FOLIA 368

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate 12(2) (2022)
ISSN 2657-8549
DOI 10.24917/26578549.12.2.7

Iuliia Bielova
ORCID ID: 0000-0002-0631-7282
State University of Intellectual Technologies and Communications, Ukraine

Volodymyr Kononovych
ORCID ID: 0000-0003-1344-3540
State University of Intellectual Technologies and Communications, Ukraine

Oksana Shvets
ORCID ID: 0000-0001-6860-7894
State University of Intellectual Technology and Communication, Ukraine

The Complementary approaches to cybersecurity of the cyberspace and telecommunications environment

Komplementarne podejścia do cyberbezpieczeństwa cyberprzestrzeni i środowiska telekomunikacyjnego

Abstrakt

Szybkiemu rozwojowi technologii cyfrowych nadal obiektywnie towarzyszy brak bezpieczeństwa. Cyberprzestrzeń to złożony system, który stał się fizyczną i wirtualną częścią naszego środowiska. Cyberprzestrzeń jako całość jest nadal chroniona fragmentarycznie, słabo chronione jest też środowisko telekomunikacyjne. Zmniejsza to IS obiektów wchodzących w interakcje w cyberprzestrzeni. Do zadań do rozwiązania należy stworzenie werbalnego modelu cyberprzestrzeni, analiza skuteczności systemu bezpieczeństwa systemów telekomunikacyjnych w państwie, opracowanie podejść do informacji i cyberbezpieczeństwa rzeczywistości wirtualnej oraz opracowanie środków i środki zapewnienia podstawowego poziomu bezpieczeństwa telekomunikacyjnego na wzór krajów rozwiniętych. Jako rekomendacje podano komplementarne podejścia do zaktualizowanej koncepcji cyber-fizycznego bezpieczeństwa publicznych sieci telekomunikacyjnych.

Słowa kluczowe: system cyberfizyczny, rzeczywistość wirtualna, bezpieczeństwo informacji, cyberbezpieczeństwo i bezpieczeństwo funkcjonalne, koncepcja bezpieczeństwa informacji telekomunikacyjnej

Abstract

The rapid development of digital technologies is still objectively accompanied by the lack of their security. Cyberspace is a complex object that has become part (physical and virtual) of our environment. Cyberspace as a whole is still fragmented, and the telecommunications environment is also weakly protected. This reduces the information security of objects

interacting in cyberspace. The tasks to be solved include the creation of a verbal model of cyberspace, the analysis of the effectiveness of the security system of telecommunication systems in the state, the development of approaches to information and cybernetic security of virtual reality, and the development of measures and means to ensure a basic level of telecommunications security following the example of developed countries. As recommendations, complementary approaches to the updated concept of cyber-physical security of public telecommunication networks are given.

Keywords: cyber-physical system, virtual reality, information security, cybersecurity and functional security, telecommunications information security concept

Introduction

This article refers to the field of cybersecurity of cyberspace and, mainly, it supporting structure – the telecommunications environment. The subject of research is information and cybernetic security of telecommunication systems and networks. Cyberspace is a complex system that has become a physical and virtual part of our environment.

The rapid development of digital technologies is still objectively accompanied by the lack of their security. New information, cyber, terrorist and military threats have emerged. The solution of urgent tasks of national security required the adoption of urgent measures. Information security (IS) strategies, Cybersecurity (CS) strategies, as well as the Regulation on the organizational and technical model of cyber defense were approved (Ukaz Prezydenta Ukrayiny 447/2021).

The information security strategy is aimed, among other things, at ensuring a protected information space of the state. The KB Strategy emphasizes cyberspace, which is defined as distinct from any physical space. The CS strategy has a priority "to ensure cyberspace to protect the sovereignty of the state and the development of society, as well as to protect the rights, freedoms and legitimate interests of Ukrainian citizens in cyberspace." There are special regulations for the protection of "information and communication and information and telecommunication systems." However, as we will see later, cyberspace as a whole is still fragmented, and the telecommunications environment is also weakly protected. This reduces the information security of objects interacting in cyberspace (Zatverdzheno postanovoyu KMU vid 2912, 2021).

