UDC 004.056:619.8:351.007

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 3, pp. 227-239

TRANSFORMATION OF INFORMATION AND SOCIAL-PSYCHOLOGICAL SECURITY PARADIGMS (Part 1)

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

The paper presents the results of a retrospective analysis of transitional paradigm of information security – from the data and information security to the minds and behavior security. Formulated modern paradigms of information security. Described new problems in critical information infrastructures security. Based on the analysis offered partial solutions to a number of partial problems. The implementation of the identity determination and management system will allow to lock the fullness of security mechanisms. Same way is achieved the ability to track each transaction online. Information and psychological security from the destructive impact of information requires the use of social psychological methods. Offered the simple model of forming group consciousness around the idea of cybercrime fighting. The received 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.

Introduction

The evolutionary process of development of methods and technologies of information security characterized by drama and high rates of acceleration. According to the International Telecommunication Union the growth of cybercrime has exponential nature [1; 2]. Number of information security incidents is growing exponentially. Volatility of terminology also shows that problems with information security are far from complete. The problem of this study constitute systematization of representations in content and directions of transformation paradigms of information security, the direction of the transformation of many paradigms of security in the field of information security.

Review of the problems and achievements needs analysis of large volume publications. Three stages in the development of security of state secrets systems of independent Ukraine considered in [3]. Judging by the materials of the foreign press the problems of information security in data processing systems were a big surprise. Since then (from 1960), when these problems were considered as separate, approaches to their solution also went through the initial three stages [4]. Known as periodization phases of information security of Kievan Rus, Lithuanian-Russian state Zaporizhzhya Sich, Cossack Hetmanate and further several stages to this day [5]. It has historical interest. When the information security problems in the Soviet Union went out of the shadows of secrecy, the materials were published in the open press, which became widely available for scientific and technical experts. In 1980, was translated and published the book by L. Hoffmann [6]. An important addition was the book by D. Xiao,

D. Kerr and S. Mednick [7]. In 1989 «Foreign electronics» journal has placed a number of materials and a special edition of «Information Security» [8]. Later, experts learned about the work of software security [9]. The principles presented in these publications remain almost intact to this day. Further transformation of information security forms out of preservation and expansion of the basic principles of all previous stages. In 1992, A. Timonin came to conclusion that «in general, the problem of security in automated information systems refers to not algorithmically solvable problems» [10]. However, a number of problems remain unresolved: still remains the closed functional completeness of the set security services, insufficient front of speakers security processes researches, needs to be expanded the modeling of social and psychological security. The urgency of these problems stems from the Cybersecurity Strategy of Ukraine.

The main *aim of this paper* is to identify the characteristics of the gradual transformation paradigms from data and information security to behavior security, individual and group mind, changes systematization of the information security paradigms; production of further transformation of information security paradigms; reasoning the implementation of identity definition and defined identity management.

Stages differentiation of information security transformation

Further stages of information security will be divided on the basis of a paradigm shift in information security. The concept of paradigm considered as a set of values, methods, approaches, technical skills and resources, problem solving methods accepted in the scientific community of experts within the established scientific tradition in a certain period of time. The paradigm is undergoing changes depending on accumulated practical experience and research results. Terms of stages separation determine the facts of the appearance of the relevant national legal documents. We consider the following stages of transformation information security technologies:

Stage 1 (1992 – 1996) – the establishment of its own system for the security of classified information in Ukraine and creation of technical security of information (TSI) in the fields;

Stage 2 (1996 – 2000) – the creation and development of the legal framework and integrated systems for information security in automated systems;

Stage 3 (2000 – 2004) – the development of the legal framework of security of state information resources and harmonization of national and international regulatory framework;

Stage 4 (2004 – 2008) – further development of information resources security in all types of public, commercial and personal data in information and telecommunication systems and information space of Ukraine. Expanding the scope of information security on public information;

Stage 5 (2008 – 2012) – development of information security against the backdrop of a foreign network-centric paradigm of information and influence;

Stage 6 (2012 – 2016) – the development of cyber cyberspace state. Expanding the scope of information security for commercial and social spheres;

Stage 7 (current) – IS update tasks as components in the plane of the information confrontation and information warfare. The establishment of security system behavior, individual and group mind.

