UDC 004.056:619.8:351.007

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 4, pp. 322-332

TRANSFORMATION OF INFORMATION AND SOCIAL-PSYCHOLOGICAL SECURITY PARADIGMS (Part 2)

S. Gnatyuk[1], V. Gnatyuk[1], V. Kononovich[2], I. Kononovich[3]

[1] National Aviation University,
Kosmonavta Komarova Ave, 1, Kyiv, 03680, Ukraine; E-mail: s.gnatyuk@nau.edu.ua
[2] Odessa National Polytechnic University,
Shevchenko Ave, 1, Odessa, 65044, Ukraine; E-mail: vl_kononovich@ukr.net
[3] Odessa National Academy of Food Technologies,
Kanatna Str, 112, Odessa, 65039, Ukraine; E-mail: kononovich@mail.ru

In this part of paper presents the results of a retrospective analysis of transitional paradigm of information security: social-centric paradigm of citizens, society, state and national security; information and cyber security transformation summary; distribution of the relative importance of measures to secure information resources; paradigm of critical information infrastructure security under the information influence conditions; the system (technology) determining the identity and identity management definition; creating a «trusted» telecom space. The received in part 1 and 2 systematization and solving problems results allows to increase the work efficiency of information, cyber social and psychological security systems and formalize directions for further researches in developing effective security systems.

Keywords: information security, cybersecurity, information & communication system, individual & group mind, social-psychological security, legal framework, paradigm.

An introduction, review of previous works and purpose of this work, is placed in the previous number of magazine [1].

Social-centric paradigm of citizens, society, state and national security

The next step 7 should serve as updating tasks IB components in the plane of the information and the information war confrontation and updating of a system of security behavior, individual and collective consciousness.

The system of national security and information security was developing for some time regardless of information security systems. The issues of social and psychological security at all stages effectively developed in the SSU, the military and other security agencies. Created significant amount of research, teaching, learning materials, and created practical working system. Regarding information security, the relevant government departments have ignored these issues. Especially because in Ukraine program of information was slowed, accumulated backlog. Thus, the introduction of «E-government» is now performed only with great obstacles.

Proposals authors on sociological and psychological security [2] also found almost no response. Then the new type of security was pointed because of the spread of information warfare operations and the emergence of the phenomenon of social media. The transition of mankind to its new type of social organization - the information society - naturally requires the development of new, so-called socio-centric paradigm of information security of state, public and private information production, which will occupy a leading position. German

military and political leader K. Clausewitz has spoken «War is the continuation of politics by other means». In the 21st century conclusions that «information warfare is the primary means of modern world politics, the dominant way to achieve political and economic power» [3]. There's information warfare is defined as «the way of the noosphere and the global information and psychological space to their advantage».

Massive computerization, introduction and development of information technology have led to the growth of information confrontation in the political sphere. Information management turned a decisive factor in winning, keeping and retention of power. The information is the main instrument of power. Information warfare, as the war is hot, has in its arsenal and immoral methods, deception, lies, half-truths, fraud, concealment and misrepresentation, etc. provocations.

The purpose of the information confrontation is a violation of information security of a hostile power, integrity and stability of its government and military control, effective information influence on leadership, political leadership (i.e., individuals who possess the greatest wealth, influence, highest status) systems, formation of public opinion and decision-making and providing of information security to gain an information advantage in information space.

In the field of information confrontation in world politics and open security of classified information is one of the decisive factors. According to the leading Chinese information warfare theorist Juan Shen Wei: «To secure the political security of the country, we must learn the information war using various media. In addition, the measures, necessary tools and technology were needed to secure against unauthorized adverse information and psychological impact» [3].

Information warfare, as a hot war, has in its arsenal many immoral practices, deception, lies, half-truths, facts of fraud, concealment, misrepresentation, manipulation, negativity, images and more. Certain types of information used to create myths or symbols that can be viable and effective. The symbol is the key to the formation of reality, the idea of building masses on how to organize life, where and why we must move. A striking example of modern myth and symbol are «Banderivets» value and power of influence which the specific individual conscience needs no comment.