Despite the abundance of educational literature on IB telecommunications of various kinds, in scientific and technical literature IS telecommunications is clearly not enough. There are objective reasons for that. The object of protection has giant geographic sizes. This is a class of complex hierarchical systems. The construction and management of the widely distributed information protection system requires a solution to a number of theoretical, technical and even philosophical problems. On the other hand, telecommunications themselves are attacked by attacks (DDoS attacks) and become a tool in the hands of intruders, terrorists and aggressors. The perfect preventive system of IS telecommunications would be. Even if the attacker penetrated the network, its use for unauthorized actions should be difficult.

The purpose of this work is to create a verbal model of cyberspace, an analysis of the effectiveness of the security system of telecommunication systems in the state, the development of complementary approaches to the information and cybernetic security of virtual reality and the development of measures and means of ensuring the basic level of telecommunications security in the example of developed countries.

Verbal model and the role of cyberspace and telecommunication environment in cyber security

From the World Wide Web, as a means of exchanging e-mail and various types of information, cyberspace has become a powerful information and communication factor for most spheres of human life and activity. In physics, information is not distinguished as a physical quantity. The real physical quantity is entropy. Today we have an alternative to physical reality – Its dual virtual reality (one might say: digital reality). Cyberspace is the place where virtual objects appear, as well as objects of augmented reality. In the context of a global pandemic, virtual reality has become a lifesaver that has allowed humanity to successfully continue remotely many types of collective social, cultural, network and industrial and technical activities.

Virtual reality has an informational nature. Information does not exist without media. Similarly, virtual reality has its own multi-level medium - cyberspace. There are three levels in cyberspace. At the upper level of virtual reality, virtual objects are formed, developed, interact and removed to perform social and industrial and other practical functions. Virtual objects, in turn, can be hierarchical. Digital transformation is reaching its heyday. Mega-universes and worlds of natural artificial intelligence are next.

At the second, middle, level of virtual reality, information and communication functions between virtual objects and physical support of virtual reality are provided. The main, but not the only, medium- level means are networks – both physical (channels) and virtual (transport information networks). There are human-machine interfaces, processing, communication, visualization and display of information, glasses, helmets, and brain implants. The means of transmitting physical reality – smells, taste, touch, multidimensional images, sensation of elements of the natural environment - are being developed. There are more devices connected to information networks than people (25 billion) (JOIN, 2020, p. 34). Reality at the middle level is mixed – physical and virtual. Virtual reality media are physical systems. Communications are provided by the virtual layers of the telecommunications environment.

The lower level of virtual reality will be considered the level of its carriers. Devices, workstations, channels, lines, nodes, systems, telecommunications networks, simulators, etc. are an integral part of the cyber environment. Telecommunications are provided by the physical level of the telecommunications environment. Telecommunications converge and integrate with computer networks. Vulnerabilities in computer systems are moving to telecommunications systems. But the specifics remain. In telecommunication networks are distributed

territorially. The "circular defense" method is not applicable. Cybersecurity must be applied end-to-end. Global telecommunications has become a sparsely populated highly automated technology. A total of hundreds of qualified specialists service the nodes at millions of connection points. Automatic troubleshooting, redundancy, workarounds, etc. are used. More than half of the telecommunications channels run in the oceans. Telecommunications management is distributed both territorially and among many owners. In the conditions when production will develop on the basis of remote cooperation of participants, when socially significant technologies (such as 5G generation systems) will function, etc., trust in telecommunications as the main means of interaction will be important.

Thus, cyberspace (cyberspace) is a complex object that has become part (physical and virtual) of our environment. Much of it is occupied by the Internet and telecommunications systems and networks, which have created essentially a telecommunications environment. Deployment of the national cybersecurity system is carried out primarily at the upper level of cyberspace. It is at this level (and partly at the second level) of cyberspace that the complexes of measures, forces and means of cyber defense, provided for by the organizational and technical model of cyber defense, are deployed. The telecommunications environment poses certain security concerns, is a source of threats, and is a provider of anonymity. This eliminates the principle of inevitability of punishment for cybercrime. It is advisable to be in a telecommunications environment. some basic cybersecurity would be provided. Cyber attacks, often carried out through telecommunications systems, directly or indirectly (via flash).

Developed countries pay serious attention to the cybersecurity of cyberspace. First of all, the principle of ensuring the "basic level of security" of information and communication systems and communication networks deserves attention. The European Union has adopted Directive (EU)

2016/1148 concerning measures for a high common level of security of network and information systems across the Union. This directive supplemented COM (2013) 48 - Directive and further allowed the transition to the implementation of high levels of security of information and communication systems: documents {COM (2020) 823 final} - {SEC (2020) 430 final} - {SWD (2020) 345 final}. Note that in the EU there are rarely specialized universities or scientific and technical publications specifically on telecommunications. Only in the former GDR was the scientific and technical journal "Nachrichtentechnic" published. Therefore, in the EU, telecommunications systems are considered as part of "electronic communications networks".