The transformation is not complete, on the contrary we have the transformation accelerating, the development of methodologies and interdisciplinary approaches. Transformations and changes of paradigms are summarized in the Table 1.

Historically, information security paradigms successively change one another, maintaining, improving and complementing the previous ones. Some paradigm enacted into life simultaneously - for example, some in the public sector, and others simultaneously in the private sector. Some paradigm implemented into action and improved for several stages.

Historically, the first standard that has made a huge impact on the security of information networks has become the standard US Department of Defense «Evaluation Criteria Trusted Computer Systems» (first published in August 1983). Thus, in the mid 80 of the last century laid the foundation of information security strategy.

Classical information security paradigm based on access control

The classic paradigm of information security based on access control was introduced on 1 phase (1992 – 1996). This is a phase of development of its own system for the security of classified information in Ukraine and creation of technical security of information (TSI) in the fields. Was first applied to the automated system of Class 1 – one machine and one user complex, which processes the information to one or more categories of confidentiality [11].

Table 1.

Stages and factors of transformation in information security

№	Paradigm	Scope of security	Security tool and technologies	Basic terminology
1	Classical, based on access control	Information security in technical information processing systems	Ensuring the confidentiality, integrity, availability (CIA), observability, guarantees	TSI, CSI, access control
2	Frontier security (perimeter defense)	Information security in automated systems (computers)	CIA + access control	CSM, security policy, security
3	Multi-layered information security system	Information security in automated systems (computer networks)	CIA + access control + firewall + privacy (P)	Government Information Resources
4	Network-centric (I)	Information Security of information resources (IS IR) of technology and major communications	CIA + access control + firewall + System of detection prevention and mitigation for IS incidents	ICS, information space, personal information
5	Network-centric (II)	Information security of critical infrastructures	CIA + access control + firewall + System of detection prevention and mitigation for IS incidents + search for vulnerabilities	Critical information infrastructure
6	Cyberspace	Cybersecurity environment, resources, social capital, information production	CIA + access control + firewall + System of detection prevention and mitigation for IS incidents + search for vulnerabilities + Audit, monitoring and insurance	Cyber security, state cyberspace
7	Sociocentric, security behavior and consciousness	National security, social and psychological security	… + Cybersecurity + Psychological security	Information impact, information war

Control access to information organized so that only authorized person or process are entitled to read, write, create, or delete information. The information system was autonomous and did not extend beyond the agency or organization. An example of such a system is autonomous personal electronic computer (the PC). The main goal of information security is to prevent information security threats, preventing information theft and computer facilities, disclosure, loss, destruction and distortion of information, ensure the normal production of all departments of the facility information. The main tasks of the security were considered: restricting who is allowed to access; creating a system of passwords and access for users to information by categories. The theoretical basis of security systems was the theory guaranteed secure systems [12]. The general principle of the information security is a maximum efficiency of risk accepted not below the fixed risk when operational risk is minimal. Organizational data security is divided into technical information security (TSI) and cryptographic security of information (CPI).

Technically, the goal of information security is to implement the rules, measures and action to prevent damage and / or loss in the case of attacks and threats to information. Security carried out comprehensive information security system (CISS), which consists of legal, organizational, methodological, technical, software, information and mathematical provisions that prevent the realization of the threat or significantly impede the realization of the attacks. The complex remedies considered as a set of functional services that combine to create the necessary functionality profile security. Each service is a set of features that allow you to withstand a certain set of threats. Security policy can be implemented using a variety of services and mechanisms, alone or in combination, depending on the objects of policy. In general arrangements belong to one of three classes, which may overlap: prevention, registration, renewal. To provide services using security mechanisms. According to international recommendations ITU-T [13] security network built in a hierarchical multi-modular, security - security services - functional security services - security mechanisms. [14].

The classic paradigm of information security was extended to automated Class 2 - localized multimachine multiuser systems that process information for one or more categories of confidentiality. An example of such a system is a local area network (LAN) connection between computers which do not go beyond the controlled area or local communication system. CISS were based on the theory guaranteed secure networking model which includes guaranteed by components and is guaranteed by channels that connect the components together. In communication systems to counter potential threats to international recommendations ITU-T [15] defined tasks such security networks: confidentiality of information that is stored or transferred; the integrity of the data, i.e. information that is stored or transferred; the integrity of the system, in particular, the problem the operating system security; reporting (this includes the problem of observability), where each object / subject should be responsible for any action which he initiated; readiness (availability) is the property of the information environment in which all legitimate objects must get correct access to information system.

