the economy and social sphere, the development of spiritual and cultural potential of society, a set of conditions that allow to realize the rights and freedoms of all social groups and resist actions that divide society, and, as well as human security, – from the results of solving the problem of

[490] Presidential Decree "On the decision of the National Security and Defense Council of Ukraine of September 14, 2020" On the National Security Strategy of Ukraine" №392/2020 https://www.president.gov.ua/documents/3922020-35037

[491] Presidential Decree "On the decision of the National Security and Defense Council of Ukraine of September 14, 2020 "On the National Security Strategy of Ukraine" №392/2020 https://www.president.gov.ua/documents/3922020-35037

[492] Decree of the President of Ukraine "On the decision of the National Security and Defense Council of Ukraine of May 14, 2021" On the Human Development Strategy "of June 2, 2021 № 225/2021 https://www.president.gov.ua/documents/2252021-39073

forecasting, timely detection, prevention and neutralization of threats to the progressive development of society in various spheres of its life.

Conclusions. The dynamic development of society requires new approaches to understanding the security of society, the state and man. The understanding of security, formed in the twentieth century, has traditionally been interpreted as the absence of danger or neutralization of threats and was primarily adapted to the needs of the state, and did not reflect the essence of human security in today's globalized and information-saturated world.

The study of the realities of the information society and the conditions of safe human existence in it, shows the need to identify patterns and trends of information threats, as well as to determine the limits of necessary and possible state intervention through legal support and institutional protection. In addition, it is necessary to study the role of man in ensuring their own information security in the context of globalization, building a democratic rule of law and the formation of civil society.

Despite active research in the field of information security of the state today there is no single approach to information security in general and information security of man, in particular his information protection. Scientific developments on the legal regulation of the information sphere, information security of the state and information security of man in particular are found in the works of Ukrainian and foreign researchers, in particular I. Aristova, I. Bachylo, R. Kalyuzhny, T. Kostetska, O. Kokhanovska, E. Makarenko, V. Tsimbalyuk. The research of V. Gurkovsky, O. Zolotar, V. Kopylov, B. Kormych, and V. Lipkan became key to studying the problem of ensuring information security.

The regulation of the sphere of information security of the state should be based, first of all, on the principle of the highest human value, guarantee of his rights, freedoms and legitimate interests and his protection.

The history of the origin and development of the concept of "security" covers a significant period of time, which actually

coincides with the emergence and development of mankind[493]. The need for means of accumulation, systematization, storage, retrieval, transmission of information, security is growing, and hence the need for information security. The transformation of the security category took place together with the definition of the environment, knowledge of natural processes, dissemination of scientific and technical knowledge, culture, etc.

Most of the provisions of the laws of Ukraine and other regulations [494], which are directly related to information relations are aimed precisely at protecting information. Provisions aimed at protecting people, society and, accordingly, states from information are in the "minority".

In the context of our study, it is necessary to pay attention to the content of the category "security", which in human life plays the role of a reference point around which the values of human existence are grouped. This concept is multifaceted, there are many opinions in science about this. Literally, security means no danger. The need for security is one of the basic motivational mechanisms in human life. In addition, security is an undoubted value that is universal in nature, as it is recognized by all people, regardless of their racial, national or social affiliation.

In the general sociological sense, the category of "security" characterizes a certain state of human society, which ensures its normal existence and stable development. In social models, security is understood as solving the problem of conditions for the optimal functioning of society and its progressive development. In a broad philosophical and ideological aspect, security is an important issue

[493] Abulmagd AK Overcoming barriers. Dialogue between civilizations: lane. with English /AND. K. Abulmagd et al., Ed. S. P. Kapitsa; lane. T.P. Evening. M .: Logos, 2002. 192 p.

[494] 1. On the decision of the National Security and Defense Council of Ukraine of October 31, 2001 "On measures to improve the state information policy and information security of Ukraine": Decree of the President of Ukraine of 06.12.01 № 1193/2001 URL: https:// zakon.rada.gov.ua/ laws/ show/1193/2001#Text

2. On the Doctrine of Information Security of Ukraine: Decree of the President of Ukraine of 08.07.09 № 514/2009 URL: https:// zakon.rada.gov.ua/laws/show/514/2009#Text

3. On the Basic Principles of Information Society Development in Ukraine for 2007-2015: Law of Ukraine of January 9, 2007 № 537-V URL: https://zakon.rada.gov.ua/laws/show/537-16#Text

4. On information: Law of Ukraine of October 2, 1992 № 2657-XII URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

for both scientific knowledge and the practice of the existence of society on the scale of an individual state and the planet as a whole[495].

Awareness of the security problem becomes complete given the dialectic of life. Full development is not possible without security. Thus, security also acts as a guarantee of sustainable development of any social system: the acquisition of new features and qualities.

Security is a concept that describes the state of stability, peace and absence of threat. It has a subjective nature, is one of the basic needs of man, social groups and states. Covers the satisfaction of such needs as existence, survival, integrity, identity, independence, peace (peace), availability and stability of development[496].

The issue of information security is an important component of the entire national security system of the country [497].

The first law in the field of information security – "On Information Protection" was adopted in the United States in 1906. However, the intensive development of legislation on information security began after the invention of computers and the creation of the ARPANET network, which was based on ideas to: complete privatization and liberalization of the information technology market, in particular, the need for public control over the development of networks and their content was emphasized; the primary role of building networks, on the basis of which services are developed (in contrast to the European model, which notes the priority development of the services sector, and only then – its technical, network support); universalization of telecommunication services for all.

A broader approach to understanding the meaning of "information security" was formulated by the representative of Sweden during the discussion of international information security at the 56th session of the UN General Assembly, according to which information and network security means protection of personal

[495] Bezzubov D.O. Public safety: (organizational and legal principles of support): Monograph. K .: MP Lesya, 2013. 451 p.

[496] Zięba R. Instytucjonalizacja Bezpieczeństwa European. Warsaw; Scholar, 2001. S. 406.

