UDC: 340:659.4.327.88(477)
DOI: https://doi.org/10.32689/2617-2224-2019-17-2-151-169

Lysenko Serhiy Oleksiyovych,
PhD in Law, Associate professor, Associate professor of the Department of Security Management and Law Enforcement and Anti-Corruption Activities, Interregional Academy of Personnel Management, 03039, Kyiv, Str. Frometivska, 2, tel.: (044) 490 95 00, e-mail: crimeconsult@ukr.net
ORCID: 0000-0002-7050-5536

Лисенко Сергій Олексійович,
кандидат юридичних наук, доцент, доцент кафедри управління безпекою, правоохоронної та антикорупційної діяльності, Міжрегіональна Академія управління персоналом, 03039, м. Київ, вул. Фрометівська, 2, тел.: (044) 490 95 00, e-mail: crimeconsult@ukr.net
ORCID: 0000-0002-7050-5536

Лысенко Сергей Алексеевич,
кандидат юридических наук, доцент, доцент кафедры управления безопасностью, правоохранительной и антикоррупционной деятельности, Межрегиональная Академия управления персоналом, 03039, г. Киев, ул. Фрометовская, 2, тел .: (044) 490 95 00, e-mail: crimeconsult@ukr.net
ORCID: 0000-0002-7050-5536

MODERN TRENDS OF INFORMATIONAL SECURITY DEVELOPMENT, AS A LITERARY OBJECTIVE

Abstract. This article deals with issues related to the experience of developed countries on information security as an object of legal relations and national experience in the structure of information law as a complex industry in the legal field of Ukraine.

The issue of information security is already reflected in the current legislation of Ukraine. In particular, the Constitution of Ukraine and a number of other regulatory acts consider information security at a level with sovereignty and territorial integrity. This concerns, first of all, information security as a component of national security. However, over time, more and more attention of researchers is paid to information security, not only at the state level, but also at the level of individual subjects of legal relations.

As part of the study, the content of the concept of "information security" is proposed to be understood as a selected type of public activity related to the creation,

circulation and use of information by certain subjects, which is expressed in the norms of the rules of conduct regarding its protection, protection, preservation and maintenance of vital needs, interests of people social communities, society, state, international community.

In the course of the research, the author analyzes the experience of forming a system of legal regulation of information (including computer) security of the United States, The United Kingdom of Great Britain and Northern Ireland, Israel, and the Federal Republic of Germany. The example of Israel is especially valuable for Ukraine. First of all, the establishment of an effective information security system requires the allocation of a significant part of the gross domestic product to the needs of scientific and technical studies of a military nature. No less interesting is the experience of creating information technology development centers like the Israeli Mamram and 8200.

Information security both at the state level and at the level of individual subjects of legal relations requires the formation of extensive and balanced legislation, adequate funding, and the like. A separate problem is the ratio of security needs and the rights and freedoms of citizens. All this requires taking into account the leading foreign experience. However, the formation of a reliable information security system of the state is extremely important for Ukraine, and therefore requires the consolidation of all forces.

Keywords: law, information security, information law, foreign experience, information technology development.

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ОБ'ЄКТА ПРАВОВІДНОСИН

Анотація. Розглядаються питання, пов'язані з досвідом розвинених країн щодо інформаційної безпеки як об'єкта правовідносин та національного досвіду у структурі інформаційного права, як комплексної галузі у правовому полі України.

Проблематика інформаційної безпеки вже знайшла своє відображення у чинному законодавстві України. Зокрема, Конституція України та ряд інших нормативно-правових актів розглядають інформаційну безпеку на рівні з суверенітетом та територіальною цілісністю. Це стосується, насамперед, інформаційної безпеки як складової національної безпеки. Однак з часом дедалі більше уваги дослідників приділяється інформаційній безпеці не лише на рівні держави, а й на рівні окремих суб'єктів правовідносин.

У межах дослідження зміст поняття "інформаційна безпека" пропонується розуміти, як виділений вид суспільної діяльності пов'язаної зі створенням, обігом та використанням інформації певними суб'єктами, що знаходить вираз у нормах правил поведінки щодо її охорони, захисту, збереженню, підтриманню життєво важливих потреб, інтересів людей, соціальних спільнот, суспільства, держави, міжнародного співтовариства.

У процесі дослідження аналізується досвід формування системи правового регулювання інформаційної (в тому числі — комп'ютерної) безпеки

США, Об'єднаного Королівства Великої Британії та Північної Ірландії, Ізраїлю, ФРН. Приклад Ізраїлю видається особливо цінним для України. Налагодження ефективної системи інформаційної безпеки потребує виділення значної частки валового внутрішнього продукту на потреби науково-технічних досліджень військового спрямування. Не менше цікавим видається досвід створення центрів інформаційно-технологічного розвитку на кшталт ізраїльських центрів "Мамрам" та "8200".

Інформаційна безпека як на рівні держави, так і на рівні окремих суб'єктів правовідносин потребує формування розгалуженого та збалансованого законодавства, належного фінансування тощо. Окремою проблемою постає співвідношення потреб безпеки та прав і свобод громадян. Все це вимагає врахування провідного зарубіжного досвіду. Однак, формування надійної системи інформаційної безпеки держави є вкрай важливим для України, а тому потребує консолідації всіх сил.

Ключові слова: право, інформаційна безпека, інформаційне право, зарубіжний досвід, інформаційно-технологічний розвиток.

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ОБЪЕКТ ПРАВООТНОШЕНИЙ

Аннотация. Рассматриваются вопросы, связанные с опытом развитых стран по информационной безопасности как объекта правоотношений и национального опыта в структуре информационного права как комплексной отрасли в правовом поле Украины.