Its highest classical paradigm of information security in automated systems reached Class 3 - Distributed multi machine and multi user complexes which process different categories of information confidentiality and where is the need to transfer information via unsecured environment. At this stage, the terminology has changed: instead of the term automated systems were used correct term: Information and Communication System (ICS) and a short – Infocommunication system. Add another important characteristic of these systems, - Class 3 assign ICS belonging to one operator (one owner), allowing it to implement a uniform security policy.

Examples of Class 3 are a special system of confidential communication or public communication networks of one operator. CISS distributes its functions for network elements. In general, the problems of CISS are to: prevent, detect, respond and scare. An adequate level

of information security can be achieved only through an integrated approach that involves the systematic use of physical, software and technical and organizational measures and means. Security is required for all components of information and telecommunication systems, lines, channels, transmission systems, hardware, software, information and personnel. The ultimate aim is the selection of effective means to counter threats in the implementation of information security, the cost of which, in any case, should not exceed the value of losses expected from the sale of threats.

Paradigm of information activity objects border security

Frontier security paradigm of information objects (perimeter defense system) operated in phase 2 (1996 - 2000) - the stage of the creation and development of the legal framework and integrated systems for information security in automated systems. Since the mid 90^{th} years widely spread personal computers, local area networks and the Internet. To access the distributed database implemented technology client - server. The situation with the information security began to deteriorate. In 1995, the open print publications appearing on the concept of information confrontation and information war. In response developed and implemented this paradigm. Frontier security paradigm based on guaranteed secure core idea around which provided several lines of circular defense and demilitarized zones [16].

Communication centers, switching centers, final system focused on a relatively small area and security system built on a «circular defense» (defense barrier or perimeter security). All items are secured, are located in a secure physical environment of the area that is secured. Station equipment switching units placed on the secured object, where the full cycle of organizational and technical measures for comprehensive information security qualified certain level. From the theoretical positions of technical security of information known as the weakest link, which is not blocked by institutional and / or organizational and technical or cryptographic means, determines the resulting level security system.

When ensuring confidentiality must allocate tasks source message non-repudiation consumer messages non-repudiation network that receives messages from source to destination delivery. The same considerations affecting the distribution of tasks and authentication of information interaction network in the transfer of information between network operators, we are different.

Telecommunication networks secured «distributed by». The concept of «distributed» systems of security applies in particular in IP-networks. The concept of channel transmission in such networks blurred. Path cannot be secured in one message. Message divided into packets, each of which can be transmitted to an arbitrary route. They can create virtual channels of communication. The security level of the network route determined by the weakest security s of all possible routes. A security route is determined by its weakest link.

To secure computer networks from unauthorized access foreign organized criminals filtering security perimeter network using a network between screens - firewall (firewall). Between the firewall – a set of hardware and software that monitor and filter network packets that pass through it, in accordance with desired configuration rules. Complex of multifrontier security provided by operating systems with multi-level security from unauthorized access, encrypted transaction methods of cryptography, start to block access cards.

But the effectiveness of the information security of computer networks proved insufficient. Up to 60% of all incidents of information security in networks account for internal attackers and the human factor: errors and not enough staff qualification, malicious actions, lack of control and so on.

Paradigm of layered multilevel information security system

The paradigm of multi-layered information security system of information resources and technologies appeared on stage 3 (2000 - 2004). This stage is characteristic by development of the legal framework of state information resources security and harmonization of national and international legal framework of information security. The paradigm has evolved with further expansion of the use of information technology, global distribution of Internet, mass introduction of remote access to distributed client - server database technology. Paradigm prerequisites are the emergence of multi-operating system secured from non-authorized access, usage of cryptography to encrypt transactions, implementation of locking connecting devices means.