[497] Zadiraka V.K. Modern methods of solving information security problems. Bulletin of the NAS of Ukraine. 2014. № 5. P. 65–69.

information about senders and recipients. unauthorized changes, protection against unauthorized access to information and the creation of a reliable source of supply of equipment, services and information, and covers the protection of information relating to military capabilities and other aspects of national security. At the same time, insufficient protection of vital information resources and information and telecommunication systems can pose a threat to international security. So, in the EU there is a clear distinction between the features of information security of man and society, information security of the state and international information security. At the same time, the interests of man and society became fundamental, which led to the intensive development of such areas as personal data security, access to information, as well as ensuring the implementation of democracy in the construction of the information society. A separate line should be noted legal support for combating cybercrime, which is due to the chosen direction of building an information society, and the traditionally defining role of the state in protecting the rights and legitimate interests of its citizens. which led to the intensive development of such areas as personal data security, access to information, as well as ensuring the implementation of democracy in the construction of the information society. A separate line should be noted legal support for combating cybercrime, which is due to the chosen direction of building an information society, and the traditionally defining role of the state in protecting the rights and legitimate interests of its citizens. which led to the intensive development of such areas as personal data security, access to information, as well as ensuring the implementation of democracy in the construction of the information society. A separate line should be noted legal support for combating cybercrime, which is due to the chosen direction of building an information society, and the traditionally defining role of the state in protecting the rights and legitimate interests of its citizens.

Given that information security is an integral part of each area of national security, the issue of its provision is of national and national importance. At the same time, information security is an

important independent area of national security[498]. The lack of an information security system makes it impossible to reliably ensure not only information but also national security[499].

Security is a complex, systemic, multilevel phenomenon, the state and prospects of which are directly influenced by external and internal factors, the most important of which are: 1) the political situation in the world; 2) the presence of potential external and internal threats; 3) the state and level of information and communication development of the country; 4) the domestic political situation in the country[500].

Kormich BA identifies the components of a modern security system: doctrine and legal basis; institutional mechanism; methodological framework used to implement specific tasks within the security policy[501].

St. 3 of the Law of Ukraine "On Fundamentals of National Security of Ukraine"[502] determines that the objects of national security are: man and citizen – their constitutional rights and freedoms; society – its spiritual, moral and ethical, cultural, historical, intellectual and material values, information and environment and natural resources; the state – its constitutional order, sovereignty, territorial integrity and inviolability.

In the next article. 4 determines that the subjects of national security are: the President of Ukraine; Verkhovna Rada of Ukraine; Cabinet of Ministers of Ukraine; National Security and Defense Council of Ukraine; ministries and other central executive bodies; National Bank of Ukraine; courts of general jurisdiction; the Prosecutor's Office of Ukraine; National Anti-Corruption Bureau of Ukraine; local state administrations and local self-government bodies; The Armed Forces of Ukraine, the Security Service of Ukraine,

[498] Doctrine of information security of Ukraine: Decree of the President of Ukraine of 29.12.2016 № 47/2017 514/2009. URL: https://www.president.gov.ua/documents/472017-21374?fbclid= IwAR 3idC8nwxYZJm

[499] Lipkan V.A., Maksymenko Y.E., Zhelikhovsky V.M. Information security of Ukraine in the conditions of European integration: Textbook. way. K .: KNT, 2006. S. 178.

[500] Morozov O.L. Information security in the current state and prospects of statehood. Chamber. 2007. №12. P. 23-25.

[501] Kormich B.A. Information law: Ed. H .: BURUN and K., 2011. P. 119.

[502] On the Fundamentals of National Security of Ukraine. Law of Ukraine: dated June 19, 2003 № 964-IV. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text

the Foreign Intelligence Service of Ukraine, the State Border Guard Service of Ukraine and other military formations formed in accordance with the laws of Ukraine; bodies and divisions of civil protection; citizens of Ukraine, associations of citizens.

Note that the term "national security" is used in a broad sense and is a state of protection of the state and its citizens from all possible threats of today. From this follows the concept of national interests, which means – a set of basic values and aspirations of citizens and the state at a particular stage of development. Information security is a component of national security.

Most subjects of the information security system are also its objects – man and citizen, the state, its individual bodies, institutions and so on.

The theory of national security refers to the subjects of national security all state and public institutions that are participants in the process of national security, namely: the state apparatus as a system of state bodies, local governments, citizens and their associations. From this list two groups of subjects are allocated those which are endowed with the state-power powers, those which are not endowed with them though in separate cases can have a certain volume of the delegated state-power powers[503].

National security is a variable. In essence, the assessment of the existing (desired, projected) level (degree) of protection of vital national interests and conditions of their implementation, in particular, the state of socio-economic system, social and political institutions in the country, the ability of national armed forces to resist threats to territorial integrity and independence. . The current assessment of the level of national security is always placed on the interval from absolute security (ideal state), when events, phenomena, processes that create dangers of national interests are completely absent, to absolute danger, when the combined impact of these dangers puts on the agenda the existence of a social system (state), for example, the question of the real threat of its collapse,

[503] Tikhomirov O.O. Ensuring information security as a function of the modern state: dis. ... the candidate of law. Science: 12.00.01 / Nat. acad. internal affairs. K., 2011. P. 109.

The approach to understanding the essence of information security of different categories of subjects may differ significantly, for example, the security of ordinary citizens or officials of public authorities. Therefore, it is quite logical and noteworthy to classify threats that have a narrower, or in other words special nature, in particular, threats to information security of network resources. In the same context, A. Pogrebnyak proposes a broader classification, in his opinion, threats can be both accidental and intentional. Accidental threats include: a) errors of service personnel and users; b) loss of information due to improper storage; c) accidental destruction or replacement; d) failure of equipment, power supply, disk systems, network components; e) incorrect operation of the software,[504]. Intentional threats include: a) unauthorized access to information and network resources; b) disclosure and modification of data and programs, their copying; c) disclosure, modification or substitution of computer network traffic; d) development and spread of computer viruses, introduction of logic bombs into software; e) theft of magnetic media and settlement documents; f) destruction of archival information or its deliberate destruction; g) falsification of messages, refusal to receive information or change of the time of its receipt; g) interception and acquaintance with the information which is transferred on communication channels.