Проблематика информационной безопасности уже нашла свое отражение в действующем законодательстве Украины. В частности, Конституция Украины и ряд других нормативно-правовых актов рассматривают информационную безопасность на уровне с суверенитетом и территориальной целостностью. Это касается, в первую очередь, информационной безопасности как составляющей национальной безопасности. Однако, со временем все больше внимания исследователей уделяется информационной безопасности не только на уровне государства, но и на уровне отдельных субъектов правоотношений.

В рамках исследования содержание понятия "информационная безопасность" предлагается понимать как отдельный вид общественной деятельности, связанной с созданием, обращением и использованием информации определенными субъектами, который выражается в нормах правил поведения касательно ее охраны, защиты, сохранения, поддержания жизненно важных потребностей, интересов людей, социальных общностей, общества, государства, международного сообщества.

В процессе исследования анализируется опыт формирования системы правового регулирования информационной (в том числе — компьютерной) безопасности США, Соединенного Королевства Великобритании и Северной Ирландии, Израиля, ФРГ. Пример Израиля представляется особенно ценным для Украины. В первую очередь, налаживание эффективной систе-

мы информационной безопасности требует выделения значительной части валового внутреннего продукта на нужды научно-технических исследований военной направленности. Не менее интересным представляется опыт создания центров информационно-технологического развития вроде израильских центров “Мамрам” и “8200”.

Информационная безопасность как на уровне государства, так и на уровне отдельных субъектов правоотношений требует формирования разветвленного и сбалансированного законодательства, надлежащего финансирования и тому подобное. Отдельной проблемой является соотношение потребностей безопасности и прав и свобод граждан. Все это требует учета ведущего зарубежного опыта. Однако, формирование надежной системы информационной безопасности государства является крайне важным для Украины, а потому требует консолидации всех сил.

Ключевые слова: право, информационная безопасность, информационное право, зарубежный опыт, информационно-технологическое развитие.

Problem statement. The security of information activities in Ukraine constantly deserves attention, and therefore its recognition as an important component of the life of various subjects of society. The activities of individual entities in the information sphere have a certain impact on the life of the state as a whole. Information security determines its role in the regulation, protection and security of various socially significant legal relations and individual processes. This can determine the main directions of state policy and the content of the activities of the state and non-state bodies related to the management of the information sphere in society. The main issue, in this direction, is information security as a way of management. All over the world management, depending on the dangers has long been accepted as the norm. The reason for this is that the interests of organizations with high performance and achievements do not require administrative intervention. And those that have any threats, demand administrative attention and intervention. Therefore, it is information security that comes to the fore as a lever of management of the organization.

The norm of part 1 of Art. 17 of the Constitution of Ukraine [1] establishes that “protection of sovereignty and territorial integrity of Ukraine, ensuring its economic and information security are the most important functions of the state, the cause of the Ukrainian people”. Thus, in legal relations in Ukraine information security is considered at the level of sovereignty and territorial integrity, as well as economic security. The above-mentioned constitutional and legal components of the country’s security are developing in the special legislation of Ukraine in certain areas of regulation, in different time frames of the existence of the independence of the modern Ukrainian state.

The Declaration on state sovereignty of Ukraine states that state sovereignty is the “supremacy, independence, com-

pleteness and indivisibility of the power of the Republic within its territory and independence and equality in foreign relations" [2]. This leads to the idea that the meaning of information security as a component of national security is determined from the fact that its source is considered not only the sovereignty of the state, but also the sovereignty of individuals and organizations as subjects of information relations.

Not so long ago, in the research of scientists the state was the main subject of information security. Most researchers supported the view that the problem of protection, security, support, preservation of information security appeared many centuries ago. At the same time, the concept that the key idea of the subject of information security is the preservation of the secrecy of information, differently linked to the ancient times dominated. The arguments for this are references to the first methods of message encryption in various branches of human activity. They date back to the 4th millennium BC. For example, one of the early dummy ciphers was the Caesar cipher, in which each letter in the message was changed by a letter through several positions from the alphabet. This cipher was named Julius Caesar cipher, after the man who used it, with a shift of 3 positions to communicate with generals during military campaigns [3, p. 35–40].

Over the course of history, the attitude of society towards understanding the essence of information security has changed. General, consolidated object or subject of legal relations, information security began to stand out with the content of special rights and obligations.

Analysis of recent publications and research. Among modern legal scholars, dealing with this issue in Ukraine, we propose to consider the studies of the following scientists: N. V. Banchuk, G. V. Vynohradova, O. D. Dovhan, R. A. Kaluizhnyi, K. I. Beliakov, B. A. Kormych, O. V. Copan, A. I. Marushchak, A. I. Movchan, E. I. Nyzenko, V. G. Pylypchuk, A. M. Podoliak and others.

The content of the category "information security" is determined by researchers from the content of the general concept of "security". It is understood, in a broad sense, as a state of security, and in special, public type of legal relations. Some issued of the history of legal research of information security in society are not systematized, for inclusion in the administrative law or information law.

For the purposes of our study, the content of the concept of "information security" is proposed to be understood as a separate type of social activity associated with the creation, circulation and use of information by certain subjects, which is expressed in the rules of conduct with respect to its protection, security, preservation, maintenance of vital needs, interests of people, social communities, society, state, international community.

Formulation of the aims of the article. On the basis of the system applied analysis of legal acts and comparative approach of foreign experience, some results of scientific analysis regarding the development of research of public understanding of information security in the world, as well as its place in information law as a complex branch of law maintenance of vital needs, interests

of people, social communities, society, state, international community are offered.