In today's global information society, information weapons no less destructive than tanks and guns. It is very important who is present in the national information space. Threats are dangerous because such information and military capabilities, as television channels broadcasting foreign campaigns, Internet resources and printed media, military leaves, Internet sites of public and quasi-religious organizations and other means of anti-Ukrainian and anti-state propaganda.

Information attack can start with a surgical strike, and then the number and density of information content increases and anti-Ukrainian moves to brutal pressure information, the information carpet bombing and tactics of «scorched drain». When efficiency and effectiveness of interventions is insufficient information in the course of the enemy embarks on conventional weapons. Unfortunately it is fully realized to Ukraine.

To survive in the information confrontation for its own independent existence and the right to have his house on Earth as information, counter-weapons, and security for their own information and information resources are necessary. The war will end one day, there will be peace, but security issues remain.

The motto of the information society is competitiveness intellectual ability. In the information society more than half the time and human resources will be used for storage, processing, analysis and transmission of information. There is incredible acceleration of growth of human knowledge. In the 70 years of the 20th century the volume of human knowledge increased twice in 10 years, 80 years - every 5 years until the end of 90 years of knowledge of mankind doubled almost every year [3].

Acceleration of information processes, enhancing communicative interactions and the whole direction of increasing vitality of the individual, community, society, social systems, but also creates a new vulnerability. In modern conditions was the phenomenon of so-called «social media», whose role is important in the context of information and the confrontation of national security and in need of security. «A mature and stable information society characterized by the desire and the ability of the state to create conditions for free access of its citizens to information products, services and other resources, and ability to secure national information resources, the interests of the individual, society and state as a whole from internal and external negative impact» [4]. In this case the security of information resources necessary to ensure reliable, safe operation of the national information infrastructure, information production and their subsequent efficient development. In the information society, security issues are essentially complex. The goals and objectives of information security in order to merge and economic objectives (social and economic) security and resolved largely by using the same security mechanisms. An integral part of a comprehensive security information society will be and security of human capital as part of social and national security. To develop information security paradigm of information resources in the new information society where information is leading, it is necessary to analyze the changes in its environment, informational, industrial, technological, social, and economic. The development of this paradigm and concepts should be relevant to the planning stages of the transition to an information society. There is the emergence of new properties and information resources; transition information to perform its crucial role as an information product, product, raw material and product manufacturing information in the virtual reality of the information society. In the information production impact on information resources has the same effect as failures, accidents and sabotage in material production. It is advisable to address emerging security issues outpaced production information to the development of the information production of the future information society. Has developed a trend of security division into two parts. In [5] performed cybersecurity division constituents to secure their own information and intelligence sphere of information technologies and cryptographic warring parties. In a recent scientific publications stated the following division: «Analysis of recent research and publications shows that the nature of destructive information impact can be divided into two main types – Information Technology (aimed at disruption of the technical information tools) and information and psychological (Way to manipulate the subconscious mind and the person or certain social groups» [6].

Accordingly there are two types of information control: information-technical and information-psychological. In the Information Technology combating the main objects of influence and security is information-technical systems, communication systems, telecommunications, electronic products and more. In the information-psychological struggle the main objects of influence and security is the mentality of the political elite, the staff of strategically important facilities and public systems, the formation of social consciousness, thought and decision-making, social objects, individuals, social groups, communities, society state, world community.

In modern conditions was the phenomenon of so-called «social media», whose role is important in the context of information confrontation and national security. Social information is a broader concept than with sociological information. Sociological information - documented or publicly announced information about the attitude of individuals and social groups to social events, phenomena, processes and facts. The sources of this information are information reflecting the results of polls, observations, and other sociological research. Unlike sociological information, social information directly functions in human society, playing the role of administering it in the processes of and interaction with the environment. The phenomenon of social media appears as communicative, attributive and functional components [4].

Communicative component of social media is a mean of establishing, organizing and implementing the interaction of information relations in their activities in terms of public relations and environment. Acceleration of information processes, enhance communicative and whole-directional interaction increases the vitality of the individual, community, society, social systems, but also creates a new vulnerability.

Attribution component of social media is to set the terms, definitions, rules, opinions, values, symbols, myths and other attributes of reality and life.

