I.J. Information Engineering and Electronic Business, **2022, 2, 23-38**
Published Online April 2022 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2022.02.02

Scientific and Methodological bases of Complex Assessment of Threats and Damage to Information Systems of the Digital Economy

Alovsat Garaja Aliyev
Institute of Information Technology of Azerbaijan National Academy of Sciences, AZ1141, Azerbaijan, Baku
E-mail: alovsat_qaraca@mail.ru; alovsat.qaraca@gmail.com

Roza Ordukhan Shahverdiyeva
Institute of Information Technology of Azerbaijan National Academy of Sciences, AZ1141, Azerbaijan, Baku
E-mail: shahverdiyevar@gmail.com

Received: 10 January 2022; Revised: 14 February 2022; Accepted: 09 March 2022; Published: 08 April 2022

Abstract: The article examines the scientific and methodological basis of a comprehensive assessment of threats and damage to information systems of the digital economy. The information infrastructure and tasks of the digital economy have been defined. Sources of information security in the digital economy sectors and their information security requirements have been studied. The results of the analysis of the situation in the countries of the world on the Global Cyber security Index are shown schematically. The graph of the dynamics of cybersecurity expenditures in the ICT segments is shown. It is argued that cybersecurity, which is formed and developed through the use of digital systems, is a priority. Many goals and methods of cyber-attacks are given on the platform of the 4.0 Industrial revolution. Cases of information security violations in the digital economy and the processes of assessing the damage caused by them have been studied. Generalized criteria for assessing information damage in the digital economy have been proposed. Threats to information and communication systems and classification of damage are given. A structural scheme of the conceptual model of threats and damage to information systems and resources in the field of digital economy of Azerbaijan has been proposed. An expert description of the ways in which information threats are disseminated has been developed using a fuzzy approach. The main types of damage caused by threats to the security of information systems are given. The security aspects of the abundance and surplus of information in the digital economy are shown. The directions of increasing the level of security and confidence in the digital economy and the structures to ensure its security are given. The main directions of information security in the digital economy have been identified, the directions of ensuring its security and increasing its confidence have been identified. Commonly used universal base technologies have been proposed in the digital economy sectors. Some methodological approaches to integrated risk and damage assessment in the digital economy have been explored. A scientific-methodological approach based on fuzzy methods has been proposed for the implementation of complex risk and damage assessment in the digital economy.

Purpose of the research. The main purpose of the research in the article was to develop ~~a~~ scientific and methodological bases for identifying and comprehensively assessing the scope of possible threats, dangers and damage to information systems that make up the infrastructure of the digital economy in its formation conditions. Attention was paid to the development of recommendations on promising areas for improving multi-criteria expert assessment methods in increasing the effectiveness of management of threats and damage to information systems of the digital economy and the assessment of their performance. By applying the results of multi-criteria expert assessments in decision-making processes it has been possible to get results. Attempts have been made to classify threats and damages in information systems and resources in the sphere of digital economy and to develop a conceptual model of their impact. The spread of information threats using a fuzzy approach has been described by expert methods. Defining the main directions of information security in the digital economy, defining the directions of ensuring security and increasing confidence, using universal basic technologies to ensure security in the digital economy sectors are also included in the research goals. One of the goals was to propose the main stages of an approach based on fuzzy methods for the implementation of integrated risk and damage assessment issues in the digital economy.

Research methods used. Research methods such as system analysis, correlation and regression analysis, mathematical and econometric modeling methods, expert assessment method, measurement theory, algorithmization, ICT tools and technologies have been used in the development of scientific and methodological bases of complex assessment of threats and damage to information systems of digital economy.

Index Terms: Digital economy, digitalization, information infrastructure, information systems, information threats, level of economic security, cybersecurity, security technologies, Industrial 4.0 Revolution, expert assessments, fuzzy estimates of losses, complex assessment of losses.

1. Introduction

The experience of countries with strong economies shows that current global development is based on innovative technologies, knowledge and information. At present, the main condition is to achieve sustainable economic development. One of the urgent issues is the formation of socially oriented, diversified national economies. In terms of economic and social development, their digital transformation has become one of the priority issues facing the country in recent years [1]. In this regard, the implementation of promising digital projects such as the development of the Internet and network technologies, which form the basis of ICT infrastructure, "Government Cloud" (GCloud), "Big Data", "Smart City", "Smart Village" and etc. Consistent reforms are underway to turn Azerbaijan into a digital hub in the region.

There is a need to expand the use of digitalization in various sectors of the economy, to improve quality. Improving regulatory mechanisms and creating a healthy competitive environment in the development of communications and information technologies is of great importance for the country. Their implementation is one of the main goals [2].

Since the first years of the XXI century, the formation of rapidly developing ICT, telecommunications and computer technology, as well as science-intensive high-tech products in accordance with the challenges of the 4.0 Industrial Revolution has become one of the main directions in the world economic development [3, 4]. Therefore, the application of the 4.0 Industrial Revolution and the components of artificial intelligence technology in the digitalization of the economy is of great importance in modern times.

However, the inability to solve their security problems in a timely manner also raises new types of issues. Thus, the integration of information and computer systems with different means of protection of users in a single corporate network usually leads to the weakening of the overall infrastructure. Weaknesses in information systems can be both overt and covert, and they cannot always be protected. The organization of a common information space increases the availability of information resources. This leads to an increase in unauthorized access to information by both external and internal users, as well as threats. In addition, the application of ICT results in integration processes in the infrastructure itself, which leads to a dangerous level of accumulation of information. As a result, a large amount of information is collected in the same place. This can completely reveal to the competitors the characteristic technologies of management and business conduct for the enterprise organization. The loss or leakage of such information can pose a serious threat to them. The integration of different types of information security systems in a single corporate network also makes it very difficult to solve the problem of information security. This fact further complicates the problem of information security at the organizational and managerial levels [5]. As a result, in the context of the information economy, a comprehensive assessment of the threats and damage to information systems as part of the digital economy sectors has become a necessary and urgent issue.

2. Problem Statement and Research Situation

The informational causes that threaten the digital economy sectors ultimately increase the risks and potential harms of information systems (IS). If the necessary measures are not taken in time, it can pose a serious threat to the sustainable development of any organization. Such negative factors can be prevented only by appropriate measures taken in a timely manner to prevent the increase of these risks and losses. One such measure is the emergence of the ISO 27000 series of standards-based on risk identification and assessment procedures for the development of information security management systems. Currently, there are a number of methods and algorithms for assessing the damage of IS, used in economic systems and processes, both corporate and general. These methods, techniques, and algorithms have been used successfully to address many issues during the audit and monitoring of such systems. However, there are differences in the nature of threats and losses in information security management systems. Due to this, higher requirements are regularly imposed on the methods and algorithms of risk and damage assessment of the IS every year. Of course, a number of studies have been conducted in this direction. However, there are still many unresolved issues in this area. Therefore, it is important to study the issues that arise during the development of methodologies and algorithms for a comprehensive assessment of information security risks and harms, based on a comprehensive analysis of the threats and risks of any enterprise or organization, and their consideration and improvement in economic development.