This paradigm layered, multi-level information security based on the idea of guaranteed secure core around which provided several lines of circular defense and demilitarized zones. The system of circular defense by multiple threats provided CISS, understood as a set of measures and means for preventing information leaks by technical, acoustic, vibroacoustic, electromagnetic (and aiming), laser, infrared, radiation, chemical channels that created the main and additional (auxiliary) technical means of processing information and security against unauthorized access to information and means of processing in automated systems. Continuous security is provided as time - at all stages of the life cycle of information security, the decision on security, development of technical specifications, design, creation of security, usage and disposal after its decommissioning. From the theoretical positions of information security is known that the weakest link, which is not blocked by means of security, determine the resulting level of security.

A characteristic feature of this paradigm for foreign countries is the transition from concepts of information security to the concept of information security technologies and information resources. In addition to the main goal of information security is added to ensure stable operation of information and communication systems, security of the legitimate interests of enterprises from illegal encroachments, prevent theft of funds, improve service quality and security guarantees property rights and interests of customers. Conceptual engineering model of multi-layered information security system represented by a group of international ISO / IEC 15408 standards [17], which determine the development of technology security profiles and security projects. [18] In Ukraine, he is introduced as the industry standard, for example, in the banking sector [19, 20]. Conceptual model of information security system additionally includes a set of security services and security mechanisms that implement services that provide monitoring functions, security and adaptation of information resources to prevent the possibility of gradual penetration offender detect the fact of penetration, object localization invasion and attack and neutralize expulsion of the offender, restore lost functions of the system. New in the conceptual model is widely used filters, firewalls that secure the perimeter. Considering that about half of information security problems associated with the human factor, the security against internal and external malicious intrusion detection systems, recognition of abnormal behavior, adaptive algorithms recovery systems and facilities security are implementing.

Network-centric paradigm of information security

Network-centric paradigm of information security of information resources launched on 4 phase (2004 - 2008). It marked a further development of information resources security in all types of public, commercial and personal data in information and telecommunication systems and information space of Ukraine. It was expanded by the scope of information security in open information. The paradigm stems from the wealth of modern international experience and scientific advances in this field, with the rapid development of infocommunication fact, the development, the complexity and the increasing role of

communications networks as a critical public resource. Since the beginning of 2000 «information security has become directly tied to the security infrastructure of the country and welfare of the nation» [21]. The network-centric (network-centric) paradigm of information security began to develop. In Ukraine, this paradigm has been recognized as inappropriate. The inertia of the previous paradigm of multi-layered information security system is not allowed to fully appreciate the importance of the new paradigm. Proposed by the concept of information security of telecommunication networks [22] found no significant response nor the scientific community nor the official agencies. However, network-centric paradigm has had a significant impact on information security business and telecommunications. For Ukraine, this paradigm can be formulated as follows:

For Phase 4 - implementation of network-centric paradigm of information security of the state critical infrastructure, including information and communication networks as the most critical public resource.

For the next 5 stage - the paradigm of increasing requirements for survivability of information systems as part of critical infrastructure and are characterized by a high degree of resource allocation and decentralization of management to enhance the role of technical operation in terms of requirements to preserve a minimal set of critical functions to the survivability of information systems, security factor to the action of destabilizing factors in the environment, including information influence. The concept of this paradigm is the main problem of increased requirements for information systems that were characterized by dispersed resources and decentralized management. Characteristic features of this paradigm are: more interlocking processes of information security management utilities – energy, transport, telecommunications, pipeline networks; access to forefront properties availability and integrity as indicators of sustainable and effective functioning of the systems; transition to the next stage of information security technology cybersecurity cyberspace to businesses, organizations and users.

For example, the Law of Ukraine «About Telecommunications» are requirements for preparedness and survivability, providing support for such properties as the reliability of the telecommunications system, its sustainability, resource availability, integrity and recoverability system structure. Information security of telecommunications networks should be ensured in the integration of information and communication technologies, various types of networks and telecommunications services, quantity and quality are constantly increasing, and activities on the networks of different ownership forms. It is necessary to harmonize methods of information security for the various components of information and telecommunication systems and networks, including information resources, applications, and telecommunication protocols. An integrated approach means a need for a network infrastructure for information security vulnerabilities as any network link can cause problems for all involved, both for the providers and operators and consumers of services. Information security in telecommunication systems are difficult complex task. Secure telecommunications network should be secured from malicious and unintentional attacks, be reliable, scalable, provide a guaranteed response time, availability of services and information, integrity of data and equipment, accurate billing information. The security components of the telecommunications network is critical to the security of the entire network, including applications and services.