The functional component of social information needed for daily activities, work, analysis, decision making and meet the immediate physical, emotional, intellectual and psychological needs. Social information is divided into three types: the present, the past, the future. Social information may be prognostic (with functions: estimated, regulatory, warning) and planned. By type of social information can be internal and external, horizontal and vertical (straight - directive and regulatory inverse - control and reporting, including sociological). The functioning of social media characterized by the following features: For circulation levels: national, regional, continental and global; Time circulation: short, medium, long-term; For comments to media: positive, negative, neutral; The method of bringing information: through the media, through intelligence, through informal communication, through diplomatic sources through various businesses; In order to bring the information, persuasion, influence, Response, compromise, creating new values and rules for community or elite.

Social information is one of the leading roles in the formation of social capital, which plays an important role in human societies.

Social capital is called the amount of shared social values, those that really were shared – a set of informal values or norms shared by the members and allow them to interact. Social Capital plays a significant role in ensuring the effective functioning of society. Social capital is formed voluntarily, based on unwritten laws, formed by self-organization of social groups for its maintenance is not required the use of force or coercion by the state, it is a manifestation of social partnership.

Social capital creates scope lifestyle, reflects the way the voluntary cooperation of social groups and its members in the group. The system TIS social capital present in that part of the organizational measures related to work with staff, users and consumers of functional information security services. With the acceleration of technological progress and information is changing the level of manipulation people person becomes less secure, develop methods of social psychology and informational impact on people. Need to manage social capital and take into account the socio-political effects of social capital. Society and the state should pay more attention to securing the information a living and achieve victory in the information war, cruelty which built up.

Information and cyber security transformation summary

In fact, in the process of transforming information security were introduced new activities to ensure information security and create new types of information security, cyber security and socio-psychological security. Older types of information security are preserved, improved and occupy every niche in the system of national security. Table 1 shows how the changed significance solved security problems old and new systems of information security.

The sheer volume of work for the security of information security increased significantly after increasing volumes of information technology. But the relative weight problems solved shifted towards the socio-psychological, ethical and aesthetic aspects of information security. According to others the relative weight of information security issues relating to the human factor (in this case organizational + psychosocial measures).

Table 1.

Distribution of the relative importance of measures to secure information resources (in %)

Years	Arrangements, regulations	Cryptographic measures	Technical & physical measures, %	Software-technical measures	Socio-psychological measures
2000	40	30	30	–	–
2005	30	30	30	10	–
2010	30	30	10	30	–
2015	20	10	10	20	40

Paradigm of critical information infrastructure security under the information influence conditions

Today are current the tasks of implementing the strategy of cybersecurity Ukraine. One of the main objectives is the security of critical information infrastructures. Under the critical information infrastructure understanding the information infrastructure of the state, disabling or destruction of objects which is detrimental to national security or harm its international image. The development of global information security technology is in global information space, cyber medium, the Internet. The role of telecommunications critical physical and information resources of the state is growing. The need of certain functions and services for the benefit of e-government, electronic document management, digital signature, the development of electronic commerce and so on is realizing.

In the field of network security (telecommunications and other infrastructures) warring parties seek to technically break the channels of information make it difficult or change processing algorithms, steal, damage or change information in the field of storage. In this area running-extensive system of secure measures. It should take into account the paradigm of 4 stages, which considered the paradigm of information security and other mainly information and communication networks as the most critical public resource. But today is acknowledged that the confrontation with violators of information security and cybercrime is not yet won. At the forefront properties availability and integrity, as indicators of sustainable and effective functioning of the systems.

«Network - centric paradigm clarifies and expands the classic evaluation criteria and strategies for information security, conceptual approach «warranty information» (information assurance) for security of information resources, information security is linked directly to security infrastructure» [7].

The current paradigm of information security developed in the US, and what still needs to develop and implement in Ukraine, considering information systems as fundamentally open, where synergy homeostasis (stable state of equilibrium) is determined by the balance of entropy (a measure of uncertainty) margin environment and survivability elements. Paradigm provides especially high demands on the survivability of information systems, which are characterized by a high degree of decentralization of resource allocation and management.