3. Research of Relevant Related Works

Due to the degree of research and development of problems on identifying and comprehensively assessing the scope of existing threats, dangers and damage to the information systems that make up the infrastructure of the digital economy in its formation conditions, it should be noted that their development and research stages, signs and features of their scientific and technological bases have been the subject of research by many foreign, including Russian, as well as local scientists. Many fundamental scientific-theoretical and applied researches have been carried out for the development of scientific, technical and technological aspects of security systems. At the same time, research work was carried out to organize the improvement activities of traditional information security processes. Different researchers have tried to study the development problems of approaches, models, new processes analyzed in the recent scientific literature in this area from different angles. Therefore, in accordance with the new ICT challenges, serious attention has become being paid to identifying perspective development directions in identifying existing threats, dangers and damage to information systems. We also paid a little attention to this problem at the time **Aliyev** [22].

In addition, many studies [13, 20, 31, 32, 33, 35-39], including **Kargina** [14], have examined the role of information security in the digital economy and have shown that it is a topical issue for the present. Issues such as the significant change in social relations as a result of the use of modern ICT technologies, the existence of a new level of work with data in the digital environment are considered here. It has been shown that the process of formation of the digital economy has taken place in the modern period, when the above-mentioned directions are relevant. Features of the use of digital technologies in improving the development efficiency of the digital economy were noted. The problems of comprehensive protection of the information security infrastructure from any accidental or harmful effects are given, the analysis of the information about the possible damage to the information itself, its owners and the infrastructure supporting it is given in this work.

Ahmet [19] examines the analysis of cyber attack risks in the Industry 4.0 ecosystem and the problems of assessing its defense strategies. The significant impact of the development and application of modern high technologies on the development of interconnected digital ecosystems has been studied and its relevance has been substantiated. It is shown that this system is based on the more use of data. The study examines the existing problems associated with the threats posed by cyber attacks in all areas where digital information is used. For this reason, it is confirmed that the need to address the problems posed by cybersecurity is big. The fact that the main base of ICT systems in modern times is data shows that the risk of cyberattacks in Industry 4.0 continues to grow. The fact that cyber-attacks will continue in the future makes it even more necessary to study the probabilities of its risk. This article examines the sources of cybersecurity threats in the Industry 4.0 ecosystem and examines its interpretation by corporate and end users. The most common cyber security application problems in Industry 4.0 systems have been identified. These were found to be unprotected item connections, unreliability of periodic tests, inability to effectively manage network devices, and unqualified personnel. The study identifies cybersecurity strategies and requirements for solving its problems, as well as gives analysis about the possibilities of how to implement security for corporate users. Research has shown that it is impossible to completely prevent cyberattacks within the Industry 4.0 ecosystem and the cyber attacks it creates. The approaches proposed in the article show that preventing the problems identified by the research can help minimize the damage in cyber attacks.

Grusho [27] explores methods for assessing the security of computer systems for information support of the digital economy. Methods for assessing the security of distributed information and computing systems using information security diagrams have been developed here. It was noted that any method of assessing information security is based on the principle of preventing losses that could damage the distributed information and computing system as a result of various threats. Prevention of threats is based on the analysis of problems and taking into account the possibility of their use in solving them. The security diagram of all distributed information and computing systems is based on elementary information security diagrams. As a result of the use of elementary diagrams developed for information security, options for how to assess the information security of the entire system described by the global information security diagram are shown. The analysis showed that the value of information in substantiating the security of the distributed information and computing system is determined using the method of classification, the amount of damage in the~~ of~~ information leakage and breach of integrity. The methods proposed in this study are determined by the requirements of mass digitalization for the development of small and medium-sized businesses in the digital economy.

Modenov [29] analyzes the features of economic and information security of the digital economy. It was noted that the efficiency of economic activity and its security is directly related to the scale of use of modern ICT technologies. It is shown here that the application of new technologies and the development of modern software in ensuring economic and information security is relevant. For this reason, the need for enterprises to produce information support products was considered one of the most important issues for the development of the country's economy.

Petrenko [40] explores methods to ensure cyber sustainability and security of the digital economy. It was noted that in some cases there is a widespread threat to the sustainability of the digital economy, in which case the attacks take place over a long period of time. In addition to phishing messages and malware, various social engineering methods have been used by criminals. It is stated that the assessment of the cybercrime market in the world is one of the most important issues for today. Cases of anomaly detection in intelligent cyber security technologies have been identified. In the aspect of intelligent cyber security technologies, issues such as the falsity or legitimacy of transactions, connection analysis, detection of fraudulent transactions, identification of accounts used for cash transactions were investigated.

Lidong [36] explores the application features of Big Data technologies in Industry 4.0, cyber-physical systems and digital manufacturing. It is shown that a cyberphysical system consists of complex systems that combine computing, communication and physical processes. It was noted that digital production is a new technology based on the application and use of computers and interconnected modern technologies to manage the entire production process. Features of the ability of Industry 4.0 to manage production more efficiently, flexibly and sustainably through communication and exploration, to increase its competitiveness are shown. The study demonstrates the application opportunities of key technologies such as the Internet of Things, cloud computing, machine-to-machine (M2M) communications, 3D printing and Big Data in Industry 4.0. The importance of the application of Big Data analytics in cyberphysical systems, digital production and Industry 4.0 is highlighted, and future research areas for some cybersecurity issues in this area are outlined.

Volodymyr [38] analyzes methods for identifying cyber threats based on machine learning technology for real-time information systems. The main purpose of the article was to develop a method for detecting cyber threats for the information system. It has been shown that cyber threats affect the performance of network resources, resulting in either a significant loss of resources or a complete failure of the system. Here the procedure of reducing the impact on the system by changing the network topology in advance by detecting countermeasures in certain threats is given. Research has shown that stopping cyberattacks eventually forces attackers to look for alternative ways to damage the system. The condition of network equipment monitoring, which is the most important task in the work of the information system, was explored in this study. With the proposed method, it may be possible to independently detect cyber threats to information systems and take countermeasures to eliminate them. The most important issue to ensure functional stability is to ensure safety measures. It was noted that it can be possible to increase the functional stability of the system operating in real time through this technology-method.