However, because the network combines a large number of elements, making progress determines their ability to interact or lack of such capacity. Information security should be implemented threats not only from each item or service, and should be provided in collaboration tools and security features in a multimedia environment with the full implementation of the overall security of information transfer from one end [14].

The complexity of modern telecommunication networks and information and communication systems (ICS), management and interaction of networks leads to the necessity and usefulness allocation separately ICS Class 4 - Global Distributed multicomputer, Multi,

multidomain complex which processes information of various categories of confidentiality and has different owners domains. Domain 3 includes class X, owned by one owner and has the CISS, securing the perimeter domain, its information security management system, its system of prevention, detection, treatment and elimination of incidents of information security, a single domain security policy. Domains of different owners may have different security policies.

In telecommunications information security is intertwined with: management of the quality of communication services where security and preparedness information resources are an integral part of assessing the quality of services; management of economic efficiency, which is the relationship between information and economic risks; tasks in technical operation of software requirements to preserve a minimal set of features critical to the survivability of information systems to the security factor by the action of destabilizing factors of the environment.

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. But the fifth stage in Ukraine did not happen.

Network-centric principle in national security system of Russia

At stage 5 (2008 - 2012) meant to be the development of information security against the backdrop of a foreign network-centric paradigm of information and influence. Expansion of the information security sphere was scheduled to the commercial and social sectors. Ignoring international experience, including neglect of network-centric paradigm has led to serious consequences for Ukraine. On the contrary, Russia reacted to carefully develop in the US new concept of network-centric war. Its foundation is the «network» and the basic principle is the principle of «network-centrism». The principle of network-centrism, in regard to information system management of Russian national security lies «in addition vertical administrative-command network structures of government by horizontal informal, self-organized network structures of civil society in all their diversity, organized by the network principle in historical time, geographical space, subordination and problem targeting national security» [23]. With the principle of «network-centrism» follows the use of «organizational weapons». «Organizational weapon - a combination of national and transnational, sympathizing network of structures that combine small, but very influential group of politicians, senior government officials, military, law enforcement officials, the media, big business, political parties, etc., who are willing on whether other reasons contribute to the promotion of Russian national interests» [23]. The use of organizational weapons can pursue constructive and destructive purposes. The design objective is to create the necessary conditions to create in their environment state «affective-cognitive-volitional consonance - unity understanding and experience of voluntary departures in the majority of its members». On the contrary, destructive goals – a state of «affective-cognitive-dissonance willful», that is a hard conflict in the area of understanding, experience and network will in member institutions whose activities are disgusted with the national interests of Russia. Selector strategic and operational decisions in the field of national and military security is the use of the totality of interacting distributed in historical time, geographical area, the subordination and problem orientation multilateral, multi-business strategic computer games, which are models of national security Russia.

Consider what we did not realize at the time until 2013. That is, consider the problem of the emergence of unfriendly and hostile information influence on Ukraine. Expanded information war (and now too hot) with Russia based on serious scientific research, particularly on solid mathematical training processes information influence and mathematical modeling. The first publications in the media on the concept of information confrontation and information war there in 1995. Published monographs [24-25] and many other publications on this topic. Attention is drawn to the mathematical side of research. In the book [25] presented a mathematical apparatus for research capacity systems self-studying, in terms of targeting. In 2001, D. Chernavskii published detailed results of research in the dynamic information theory. Described model generating valuable information «can be used in various fields of biology, linguistics, sociology and history» [26]. There are research results risks modernization, management of regional industrial complexes, of socio-historical development ... and the language of war. Objectivity model tested and refined on the historic under-lays, in our time tested in practice, realized in an aggressive policy of Russia. Here is a brief description of this model.