The American Telecommunications Act (Telecommunication Act, 1996, p. 104) provides a good example of an approach to the "basic level of security of communication networks". The document gives a clear and broad picture of the information security system, telecommunications networks, telecommunications services and services. A tough approach is assumed in the Concept of Information Security of the Russian Federation. This document introduces the concept of "basic level of security of communication networks". It is important. Operators have specific requirements. In addition, a single entry level security is provided. You cannot go below this basic level.

In Ukraine, this issue needs to be resolved immediately. The first version of the Law of Ukraine "On Telecommunications" contained significant requirements for the system of information protection and information security of telecommunications systems, which corresponded to the then level of technical protection of information. There were uniform requirements for accessibility, integrity, observability of information, sustainability, survivability and reliability of networks. The latest version of the Law provides for information security only for special communication. The connection of public use in the interests of information systems, where information is processed, is important for people, society and the state, for industrial production, etc., may remain without basic protection. This is a gross mistake.

It is not possible or necessary to return to the previous versions of the Law on Telecommunications. Telecommunications have developed significantly. The composition of threats to telecommunications has changed. Cybersecurity challenges have become more complex. The task is to build a national cybersecurity system. Establishing a certain basic level of cybersecurity of telecommunications will make it possible to meet an attacker on the "far frontier".

A comlementare approach to ensuring the cybersecurity of the cyberspace and telecommunication environment

Let us turn to the approaches to information and cybernetic security in modern technological control systems, for example, in industrial systems. Artificial intelligence is being actively implemented in these systems, virtual reality complements physical reality. The most important feature here is the convergence of functional security, information security and cyber security. The concept of "information" is considered broader than the concept of "cybernetic". However, the tasks of the CS include not only the protection of cyber technology, but also the protection of the "cyber environment". Additionally, it is necessary to implement cyberspace. The CS covers information, information technology, staff, users and everything that arises in the communication of subjects and objects and their interaction with each other. Cybersecurity is provided in the following areas: security of applications and operating systems, security of information and communication networks, security of the Internet, protection of information in key information infrastructure systems and, in particular, in critical infrastructure, as well as in the fight against cybercrime and ensuring safety in cyberspace".

In our case, we will consider the so-called cyber-physical systems (CPS). Let us emphasize the characteristic differences between classical computer automated systems (AS) and industrial systems of the CPS class. Information security in the AS is multilaterally regulated by numerous domestic legal documents on technical protection of information. In the classical case, information and information resources are protected in the AS, where the information product is obtained as a result of processing information raw materials by information means. At all stages of operation of the AS there is no fundamental difference between the information product and the information means of its processing. Physical systems are present here as storage media, storage devices, processors, etc.

In CPS information security is provided, where a technical (physical) or technical-information product is obtained as a result of processing of information-physical raw materials by cyber-physical (SCADA with executive devices) means. Information and physical objects interact closely with each other in both the processing and the source technical information product. Support for the survivability, sustainability and functionality of the CPS is added to the tasks of protecting the confidentiality, integrity, accessibility and, at the same time, the necessary monitoring of information. In other words, the CFS must provide information security, as in any automated system, cyber security, as in any automated process control system (APCS), and functional and physical security, as in any technical system. There are many classic AUs in the industrial infrastructure, each at its own level: office computer network, demilitarized zone (DMZ-network), network (SCADA / DCS), technological network, and at the field level, where programmable logic controllers operate (PLC).

Based on the virtual reality model, approaches to the levels of cyber-physical security of the CFS can be shown in Fig. 1

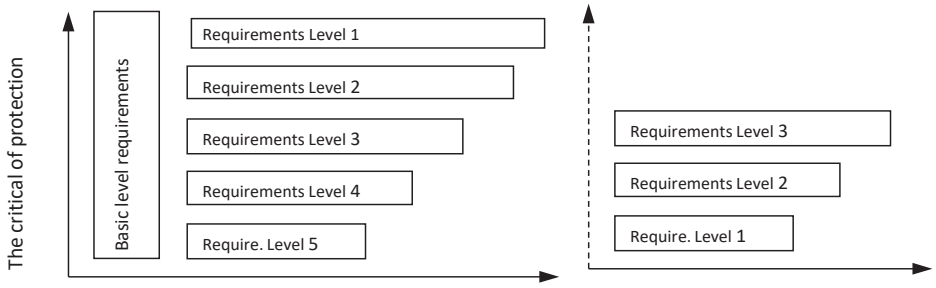

Figure 1. Approach to the requirements of cyberphysical security of CFS and cybersecurity of telecommunications using the concepts of security levels.