The role of technical operation is to ensure the preservation requirements to a minimum set of features critical to the survivability of information systems to the security factor by the action of destabilizing factors of the environment. «Homeostasis communications network supports the provision of network integrity, its vitality, bandwidth and active elements (Fig. 1), violation of the integrity and survivability of the network results in loss of critical functions; significant reduction in capacity, activity and vitality elements leads to a loss of flexibility of the network; and violation of the integrity system activity and throughput elements induces disruption of telecommunication network» [7].

Information security includes concepts such as integrity (integrity) of information, confidentiality (confidentiality), secured from unauthorized access (authentication, non-

repudiation). Now is added the ensure reliability (availability) information and communication systems functioning and its survivability (survivability). Exceptional role in modern telecommunication infrastructure of the country determined that national security depends on the integrity, reliability and readiness of critical physical and information infrastructure. The term «critical infrastructure» includes a set of physical or virtual systems and important for the country so that their failure or destruction can lead to disastrous consequences in the economy, defense, health and national security.

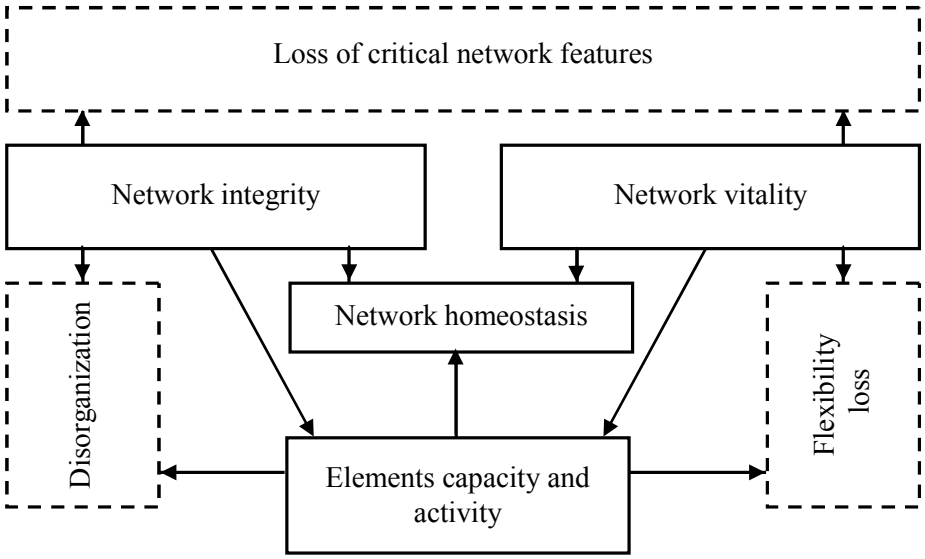

Fig. 1. Critical Information Infrastructure properties (Figure was copied from [7])

Violations of system integrity against the background of decreased activity of elements causes a disruption management, simultaneously reducing the activity of cells and their vitality - the loss of flexibility, and lower vitality and violation of the integrity of the system - the loss of major functions.

The concept involves survivability systems, its ability to timely perform its functions in terms of destabilizing factors (physical destruction, partial loss of resources, failure and crashes elements unauthorized interference in the control circuit). This technical reliability, which manifests itself as the ability of the system to work without regular system failures, defines the minimum threshold stability system, which without a recovery of lost items and functions may come full stop functioning. The persistence of information systems is important for information security in general.

It is a great dependence on technology information technology threats and vulnerabilities latter. The threat is a software-mathematical impact on Infocommunication systems (cyber attacks), as a means of information confrontation aimed at the use, modification, substitution or deletion of information contained in computers and information networks, reducing the efficiency of or disabling themselves computers and information networks.

The hazard level threats target information influence is directly proportional to the level of technological development and scale networks use computers in a network management system, the industry and the state as a whole. For the growing importance of telecommunication networks requirements to ensure the integrity and reliability of information transmission, security violations routing accuracy and timeliness of information delivery (minimum delay messages), and secure against unauthorized access to information resources, networking and physical security infrastructure.