Use mathematical apparatus of the theory of dynamical systems. The system is composed of several types of *i* objects, which belong to the same set of power system N. Each element has a type of information. Information may be language, culture characteristics, production capacity, psychological parameters and more. Element system can occur and disappear. The life of each *i* -then element of τ_j is less life expectancy on the same system. Each *i*-th element contributes to the objects of the same type. «We can offer in information distributed in the space of a dynamic system type» [26]

$$\frac{\partial u_i}{\partial t} = \frac{1}{\tau_i} u_i - \sum_{j \neq i} b_{ij} u_i u_j - a_i u_i^2 + D_i \Delta u_i,\ a_i < b_i, \qquad (1)$$

where u_i – the concentration of i - type elements and each element has i-type information. $(1/\tau_i)u_i$ describes autocatalytic (mutually supported) by reproducing the characteristic time of autoreproduction. $b_{ij}u_i u_{ij}$ describes the interaction of elements. Sign «minus» means that the interaction is antagonistic (or competitive) nature. At a meeting of two different elements, each of them or seeking to impose their information second or «destroy» him. $a_i u_i^2$ describes the effect of «struggle» or destruction at the meeting of the two identical items due to competition for resources environment. This significant member when the concentration of the same elements becomes too large. The latter term describes the diffusion element when the elements are moved and mixed in space. D_i – elements diffusion coefficient.

Equation (1) used to describe the emergence of a single genetic code, description of the violation of punitive symmetry to describe historical events when added to the equation (1) members describing the geography of a territory that is modeled. The model was tested on the description of the main events of European history, from the Middle Ages to the present day. During the events understood the formation of new powers and disappearance of others. Simulation shows satisfactory resemblance to the real facts of history, if choose appropriate coefficients model. The model allows global forecast more or less distant future.

Unfortunately, this model can be used for planning the language of war. For example, when modeling the dynamics of ethno received the following conclusion: «With increasing migration length (which is inevitable with the development of techniques and technologies), physical obstacles and cease to play the role of space can be considered homogeneous. Then all clusters are driven one, which is - it is impossible to present. In other words, the world will be global and will be managed by another state. There will be one state language and common rules of conduct that is – clearly cannot provide ...» [26].

In the face of all this kind of dangers and threats to Ukraine was disarmed physically and psychologically information. Only decisive action conscious of society turned then lost its political independence.

Paradigm of enterprises and organizations cyberspace security

The paradigm of cyber environment cybersecurity of companies, organizations and users within 6 phase (2012 - 2016) is still in its infancy. To be implemented cyber cyberspace development of the state and expand the scope of information security to the commercial and social sectors. Meanwhile, the problem of cyber security has become topical in the world. Tools cyberattacks were used to obtain advantages in information exposure and cyberwarfare. In many countries «formed special units that have a purpose: conducting exploration work in networks, securing their own networks, blocking and» collapse «of enemy structures using cyberspace capabilities» [27].

Among the starting legal documents approved «Cybersecurity Strategy of Ukraine». Terminology and regulatory framework moves to the development stage. We know that cybersecurity (or rather «the sphere of cyber security» in terms of specialists ICS - Ed.) - A set of tools, strategies, security principles, security guarantees, guidelines, approaches to risk management, performance, training, practical experience, insurance and technology that can be used to secure cyber environment, resources, organization and person. «Resources include user or organization connected computer devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and / or stored information in cyber environment. Cybersecurity is to try to achieve and preserve the properties of the security resources of the organization or user directed against the relevant threats cyber environment. General security tasks include: accessibility; integrity, which may include authenticity and non-recovery; confidentiality. Cyber environment includes users, network devices; all software processes are stored or transit information, applications, services and systems that can be directly or indirectly connected with the networks» [28]. In other words, should reflect the paradigm shift from information security technologies and important communications to various kinds of cyber security and resources cyber environment all businesses, organizations and users. Especially emphasizes critical information security (especially information) infrastructures. «Cybersecurity includes a social capital, information production. In today's business environment concept perimeter disappears. The boundaries between internal and external networks become more blurred» [28]. Security is ensured at all levels of telecommunications networks, network access, network, and transport levels, levels of network management and provision of services. Among the strategic aspects of cybersecurity Ukraine formulated the problem of «Building effective mechanisms to secure national interests and the need to develop a single vision of cybersecurity as state bodies and business structures» [29].

Conclusions

In this paper classified transformation stages and directions of information security paradigms, shows change relative importance of types of information security. In the second part will be 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.