Presentation of the main material of the study. Modern information law operates in public relations, which arise, are implemented and terminated in the interaction of subjects for information. Its aim, right, its main component havethe function of ensuring, namely, compliance with the desired norms in society rules of behavior of subjects and of avoiding deviations that defines the content of the rule of law [4, p. 13–14].

The adoption of the Law of Ukraine "On information" was a significant historical stage in the Ukrainian society on the way of creating a common view on information relations and, accordingly, information security [5]. However, in this Law, the wording of information security has not been provided.

According to legal researchers, there are methodological differences in the understanding of information security at different levels of social relations (national, state, regional, individual organizations). A separate approach was applied to the legal reflection of the security organization of the Unified State Register of Enforcement Proceedings of Ukraine. This approach differs from the approach to the security of a local network in a separate company. This necessitates the definition of such unified regulatory methods, models of protection and protection of information in respect of any entity.

It is believed that state departments of the USA in the late 60-ies of XX century were one of the first to understand and make a confident step towards the decision of the problems of computer information security, when computers cost a lot of money, and the Internet was born of the few, only military and scientific information networks [6, p. 17].

As to the the paradigm of information security of society. Every human community has its own system of values in the context of information security. It is determined by the history and mentality of the people in which there is any community. This system of values is developed by the experience of previous generations of individual social groups, corporations and the like. The destruction of community values inevitably leads to negative social consequences.

Until recently, the problem of complexity of human information security, social communities, society, state, in Ukraine were considered to be fragmentary. It was believed that only by introducing a legal regime of secrecy, declaring various legal restrictions in the field of preservation, transmission and dissemination of information, it is possible to solve the problems of support, guarantee and protection of information.

Despite the fact that information security as a separate problem was formulated only in the period of intensive computer-telecommunication informatization, it is of general character. It exists as long as humanity exists. It was simply called something else, and it manifested itself in all spheres of activity of people, societies and states. In this era, there is a danger pointed out by Professor Masuda, the author of the concept of informatization of Japan created in the early 70s. He was afraid that people and machines striving to build a democratic state, the implementation of the idea of an open society, would create a police state [7].

Another problem can be considered, for example, on the basis of the analysis of the crisis of the thirties, made by one of the most authoritative sociologists in the world Pytyrym Sorokin. He tried to find the answer to the question: what led to the appearance of such people as Hitler, Mussolini, Stalin? According to Sorokin, there are three reasons for this, each of which is of information origin. The first is a crisis in the system of law, the second is a crisis in the system of truths, the third is the crisis in the system of culture and arts. There is another problem that has been neglected both in the documents and in the already extensive literature on information security. This is a problem of information exchange that deserves separate consideration. [7]

Researches of world experience in this direction remains especially useful for domestic scientists. Therefore, further coverage and study of the formation of understanding of information security in the world is an important step to improve Ukrainian law. Special attention is paid to the countries where the world, advanced technologies, models of implementation of the integrated organization of information security are generated.

Let us draw attention to the foreign experience of the complexity of the study of information security issues arising under the influence of threats of mass dissemination of new information technologies. In 1967, an initiative group of computer security researchers was founded under the patronage of the National Committee of Standards. It included representatives of universities, computer companies, research centers and other organizations. As a result of such a combination of efforts of industrial and scientific specialists of the United States, the so — called conditionally "rainbow series" was formed — a number of standards and requirements for equipment, software and personnel of various automatic data processing systems belonging to such us government agencies as NASA, the Ministry of Defense, the National Committee of standards, the Ministry of Labor, the Office of Environmental Protection, the Ministry of Arms Control, the National Scientific Society, the Federal Reserve System and finally the Center of the Joint Command of the Armed Forces. According to this model, later a National Center for Computer Security was established, which dealt with these issues systematically in the applied aspect, purposefully and comprehensively, coordinating researchers from public and private organizational structures [8].

In 1981, a similar special center at the US Department of Defense was established, it developed and implemented a specialized "rainbow series" in 1985. Thee standard "Criteria for evaluating trusted computer systems", called the Orange book (named after the color of the cover (orange) became the most important for assessing the quality of commercial digital products, that process and maintain confidential information. It is now considered as an approximate (model) world standard, including the specification for laser audio disc and shader model OpenGL. Traditionally, although improved, computer security standards in different countries are also called "Orange books". The model feature of such standards is the maximum flexibility and universality of infor-

mation security assessment of various subjects of social relations under the conditions of their functioning in the Information Society (at the global level of computer telecommunications) [6].

International legal acts can be considered as a way to form universal models of information security organization at the cross-border level. In particular, in the Memorandum of understanding on cooperation in the field of telecommunications and the development of global information infrastructure between the government of Ukraine and the U.S. government, the parties noted their intention to be guided by the principles of creating a global information infrastructure, which introduce private investment, competitive market, flexible regulatory system, access without discrimination and universal service. Such approaches were recorded in the decisions of the First World Conference on telecommunications' development of the International telecommunication Union (Buenos Aires, 1994) [9].

Information security in the UK has its own history and features. The UK does not have its own Constitution. In 1998, the British Parliament approved the Human Rights Act, which gives the European Convention on Human Rights the force of law. The act entered into force in October, 2000.

In July 1998, the British Parliament passed the Information Protection Act, which brings a similar act of 1984 into line with the requirements of the Information Protection Directive adopted by the European Union. This law applies to accounts maintained by public institutions and private companies. It imposes a number of restrictions on the use of personal data and access to accounts. In addition, the law obliges legal entities holding such records, to be recorded at the office for the protection of information.

The Information Protection Commission is an independent agency that ensures compliance with the requirements of the law. In 1997–1998, the Commissioner received more than 4,000 complaints and issued guidance to private, financial intermediaries and debt tracking agencies.