Sidorov [9] analyzes the issues of assessing the levels of development of the regional digital economy. The composite index model for assessing the level of development of the digital economy of regions of different sizes is proposed in the study. It is based on the principles of hierarchy, modularity and balance, as well as a functional network as a kind of oriented graph, structured by levels, based on the availability of information on the development of the digital economy. The influence of the subjective factor was excluded using the calculation based on the standard deviation in the expert determination of the weights of certain indicators included in the composite index. The proposed approach was used to determine the differentiation of the development level of the regional digital economy, as well as to compare the experience of some countries on sustainable ICT infrastructure.

Soshina [28] explores the main problems of ensuring the level of economic security of the regions in the digital economy. Some recommendations are given for ICT infrastructure and information systems with regional sustainable features.

Such analyzes of the scientific literature show that there is a growing need to analyze new global trends in this area, develop the problem on the Industry 4.0 Platform, to study the application of modern technologies in the security of information systems such as the Internet of Things, artificial intelligence, big data, etc., to study the features of their protection and regulatory mechanisms, and to develop recommendations for the modernization and use of these systems with the application of ICT technologies.

4. Research Methodology

The article takes information systems, which are the infrastructure basis of the digital economy, as the object of research. The subject of research is a comprehensive assessment of threats and damage to information systems. Attempts were made to develop scientific and methodological bases for a comprehensive assessment of threats and damage to information systems. Comprehensive assessment of threats and damage to information systems of the digital economy is carried out on the basis of appropriate methods and technologies. In proposing a conceptual model of the impact of threats and damage on information systems and resources in the regional digital economy, international economic development trends, requirements of high and modern ICT technologies, the main trends of the Industry 4.0 platform were taken into account. It is shown that the main tool is the expert assessment of the methods of dissemination of information threats using a fuzzy approach.The main directions of information security in the digital economy have been identified, the directions of ensuring its security and increasing its confidence have been substantiated. Commonly used universal base technologies have been proposed for the security of the digital economy sectors. Threats and damage in the digital economy have been classified, and a scientific-methodological approach based on fuzzy methods has been proposed to address the issues of their complex assessment. Generalized criteria for assessing information damage in the digital economy have been proposed. A comprehensive assessment of the threats and damage to the information systems of the digital economy has been calculated based on the inclusion of a specific loss function of eliminating them and final damage indicators.

5. The Role and Tasks of Information Infrastructure and Technologies in the Digital Economy

All existing threats in the field of economic information have very important economic characteristics. At the same time, it should be noted that the sustainability of the level of economic security of the national economy depends entirely and directly on the level of its information security [6, 7].

Along with the tasks of the traditional industrial economy, new requirements, issues, and goals have been set for the new economy. These are to more fully and effectively meet the needs of the country's citizens for products and services in both traditional and digital forms to improve their material and spiritual well-being and quality of life. This is possible in the context of wider use of digital technologies, increasing the digital literacy of the population, increasing the level of information provision of people, facilitating access to public services. Therefore, it is considered that the emerging modern information and knowledge, innovation economy [8-10] can operate effectively only on a platform consisting of the highest ICT infrastructure, means of communication, and cyber-physical systems. Such a platform provides a highly developed information security system, reliable telecommunication network, wireless lines, permanent monitoring systems, technical regulatory structures, relevant highly qualified personnel, high-level organizational, legal, financial, regulatory, environmental, social problems that can be protected from threats and dangers must have denial mechanisms. As you can see, the key issue here is to achieve an effective solution to the information infrastructure and security. In order to apply global technologies in this direction, specialized technology centers, technopolises, technoparks, etc. to transfer new knowledge and technologies in order to put them into practice in relevant fields must be created.

The main ICT technologies that affect the formation of the digital economy can be presented as shown in Figure 1 [11]. These technologies and the network and hardware-software complexes that enable their application, in general, create a relevant information infrastructure of the digital economy, but also further complicate its security situation.

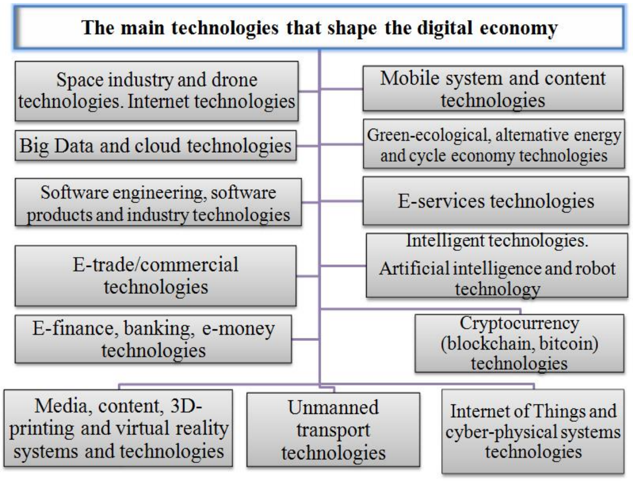

The main technologies that shape the digital economy
Space industry and drone technologies. Internet technologies
Big Data and cloud technologies
Software engineering, software products and industry technologies
E-trade/commercial technologies
E-finance, banking, e-money technologies
Mobile system and content technologies
Green-ecological, alternative energy and cycle economy technologies
E-services technologies
Intelligent technologies. Artificial intelligence and robot technology
Cryptocurrency (blockchain, bitcoin) technologies
Media, content, 3D-printing and virtual reality systems and technologies
Unmanned transport technologies
Internet of Things and cyber-physical systems technologies

Fig. 1. The main technologies that form the digital economy *(suggested by the author)*

6. Sources of Information Security in the Digital Economy Sectors

Information security of information resources, systems, products, and services that shape the essence and content of the digital economy can be exposed to the following risks, threats, and dangers [12-14]: prevention of privacy and threats to the privacy of users in the digital environment; ensuring personal rights, identification of persons, storage and protection of personal data belonging to them; increasing their confidence; threats and intimidation to individuals, businesses and the state arising from the remote use of hierarchical telecommunications systems and resources; increase of external information-technical influence on critical information infrastructure; increasing the level of internal and external computer crime; to lag behind the leading, strong foreign countries in the level of ICT development; dependence of socio-economic development on the export policy of foreign countries. Basic principles such as completeness, confidentiality, and accessibility must be fully adhered to to ensure information security in the information and digital economy sectors [7, 15]. It should also be noted the relative weakness of research in terms of the overall development and security of ICT infrastructure in the digital economy and the lack of sufficiently highly qualified staff.