References

1. Обисо, М. Развитие международного сотрудничества в области кибербезопасности. Глобальный ответ на глобальный вызов / Марко Обисо // Межрегиональный семинар для стран Европы, Азиатско-Тихоокеанского содружества независимых государств (Европа-АТР-СНГ) «Современные методы борьбы с киберпреступностью». – Одеса, Украина, 28-30 марта 2012.
2. Бурячок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. – К.: ДУТ, 2015. – 288 с.
3. Корченко, О.Г. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці: Монографія / О.Г. Корченко, О.С. Архипов, Ю.О. Дрейс. – К.: наук.-вид. центр НА СБ України, 2014. – 332 с.
4. Герасименко, В.А. Проблемы защиты данных в системах их обработки / В.А. Герасименко // Зарубежная радиоэлектроника. Защита информации. – 1989. – Специальный выпуск. № 12. – С. 5-21.
5. Гуз, А.М. Історія захисту інформації в Україні та провідних країнах світу: Навчальний посібник / А.М. Гуз. – К.: КНТ, 2007. – 260 с.
6. Гофман, Л.Дж. Современные методы защиты информации / Л.Дж. Гофман. – М.: Сов. радио, 1980. – 264 с.
7. Сяо, Д. Защита ЭВМ / Д. Сяо, Д. Керр, С. Мэдник. – М.: Мир, 1982. – 203 с.
8. Защита информации. Специальный выпуск / Зарубежная радиоэлектроника. – № 12/1989. – 112 с.
9. Защита программного обеспечения, Пер. с англ. / Д. Гроувер, Р. Сатер, Дж. Фипс и др. // Под редакцией Д. Гроувера. – М.: Мир, 1992. – 288 с.
10. Грушо, А.А. Теоретические основы защиты информации / А.А. Грушо, Е.Е. Тимонина. – М.: Издательство «Яхтсмен», 1996. – 192 с.
11. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електронний ресурс]. – К.: ДСТСЗИ СБУ, 1999. – 20 с. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=403818&cat_id=38835
12. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.Г. Ивашко. – Г.: Горячая линия - Телеком, 2000. – 452 с.
13. Recommendation ITU-T X.800. Security architecture for Open Systems Interconnection for CCITT applications [Електронний ресурс]. – Geneva, 1991. – 48 с. – Режим доступу: http://www.itu.int/rec/T-REC-X.800-199103-I
14. Кононович, В.Г. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Частина 3. Архітектура безпеки Концепція захисту інформації: [навч. посібник для вузів, затверджено Міністерством транспорту та зв'язку України] / Кононович В.Г. – Одеса, ОНАЗ, 2009. – 194 с.
15. Рекомендация МСЭ-Т Е.408. Требования к безопасности сетей электросвязи [Электронный ресурс]. – Женева, 2004. – 21 с. – Режим доступу: https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiw6pmYjZvQAhVBEywKHTkKDrgQFggcMAA&url=https%3A%2F%2Fwww.itu.int%2Frec%2Fdologin_pub.asp%3Flang%3De%26id%3DT-REC-E.408-200405-I!!PDF-R%26type%3Ditems&usg=AFQjCNFq_wLxyafcx223VwO6vGv0bzGbhA&sig2=TtlAbZuD4XmAX9XuYOBCeA&bvm=bv.138169073,d.bGg
16. Кононович, В.Г. Аналіз проблеми розподілу витрат на інформаційну безпеку інформаційно-телекомунікаційних систем / В.Г. Кононович, М.Ф. Тардаскін, Т.М. Тардаскіна // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – 2004. – Вип. 8. – С. 62-68.
17. Standart ISO/IEC 15408:2000. Information technology - Security techniques - Evaluation criteria for IT security. - Part 1: Introduction and general model. - Part 2: Security functional requirements. - Part 3: Security assurance requirements.
18. Бондаренко, Г. Перспективы применения международного стандарта ISO/IEC в Украине / Г. Бондаренко, Л. Скрыпник, А. Потий // Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине. – 2001. – Вып. 3. – С. 7-26.
19. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 (ISO/IEC 27001:2005, MOD). Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги [Галузевий стандарт України]. – К.: Національний банк України. 2010. – 49 с.
20. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 (ISO/IEC 27002:2005, MOD). Інформаційні технології. Методи захисту. Звід правил управління інформаційною безпекою [Галузевий стандарт України]. – К.: Національний банк України. 2010. – 163 с.