«The level of security government and commercial information and communication systems determines the security infrastructure of the state as a whole and vitality of these systems - mobilization readiness of the armed forces, industry, the economy, the economy and

society as a whole, as to the conduct of war and to mitigate the consequences of terrorist attacks, natural disasters and man-made disasters. To use and save a minimum set of features critical information and telecommunications system must have a certain margin of survivability and resilience to external destabilizing influences of the environment. Implementation of network - centric paradigm of information security, taking into account all these factors ensures that, even at random or malicious misrepresentation of information, unauthorized access to the control circuit, loss of resources and congestion of traffic, complex organizational and technical measures of security will ensure that the most important problems. It is not only rejection and failure of equipment, distortions, leaks and sabotage and personnel espionage hacking attempt of sabotage and that, terrorist acts on objects of information structure considered not as a potential threat, but as a system of external technical factors environment» [7].

The implementation of this paradigm requires many tasks of organizational, technical, programmatic, social, and psychological and information. Violation of information security can step cybercrime, cyber terrorism act, information operations or war. A major problem is complex cybercrime.

«Computer crime – a relatively massive, historically changing phenomenon, which has a certain spatial and temporal distribution and represents a single integrated system of socially dangerous acts where computers, networks and provided them information is a weapon crimes or crimes subject» [8]. Cybercrime - is «illegal collection, storage, use, destruction, distribution of personal data, illegal financial transactions, theft and fraud on the Internet» [9]. According to the recommendations of UN expert's term cybercrime covers any crime that can be committed through a computer system or network within a computer system or network or to a computer system or network. Thus, the cybercrime can be assigned any crime committed in an electronic environment. Cybersecurity - a state of security of vital interests of man and citizen, society and the state, which is achieved using a complex set of legal, organizational, informational events. The system creates a cyber-security component of Ukraine [9].

The crime rate is an important indicator of the society. Humanity meets a sharp increase in crime not for the first time. At the end of XVIII - early nineteenth century France, Britain, Russia is literally drowning in a swamp of crime, violence and lawlessness. For industrialized and urbanized societies dominated by public relations, strongly developed individualism, personal success is the most important in the value system of the population enjoys great freedom and initiative, characterized by significant pain crime. But especially high level of crime comes up in societies that undergo major changes in the cultural, social and political orientations. And now, as then, we are experiencing a global change of technological structures. You can carry out historical analogies for the removal of the growth of crime.

Indeed, while the police was established, the purpose of which belonged not to secure the king and overlords, and the security of law and public order. Now cyber police is created. But it should secure «network cyber rules» and the legitimacy of not only industrial society that does not go away, though transformed, and a new society with new economic, social and legal relations. They must reflect and embody in life.

Then the work of the police often was enlisted former, but well trained criminals are bad cope with their new responsibilities. Now we must boldly transformed employ hackers. Often the cause of crime is hopelessness, inability to socialize and solve their own problems. Provision of legal ability earnings can significantly reduce social tensions.

Then forensic training was organized in universities. Now this training is rapidly gaining momentum. Then under attack was located private property. Now under attack are confidential and other information, real industrial, energy and other equipment and devices, infrastructure and processes that underpin our lives. Then created a legal and regulatory framework of capitalist society and relationships. Now the corrupt bureaucracy has not moved in the direction of a legal and legal framework of virtual communities, social relations and new high-tech society. For example, from a legal point of view cyberspace is not a public

property. Technology and computer networks that make up cyberspace belong to multinational companies that serve them.

While there have been breakthrough research and theoretical results and achievements. Anthropometric methods were invented - a verbal description of the offender portrait, fingerprinting, developed the theory of criminology. Now successes in managing behavior, consciousness and collective mind people, information operations techniques, theory of security. This work is just beginning. New threats and vulnerabilities arise faster than they are opposition. Not achieved success in a safe operating systems. New scientific achievements primarily used to create new wars and threats. The crime in computer technology so far seems to be specific. They have high latency that, according to various estimates, up to 85-90%. Legislation old industrial age often is not competent to investigate cybercrime. Easy access to information erodes the moral barriers. The information stolen, but it does not disappear, but remains in the host. There is widespread use of free software which is violating copyrights. On the other hand, the victims of hackers often hide them for fear of losing credibility.