The strength of the requirements for the protection of the CPS, for the protection of the telecommunication

Source: the left part of fig. 1 copied from an IAEA – Computer security techniques for nuclear facilities / International Atomic Energy Agency. Description: Vienna 2021. IAEA nuclear security series, ISSN 1816–9317; no. 17 -T (Rev. 1).

IAEA standards provide an example of the application of the cybersecurity level model. Based on this example of protection of nuclear facilities, the recommended distribution of security levels of facilities and telecommunications security is shown in the coordinates of the importance of systems for the safety of industrial and transport installations and the degree of protection (Computer security techniques for nuclear facilities, 2021).

For all installation equipment and means of telecommunications it is provided that:

– basic measures should be applied to all computer and telecommunication systems;

– levels of cyber-physical security are different: from level 5 (minimum protection required) to level 1 (maximum protection required);

– levels of cybersecurity of telecommunications are different: from level 1 (channel) to level 3 (transport level);

– direct connection channels passing through several zones are not allowed;

– measures corresponding to each level are not cumulative (therefore repetitions are possible).

– the basic level of protection must be not less than the established level of protection of information systems used in government agencies and enterprises.

The right part of fig. 1 is the original. It applies, respectively, to the levels of cybersecurity of the primary telecommunications network (functional security at the physical level), the network layer of the telecommunications network (cyber-physical security) and the transport and application layer of the telecommunications network at critical infrastructure.

To explain the principle of building a cyber-physical security architecture, we quote from the IAEA publication: "The division of equipment into zones should be properly documented, including a brief overview of all computer systems, all relevant communication lines, all zonal intersections and all external connections, and taking into account analysis of cyber-physical security risks, specifics of the environment and installations of industry and transport" (Ibidem).

It should be recalled that in the digital transformation, in terms of information security, telecommunications networks have a number of features in their role in the infrastructure of the state and society and the nature of information processing.

The first feature. Telecommunications systems and networks are classified as "critical infrastructure facilities". The latter include a set of physical or virtual systems and tools that are so important to the state that their failure or destruction can have detrimental effects on the economy, defense, health and national security. It is crucial to develop measures for the protection, duplication, mobility, interconnection, recovery and security of the country's telecommunications systems for use in the interests of government critical information services and telecommunications resources both in emergencies and in normal operation. The information security of the information infrastructure of public telecommunications networks (PTNWs) includes the requirements of ensuring survivability, which involves maintaining such properties as the reliability of the network, sustainability, availability of information resources, the integrity of the structure, renewability.

The second feature of telecommunications is related to the problem of ensuring the security of socio-political relations, in particular with the emergence of threats of a new type – the impact on communication systems, collection and processing of information. Such means of influence are based on automated analysis of the structure of messages, tracking keywords, synthesizing language in real time. The result of the impact is the creation of invisible barriers to intellectual influence by blocking, substituting key elements in messages and even introducing false or false key elements into messages. In this regard, for telecommunications networks, the importance of ensuring the integrity and reliability of information transmission, protection against routing violations, timely delivery of information (minimum

message delay), as well as protection against unauthorized access to information resources of networks, including physical security.

The third feature is the nature of information processing – telecommunications provide transportation of information in the interests of its processing by automated systems at the objects of information activities. In this case, the transportation of information in accordance with the recommendations of ITU-T means not only the functions of transfer (transmission) of information in space, but also network functions such as monitoring the transfer of information, audit and operational switching of channels and routes, timely recovery information, network management, administration. The cost of transportation (delivery) of information does not depend on the value of information, or rather the value of information is determined not by the operator but by the customer, who chooses the appropriate quality and type of telecommunications services. The operator provides telecommunications services according to a certain scale of service quality or a certain level of security of information when it is transmitted over the network.