7. Information Security Requirements in the Digital Economy

In general, the security of information systems in the digital economy is carried out at the legislative, administrative, organizational, software, and technical levels. Its level depends on the establishment of an appropriate security system. To establish such a system, it is necessary to define specific requirements, national and international requirements tried and tested practices, standards, methodologies, division of responsibilities and responsibilities, general security policy, security management, sources of damage, their calculation and methods of risk assessment [16, 17]. The main metric of information security is to identify possible losses and their probabilities during risk assessment. They are associated with many value indicators. The main purpose of risk analysis is to assess the sources of danger. In assessing the risks, the value of resources, the importance of the threat, weaknesses, efficiency, etc. such factors must be taken into account.

Some results of the analysis of the situation in the countries of the world on the Global Cybersecurity Index. The Global Cybersecurity Index [18] has been calculated for many years. At the time of the release of the first iPhone, Facebook was only open to users outside of US universities for a year. One billion people worked online. There were problems with the amount of data generated (255 Exabytes) being more than the available memory. Some of the results of the analysis of the situation in the world on the Global Cybersecurity Index can be given as shown in Figure 2.

Today, smartphones have changed everyday life and social media has entered a larger area of society. More than 3.5 billion people work online. Thanks to cloud computing, the digital world is estimated to be 44 zettabytes without the risk of inaccessible memory. In addition, as a result of the spread of ICT, the wider national ecosystem has new organizational capabilities, such as e-government services, economic and business models. 4.0 The Industrial Revolution is one of the main paradigms of the digital economy, applying to all sectors of the economy. There are some digital gap problems in the world. Cybersecurity is one of the top priorities of the economy and society, which is formed and developed through the application of digital systems.

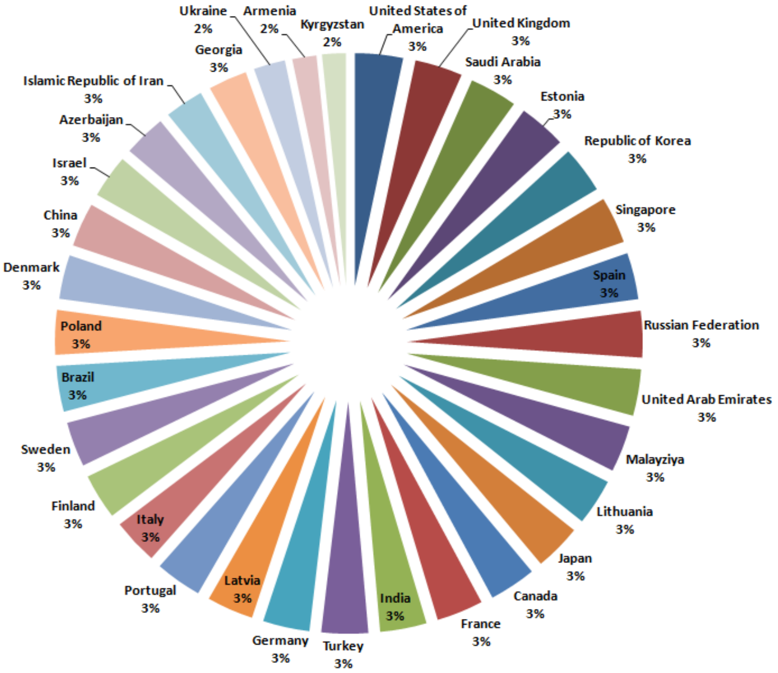


Fig. 2. Results of the analysis of the Global Cybersecurity Index in some countries of the world (suggested by the author), [18]. Source: Global Cybersecurity Index, 2020. International Telecommunication Union. ITUPublications. 172 p.

Sensitivity and vulnerability tests such as network, mobile, customer-oriented, database, social engineering can be used to perform cybersecurity analysis of information systems [19]. The threats posed by the system as a result of cyber-attacks in the 4.0 Industrial Revolution, in which the human factor is minimized, are greater than in other industrial revolutions. In particular, attacks on intelligent production systems can negatively affect the production activities of enterprises.

There are many goals, consequences and methods of cyber attacks on enterprises and organizations in the 4.0 Industrial platform [19]. There are methods of cyber attack such as 1)attack, unpredictable behavior, 2)confidentiality of information, 3)manipulation, malware, 4)viruses, 5)life cycle in background programs, 6)eavesdropping. The goals of a cyber attack include the human factor, process, control, network, system, device and communication, and so on. levels such as. Deformities and misunderstandings, data and rule violations, inaccuracies and failures, service denials, failures, loss of ability to work and communication, etc. are among the effects of cyber attacks. includes.

Many problems in modern times, reduce the confidence in online systems and create some barriers to the full potential of the digital society. Thus, global losses due to cybercrime are estimated at $ 1 trillion in 2020 and $ 6 trillion in 2021. To ensure the security of society and a secure digital environment, it is important to develop a legal and regulatory framework and to carry out certain work in the field of cyber security.

According to the International Report of the International Telecommunication Union's Global Cybersecurity Index 2020 [18], Azerbaijan improved its position in the ranking by 15 points and ranked 40th with 89.31 points. It should be noted that the relevant data have been collected since 2014 in order to determine the Global Cybersecurity Index of the countries. The Global Cybersecurity Index aims to rank states by assessing the level of cyber security in five key areas: 1)Legal measures (legislation, regulation, and control). 2)Technical measures (CERT, standards, certification). 3)Organizational measures (policy, strategy, responsible organization, national evaluation). 4)Measures to strengthen human resources (development of standards, human resource development, certification of professionals and organizations). 5)Cooperation (interdepartmental, intra-departmental, public-private sector, international). The Global Cybersecurity Index combines 20 indicators that characterize these five areas into one index. According to the report, Azerbaijan ranks third among the Commonwealth of Independent States (CIS) countries after Russia and Kazakhstan (Figure 3).

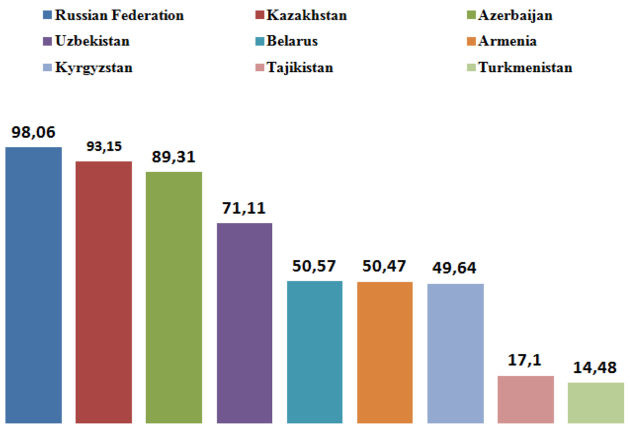


Fig. 3. Results of the analysis of the situation in the CIS countries on the Global Cybersecurity Index (suggested by the author)

Among the 194 member countries of the International Telecommunication Union of Azerbaijan, Switzerland (42), Tunisia (45), Ireland (46), Iran (54), Georgia (55), Iceland (58), Romania (62), Slovenia (67), the Czech Republic (68), ahead of many countries such as Ukraine (78). According to the report, the first places in the ranking are shared by the United States, Great Britain, Saudi Arabia, Estonia, South Korea, Singapore, and Spain. It should be noted that the Global Cybersecurity Index is also affected by the amount of cybersecurity spending [20]. In this regard, it is appropriate to express the dynamic change in cybersecurity spending on ICT segments (2017-2019, $ million) as shown in Figure 4.