Thus, not all capabilities used to perform tasks to overcome growth of cybercrime. Turf negligence, incompetence persons employed to address cybercrime, insufficient funding and so on. On the other hand info, cognitive and other technologies will be developed. They certainly appear to be vulnerable and error. And sooner or later vulnerabilities will be found and used.

As part of this paradigm the authors propose introducing ideas that can lead to full functionally closed system security features. The idea is as follows.

The system (technology) determining the identity and identity management definition can reduce latency cybercrime, improve conditions for the monitoring of information security to ensure control over any transaction and, accordingly, access control. The technology can be used to secure information in open systems. This access control is a candidate for a functionally complete set of mechanisms to secure information. An attacker can go in, but he had not authorized for access. And in this case will be a useful application techniques identity determination.

Category of identity definition technologies and management introduced the definition of identity Recommendation ITU H.1250 - H.1279, Y.2720 - Y.2739 and invited authors for the total implementation of telecommunication networks in Ukraine and maybe in cyberspace. We present the essence of technology. In a network environment determine identity management (MBI – identify management) should provide the opportunities provided to ensure safe information exchange between objects. The exchange of information based on the developed policies and trust established between objects in the environment of multi-service providers. Such confidence is based on the approval (assertion) and verifying the reliability (validation) the identity of objects in all systems of distributed telecommunications: the execution of transport (network access control functions joining networks, transport functions, management functions and resource admission, features user profile transport); in execution services (multimedia services components, telecommunications components, functions of service management, applications, application support functions and support services, features user profile services); User finite systems (conventional terminals, subscriber networks, data transmission terminals); other networks. MBI provides opportunities for privacy security facilities and ensure that telecommunications was spread only authorized information. Identity – information about the object, which is enough to identify the object in a particular context. Management defined identity – MBI – a set of functions and capabilities (e.g., administration, management and maintenance, detection, messaging, comparison and coordination, ensure implementation of policies, authentication and approval), which are used for guaranteeing information confirms identity (eg, identifiers, credentials, attributes); to guarantee the identity of the object; provision of commercial applications and application security [10].

Many modern information services such as e-commerce, e-government, require enhanced observability telecommunications environment. The necessary software determine

the identity of objects and their information flows at all levels and in all components of telecommunications networks while maximizing promoting free but controlled rotation information. Along with other mechanisms of security, firewall, intrusion detection systems, virus security, MBI plays an important role in securing infrastructure, telecom services and application of cyber crime, such as fraud and theft of identity data. Transactions in telecommunications will be secure and reliable.

Beneficial effect of determining the identity is that it partly reflects the properties of direct contacts between people. People perceive directly (using all their senses) of each other and have the opportunity to know the physical, psychological and individual features inherent in each side. Participants in the contacts are able to make more or less objective impression that is a communication partner, to get into his inner world, to understand the motives, habits; attitudes assess the facts of reality. It is desirable to provide telecommunications least some of these opportunities.

From a theoretical point of view, a technology which is part of the identity of functionally complete set of technologies for information security. In the field of information security principle of functional completeness must be combined with the principle of continuity of security (the principle of «circular defense»). The security object depends on the level of security the weakest link. Access control systems are typically available only on entering the system and do not control the future of the subject. The technology used to determine the identity of each transaction, closing the functional completeness technologies. And in distributed systems, information security technology determines that identity is not interchangeable.

The system determining the identity and identity management system defined in the ICS will monitor (monitor) every transaction in the system. The effectiveness of these measures is due to the important role of the human factor. The system determining the identity aimed at detecting perpetrators of information security and facilitates next inevitability of punishment.

While discussing this technology there appear questions about limiting people freedoms. Consider the problem along with the following strategy.

Creating a «trusted» telecom space. In other words, the provision of telecommunications networks properties of attorney, to ensure that they have a certain level of information security. This requires a certain control over the flow of information in the telecommunications network. The same problem applies to the world «web». It seems that in this case, there is a contradiction between the rights (of freedom) rights and control of information. First of all, note that democracy - is not permissiveness and collapse, and the firm order, based on respect for the interests of others. Consider, from this point of view the situation from two control information implemented in.