Other legislation also contains provisions on privacy and information. In particular, the laws regulating the maintenance of medical records and the storage of information on consumer loans. The same group includes the law "On rehabilitation of offenders" (1974), the law "On telecommunications" (1984), the law "On police" (1997), the law "On broadcasting" (1996) and the law "On protection from prosecution" (1997). The provisions of these laws are constantly supplemented or partially repealed by the adoption of the Information Protection Act, dated 1998. The law "On witness testimony for the police and criminal investigation authorities" (1984) gives the police the right to enter private homes and conduct searches without a warrant if the owner is arrested for an offence. Although the police have no right to demand documents from a person before arrest, they are allowed to stop and search anyone who is suspected, right in the street. Everyone who is arrested passes a DNA sample for inclusion in the national database [9].

The Law "On interception of communication", adopted in 1985, establishes a number of restrictions that are relevant to the control of telecommu-

nications. In June 1999, the Ministry of the Interior Affairs issued recommendations for the installation of eavesdropping devices, which included numerous amendments to existing legislation. There is a provision aimed to facilitate the installation of eavesdropping devices by Internet service providers. The validity of these devices for up to three months is extended. It is allowed to use eavesdropping devices with roaming capabilities. However, such problems as the control of the judiciary and state oversight of the interception of the information in the recommendations is not affected.

For more than twenty years, steps have been taken repeatedly towards the adoption of the law "On freedom of information". The "Code of practice on access to government information", adopted in 1994, provides access to state archives, but includes 15 serious exceptions. Persons whose applications for information have been rejected may file a complaint through the Parliamentary Minister to the Parliamentary Ombudsman. In May 1999, the British government tabled a draft law allowing access to government archives and establishing a Commissioner of information to enforce the laws. This draft contains a number of significant exceptions, and is considered to be even weaker document than the current code. It has been harshly criticized by many politicians who hold different political views, as well as by non-governmental organizations. The "Freedom of information company", Charter 88 and 23 other organizations launched an action in June 1999 to request a review of the draft law. In response to criticism, Interior Minister Jack Straw announced his intention to rewrite a number of provisions, but the amended version of the draft has not yet been published [10].

The Scottish Parliament also promised to adopt a stronger Freedom of Information Act as a priority measure. The current British law "On freedom of information" provides for a number of restrictions.

The law "On the observance of state secrets" is the basis of the charges currently against Tory Herat, author of the book "Irish war", which describes in detail the tracking technique used in Northern Ireland and the UK by police and security services.

The United Kingdom is a member of the Council of Europe and has signed and ratified the Convention on the protection of persons in connection with the automatic processing of personal data, together with the European Convention on the protection of human rights and fundamental freedoms. In addition, the United Kingdom is a member of the Organization for economic cooperation and development. It adopted the OECD Directive on the protection of privacy and international exchanges of personal data.

Each of the British protectorates-the Isle of Man, the Isle of Guernsey and the Isle of Jersey has its own law and its own Commission for the protection of personal data.

On December 11, 2014, the British government released some data on the National Cyber Security program, aimed at combating cybercriminals and protecting the public interest. It became known where it is planned to spend money from the program budget, the annual volume of which exceeds 200 million pounds [11].

In 2015, most of the money was allocated to "strengthen the ability to conduct a sovereign fight against threats". This item of expenditure provided funding for the British intelligence service GCHQ (analogue of the American CIA), which is the guardian of key networks of national importance. In 2015, GCHQ shared a lot of information about cyber threats with communication companies so that they could strengthen the protection of their networks.

About 30 million pounds from the National Cyber Security program were spent on attracting the Defense Department to combat the hackers. At the same time, the armed forces have their own programs (the budget is about 500 million pounds) in the field of information security.

In 2014, the UK government reported that hackers sponsored by the authorities of some Eastern countries have managed to crack a secure local network at the national level. The defense industry has long been a target for cybercriminals hunting down military secrets.

Other items of expenditure of the government's anti-hacker program are improving the police response to cyber attacks and raising public awareness.

The report also reported that 81 % of large organizations and 60 % of small companies faced illegal penetration into their computer systems. The size of losses from such break-ins ranged from 65 to 115 thousand pounds for small businesses and 600–1150 thousand pounds for large businesses.

The policy of protecting government secret information in the UK is determined by the Security Policy Framework (SPF) [12], which replaced the previously existing document, Manual of Protective Security (MPS). SPF contains the basic principles of security policies and guidance on safety and risk management for UK government agencies and related bodies. SPF includes around 70 recommendations in the area of information security policy, grouped in 7 sections:

1. Risk management
2. Access control and information classification
3. Staff responsible for information security
4. Ensuring information security
5. Physical security
6. Counter-terrorism activities
7. Business continuity.

The content of SPF is partly developed by the Security Department of the Cabinet of Minsters of UK, partly — by the center for government communications, the main body of the UK in the field of cryptography and protection of government information [7].

Israel takes a separate place among the countries whose experience in the field of information can be useful for studying and borrowing. The way of formation of national and information security has its own unique features. Faced with many unique geopolitical challenges, Israel's founders knew that the nation's success would depend on their knowledge, ingenuity, and imagination. The negative environment in which Israel is located has forced it to rapidly form armed forces and intelligence units that were able to take part in a continuous war. The need for continued security has become the driving force of ingenuity that would spread from this tiny country around the world.

The Israelis, having firmly grasped the fact that innovation was the guarantee of national security, have directed their efforts and skills to the development of high technologies in various fields.