The information sphere, which is a combination of information infrastructure and information resources, is subject to protection in PTNWs. According to the legal documents of the technical protection of information, the responsibility for ensuring the confidentiality of information lies with the owner of the information. The Operator may provide privacy services only under an agreement with the owner of the information. The confidentiality of information transmitted by the telecommunications network is ensured by the owner of the information, and other properties of the information transmitted by the network – integrity, availability and observability – are protected by the network operator or telecommunications service provider. With regard to technological information, control information, signaling and technological information resources, in the interests of the operator or provider, they must protect all properties of information resources: confidentiality, integrity, availability of technological information and observation of service processes.

The fourth feature of telecommunications is manifested in the introduction of electronic document management, electronic digital signature, e-government, e-commerce, etc. The telecommunications network used to build these systems must provide a new level of information security and, in particular, ensure privacy, mutual authentication and integrity. The latter means ensuring the impossibility of denying the fact of transmission or reception of messages (data) in the process of interaction between the network and users and between the interacting elements of the network.

Ensuring information security of telecommunications networks should include these and additional concepts, which in order of importance are in the following order: integrity (integrity) of information, confidentiality (confidentiality), security against unauthorized access (authentication) to information, information resources and network equipment, irrefutability of the fact of transmission and / or reception of information (non-repudiation), ensuring the reliability (availability) of the functioning of the telecommunications system and its survivability. The problem of ensuring the integrity and authenticity of the user is most effectively implemented through the use of digital signatures based on asymmetric cryptographic algorithms

with two keys – personal and public – in combination with the infrastructure of certification authorities.

In order to use the existing domestic regulatory framework, it needs to be supplemented and modernized by taking better account of international experience and developing new regulations. The regulatory framework for information and telecommunications systems, which mimics automated systems, may be partially extended to telecommunications systems. The priority is to develop technical requirements and regulations for cybersecurity of telecommunications equipment and technologies purchased from foreign manufacturers. Next, an acceptable telecommunications cybersecurity system needs to be developed and integrated into the state cybersecurity system.

Creating and providing security management services is relatively simple. Today, any established telecommunications system must meet the requirements of the ITU Recommendations and have built-in information security mechanisms. An example is CISCO telecommunications equipment. Ukraine produces little of its own telecommunications equipment. It is urgent to develop appropriate regulations, instructions and other documents such as "System requirements, mechanisms and interfaces for information and cybersecurity of purchased equipment".

Main provisions of the update concept of cyber-physical security of the common telecommunication network

Problems of the updated concept of cyber-physical security of public telecommunication networks of Ukraine (PTNWs). At one time, the authors of this work presented the relevant concept in the light of the then Law "On Telecommunications" (Tardaskín, Kononovich, Tardaskína, 2006, pp. 15–22). A number of adjustments now need to be made. The process of ensuring information security largely intersects with the processes of quality management of telecommunications services, where the security of information resources is an integral part of the system of assurance and quality assurance; with economic efficiency management processes, where information security risks are interrelated with economic risks; with processes and tasks of technical operation in terms of ensuring the requirements for maintaining a minimum set of critical network functions in emergencies, the survivability of information systems, the margin of safety in the event of destabilizing environmental factors.

Analysis of the relationship and interdependence of information security tasks with tasks in these areas shows that at different stages of the life cycle of information security systems at different stages and stages of design, construction and operation are formed indicators of security, guarantees, quality and related technical economic indicators. We compare the following pairs of information properties or protection systems: survivability of systems – performance and reliability of systems, data integrity – data reliability, structure integrity – system resiliency and redundancy, process observation – controllability of operational processes, stability of algorithms – resistance of systems to external destabilizing environmental influences.

Statement and solution of information security problems stems from the "increased requirements for the survivability of information systems, which are characterized by a high degree of resource allocation (service, logic, algorithms, software and hardware, telecommunications). In order to fully operate and maintain a minimum set of critical functions, the telecommunications system must have a certain margin of resistance to destabilizing environmental factors".

Violation of the integrity of the system against the background of reduced activity of its elements entails disorganization of management, simultaneous reduction of activity of elements and their survivability – loss of flexibility, and reduction of survivability and violation of system integrity – loss of critical functions.

The concept of survivability of the system implies its ability to perform its functions in a timely manner under destabilizing factors (physical destruction, partial loss of resources, failures and failures of elements, unauthorized interference in the control circuit). In this case, technical reliability, which is manifested as the ability of the system to work for a specified period of time in the regular system without failures, determines the minimum threshold of stability of the system, beyond which without recovery of lost elements and functions may occur complete shutdown. The survivability of information systems is crucial for information security in general.