The first situation. The draft amendments to the communication law, the Code provides for a fine for Internet access via Wi-Fi in common areas without specifying personal data. That is, there is no possibility to enter the Internet anonymously.

The second situation. Developed a set of measures "of content and increasing confidence in the Internet", which will include the following points: blocking content and limit access to it; the fight against anonymity on the web; control over the information that distribute anonymous; encrypt traffic; its «monitoring and filtering» in RuNet; control of Internet companies, with the use of personal data. In the first situation, not democracy pressing although anonymity is prohibited. Indeed, in this situation just secured the rights of the client for blocked channel for criminals. While withdrawing money through mobile banking from another account, free Wi-Fi network without identification, the criminal can be lost. Investigation crime is difficult. Thus, universal definition of identity appliances is much easier solution. In everyday life, there is a steady downward trend in anonymity. Everywhere installed surveillance cameras, chips implants for automatic identification. The ban anonymity does not mean limiting our freedom. We act where we need and do what the law, which is our interest. But do it openly, as do other people.

In the second situation, there are signs of violation of human rights to free access to information. At the same time, limit access to content is required, for example to secure children from pornography and violence propaganda. We have a complex problem that includes political, legal, social, ethical, psychological and cultural aspects. These problems are solved mankind throughout its existence. In Russia the interests of man and society deliberately opposed to each other. Aim to balance the interests of security concerns objective. In fact, the lack of balance is one of the threats to be addressed in the security of rights and interests. In a democratic society human interests provided so as not to prejudice the interests of others. The Russian approach is also taken from the military. Objectives interim military operations may be in contradiction with the general ultimate goal. Some technical details. In the Russian Federation «Yarova law» extended storage of telecommunications traffic. This increases costs and tariffs for connection by 2-3 times. Meanwhile, the introduction of identity technology more effectively solves the same problem. Kim addition, they improve the condition monitoring information security enable tracking of and rapid response to destructive processes and increase the degree of automation of technical operation.

Conclusions

In this paper classified transformation stages and directions of information security paradigms, shows change relative importance of types of information security, supplemented by a list of actual problems in information security, proposed application of the definition of identity and identity management definition. The results will improve management information systems, information-psychological and cyber security. Without proper attention to scientific development, scientific and technological breakthroughs in information and cyber security, socio-psychological, informational and psychological security without the network of State and local business information-cognitive intelligence, «free Ukraine is impossible».

References

1. Gnatyuk, S. Transformation of information and social-psychological security paradigms (part 1) / S. Gnatyuk, V. Gnatyuk, V. Kononovich, I. Kononovich // Інформатика та математичні методи в моделюванні. – 2016. – Том 6. – №3. – С. 227-239.
2. Кононович, В.Г. Соціальний захист інформації в класах систем захисту інформації / В.Г. Кононович // Науково-технічний журнал «Захист інформації». – 2008. – № 4(41). – С. 4-16.
3. Панарин, И.Н. Информационная война и третий Рим безопасность / И.Н. Панарин. – М.: 2008. – 132 с.
4. Бойко, К.В. Доклад на открытии II международной научно-практической конференции „Безопасность современных информационных и телекоммуникационных сетей" [Электронный ресурс] // Бизнес и безопасность, 2005. – № 5. – С. 101-102. Режим доступа: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=43932&cat_id=38710
5. Корченко, О.Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти / О.Г. Корченко, В.Л. Бурячок, С.О. Гнатюк // Безпека інформації. – 2013. – Том 19. – № 1. – С. 40 – 44.
6. Сніцаренко, П.М. Методика оцінки рівня деструктивного інформаційного впливу на об'єкти інформаційної інфраструктури держави / П.М. Сніцаренко, Ю.О. Саричев, П.Д. Рогов // Збірник наукових праць ВІТІ ДУТ. – 2014. – № 1. – С. 88-96.
7. Леваков, А. Анатомия информационной безопасности США. Информационная безопасность / А. Леваков // Информационный бюллетень. – М.: Jet Info online. – 2002. – № 6 (109). – 40 с.
8. Інформаційна безпека держави: підручник / [В.М.Петрик, М.М.Присяжнюк, Д.С.Мельник та ін.] ; в 2 т. – Т. 2. – К., 2016. – 328 с.