Law of Ukraine "On the basic principles of information society development in Ukraine for 2007 - 2015"[505] the following definition of the term "information security" is proposed: "information security is a state of protection of vital interests of a person, society and the state, which prevents damage due to: incompleteness, untimeliness and unreliability of the information used; negative information impact; negative consequences of the use of information technology; unauthorized dissemination, use and violation of the integrity, confidentiality and availability of information ".

Information security is a component of the general problem of human information support, aimed at the realization of information rights and legitimate interests of man in every sphere of his life.

[504] Pogrebnyak A.V. Computer security technologies: Monograph. Rivne: MEGU, 2011. P. 46-47.

[505] On the Basic Principles of Information Society Development in Ukraine for 2007-2015: Law of Ukraine of January 9, 2007 № 537-V. URL: https:// zakon.rada.gov.ua/laws/show/537-16#Text

By "information rights" we mean the extent of possible behavior of individuals, the object of which is information. In Ukraine, the legislative definition of "information" is contained in the Law of Ukraine "On Information", according to Art. 1 of which: "Information is any information and / or data that can be stored on physical media or displayed electronically"[506]. A similar definition is contained in Part 1 of Art. 200 of the Civil Code of Ukraine.

The information rights include the following:

- the right to refute inaccurate information about oneself and one's family members and the right to demand the seizure of any information, as well as the right to compensation for material and moral damage caused by the collection, storage, use and dissemination of such inaccurate information (Part 4 of Article 32 Constitution of Ukraine [507], part 1 of Art. 277 CCU);
- the right to freely collect, store, use and disseminate information orally, in writing or otherwise – at their discretion (Part 2 of Article 33 of the Constitution of Ukraine, Article 302 of the CCU, Article 5 of the Law of Ukraine "On Information")[508]; - the right of free access to information on the state of the environment, the quality of food and household items, as well as the right to its dissemination (Part 2 of Article 50 of the Constitution of Ukraine, Part 1 of Article 293 of the CCU);
- the right to reliable and complete information about the state of their health (Part 1 of Article 285 of the CCU), etc.

According to AI Marushchak, information human rights are state-guaranteed human capabilities to meet its needs in obtaining, using, disseminating, protecting and protecting the amount of information necessary for life[509]. Whereas, the universal constitutional right to information contains certain specific possibilities, which together constitute the information rights of the

[506] About information: Law of Ukraine of October 2, 1992 № 2657-XII. URL: http://zakon.rada.gov.ua/laws/show/2657-12.

[507] Constitution of Ukraine: Law of Ukraine of June 28, 1996 № 254k / 96-VR. URL: //www.zakon4.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

[508] About information: Law of 02.10.92 № 2657-XII. URL: http://www.zakon2.rada.gov.ua/laws/show/2657-12.

[509] Marushchak A.I. Definition of "information human rights". Information and law. 2011. № 2 (2). P. 21-26.

subjects of information relations, which are not only people but also legal entities, the state and so on.

The enshrinement of information rights in the Constitution of Ukraine, as well as the proclamation of information security of Ukraine declared: "Protection of sovereignty and territorial integrity of Ukraine, ensuring its economic and information security are the most important functions of the state, the business of all Ukrainian people" (Article 17)[510].

Thus, information security from the narrowly specialized field of use of specialists of applied nature was raised to legal consolidation at the level of the Basic Law. As can be seen, in the scientific thought of that period there was a significant identification of the concepts of "information security", "information security", "information protection", which still occurs in many countries.

In different periods of historical development of human civilization, the intensity of the use of information influence, as well as the perfection of its organization, differed greatly.

The first written mention of the informational impact on society in ancient China. In the already mentioned Treatise on the Art of War by Chinese General Sun Tzu[511] the description and bright examples of application of receptions and methods of psychological influence which gave the chance to reach a victory without battles or with the minimum losses are given. An important place, in particular, is given to misinforming the enemy, psychological treatment of their own population and troops in order to achieve unity in society before and during the war, the implementation of information sabotage to disrupt military alliances of enemy states with other states and more.

In society, at any stage of its development, the creation, dissemination and use of information that is directed against or to weaken the state, society and man, belongs to the category of unauthorized actions. But it should be borne in mind that any improved, at first glance, regulatory framework always has "gaps",

[510] Constitution of Ukraine of June 28, 1996 URL: http://zakon5.rada.gov.ua/laws/show/254k/96-vr.

[511] Sun Tzu. The art of war. K .: Arius, 2014. 128 p.

and then the rule comes into force: "what is not forbidden is allowed." Based on this, in the definition of "information security"[512].

Let's pay attention to "the state of protection of vital interests of the person, society and the state at which harm is prevented because of: incompleteness, untimeliness and unreliability of the information used; negative information impact... " is more correct to replace with: the state of protection of vital interests of man, society and the state, which prevents harm through: negative information impact through, primarily unauthorized creation, dissemination, use of intentionally aimed incomplete, untimely, unlikely and biased information.

Human information security, at the same time, is both a state and a process, as it is an integral part of life, in which a person is constantly under the influence of specific information influences.

The formation of a person as a person occurs under the influence of the information array in which he is from birth. The information that a person receives affects his consciousness and subconscious. It is natural that information affects, especially at the subconscious level, human behavior – both in the direction of adjustment and in the direction of complete change. This is both good and dangerous for both man and society.

A person receives information by various means: voice (communication, listening, radio), in writing and in print (books, print media, correspondence, etc.), audiovisual (television), electronic (from a computer monitor, e-book ", Mobile phone screen, etc.).