From a practical point of view, it is important that within the system of technical operation of telecommunications networks developed tools to maintain a given level of reliability of data transmission and reliability of telecommunications systems and other indicators of information quality and such indicators are related to information security.

"Confidentiality depends on integrity and, in turn, on reliability. If the integrity and reliability of the system is compromised, the effectiveness of privacy mechanisms is likely to decline. On the contrary, breaches of confidentiality, such as technological information, will lead to circumvention of the mechanisms of integrity, accessibility and monitoring. Also, if the integrity of the system is violated, it will compromise the mechanisms of accessibility and monitoring".

Indicators of information delivery – the probability of loss and distortion of messages (reliability), delay time, errors in addressing the consumer and the source of messages – affect the effectiveness of the mechanisms of confidentiality and integrity.

Quality indicators in generalized form are included in the characteristics of integrity and accessibility. Characteristics of information delivery to the consumer and other information and telecommunication services in general form are included in the indicators of accessibility and, in part, in the indicators of confidentiality and integrity. Reliability and reliability are indirectly interrelated with the properties of confidentiality, integrity, accessibility. Quantitative or qualitative insufficiency of system components affects the effectiveness of information resources protection.

Of course, in the technical field and in the field of information security there are different approaches to a number of considered concepts and in different areas they have different meanings. Thus, the concept of integrity includes not only the preservation of quantitative characteristics of information – bits and bytes, but also the semantic characteristics of information – the content of messages. In the field of

security, the properties of information are considered in terms of both man-made and anthropogenic impacts. However, differences in concepts cannot be an obstacle to a comprehensive analysis. Integrity indicator is a complex function of reliability, noise immunity, observation and accessibility. It is rather impossible to separate such concepts.

Thus, the essence of the relationship between the basic concepts of information security system with the concepts of other interpenetrating systems of quality assurance, network management, management and technical operation is that the basic concepts and properties of other systems are based, in general, on man-made factors an important part of the basic concepts and properties of the information security system. The latter are based on both man-made factors and, above all, on anthropogenic factors.

Goal and objectives concept. The introduction of new technologies at the PTNWs should be accompanied by adequate solutions to information security problems that affect the industry as a whole:

– methodological bases for ensuring information security of transport functions of PTNWs;

– normative-legal and normative-administrative base of information security of PTNWs;

– PTNWs information security requirements system;

– organizational structure of information security of PTNWs;

– domestic means of information security PTNWs;

– training systems.

The main objectives of information security of PTNWs are to support and preserve in the conditions of the violator's influence on the information sphere of PTNWs the following main characteristics of information security of PTNWs:

– integrity of the information sphere of PTNWs;

– confidentiality of the information sphere of PTNWs, including the confidentiality of information of the management system;

– availability of PTNWs information sphere;

– observation (accountability) of the information sphere of PTNWs;

– indisputability of the fact of transmission or reception of information;

– inviolability of traffic routing;

– secrets of communication and privacy;

– prevention of unauthorized access to the information sphere of PTNWs;

– reliability of telecommunication systems operation and survivability of PTNWs.

Ensuring the information security of PTNWs should be achieved through the integrated use of organizational, technical, hardware-software and cryptographic means of protection of the information sphere of PTNWs, as well as continuous monitoring of the effectiveness of implemented measures to ensure information security of PTNWs.

Ensuring the information security of PTNWs involves creating obstacles to possible unauthorized interference in the operation process. In this sense, the problem of information security PTNWs includes both the task of protecting information

from unauthorized access, and a number of other tasks. Work to ensure the information security of PTNWs is divided into three groups.

1. Improving the regulatory and regulatory framework for information security which includes:

– principles of information security in the interaction of various telecommunication networks with each other and global communication infrastructures, in particular, with the Internet;

– the procedure for providing communication services to special users;

– the procedure for managing PTNWs in the "special period" and in emergencies;

– a list of the most critical in terms of information security segments of PTNWs, which provide the transfer of state information resources;

– information security requirements for PTNWs information security facilities;

– methods of assessment and control of the state of information security PTNWs;

–interaction, rights and responsibilities of the subjects of the information security system at the stages of its development;

– the procedure for preparation for certification and state examination of hardware, software and hardware and software for information security PTNWs and certification of information security in general in accordance with the requirements of information security

– organization of work to identify bookmarks and undeclared opportunities in the technical means of PTNWs;

– organization of work on the implementation of state and industry standards for technical and software tools and mechanisms for information security PTNWs.