Intelligence services have been constantly engaged in the development and implementation of new and innovative ways of interception, decoding and analysis — no matter how they are transmitted and from what sources they would not come out. Since its inception, the closed world of electronic intelligence has existed in almost complete secrecy. For this reason, the intelligence services and divisions do not limit the use of external suppliers of special equipment and innovative technology. Instead, they had to rely on their own development and methods. As a result, it gave impetus to the emergence and development of innovations that gave rise to the most advanced technologies. Unlike many of its neighbors, the Israelis could not just drill wells and extract oil. Their main resource was their own brain. From the very first days as citizens of the new power, they turned science into an instrument of nation-building.

Immigration has become the lever that has set in motion the wheel of Israeli society, turning it into a kind of orderly chaos. The constant flow of immigrants formed a culture that was in constant motion. With this combination of different biographies, skills and abilities bright mosaic of mutual relations and mutual influences appeared. Due to these conditions, the legal information field and administrative bases of information security were created.

In the days of the formation of Israel, David Ben-Gurion made the right conclusion that the information security of the country should be based on the development of science. Internal development has always been critical for the country, especially since the army's needs for weapons could no longer be met by external supplies. It is not surprising that every new government of Israel has allocated a significant portion of gross domestic product on defense, spending significant funds on scientific and technological research. According to published data, Israel allocated $ 8,97 billion to the armed forces in 2002, which is 8,75 % of the gross domestic product. For comparison, Egypt, with a population that is almost 10 times bigger than that of Israel, has spent about half that of its Western neighbour for the same purposes. Israel spends more on national security than on any other need. During the 2003 elections, when the country's economy was in a very poor state and the unemployment rate was almost 10 %, security problems were considered the number one priority and helped Ariel Sharon to take up the position of the Prime Minister.

Around this time, the Mamram center was established, which was to play an important role in information technology development. It was this center that helped to turn this country of kibbutzes and diamond cutters into one of the most vibrant economic high-tech systems in the world. All units of the armed forces own computer and research centres staffed by personnel were trained at Mamram. In addition to military intelligence, Mamram is responsible for the infrastructure of data transmission systems, the introduction of new technologies [7].

At first, Mamram used Philco mainly for data processing and logistics research. However, for operation, management and maintenance, the system required specialists capable of ensuring the smooth operation of the equipment in hot and humid climates. The insects that penetrated into the equipment were of particular concern — that is how the phrase "computer bugs" appeared. Since the computer center was formed a few years before computer science became an academic discipline, Mamram established its own school of computer science education. Graduates of this school have formed an impressive community of information technology specialists. Many people strive to get into this unit, because everybody who serve in it, become very needed in the civil professions. A special approach developed in this unit (in the style of commandos) to solving problems of any complexity, as well as the ability of specialists to find creative solutions with fast and extraordinary methods, are highly demanded by the Israeli society in the field of information security business.

Since its appearance, Israel has not really known what peaceful life was like, and each of the wars has been nothing more than a war for survival. For Israelis, all regional conflicts are as memorable as for Americans their famous baseball championships: the war of independence (1948), the Sinai campaign (1956), the six-day war (1967), the war of attrition (1969–1971), the war of Yom Kippur (1973), the war with Lebanon (1982), the first intifada (1987), the Gulf war (1991), the Al-Aqsa intifada (2000). Perhaps unwittingly, the Israeli security and armed forces have become something of a national heritage and an industry. From the first days of the state's existence, its leaders understood that Israel needed one of the best information security systems in the world. Being surrounded by strong enemies, Israel had to compensate for the lack of military power with its only resources — people. The country's defense capability needed to be supported by the ingenuity of its people and the availability of reliable information [6].

Another Israeli unit called "8200" can be considered the most powerful intelligence service in Israel. Until the former soldiers began to join the ranks of entrepreneurs, this topic was perhaps the most classified. For decades, nothing was known about it at all. The Israelis guarded this secret so carefully that only a very narrow circle of educated people could accurately assess the role it played in the information wars. However, if one follows the activities of the unit in the past years, one can understand what a huge impact it has had on the development of high technology in Israel. This influence was a striking example of a special brand of Israeli innovation, formed on the background of constant threats to national security. In addition, this brand was formed largely under the influence of high creative potential, prioritization of science, technology and education — as a means of compensating for the lack of territory, resources and personnel of Israel.

In foreign sources, the unit "8200" was often compared with the National Security Agency of the United States of America. The task of this unit is to ensure the information security of Israel, as well as the collection, decoding and analysis of millions, if not billions, of

bits of data that this service collects and intercepts with the help of its complex electronic network. It is known that communications within the Palestinian authority and with other Arab countries are closely monitored by Israel. The "8200" division directly monitors the exchange of electronic messages, voice and electronic data flows through communication networks. Yoshi Melman, a correspondent for the daily newspaper Ha'aretz and co-author of the book "Every Spy a Prince", who has long kept a chronicle of the intelligence services of Israel, calls this unit "the main service in the field of data collection". It is of a higher rank than military intelligence [9].

In all its goals and tasks, the unit "8200" acts as a giant electronic agency to collect information. Every day and every minute the units of the system accumulate countless electronic signals intercepted by base stations and various interception stations. The division is a team of engineers, mathematicians, scientists, and cryptograph analysts. They all perform various tasks of electronic intelligence, the interception of mainly the output signals of different kinds. That is, employees of the Department monitor and record telephone conversations, intercept fax messages and e-mail messages, monitor the radio exchange and decrypt the message encoding. Information is transmitted to the intelligence center, where computers and complex software sort it, check for keywords and "break" the codes of encrypted messages. Then special analysts and linguists evaluate the information collected.