The information that a person receives affects his consciousness and subconscious. At the subconscious level, information affects human behavior – both in the direction of adjustment and in the direction of complete change. In itself, incomplete, untimely, unreliable or biased information used, in most cases, does not cause such harm to a person that we can talk about his danger. A person is constantly confronted with such information in everyday life, and believes that this information is complete, timely

[512] On the Basic Principles of Information Society Development in Ukraine for 2007-2015: Law of Ukraine of January 9, 2007. № 537-V. URL: http:// zakon.rada.gov.ua/laws/show/537-16#Text

and reliable. After some time, you can assess the degree of its completeness, timeliness and reliability or not evaluate at all.

At the same time, incomplete, untimely, unreliable or biased information affects a person's consciousness or subconscious. Consequences can be disturbance / change of a condition of its health, a mental condition, behavior, etc., in that case it is possible and it is necessary to speak about information danger for the person, and when it concerns not one person, and group of people, their mental condition, behavior, etc., then we can and should talk about the information danger to society. When incomplete, untimely, unreliable or biased information influences decisions that are not in the interests of society, state and the individual.

That is, when operating on information, you need to be sure that the information used in the transmission process, the dissemination was not distorted.

At the turn of the XIX – XX centuries there is a scientific interest in the phenomena of influence on human consciousness, in particular on the consciousness of the masses. In 1879 p. the first psychological laboratory was opened in Leipzig on the initiative of the scientist W. Wundt. Fifteen years later, France published "Psychologie des foules" (Crowd Psychology) by G. Le Bon, who announced the arrival of the "crowd era". Fundamentally new tasks were set in the same period by ideologues of work with the mass consciousness. There is the emergence of the type of advocacy, which is commonly called the English phrase "public relations" (PR). The main task of PR specialists was to create advanced communication technologies, ie such options for organizing the supply of information to society that can guarantee, or at least.

With the development of society and improved methods of obtaining the necessary information and its protection. The desire to obtain confidential information has always been contrasted with the desire of the other party to protect that information. Ancient methods of information protection have essentially survived to the present day, only the technique of their implementation is being improved. For example, in order to hide the very fact of the

availability of information in ancient Rome, the message written on the board was hidden from prying eyes by filling it with wax.

In modern conditions, such steganographic methods as hiding the content of messages in pictures, television and audio signals, etc. are common[513]. In parallel, methods of encryption and encryption (cryptographic methods), the history of which dates back to the origins of writing in Ancient Egypt and China. Some authors divide the process of information protection development into relatively independent periods, which are based on either the evolution of types of media, or the development of information communications.

Yes, Semkin SN distinguishes three periods of development of means and methods of information protection. The first period is determined by the beginning of the creation of meaningful and independent means and methods of information protection and is associated with the emergence of the possibility of recording information messages on solid media.

V.Ya. Nastyuk's monograph was devoted to administrative and legal protection of the information sphere. and Beletseva VV "Administrative and legal protection of information", which substantiates that "the protection of information in its content involves, on the one hand – leveling the danger, on the other - maintaining the state of protection of vital interests of society, the state from various challenges and threats"[514].

In the State Standard of Ukraine "Information Protection. Technical protection of information. Substantive provisions." DSTU 3396.0-96 there is no direct formulation of the classification of threats, but it provides possible ways to implement threats. They provide an opportunity to imagine or identify potential threats to information relations (relations for the collection, processing and accumulation of information). Part 4.1.3 of sub-clause 4.1 of clause 4 defines that threats may be carried out by: technical channels, including channels of incidental electromagnetic radiation and interference, acoustic, optical, radio, radio engineering, chemical and

[513] Semkin S.N., Semkin A.N. Fundamentals of legal protection of information protection. Uch. pos. for universities: Hot Line - Telecom, 2008. 238 p.

[514] Nastyuk V.Ya., Belevtseva V.V. Administrative and legal protection of information: problems and solutions. X. : Pravo, 2013. 128 p.

other channels; channels of special influence by forming fields and signals in order to destroy the protection system or violate the integrity of information; unauthorized access by connecting to equipment and communication lines[515].

Paragraph 5 "Threat to information" contains the following definitions: leakage of information – uncontrolled dissemination of information, which leads to its unauthorized receipt; violation of the integrity of information – distortion of information, its destruction or destruction; blocking information – preventing authorized access to information.

O.B. Oliynyk, based on the analysis of current legislation and taking into account the experience of other countries, proposed four levels of organizational and functional system of information security. The first level is strategic, national, which includes the Verkhovna Rada of Ukraine, the Cabinet of Ministers of Ukraine and their advisory bodies. This level covers political decisions, legislative and regulatory support, establishing the order of international cooperation, the use of forces and means of information confrontation, the behavior of actors in critical situations.

The second level is organizational-executive, departmental-territorial, which includes central executive bodies and local self-government bodies, the military organization of the state, law enforcement bodies and judicial authorities. At this level, organizational and methodological support of information security in the relevant industries and administrative-territorial entities, coordination and control of activities in the areas of responsibility of state authorities[516].

The third level is the critical infrastructure of the country, which includes the inclusion of enterprises, institutions and organizations, communications of the national space and other facilities, which are managed using electronic means of communication and information technology. At this level, powers should be exercised to ensure the safe operation of national,

[515] Information protection. Technical protection of information. Main provisions: DSTU 3396.0-96. The publication is official. Kyiv, State Standard of Ukraine, 1996.

[516] Oliynyk O.V. Theoretical and methodological principles of administrative and legal support of information security of Ukraine. Monograph. K., Ed. support "Ukrainian priority", 2012. P. 290.

departmental and territorial critical infrastructures, guaranteed prevention of external and internal threats and dangers that may harm citizens, society and the state.

Ensuring information security should be regulated by norms on: legal consolidation of national interests of man, society and the state in the information sphere; subjective information rights of man and citizen; systems of bodies responsible for information security; forms of participation of civil society in ensuring information security.