2. Ensuring technical protection of data transmission processes in PTNWs:

– detection and elimination of vulnerabilities in the information sphere of PTNWs;

– ensuring the confidentiality of information about the information sphere of PTNWs;

– prevention of unauthorized access to PTNWs and information transmitted by it;

– detection and prevention of the violator's influence on the information sphere of PTNWs

– audit, quality control of service and quality characteristics of the data transfer process in PTNWs in the conditions of intentional actions of the violator;

– timely detection of the consequences of the violator's influence on the information sphere of PTNWs;

– localization of the place of action of the violator;

– elimination of the consequences of the violator's influence on the information sphere of PTNWs and restoration of the disrupted process of functioning.

3. Ensuring organizational and technical protection of objects and processes of data transmission: development and implementation of policies to ensure information security of enterprises, branches, telecommunication centers, communication nodes, etc .; organization of control over the state of information security of PTNWs; technical support of information security of PTNWs; development of measures to

ensure the secrecy of communication; taking measures to eliminate the consequences of violators and restore the disrupted process of functioning; ensuring compliance with the procedure for routing traffic established by regulations; improvement of physical and engineering protection of PTNWs facilities and prevention of unauthorized access to the information sphere of PTNWs; selection, training and work with staff in the interests of information security.

International Standards of the International Telecommunication Union (ITU-T) define the system of security requirements for both cyberspace and PTNWs. Of particular value for the implementation of cybersecurity are the requirements of the ITU-T International Guidelines attention - each) network transactions and identity management.

In the final part of the work, complementary approaches are used to develop the updated concept of information and cyber-physical security of the telecommunications environment (telecommunications networks and public systems) proposed by the authors.

References

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. 19.7.2016. Official Journal of the European Union. L 194/1.

Computer security techniques for nuclear facilities / International Atomic Energy Agency. Description: Vienna 2021. IAEA nuclear security series, ISSN 1816–9317 ; no. 17 -T (Rev. 1).

JOIN (2020). 18 final. Joint Cjmmunication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade/ Brussels, 16.12.2020.

Polozhennya pro orhanizatsiyno-tekhnichnu model' kiberzakhystu. Zatverdzheno postanovoyu KMU vid 2912.2021 r. № 1426.

Pro Stratehiyu informatsiynoyi bezpeky. Ukaz Prezydenta Ukrayiny 685/202 vid 28.12.2021.

Strateiya kiberbezpeky Ukrayiny. Bezpechnyy prostir – zaporuka uspishnoho rozvytku krayiny. Ukaz Prezydenta Ukrayiny 447/2021 vid 26.08.2021.

Tardaskín M.F., Kononovich V.G., Tardaskína T.M. (2006). Osnovní polozhennya kontseptsíĭ sistemi ínformatsíynoĭ bezpeki telekommunikatsíynikh merezh zagal'nogo koristuvannya, *Zv'yazok,* № 3 (63).

Telecommunication Act (1996). An Act To promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies. Public Law 104-104 104th Congress. FEB. 8.

Author's Bionote

Iuliia Bielova – Senior Lecturer, Department of Cybersecurity and Technical Information Protection, State University of Intellectual Technology and Communication, research interests – cybersecurity, case studies on information security requirements, cryptographic methods of information security. Author of 10 scientific works and 6 works of educational and methodical direction.

Volodymyr Kononovych – Ph.D., Associate Professor, Department of Cybersecurity and Technical Information Protection State University of Intelligent Technologies &

Telecommunication. Qualifications: cybersecurity specialist. Since 2000 he has worked for 10 years as a leading specialist at the Odessa Regional Center for Technical Protection of Information. Teaching experience: 52 years. Research interests: information theory, neocybernetics and cybersecurity. Publications: more than 200 scientific publications, textbooks and copyright certificates.

Oksana Shvets – Senior Lecturer, Department of Cybersecurity and Technical Information Protection, State University of Intellectual Technology and Communication. In 2007 she graduated from the Odessa National Academy of Communications. O.S. Popova, specialty "Telecommunication systems and networks". From 2009 to 2012 she studied at the graduate school of the Odessa National Academy of Communications. O.S. Popova, specialty 05.12.13 – radio devices and means of telecommunications. In 2019 she passed advanced training at the Odessa National Polytechnic University, specialty 125 – Cybersecurity. Author of 13 scientific works and 4 works of educational and methodical direction.