"8200" performs the same tasks as the General Communications Headquarters in the United Kingdom and the Office of National Security in the United States on a daily basis. However, unlike its foreign counterparts, which are civilian government agencies, "8200" is a part of Israel's military infrastructure. The second difference is that the unit is a serious player in the region and has a significant similarity with similar foreign formations, it can not be compared with global in its capabilities systems and services of the United States, leading projects such as satellite programs Echelon. Around this program, there are many assumptions about the almost unlimited capacity of the Office of National Security to intercept and analyze billions of electronic communications between the United States and other countries. However, the unit has always compensated for the lack of its own resources and budget with ingenuity. In addition, in recent years, Americans and Israelis have established cooperation in matters of information security, politics and intelligence.

Based on this, it can be noted that the administrative regulation of information security of Israel has strict legal regulation as part of the military system of the country. But this regulation has only a general model. The main difference is that against the background of strict regulation, subjects and performers in the field of information security are given a certain freedom to choose ways to overcome threats and risks. A large place is given to the unique human factor and the ability to act freely at its discretion, which is regulated by departmental norms [12].

As to education, Israeli schools and universities pay great attention to the development of STEM-education, in

addition, the practice of cooperation between venture entrepreneurs and University professors is actively introduced. For example, Adi Shamir, who develops cryptosystems, also teaches applied mathematics at the Weizmann Institute. Shamir was one of the founders of NDS, a company specializing in software development for the television industry. In 2012, it was sold to Cisco for $ 5 billion.

In Israel, the military and commercial spheres are closely linked, and information security is considered to be a priority investment. In Israel, unlike the United States, military service is mandatory, after its passage, soldiers can find themselves in the commercial sphere, as highly qualified specialists. For entrepreneurs, such personnel are of particular value, because they have not only theoretical knowledge, but also practical skills in this area.

Many companies such as Cisco, EMC, Google, Microsoft, IBM and others have opened cyber development centers in Israel. The advantages are obvious — in addition to the use of Israeli technologies, these firms have the opportunity to cooperate with highly qualified specialists.

Over time, there are more and more threats to information security, so, according to Tirosh, the demand for high-tech developments in this area will only grow. Therefore, together with the practical, legislative sphere is keeping pace.

On December 1, 2016 a law prohibiting any electronic spam, including the distribution of advertisements via sms and voice messages recorded on the tape recorder came into force in Israel.

On October 29, 2016, the Knesset adopted the law "On creation of biometric archive". Its goal is preventing the manufacture of counterfeit ID cards with the help of comparison of fingerprints and photos with those that are kept in biometric police records. All Israeli citizens over the age of 16 will have to go through the procedure of fingerprinting in one of the offices of the Ministry of Internal Affairs [6].

But this is only the external legal side of the information security of Israel. Many regulatory mechanisms are adjusted by departmental acts, which gives some flexibility to the information security procedure.

Among the latest innovations from abroad, it should be noted that on July 15, 2016 the German government approved the White paper plan on defense policy and security, including information security. It clearly states that the Russian Federation has become a real threat, which harms the existing international order and European security. First of all, it is connected with its aggression against Ukraine. Germany announced changes in its information policy towards Russia in the near future. It identifies priority interests that should be protected by the government and law enforcement agencies of the country. We are talking about increasing the amount of funds allocated for defence. The need to improve the overall information security of the entire NATO bloc was declared, for which a number of measures to reprogram the information security and update the organization of its technical equipment is carried out. The special importance of creation of the European missile defense and updating of mechanisms of implementation of information security is noted. Thus, Berlin, together with

NATO countries, declared their position on Russia's policy in Ukraine and the world, starting to create a fundamentally new system of information security of the continent [6].

According to research, information security issues today play a huge, modernized role in the field of high technology, because it is there that information (especially in digital form) becomes both a product and raw material. Modern mass community in the field of information technologies of computer telecommunications (IT) is built on the flows of so-called electronic data from different parts of the world. It is produced, processed, sold and, of course, stolen.

If we consider the security of information that is stored on traditional media (paper, photo prints, etc.), it is achieved, as always, through compliance with physical protection measures. The second side of the protection of such information is related to natural and man-made disasters. At the same time, computer information security, in general, is a broader concept than information security with respect to traditional media. This requires the formation of safety models based on the methods of an integrated approach.

As to the latest challenges of information security in the development of the Global Information Society. Some researchers draw attention to the fact that sometimes in computer networks, the attack lasts a fraction of a second. Sometimes probing for vulnerabilities being slowly stretched on the watch, making the suspicious activity of criminals practically invisible. The main purpose of attackers is always violation of the components of information security-availability, integrity or confidentiality [13].

On the way to overcome the problems of information security of organizations and the state, within a fairly short period of time, Ukrainian scientists initiated a number of regulations. First of all, they concerned the prevention by legal means of interference on the personal rights of people, citizens, their social communities, enterprises, organizations, institutions of all forms of ownership, and the like.

Carrying out a legal, comparative analysis of the content of certain international legal acts on human rights and the relevant norms of Ukraine, there are non-isolated facts when unlawful interference of the relevant state bodies in the sphere of private information and the establishment of appropriate departmental regulatory legal restrictions of constitutionally defined rules of conduct in society are allowed. This naturally causes public resistance, conflicts of interests of citizens with the authorities. However, modern Ukrainian scientists are increasing their research in this area. The main directions of activity on the organization of adequate models of information security of a person, a citizen, individuals, society and the state were identified [10].

According to Ukrainian scientist B. A. Kormych, the legal practice is based primarily on the principle of freedom of information and guarantees of information rights and freedoms of a person, while considering the rights of the state to regulate the information processes in the context of its general sovereign rights [14, p. 91–92].