21. Леваков, А. Анатомия информационной безопасности США. Информационная безопасность [Электронный ресурс] / А. Леваков // Информационный бюллетень. – М.: Jet Info online. – № 6 (109), 2002. – 40 с. – Режим доступа: http://www.jetinfo.ru/Sites/info/Uploads/2002_6.DF9C812FFBD9496BAE9694E27F2D9D1D.pdf
22. Кононович, В.Г. Основні положення концепції інформаційної безпеки телекомунікаційних мереж загального користування / В.Г. Кононович, М.Ф. Тардаскін // Захист інформації. – 2006. – № 1(28). – С. 18-30.
23. Никитенко, Е.Г. Облик перспективной информационно-управляющей системы обеспечения национальной безопасности России / Е.Г. Никитенко, Н.А. Сергеев // Оборонно-промышленный комплекс России. – 2012. – Т. 8. – С. 491-506.
24. Почепцов, Г.Г. Информационные войны / Г.Г. Почепцов. – М.: Рефл-бук, –К.: Ваклер, 2000. – 576 с.
25. Расторгуев, С.П. Информационная война / С.П. Расторгуев. – М: Радио и связь, 1999. – 416 с.
26. Чернавский, Д.С. Синергетика и информатика: Динамическая теория информации / Д.С. Чернавский // Предисл. и послесловие Г.Г. Малинецкого. – М.: Книжный дом «ЛИБРОКОМ», 2001, 2009. – 304 с.
27. Дубов, Д.В. Кібербезпека: світові тенденції [Електронний ресурс] / Д.В. Дубов, М.А. Ожеван // Доповідь на Міжнародній конференції 26 травня 2011 р. – К.: НІСТ, 2011. – 30 с. – Режим доступу: http://www.niss.gov.ua/articles/510.
28. Recommendation ITU-T X.1205. Telecommunication security. Overview of cybersecurity. – Geneva: 2008. – 56 p.
29. Дубов, Д.В. Стратегічні аспекти кібербезпеки [Текст] / Д.В. Дубов // Стратегічні пріоритети. – 2013. – № 4 (29). – С. 119-126.

ТРАНСФОРМАЦІЯ ПАРАДИГМ ЗАХИСТУ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНОЇ ТА СОЦІАЛЬНО-ПСИХОЛОГІЧНОЇ БЕЗПЕКИ (Частина 1)

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 роботі представлені результати ретроспективного аналізу етапів трансформації парадигми сфери інформаційної безпеки – від захисту інформації та інформаційної безпеки до захисту свідомості та поведінки людей. Сформульовані сучасні парадигми інформаційного захисту. Описані нові проблеми забезпечення захисту критичних інформаційних інфраструктур. В результаті аналізу запропоновано способи вирішення низки часткових задач. Впровадження системи визначення ідентичності та управління визначенням ідентичності дасть можливість замкнути повноту механізмів захисту. Тим самим досягається можливість відслідковувати кожну транзакцію в мережі. Інформаційно-психологічний захист від деструктивного інформаційного впливу вимагає застосування соціально-психологічних методів. Пропонується проста модель формування групової свідомості навколо ідеї боротьби з кіберзлочинністю. Отримана систематизація та результати вирішення задач дозволяє 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 1)

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 работе представлены результаты ретроспективного анализа этапов трансформации парадигмы в сфере информационной безопасности – от защиты информации и информационной безопасности до защиты сознания и поведения людей. Сформулированные современные парадигмы информационной защиты. Описаны новые проблемы обеспечения защиты критических информационных инфраструктур. В результате анализа предложены способы решения ряда частных задач. Внедрение системы определения идентичности и управления определением идентичности даст возможность замкнуть полноту механизмов защиты. Тем самым достигается возможность отследить каждую транзакцию в сети. Информационно-психологическая защита от деструктивного информационного влияния требует использования социально-психологических методов. Предлагается простая модель формирования группового сознания вокруг идеи борьбы с киберпреступностью. получена систематизация и результаты решения задач позволяет 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.