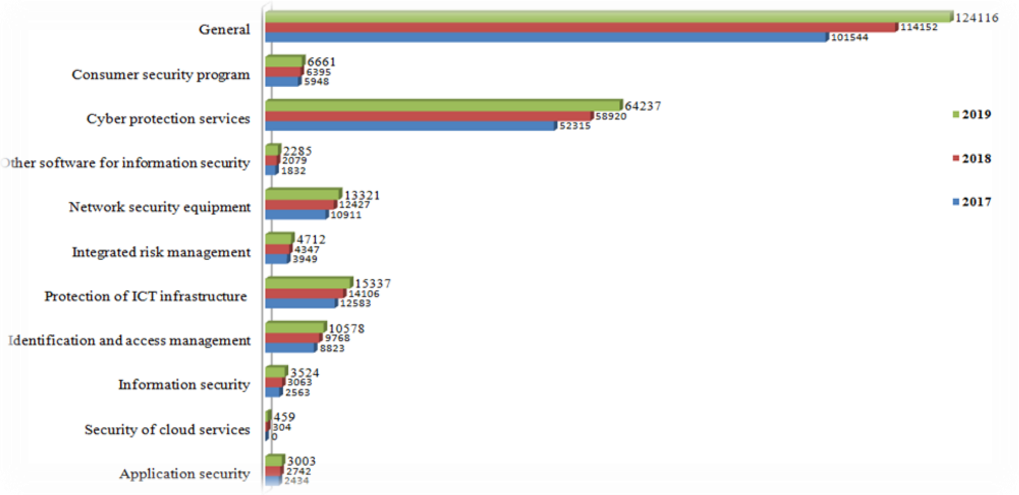


Fig. 4. Dynamics of cybersecurity expenses in ICT segments around the world (suggested by the author)

8. The case of Information Security Breaches in the Digital Economy and the Damages Caused by Them

In the digital economy, damage assessment is sometimes limited to information and software damage, in other words, information damage. Information damage is the failure of an information resource to perform all the tasks of the system, violation of the security function, making unfavorable decisions, violation of the operational process, etc. negative processes that lead to the occurrence of circumstances or increase the cost of achieving the ultimate goal, as well as large material losses. The assessment of such losses may be based on the inclusion of a specific Loss Function (LF) and final damage indicators (Z_1, Z_2,...). Information damage is related to information security breaches and manifests itself in the following ways [21, 22]: Violation of confidentiality of information (Z_1), loss of value (Z_2), destruction of information resource (Z_3) in case of unauthorized intrusion, and interaction of access subjects and objects; destruction (Z_4), its complete (Z_5) or partial loss (Z_6), violation of various tables of databases (Z_7), inaccessibility or inaccessibility of information resource for a certain period of time (Z_8), data collection, exchange, supply and transmission distortion of information resources (Z_9), detection of biased and unbiased errors in software, unforeseen opportunities (Z_{10}).

$$\mathrm{LF} = \sum_i Z_i \rightarrow \min \qquad A_i \geq Z_i \geq 0 \tag{1}$$

The generalized criteria for estimating information damage in the digital economy can be as follows:

K_1 - Damage to national security;
K_2 - Damages caused by violation of the legislation;
K_3 - Losses caused by financial losses as a result of loss of value of information;
K_4 - Damage to the image of the organization;
K_5 - Damage to international information exchange;
K_6 - Damages caused by financial losses related to the restoration of information resources;
K_7 - Damages caused by defects in the activities of the organization;
K_8 -Damages caused by the dissemination of personal information.

A five-point rating scale can be used to assess information security, according to a certain final level of losses: very high - 5 points, high - 4 points, medium - 3 points, low - 2 points, very low - 1 point.

Determination of the rating scale of information security violation is carried out by an expert on the basis of the following final indicators on the basis of preliminary data collected during the analysis of facts of information security violation of any particular enterprise, organization:

P_1-Volume of corrupted, distorted and destroyed information;
P_2-Volume of corrupted, distorted and destroyed general and special software;
P_3-Number of outdated database servers;
P_4-Number of disconnected communication channels and communication devices;
P_5-The amount of negative effects of general use of the Internet on specific information resources; P_6-Time spent on system and network recovery.

Currently, a special rating scale is being developed for the Generalized Criteria for assessing Information Damage to the system (GCD). For example, damages caused by the organization's inability to access service information at a certain time interval can be set in the form of a special scale: (5, 4, 3, 2, 1) - more than a day, 8 hours up to a day, 3 to 8 hours, 1 to 3 hours, less than 1 hour respectively, according to service information no access.

In general, in the digital economy, when determining the indicators of losses (g_1, g_2, ...), there is an important role in determining the Coefficient of Information Loss (CIL), which characterizes the degree of violation of some functions of the system. These allow you to determine the value of information resources in the organization by interacting with possible damage to the information security system.

9. Threats and Damages to the Information and Communication Systems of the Digital Economy

In developing the methodology and algorithms for assessing the risks and harms of information security in the digital economy, it is necessary, first of all, to make reasonable choices for the classification of losses, along with other information threats. In order to model and calculate the main damage of information systems, it is possible to use the classification of threats according to the characteristics of the methods of spread. There are many different information systems and databases in the information space that shape the digital economy. They can be informational threats in many areas. These threats can come from external organizations, the Internet, as well as domestic enterprises and corporate/local networks. The fight against all of them has specific, regional, technical and technological features.

It is intended to use a fuzzy approach based on the above-mentioned notation to describe the methods of dissemination of information threats, damage assessment in an expert way and to develop appropriate models and methods in the future. A block diagram of the conceptual model of threats and damage to information systems and resources in the digital economy of Azerbaijan can be proposed as shown in Figure 5.