Today one of the important state tasks is the formation of a single information and legal space of the country. Such relations, in general, contribute to the protection of the constitutional rights of citizens to information, provide a mechanism for information exchange of information, information security and information communications.

It is an indisputable fact that the threat to the safe development of man and society is also the lack of desire of one or another part of the population to reconcile their interests with the public. This threat is a complex problem of socio-economic and socio-political development, especially in countries where there is a significant imbalance of interests of social groups. Therefore, the positive results of improving the socio-psychological situation in society, team, family are possible provided that the predominance of citizens collectivist type of motivation

At the same time, as IM Sopilko rightly points out, "the information space is key to the country's development, because it allows us to perform many tasks. In modern conditions, we are witnessing how the Ukrainian information space is formed mainly under the strong influence of external and internal factors. These include the ongoing military actions in the East, the economic crisis, the devaluation of the national currency, the influence of international organizations on resolving the conflict in Ukraine, and so on. In such conditions, we are constantly taught, but in fact -

actually impose behavioral algorithms, turning into good subjects of information relations – information zombies[517].

Today, the main threat to man and society remains violence in order to gain or maintain political, economic and cultural domination of a social group, which is often accompanied by strong informational and psychological influence through the media and discriminates against a person or social group, restricting their rights and freedoms.

Determining the definition of the protected interests of citizens in the field of information relations, it is necessary, in our opinion, to rely on the practice of the Constitutional Court of Ukraine. The latter, in particular, notes that the interests protected by law are the interests of a particular person (or group of persons), which are based on the law or follow from other legal norms and are protected by the state along with rights. The list of interests of citizens in the information sphere is not defined by the domestic legislation, and therefore the question of existence of the corresponding protected interest is solved in each separate case. Protection of rights is a complex category, which is often identified with related concepts such as "protection", "defense", etc. However, they all have a different meaning and therefore can not be used as synonyms. The legislator of Ukraine establishes some definitions of these concepts, however, it narrows their content and notes that the above definition can be applied only to the normative act in which it is given. According to GM Stoyakin, legal protection includes three points: the publication of rules that establish rights and responsibilities, determine the implementation of their protection and the application of sanctions; activities of subjects to protect their subjective rights; preventive activities of the state and public organizations, as well as activities for the implementation of legal sanctions;activities of subjects to protect their subjective rights; preventive activities of the state and public organizations, as well as activities for the implementation of legal sanctions; activities of subjects to protect their subjective rights;

[517] Sopilko I.M. Information threats and security of modern Ukrainian society. Legal Bulletin. 1 (34). 2015. P. 75-80.

preventive activities of the state and public organizations, as well as activities for the implementation of legal sanctions.

In the EU, information security is aimed at creating conditions under which the state of human rights protection in the information sphere is ensured, as the main goal and value of information security. As a result, information security becomes one of the guarantees of human and civil rights in the information sphere. Guarantees of human and civil rights are understood as a system of conditions, means and methods by means of which equal opportunities for realization, protection and protection of human and civil rights are provided. Ensuring information security as a guarantee of human rights is inextricably linked with other types of guarantees and finds its expression in them[518].

In the information sphere of Ukraine, the following vital interests of a person are distinguished: protection from negative information influence (including in cyberspace); ensuring the constitutional rights and freedoms of man and citizen to collect, store, use and disseminate information; prevention of unauthorized interference with the content, processes of processing, transmission and use of personal data.

The conditions for protecting human rights in digital and offline environments are different. From the point of view of the Cyber Security Strategy of Ukraine, the digital environment is characterized by technical guarantees of human rights, which are presented in the form of hardware and software and technical standards. Hardware and software (hereinafter – hardware) include computers and specialized devices based on them, operating systems, programming systems, system-wide and application software[519]. Technical legal norms determine the conditions of design, manufacture and use of technical means. In ensuring information security in the digital environment, the role of technical and legal (hereinafter – technical) guarantees of human rights is growing, due to technical means of

[518] Serhii Yesimov, Rostyslav Sopilnyk, Myroslav Kovaliv, Ruslan Skrynkovskyy. Human and Citizen Rights Guarantees While Providing Information Security. Path of Science = Path of Science. 2018. Vol. 4, No. 5

[519] Pavlysh, VA, & Holinenko, LK (2013). Osnovy informatsiinykh tekhnolohii i system [Fundamentals of Information Technology and Systems]. Lviv: Lvivcka politekhnika P. 121.

protection. In this aspect, it is advisable to agree with O. Kharitonova and other scientists that the Internet relationship is a new type of social relations that arise, change and cease in cyberspace[520].

The technical guarantees of human rights correspond to the concepts of "privacy through design decisions" and "security through design decisions".

Privacy due to design decisions provides a system of protection of personal information built into technical means, which excludes its transfer to other persons. Security through design decisions includes both the protection of the right to privacy and the protection of the rights of all participants in information interaction, which allows the transfer of confidential information necessary to protect the rights of others. A. Cavoukian[521]provides the following principles of privacy through design decisions: proactivity (preventive and non-corrective action); confidentiality as a default parameter; privacy is built into the design; full functionality; permanent security (complete protection of the life cycle); visibility and transparency; respect for user privacy.

For example, manufacturers of hardware (Microsoft, IBM, Sun Microsystems, Hewlett-Packard, etc.) have implemented the principles of privacy through design solutions.

Technical guarantees of human rights are becoming a necessary component of information security of the state in combination with legal guarantees, as indicated by the tendency to recognize the principles of privacy on the basis of design decisions in European Union law as legal acts. In Ukraine, the legislator defines legal guarantees through a number of Laws of Ukraine "On technical regulations and conformity assessment", "On metrology and metrological activities" and other regulations. Such legal guarantees are provided by the state within the framework of the function of ensuring the security of society as a whole and the individual.