9. Кавун, С.В. Економічна та інформаційна безпека підприємств у системі консолідованої інформації : навчальний посібник / С.В. Кавун, А.А. Пилипенко, Д.О. Ріпка. – Х.: Вид. ХНЕУ, 2013. – 364 с.
10. Кононович, В.Г. Визначення ідентичності об'єктів у системі соціальної та інформаційної безпеки / В.Г. Кононович, І.В. Кононович, С.В. Стайкуца, О.О. Цвілій // Сучасний захист інформації. – 2015. – № 1. – С. 19-27.

ТРАНСФОРМАЦІЯ ПАРАДИГМ ЗАХИСТУ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНОЇ ТА СОЦІАЛЬНО-ПСИХОЛОГІЧНОЇ БЕЗПЕКИ (Частина 2)

С.О. Гнатюк[1], В.О. Гнатюк[1], В.Г. Кононович[2], І.В. Кононович[3]

[1] Національний авіаційний університет,
просп. Космонавта Комарова, 1, м. Київ, 03680, Україна; e-mail: s.gnatyuk@nau.edu.ua
[2] Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: vl_kononovich@ukr.net
[3] Одеська національна академія харчових технологій,
вул. Канатна, 112, м. Одеса, 65039, Україна; e-mail: kononovich@mail.ru

У цій частині роботи представлені результати ретроспективного аналізу етапів трансформації парадигми сфери інформаційної безпеки: соціально-центрична парадигма інформаційної безпеки особи, суспільства, держави та, в цілому, національної безпеки; резюме щодо трансформації сфери інформаційної та кібернетичної безпеки; розподіл відносної значимості заходів захисту інформаційних ресурсів; парадигма мережної безпеки критичної інформаційної інфраструктури в умовах деструктивного інформаційного впливу; критичні властивості інформаційної інфраструктури; система (технологія) визначення ідентичності та управління визначенням ідентичності; створення «довіреного» телекомунікаційного простору. Отримана в частинах 1 та 2 систематизація та результати вирішення задач дозволяють підвищити ефективність роботи систем забезпечення інформаційної, кібернетичної та соціально-психологічної безпеки й формалізувати напрямки подальших досліджень щодо розробки ефективних систем безпеки.
Ключові слова: захист інформації, інформаційна безпека, кібербезпека, інформаційно-комунікаційні системи, індивідуальна та групова свідомість, соціально-психологічний захист, правова система.

ТРАНСФОРМАЦИЯ ПАРАДИГМ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННОЙ И СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ (Часть 2)

С.А. Гнатюк[1], В.О. Гнатюк[1], В.Г. Кононович[2], И.В. Кононович[3]

[1] Национальный авиационный университет,
просп. Космонавта Комарова, 1, г. Киев, 03680, Украина; e-mail: s.gnatyuk@nau.edu.ua
[2] Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: vl_kononovich@ukr.net
[3] Одесская национальная академия пищевых технологий,
ул. Канатная, 112, м. Одесса, 65039, Украина; e-mail: kononovich@mail.ru

В этой части работы представлены следующие результаты ретроспективного анализа этапов трансформации парадигм в сфере информационной безопасности: социально-центрическая парадигма информационной безопасности личности, общества, государства и, в целом, национальной безопасности; резюме по трансформации сферы информационной и кибернетической безопасности; распределение относительной значимости мер защиты информационных ресурсов; парадигма сетевой безопасности критической информационной инфраструктуры в условиях деструктивного информационного влияния; критические свойства информационной инфраструктуры; система (технология) определения идентичности и управления определением идентичности; создание «доверенного» телекоммуникационного пространства. Полученная в части 1 и 2 систематизация, и результаты решения задач позволяют повысить эффективность работы систем обеспечения информационной, кибернетической и социально-психологической безопасности и формализовать направления дальнейших исследований и разработки эффективных систем безопасности.
Ключевые слова: защита информации, информационная безопасность, кибербезопасность, информационно-коммуникационные системы, индивидуальное и групповое сознание, социально-психологическая защита, правовая система.