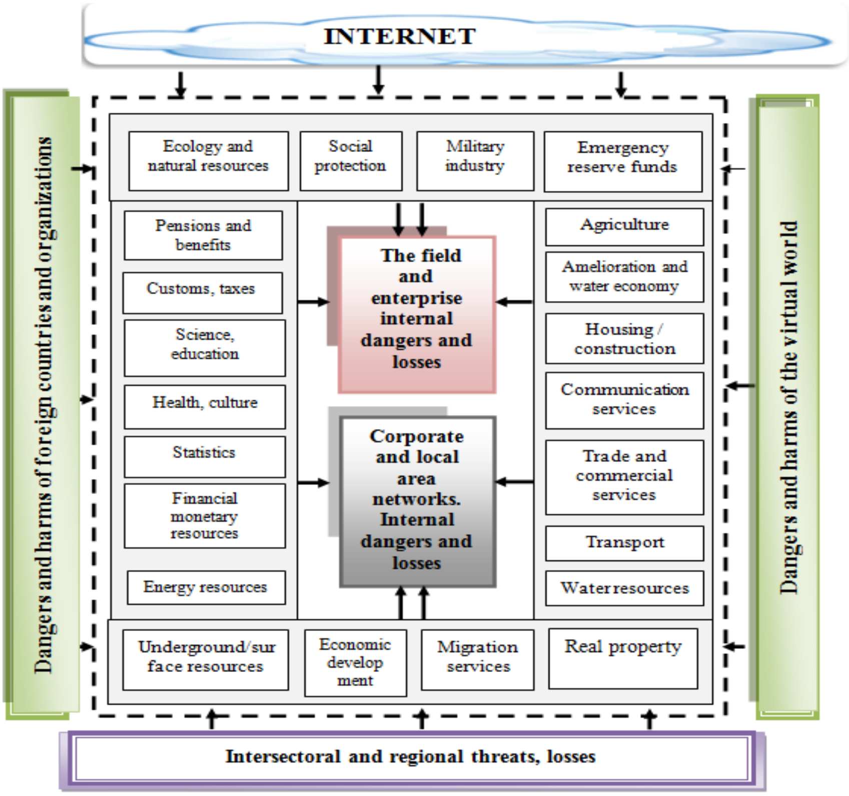

INTERNET
Dangers and harms of foreign countries and organizations
Dangers and harms of the virtual world
Ecology and natural resources
Social protection
Military industry
Emergency reserve funds
Pensions and benefits
Customs, taxes
Science, education
Health, culture
Statistics
Financial monetary resources
Energy resources
The field and enterprise internal dangers and losses
Corporate and local area networks. Internal dangers and losses
Agriculture
Amelioration and water economy
Housing / construction
Communication services
Trade and commercial services
Transport
Water resources
Underground/surface resources
Economic development
Migration services
Real property
Intersectoral and regional threats, losses

Fig. 5. Structural scheme of the conceptual model of threats and damage to information systems and resources in the sphere of digital economy of Azerbaijan (suggested by the author)

It is known that the issue of assessing the damage to information security as a result of threats in the management and use of information systems, ie damage to information security in information systems, remains acute. Information Systems Damage (ISD) is a measure of the amount of damage to an organization's operations as a result of security threats, given the breach of confidentiality, completeness, and accessibility of information. The main types of damage to information systems as a result of threats to information security are as follows [23, 24]:

1)Damage caused by information security breaches (DISB): Damage caused by violation of the diversity of user information; Damage caused by the breach of completeness or accessibility of user information; Damage caused by violation of the completeness or accessibility of technological information.

2)Financial damages and losses (FDL): Expenses for the re-creation of user data, development, acquisition, and installation of the application or system software; Expenditures on information security - purchase, installation, operation of security equipment, maintenance of software and hardware, organization and conduct of organizational and technical measures for security, training of individuals, etc.; Costs of restoration, repair or replacement of hardware; Losses due to inability to use the system and idle time; Losses related to the use of confidential information to the detriment of the organization or unauthorized alteration of data or applications; Fines for violation of agreements or legal norms.

3)Material damages (*MD*): Failure of hardware and information carrier; Control device failure; Loss or destruction of other assets.

4)Ecological damages (*ED*): Damage due to the occurrence and development of natural disasters and emergencies.

5)Economic losses (*EL*): Labor costs of restoration and repair of facilities; Labor costs in restoring and configuring application and system software.

6) Direct damage to an individual's health (DDIH);

7)*Moral damage* (*MD*): Losses related to the decline or loss of the business image of the organization; Losses due to the impossibility to fulfill its obligations; Damages related to the dissemination of personal data of individuals; Damages related to misconduct in the activities of the organization; Damages caused by violation of legal norms; Damages caused by violation of international agreements and treaties, etc.

10. Some Methodological Approaches to a Comprehensive Assessment of Threats and Losses in the Digital Economy

There are many qualitative and quantitative scales for quantitatively assessing damage to information systems. For example, in a system based on empirical operations and mathematical concepts, scales that called series, interval, ratio, and so on are considered. A quantitative polarity scale based on the construction of pole points that determine at least two opposites, ie the extreme opposite effects of damage estimates on the scale (eg, no damage and unacceptable damage), is more appropriate for quantifying losses. On such scales, several types of the quantitative, interval, and verbal assessments in the form of points are considered. Metric or series scales can also be used. However, the use of such scales does not allow for a comprehensive assessment of the damage caused by various threats [25].

In the absence of analytical dependence of the degree of damage on threats and operating parameters of information systems, such compatibility can be established on the basis of fuzzy set mechanisms. Through the expert, the correlation between the hazards expressed by the divisions and the possible damages is established in the established scale of damages. To calculate the uncertainty of expert knowledge about the degree of damage, the size of the damage, presented in the form of a fuzzy triangular number and a function of belonging, can be used. In this case, the individual differences of opinion of experts can be assessed on the basis of the calculation of the coefficient of concordance (agreement, adaptation) in the traditional way. In order to bring the assessment of different types of damage to a common scale, it is necessary to normalize the entire amount of damage on the basis of the maximum possible damage.

In this case, the ratio of the assessment of such damage to its maximum value is obtained. This ratio can be called the index of damage caused by the threat. It should be noted that at the present stage of the development of ICT, more and more fuzzy set theory is used to solve various applied problems. This trend has led to the creation of fuzzy models and systems for solving problems in the field of information security. First of all, this is due to the fact that the processes that take place in the object under study are characterized by high uncertainty, randomness, instability, various influences, and so on. These factors make it extremely difficult to build accurate models based on classical theories and models.