[520] Kharitonova, OI, Ulyanova, GO, Kirilyuk, AV, Simonyan, Yu. Yu., Baadzhi, NP, Pozova, DD, Martyniuk, IV Problematic issues determination of the legal nature and structure of intellectual property relations arising on the Internet. *Scientific works of NU OYUA* (2015), P. 160.

[521] Privacy by Design Center of Excellence. (nd). The Seven Foundational Principles. Retrieved April 1, 2018, URL: https://goo.gl/ofgwa6

In ensuring information security, legal regulation is complemented by self-regulation, which creates conditions for resolving conflicts with minimal involvement of public authorities, whose intervention is mainly limited to prosecution for offenses. Internet access providers, within the framework of agreements between public authorities and providers, set up hotlines, adopt codes of conduct for industry associations, develop other forms of partnership between the state and non-governmental organizations, on the basis of which information intermediaries block and filter information, thereby limiting freedom of expression and the right of access to information.

Restrictions on human rights in the digital environment are formally enshrined in regulations and are complemented by factual restrictions, which are expressed in the responsibilities of technical actions imposed on developers of technical means and information intermediaries. At the same time, coercion in the information sphere, carried out using technical means, is one of the ways to ensure public access to personal information and acts as a restriction of the right to privacy, but is carried out to ensure information security of the state.

Quite often there is an absorption of personality by information technology, in which people lose their spiritual freedom and personality in general for the material benefits obtained from participation in various network systems,

Today there are risks and threats to business, and through it to national security, in economic, technological, environmental, political and other areas that await business today and in the future.

A separate aspect of specific threats in various areas of entrepreneurship is the staff and, in particular, the lack of skilled workers. For the pandemic situation in 2020, and possibly in the next few years, a significant increase in unemployment can also be expected against the background of a shortage of skilled workers and unwillingness to occupy low-paid or socially unattractive positions. consequences of the impact of the COVID-19 pandemic on the functioning of the modern labor market. Thus, the key negative consequences of the coronavirus outbreak are: threat to the health of Ukrainian citizens, reduced economic activity and restricted

movement of people, delayed investment processes, reduced jobs, reduced hours worked, reduced labor supply, reduced employment, the spread of part-time and informal employment, rising unemployment, declining wages, significant losses of workers' incomes, deteriorating social protection, the emergence of "working poor", growing inequality. At the same time, the loss of labor income will lead to a decrease in consumption of goods, services and works, which, in turn, will exacerbate the problems of doing business and lead to a sharp decline in the economy in the regions of Ukraine.

Undoubtedly, with the introduction of quarantine in schools and the introduction of a number of other measures to combat the spread of coronavirus infection COVID-19 from March 12, 2020, and from March 25, 2020 – the introduction of an emergency in Ukraine, many employees were deprived of the opportunity to walk to work. Interruptions in the work of enterprises, regardless of their size, loss of jobs, significant reduction of incomes of our citizens, shutdown of subways in Kyiv, Kharkiv and Dnipro, termination of long-distance and interregional road, rail and air connections, forced many people to gain new experience – work from home, taking advantage of the opportunities offered by modern technologies. At the same time, in the regional labor markets of Ukraine there was an active increase in the number of vacancies for remote work. Therefore,

As O. Myronets rightly points out during COVID-2019 and after COVID-2019, the security environment in this area should be supported by modern legislation on legal technologies as regulatory and protective instruments used by national governments and involved international organizations[522].

The protection of information security of young people remains an important issue. As envisaged in the Joint Report of the Council and the EU Commission on the implementation of the renewed framework of European cooperation in the youth field (2012-2020), forms of cooperation for young people in 2018-2020 should aim to empower young people, especially those at risk of social exclusion. This issue remains relevant in the context of remote work during the

[522] Myronets O., Olefir V., Golosnichenko I., Pyvovar Yu. (2021). Legal technologies as instruments of civil aviation safety improvement in conditions of the fight against COVID-2019. Magazine of the University of Zulia. 12, 32, 445-459. DOI: 10.46925//rdluz.32.26

fight against the epidemic of coronavirus Covid-19. To this end, the EU has several initiatives to support the actions of Member States. In line with the Union's action in the fields of education, training, youth and sport, as regulated by the Erasmus + Regulations, EU funding under this program complements political cooperation in the fields of youth policy, volunteering and participation in democratic life. Other institutions, such as the European Social Fund (ESF) and the Youth Employment Initiative (YEI), will provide funding to attract young people to the labor market and develop their social potential. The formation of the legal culture of youth in modern society is carried out in the context of international practice.

For example, the Code of Conduct on Illegal Online Hate Speech, developed by the EU in conjunction with Microsoft, Facebook, YouTube and Twitter, sets out an obligation to deal with complaints about profanity within twenty-four hours. One of the most interesting aspects of content quality regulation is the clear regulation of the right to rebut or respond. Compared to the print media, online media must review a counterargument or response within five days. This is due to the high speed of information exchange on the Internet. This situation is illustrated by the case of Douglas v. "Hello!", Where an English court found that in the case of illegal dissemination of negative information, each new review of such material constitutes a new invasion of privacy.

The need for legal regulation of Internet activity of young people is due to the fact that according to a number of sociological studies, the socio-demographic group of young people is the main user of the Internet, indicating the impact on their behavior and social practices, including those related to law. In the information field there are both positive factors in the formation of legal culture, such as expanding access to information legal resources, and negative: the promotion of deviant behavior, including extremism and terrorism. The legal culture of youth is a complex and multifactorial phenomenon of modern reality that directly affects society. Factors of informatization and computerization of modern society have a significant influence on its formation and development. In addition to the positive aspects of information and

technological progress, such as expanding young people's access to legal information, opportunities for self-education and legal information of citizens, there are also negative ones, such as simplifying and accelerating the dissemination of extremist information. Thus, the Internet not only simplifies the speed of dissemination of extremist and terrorist information, but also allows attackers to anonymize their manifestations. The problem of using new technologies for extremist purposes especially affects such a vulnerable part of society as young people. The Internet not only simplifies the speed of dissemination of extremist and terrorist information, but also allows attackers to anonymize their manifestations. The problem of using new technologies for extremist purposes especially affects such a vulnerable part of society as young people. The Internet not only simplifies the speed of dissemination of extremist and terrorist information, but also allows attackers to anonymize their manifestations. The problem of using new technologies for extremist purposes especially affects such a vulnerable part of society as young people.