In the analytical report of the Ukrainian scientists of the National In-

stitute for Strategic Studies, the problem of information security was considered from a slightly different angle. They put the issues of adequate development of information space and information processes, above all their economic component in the foreground. It was emphasized that "the key problem of information security is to assess the compliance of the information space existing in the state with the needs of its citizens, the demand and supply of information services in the places close to the users and at a convenient time for them. Historical experience shows that countries that have not been able to replenish the information space with more effective technologies in a timely manner have slowed their economic development. Conversely, countries that had strong information potential quickly regained their role in the global division of spheres of influence even after military defeats (for example, Japan after World War II). Therefore, filling the information space with the latest technologies that can significantly improve both the adequacy of the reflection of reality and the productivity of information activities in society is an urgent need, which, in turn, determines the possibility of protecting national interests" [15].

The law of Ukraine "On the basics of national security of Ukraine" [5] does not contain a separate interpretation of the concept of information security, considering it only as one of the components of national security, which is determined by the specific threats, challenges, dangers to national interests. This indicates a lack of consideration by the developers of this legislative act of all scientific developments of Ukrainian researchers.

Most importantly, a significant drawback of many scientific definitions of national and information security in its composition is their focus only on the protection of interests, and not the creation of preventive conditions for the existence of subjects of this security. This approach narrows the content of public understanding of its functional sphere, which replaces the usual (traditional) functions of the state and significantly limits democratic human rights and freedoms.

It should be noted that in the Ukrainian legislation, in some special laws, the definitions of information security are submitted one-sidedly. For example, the legal definition of information security presented in the National Informatization Program has such a drawback. In particular, paragraph 3 of section IV of this Program states: "Information security is an integral part of political, economic, defense and other components of national security. The objects of information security are information resources, channels of information exchange and telecommunications, mechanisms for ensuring the functioning of telecommunication systems and networks and other elements of the country's information infrastructure" [8, 15].

At the same time, the concept of information security of man and society, the conditions of existence of which are determined primarily by their natural rights and duties, becomes relevant only in the context of the development and implementation of the ideas of natural law, in particular human rights, citizens' rights. Everything else is secondary, including substantive techno-

logical aspects of information relations. Therefore, it is extremely important to take into account the foreign experience of developed countries to restore their own sphere of information security.

Summary. We are confident that our own information security will be unique, built on the principles of harmony and interaction of state influence and non-governmental organizations, organized based on clear regulations, but with a certain range of opportunities for improvisation of its subjects.

REFERENCES

1. Zakon Ukrainy "Konstytutsiia Ukrainy" : vid 28.06.1996, № 254k/96-VR [Law of Ukraine "The Constitution of Ukraine" : from 28.06.1996, № 254k/96-VR]. (1996). Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of the Verkhovna Rada of Ukraine, 30 [in Ukrainian].
2. Deklaratsiia pro derzhavnyi suverenitet Ukrainy : vid 16.07.1990, № 55-XII [Declaration on State Sovereignty of Ukraine : from 16.07.1990, № 55-XII]. (1990). Vidomosti Verkhovnoi Rady URSR — Bulletin of the Verkhovna Rada of USSR, 31 [in Ukrainian].
3. Yuliy Tsezar, Zapysky pro Halsku viinu [Julius Caesar, Commentaries on the Gallic War]. (1999). Moscow: Azbuka-klasyka [in Russian].
4. *Vynohradova H. V.* (2006). Informatsiine pravo Ukrainy [Information Law of Ukraine]. Kyiv: MAUP [in Ukrainian].
5. Zakon Ukrainy "Pro informatsiiu" : vid 02.10.1992, № 2657-XII [Law of Ukraine "On information"]. (1992). Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of the Verkhovna Rada of Ukraine, 48 [in Ukrainian].
6. *Skulysh Ye. D.* (2012). Istoriia informatsiino-psykholohichnoho protyborstva [History of information-psychological confrontation]. Ye. D. Skulysh, Ya. M. Zharkov, L. F. Kompantsev, V. V. Ostroukhov, V. M. Petryk (Eds.). Kyiv: Nauk.-vydav. Viddil NA SBU [in Ukrainian].
7. *Korzh I. F.* (2012). Derzhavna bezpeka: metodolohichni pidkhody do systemy skladovykh poniattia [State security: methodological approaches to the system of constituent concepts]. Pravova informatyka — Law Informatics, 4 (36), 69–75 [in Ukrainian].
8. Zakon Ukrainy Pro Kontseptsiiu Natsionalnoi prohramy informatyzatsii: vid 04.02.1998, № 74/98-VR [Law of Ukraine "On the Concept of the National Program of Informatization": from 04.02.1998, № 74/98-VR]. (1998). Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of the Verkhovna Rada of Ukraine, 27–28 [in Ukrainian].
9. *Kissinger H.* (2015). Mirovoy poryadok [World Order]. Moscow: AST [in Russian].
10. *Lysenko S. O.* (2015). Orhanizatsiini zasady ta pryiomy modeliuvannia i rekonstruktsii pry rozsliduanni pravoporushenn shchodo informatsiinoi bezpeky pidpryiemstv, ustanov ta orhanizatsii [Organizational Principles and Techniques for Modeling and Reconstruction in Investigation of Offenses in relation to Information Security of Enterprises, Institutions and Organizations]. Naukovi pratsi MAUP — Scientific Papers of the IAPM, 45, 24–29 [in Ukrainian].
11. *Dovhan O. D.* (2014). Natsionalnyi informatsiinyi suverenitet — obiekt informatsiinoi bezpeky [National Information Sovereignty is Information Security Object]. Informatsiia i pravo — Information and Right, 3 (12), 102–112 [in Ukrainian].
12. *Bilenchuk P. D., Hel A. P., Semakov H. S.* (2007). Kryminalistychna taktyka i