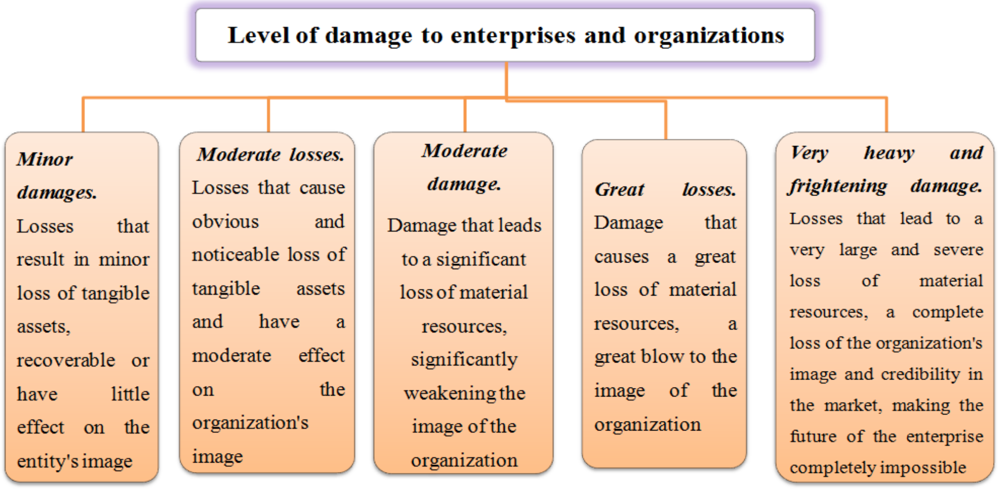
11. Issues of Fuzzy Assessment of Threats and Losses in the Digital Economy

As is well known, the basic concept of fuzzy set theory is the relation function. Therefore, the determination of the degree to which the elements belong to the set and the establishment of the function of belonging are the main issues of practical realization, regardless of their field.

Different methods of forming the function of affiliation can be used in solving the problem of assessing the damage to information security of information systems, as well as in modeling management decision-making processes in uncertain conditions in this area [22, 26, 27]. In this case, in order to effectively address this issue, it is necessary to choose the right method of forming the affiliation function. All these factors indicate the need for timely selection and development of an accepted methodology for integrated assessment of damage to information systems. Such methods, which are associated with the construction of a fuzzy set of damage to information systems, usually use the views of experts in the field of information security. In this regard, experts create an initial fuzzy set of levels of impact of certain threats to the information system. These are summarized in a fuzzy set of general final effects of all classes and degrees of dangers. The damage assessment of information systems is obtained as a result of the generalized affiliation function of all experts on the final overall impact of all types of threats.

It should be noted that the methods of calculating the damage can also be expressed as the level of damage to the organization, as shown in Figure 6 [23, 28]. Here, the assessment of the level of damage to information systems, depending on the nature, frequency, degree, and conditions of the occurrence of this or that threat, is expressed in the form of fuzzy sets.

When establishing the function of the level of damage to information systems, the group of experts is asked to assess the relationship between the frequency and characteristics of the types of threats and the level of damage to the organization. This dependence usually manifests itself as an analytical function of one of the main trends, such as linear, exponential, logarithmic, polynomial [25]. It should also be noted that the linear trend is increasing, the exponential and logarithmic trend is increasing non-linearly monotonously, and the polynomial trend is periodically increasing and decreasing. For experts, it is necessary to choose a more accurate, typical affiliation function of the level of damage to information systems for each threat. Each expert enters the results of his assessment in the questionnaire.



Level of damage to enterprises and organizations

Minor damages. Losses that result in minor loss of tangible assets, recoverable or have little effect on the entity's image

Moderate losses. Losses that cause obvious and noticeable loss of tangible assets and have a moderate effect on the organization's image

Moderate damage. Damage that leads to a significant loss of material resources, significantly weakening the image of the organization

Great losses. Damage that causes a great loss of material resources, a great blow to the image of the organization

Very heavy and frightening damage. Losses that lead to a very large and severe loss of material resources, a complete loss of the organization's image and credibility in the market, making the future of the enterprise completely impossible

Fig. 6. Level of damage to enterprises and organizations (suggested by the author)

Completely filling it allows forming a fuzzy function of the level of damage to information systems as a result of each specific threat. In order to obtain a generalized fuzzy set of levels of damage to information systems as a result of all types of threats, the initial fuzzy sets obtained must be summed by algebraic methods. The final fuzzy set of information system losses presents itself as the result of all pre-generalized fuzzy sets. The result of the processing of the final fuzzy sets of information system losses obtained by all experts is an integrated assessment.

12. Security Aspects of Information Abundance and Surplus in the Digital Economy

In the digital economy, the proliferation of computers, networks of various types and purposes, and the increasing use of them by people are creating an increasing abundance of information systems and resources [7, 14]. As a result, the amount of information systems and resources increases exponentially and it becomes increasingly difficult to separate unnecessary information from the necessary systems, leading to the loss of additional time and financial resources. The abundance of information creates a "garbage" of information after a certain period of time. Failure to cancel them in time causes serious problems. The obsolescence of the systems of any person or organization, even if the information resources are stored in digital form for years, their systematization requires a re-approach to security technologies in terms of storage, organization, protection, and transmission of information. Information culture, use of information, methods of information retrieval should be developed from the same position. Big Data technologies for managing large amounts of data also need to be redesigned so that unnecessary data can be selected from those large amounts of information.

However, along with the abundance of information, there is the opposite. In relevant fields - transport, agriculture, trade, medicine, etc. The timely availability of the most important information creates enough "real waste" of the industrial economy and leads to a large loss of time and money, becoming a source of danger. Therefore, the rapid and strong development of the informatization process is desirable and is a driving force for the development of society. At the same time, the process of informatization is one of the development technologies that must be implemented in various sectors of the industrial economy.

13. Directions to Increase Security and Level of Confidence in the Digital Economy

In the current context of technological development, there are many conceptual technological approaches to ensuring the security of the digital economy. Thus, the concept of e-science development, which takes into account the security factor in the field of research, the e-region platform, which promotes economic and information security of the regions, supports the solution of these problems. In addition, the concepts and paradigms of e-military industry, e-demography, e-agriculture, e-innovation, e-ecology, and green technology provide a scientific and technological solution to this problem. Based on the above technological solution platforms, the security structures of the digital economy can be proposed as shown in Figure 7 [28].