Prevention of human rights violations is a key part of the protection policy of every country in the world Prevention of human rights violations is a key part of the protection policy of every country in the world[523].

Hybrid warfare remains an acute problem of human protection. The state of danger in which not only the occupied part of Ukraine, but the whole state found itself, largely depends on the state policy of guaranteeing human security, human rights and freedoms in every sphere, including information. Various negative informational and psychological influences lay the groundwork for further operations directed against the interests of Ukraine at all levels – individuals, society and the state.

The Allied Commander Europe, Breedlove, said, "This is the most amazing information blitzkrieg we have ever seen in the history of information wars." The information front of the "hybrid war" is unfolding in several directions at once. First of all: (1) among the

[523] Myronets, OM, Burdin, M, Tsukan, O, Nesteriak, Yu (2019). Prevention of human rights violation. Asia Life Sciences. 21 (2). R. 577-591. http: //www.scopus.com/inward/record.url? Eid = 2-s2.0-85077194650 & partnerID = MN8TOARS (Scopus)

population in the conflict zone; (2) among the population of the country against which aggression is being carried out, but whose territory is not affected by the conflict; (3) among the citizens of the aggressor's country and (4) among the international community".

In a hybrid war, a state that has become the object of aggression inevitably faces a wide range of information threats, the neutralization of which, on the one hand, requires emergency legal and administrative measures, and on the other – may be accompanied by a significant curtailment of democratic rights and freedoms. Finding a balance between the interests of national security and the ideas of the rule of law is a strategically important task of the state.

The media is perhaps the most effective weapon used in modern hybrid wars. In view of this, the state policy in the field of information law should focus on the selective application of restrictions on specific media, which have proven to be unfriendly, biased and manipulative. This approach requires maximum legal certainty of restrictive criteria, as in their absence there is a risk of banning unbiased and politically neutral media (for example, in the case of unintentional dissemination of inaccurate information). At the same time, a wide range of public figures and organizations emphasize that the established prohibitions are devoid of factual grounds, have no legal basis, contradict the Constitution, and oppress democratic rights and freedoms. Therefore, any restrictions in the information environment should be specific and apply only to those resources that have compromised themselves by specific actions or are a source of threats to the state and society[524].

It should be noted that currently the situation regarding the information security of Ukrainian citizens can be conditionally classified into several categories: 1) information security of Ukrainian citizens living in the Autonomous Republic of Crimea and in the temporarily occupied territories; 2) information security of servicemen and other persons directly involved in the anti-terrorist operation, members of their families, as well as the civilian

[524] Gurzhiy T. Information law: challenges of hybrid warfare. Foreign trade: economics, finance, law. 2018. № 4. P. 16–26.

population of the Ukrainian territory where the anti-terrorist operation takes place; 3) information security of the population of Ukraine living in "peaceful" territories. The state has a duty to protect people from real and potential threats, as well as abuses of "information power" in any sphere of society and the state[525].

Information and psychological influences are exacerbated by traditional administrative methods of violating information rights and human freedoms – obstructing the media, restricting access to the network or certain resources. In addition to new media, traditional methods of propaganda through the press, radio, television, film and print products are actively used. It should be noted that the protection of Ukraine's information space was not started even immediately after the beginning of the anti-terrorist operation, numerous TV series and movies, radio and TV programs with anti-Ukrainian sentiments were broadcast nationwide on Ukrainian air.

A striking example of information and psychological influence on the minds of children in the confrontation between Ukraine and Russia is the printed materials. A new illustrated children's educational and entertaining magazine "Polite People" was presented in occupied Luhansk. The products are designed for preschoolers and children of primary school age. The main characters of the story are heroic children in the images of the so-called "fighters of Little Russia", and in the negative characters of this story it is not difficult to recognize the President of Ukraine, the Prime Minister and the Secretary of the National Security and Defense Council. Such distortion of facts, insults and contempt for the first persons of the state form in children's minds a distorted picture of perception of the present, changes their values and life orientations and is unlikely to bring up a decent person with a high level of legal awareness and civil position[526].

Thus, the state information policy should take into account the specifics of different categories of the population that are exposed to information and psychological influences with different intensity and

[525] Pilipchuk VG, Brizhko VM Information security and privacy in the field of personal data protection. **Information and Law. 2016. № 4 (19). P. 60-70.**

[526] The children's magazine "Polite People" was published in Luhansk People's RepubliP. URL: http://korrespondent.net/ukraine/3630876-v-lnr-yzdaly-detskyi-zhurnal-vezhlyvye-chelovechky

different methods. Given the realities of the information society, the state must take care of the person and direct all efforts to protect it and ensure the integrity of the person, his ability to develop as the defining categories of human existence.

A separate category is the risks associated with the problem of personal data protection. IP by its nature is focused on collecting large amounts of data. Among them may be data that should be classified as personal. An important feature of IP systems is that the active use of a large number of sensors creates the conditions for the formation of data sets, including personal. The main aspects of the current problem of personal data protection are contained, for example, in the report of the US Federal Chamber of Commerce:

- the benefits of implementing IP are minimized by the presence of negative consequences, such as threats to the confidentiality of personal data;
- over-regulation of personal data protection can lead to a slowdown in investment in any sector;
- adoption of the necessary regulations for guaranteed protection of personal data will increase consumer confidence in new technologies;
- it is necessary to wait for the manifestations of negative consequences and, only after that, to take regulatory measures;
- it is advisable to use self-regulatory mechanisms instead of regulation by legislation. It should also be noted that in our time the very concept of personal data has undergone some expansion compared to the traditional understanding of them as "passport data". According to the General Data Protection Regulation (GDPR), which operates within the framework of the European Union legislation on personal data protection, this concept is defined as **"інформація any information concerning an individual who has been identified or can be identified"**[527]. Similarly, this concept is defined by the Law of Ukraine "On Personal Data Protection".