metodyka rozsliduvannia okremykh vydiv zlochyniv [Forensic tactics and methods of investigation of certain types of crimes]. Kyiv: MAUP [in Ukrainian].
13. *Lysenko S. O.* (2015). Rekonstruktsiia yak metod otsinky ta analizu modelei informatsiinoi bezpeky [Reconstruction as a Method of Assessment and Analysis of Models of Information Security]. Fundamental and Applied Reserches in practice of Leading Scientific Schools, 6(12). Retrieved from http://vabb.com.ua/news/rekonstrukczya-metod-ocznki-analzu-nformaczino-bezpeki.html [in Ukrainian].
14. *Kormich B. A.* (2004). Informatsiina bezpeka: orhanizatsiino-pravovi osnovy [Information Security: Organizational and Legal Foundations]. Kyiv: Kondor [in Ukrainian].
15. Zakon Ukrainy "Pro Natsionalnu prohramu informatyzatsii" : vid 04.02.1998, № 74/98-VR [Law of Ukraine "On the National Program of Informatization": from 04.02.1998, № 74/98-VR]. (1998). Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of the Verkhovna Rada of Ukraine, 27–28 [in Ukrainian].
16. Ofitsiinyi sait Departamentu kiberpolitsii Natsionalnoi politsii Ukrainy [Official site of the Department of Cyberpolicies of the National Police of Ukraine]. www.cybercrime.gov.ua. Retrieved from https://www.cybercrime.gov.ua [in Ukrainian].
17. Zakon Ukrainy "Pro osnovy natsionalnoi bezpeky Ukrainy" : vid 19.06.2003, № 964-IV [Law of Ukraine "On the Fundamentals of National Security of Ukraine": from 19.06.2003, № 964-IV]. (2003). Vidomosti Verkhovnoi Rady Ukrainy — Bulletin of the Verkhovna Rada of Ukraine, 39 [in Ukrainian].
18. *Tsymbaliuk V. S.* (2003). Problemy vyznachennia katehorii "informatsiina bezpeka pidpryiemnytskoi diialnosti" v pravi Ukrainy za umov formuvannia informatsiinoho suspilstva [Problems of definition of the category "information security of entrepreneurial activity" in the law of Ukraine in the conditions of the formation of information society]. Malyi i serednii biznes — Small and Medium Business, 1–2, 43–54 [in Ukrainian].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР // Відомості Верховної Ради України. — 1996. — № 30. — С. 141.
2. Декларація про державний суверенітет України від 16.07.1990 р. № 55-XII // Відомості Верховної Ради УРСР. — 1990. — № 31. — С. 429.
3. Юлий Цезарь. Записки о Гальській войне. — М.: Азбука-классика, 1999. — 284 с.
4. *Виноградова Г. В.* Інформаційне право України: навч. посіб. — К.: МАУП, 2006. — 144 с.
5. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII // Відомості Верховної Ради України. — 1992. — № 48. — Ст. 650.
6. *Скулиш Є. Д.* Історія інформаційно-психологічного протиборства: підручник / заг. ред., авт. Є. Д. Скулиш, Я. М. Жарков, Л. Ф. Компанцев та ін. — К.: Наук.-видав. Відділ НА СБУ, 2012. — 212 с.
7. *Корж І. Ф.* Державна безпека: методологічні підходи до системи складових поняття // Правова інформатика. — 2012. — № 4 (36). — С. 69–75.
8. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 р. № 74/98-ВР // Відомості Верховної Ради України. — 1998. — № 27–28. — С. 182.
9. *Кісінджер Г.* Світовий порядок. — М.: АСТ, 2015. — 511 с.

10. *Лисенко С. О.* Організаційні засади та прийоми моделювання і реконструкції при розслідуванні правопорушенъ щодо інформаційної безпеки підприємств, установ та організацій // Наук. праці МАУП. — К.: МАУП, 2015. — С. 24.
11. *Довгань О. Д.* Національний інформаційний суверенітет — об'єкт інформаційної безпеки // Інформація і право. — 2014. — № 3 (12). — С. 102–112.
12. *Біленчук П. Д., Гель А. П., Семаков Г. С.* Криміналістична тактика і методика розслідування окремих видів злочинів: навч. посіб. — К.: МАУП, 2007. — 512 с.
13. *Лисенко С. О.* Реконструкція як метод оцінки та аналізу моделей інформаційної безпеки, Fundamental and Applied Reserches in practice of Leading Scientific Schools, 2015-6 (12) // http://orcid.org/0000-0003-4037-9652
14. *Корміч Б. А.* Інформаційна безпека: організаційно-правові основи. — К.: Кондор, 2004. — 384 с.
15. Про Національну програму інформатизації: Закон України від 04.02.1998 р. № 74/98-ВР // Відомості Верховної Ради України. — 1998. — № 27–28. — С. 181.
16. Офіційний сайт Департаменту кіберполіції Національної поліції України. — Режим доступу: https://www.cybercrime.gov.ua
17. Про основи національної безпеки України: Закон України від 19.06.2003 р. № 964-IV // Відомості Верховної Ради України. — 2003. — № 39. — С. 351.
18. *Цимбалюк В. С.* Проблеми визначення категорії "інформаційна безпека підприємницької діяльності" в праві України за умов формування інформаційного суспільства // Малий і середній бізнес. — К.: НДІ Приватного права і підприємництва. — 2003. — № 1–2. — С. 43–54.