Therefore, the dissemination of personal data does not necessarily have to be purposeful. Large amounts of information can

[527] On the protection of individuals with regard to the processing of personal data and on the free movement of such data, and the repeal of Directive 95/46 / EC (General Data Protection Regulation): Regulation (EU) 2016/679 of 27.04.16 URL: https://gdpr-text.com/? Col = 2 & lang1 = ukr & lang2 = en & lang3 = rumain (access date: 09.11.2020).

be disseminated, which include, but are not limited to, personal data. And this makes it extremely difficult to control the operation of the system. As a result, we have a significant complication of the issue of liability for such unauthorized dissemination of personal data. After all, it is unknown in advance whether personal data is disseminated or not.

If we talk about human information security, the policy on it is at the intersection of several priority areas of public policy – first of all, information policy, national security policy and human rights policy, but also legal policy, social policy, education and science policy. , and even foreign policy. At the same time, in each direction, a single approach to ensuring human information security should be taken into account – creating conditions for timely detection of potential and real threats; development and implementation of measures and means to prevent and counter challenges; neutralization or mitigation of hazards. Therefore, it is considered expedient to determine at the level of an independent state body to consolidate the institution of the Commissioner for Information Security, as an analogue of the institution of the Information Commissioner adopted in the EU.

Ensuring the prosperity and security of citizens requires resources that, with the involvement and efficient use of external sources, can ensure sustainable and dynamic economic growth. It is necessary for this[528]:

- to develop market competition, ensure demonopolization of the economy and de-shadowing of economic relations;
- protect property rights;
- ensure deregulation and prevent pressure on business;
- create competitive conditions for attracting investments, in particular foreign ones;
- ensure the sustainable functioning of the financial system, consistency of monetary policy and increase confidence in national financial institutions;

[528] Presidential Decree "On the decision of the National Security and Defense Council of Ukraine of September 14, 2020. " On the National Security Strategy of Ukraine" №392/2020 https://www.president.gov.ua/documents/3922020-35037

- improve legislation on the organization of the judiciary and ensure fair justice;
- create favorable, in particular financial, conditions for the development of science, ensure the development of research infrastructure, as well as effective interaction of scientists with the public and private sectors, stimulate innovation and introduce new technologies, including security and defense, health, industry, energy, mechanical engineering, agriculture, construction and infrastructure, sports, information and telecommunications;
- to promote the development of the aviation and space industries as having significant potential and opportunities for the production of high-tech products for civil and defense purposes;
- identify and implement a reliable control mechanism for the use of new technologies to ensure human and environmental safety;
- to reform land relations, providing for the introduction of the circulation of agricultural land, the implementation of measures to streamline the accounting of land resources, to ensure environmentally oriented development of the agro-industrial complex and food security;
- to modernize transport infrastructure - roads, railways, pipelines, airports, sea and river ports, etc., including through public-private partnership mechanisms, to conduct transparent privatization in order to attract domestic and foreign investment in modernization and development of the enterprise, to promote productivity in the economy.

When a citizen feels safe, it is safe to say that national security is appropriate. It is important for Ukraine today to affirm the constitutional principle of the rule of law, equality before the law. In order to implement the constitutional principles of individual legal responsibility and the inevitability of punishment, the state will: resolutely oppose attempts to incite national, racial or religious hatred and hatred, humiliate national honor and dignity, insult the feelings of citizens through their religious beliefs race, color, political, religious and other beliefs, sex, health status, ethnic and social origin, property status, place of residence, language or other characteristics. Important actions must be resolute opposition to humanitarian

aggression, the development of Ukrainian culture as the basis for the consolidation of the Ukrainian nation and the strengthening of its identity. Law enforcement agencies should investigate criminal offenses committed in the temporarily occupied territory of Ukraine, as well as in areas of national security and defense, as well as deter the armed aggression of the Russian Federation in Donetsk and Luhansk regions.

Summary. Conclusion. Human information security is determined by its essential features, basic functions, taking into account the constant dynamics of information and social systems.

The development of legislation in the field of human information protection requires effective cooperation between public authorities, civil society institutions, commercial structures and the scientific potential of the state. The development of legislation on human information security requires the creation of effective mechanisms for active participation in the legislative activities of its subjects – proper access to draft regulations in these areas, real public discussions, as well as taking into account their results.

Doctrinal research requires issues related to the legal provision of the use of artificial intelligence and robotics, big data analysis technologies, and the use of genetic information.

The content of two basic categories that are decisive for the legal basis of information security of a person – information rights and human freedoms, as well as human rights and freedoms in the information society are singled out and substantiated. Under information rights and freedoms, it is proposed to understand a set of rights derived from freedom of information, as a fundamental human right, which includes: 1) information rights related to the person (personality) of man; 2) ownership of information; 3) the right to access information; 4) freedom to disseminate information in any lawful manner; 5) the right to a secure information environment.

Along with the legal restrictions on human rights in ensuring information security is the development of de facto restrictions, which are expressed in technical coercion, which is to impose responsibilities on information intermediaries and developers of

technical means, the implementation of which affects the boundaries of human rights.

However, the main problem in protecting society from the impact of harmful information is not so much the lack of legal framework, as non-compliance with current legislation by government officials, inaction of authorized bodies, improper response or illegal response. Another problem is the lack of coordination between different authorities, setting personal ambitions above the common good, unprofessionalism and irresponsibility of officials in the performance of their duties. Problems of sabotage or lack of coordination cannot be solved by adopting any new document. They are solved by systematic and systematic work of senior officials of the state on the implementation of current legislation.