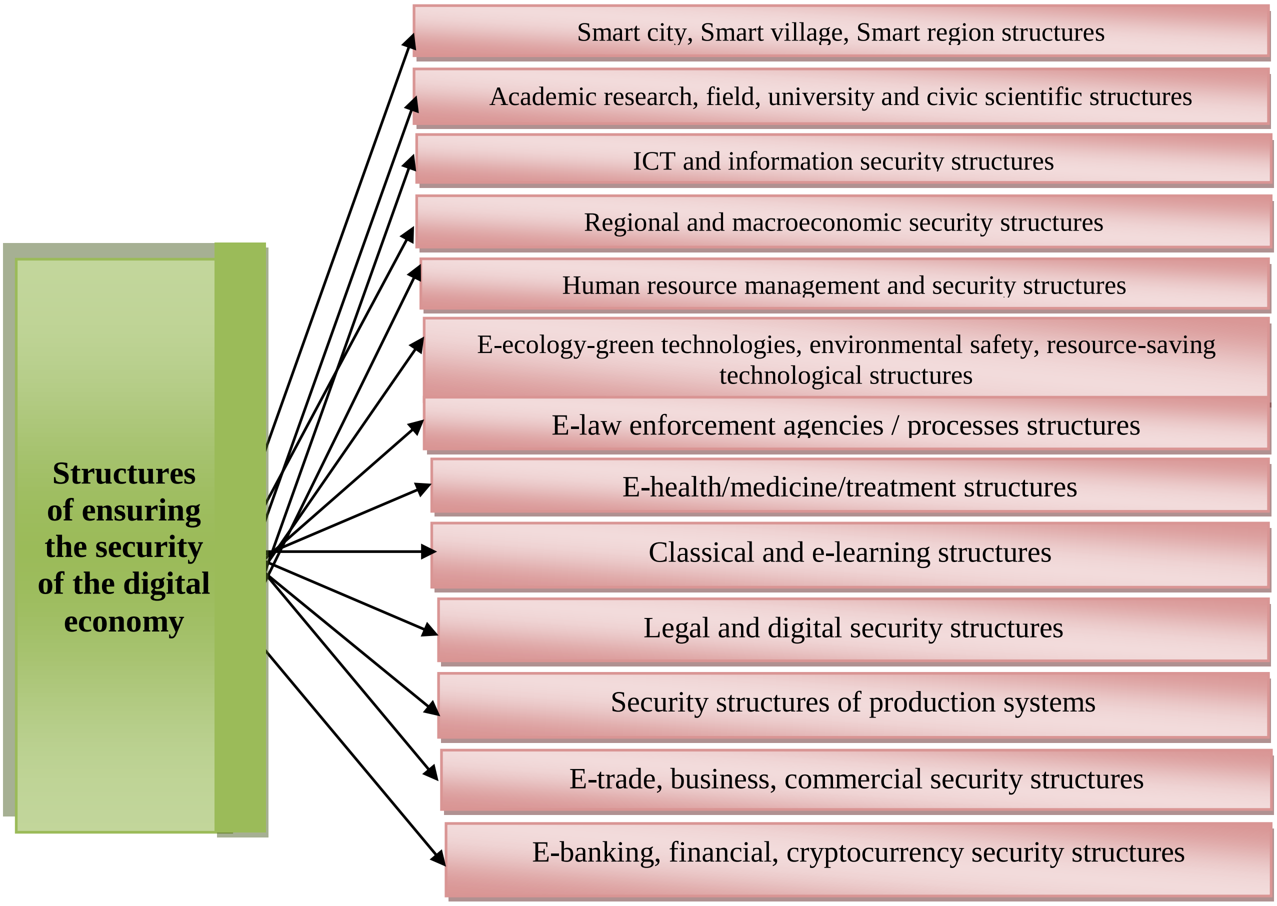

Structures of ensuring the security of the digital economy
Smart city, Smart village, Smart region structures
Academic research, field, university and civic scientific structures
ICT and information security structures
Regional and macroeconomic security structures
Human resource management and security structures
E-ecology-green technologies, environmental safety, resource-saving technological structures
E-law enforcement agencies / processes structures
E-health/medicine/treatment structures
Classical and e-learning structures
Legal and digital security structures
Security structures of production systems
E-trade, business, commercial security structures
E-banking, financial, cryptocurrency security structures

Fig. 7. Structures of ensuring the security of the digital economy (suggested by the author)

As a result of mass informatization, many socially dangerous situations arise [22, 27]. The directions of their elimination include: 1)creation of anti-radioactive technologies, 2)formation of information ecology and culture, 3)development of ICT sphere on innovative bases. Development of technologies for the development of cosmic information industry, 4)Development of modern methods of solving the problem of e-waste, 5)Development of technologies and mechanisms to eliminate information shortages in various fields, 6)Development of cleaning of unnecessary information resources, new text mining, Big Data, Data mining technologies. The main directions of information security in the digital economy occupy one of the main places in recent research [29]. The main directions of this problem can be expressed as shown in Figure 8.

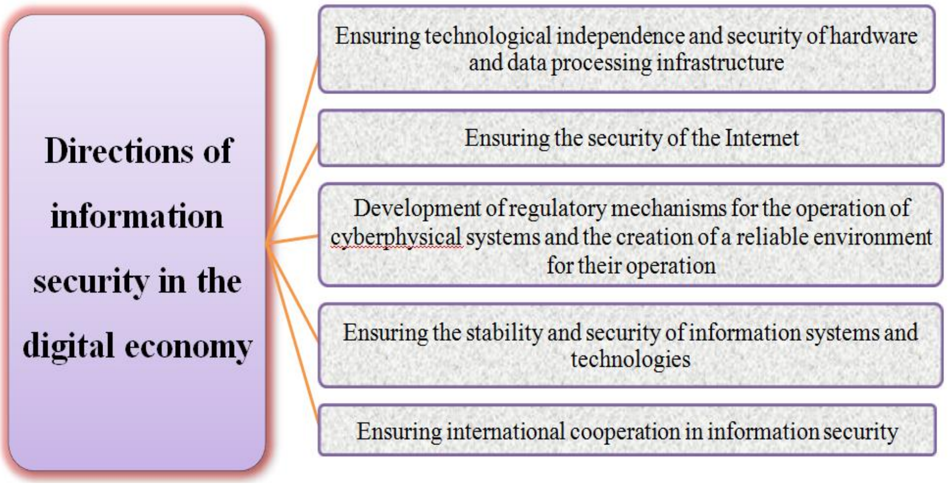

Directions of information security in the digital economy
Ensuring technological independence and security of hardware and data processing infrastructure
Ensuring the security of the Internet
Development of regulatory mechanisms for the operation of cyberphysical systems and the creation of a reliable environment for their operation
Ensuring the stability and security of information systems and technologies
Ensuring international cooperation in information security

Fig. 8. Directions of information security in the digital economy (suggested by the author)

In the digital economy, security and confidence-building practices [30] should help achieve targets and security indicators. They should cover issues related to the security of the information infrastructure and increasing citizens' trust in business, digital technologies, and e-services (Figure 9).

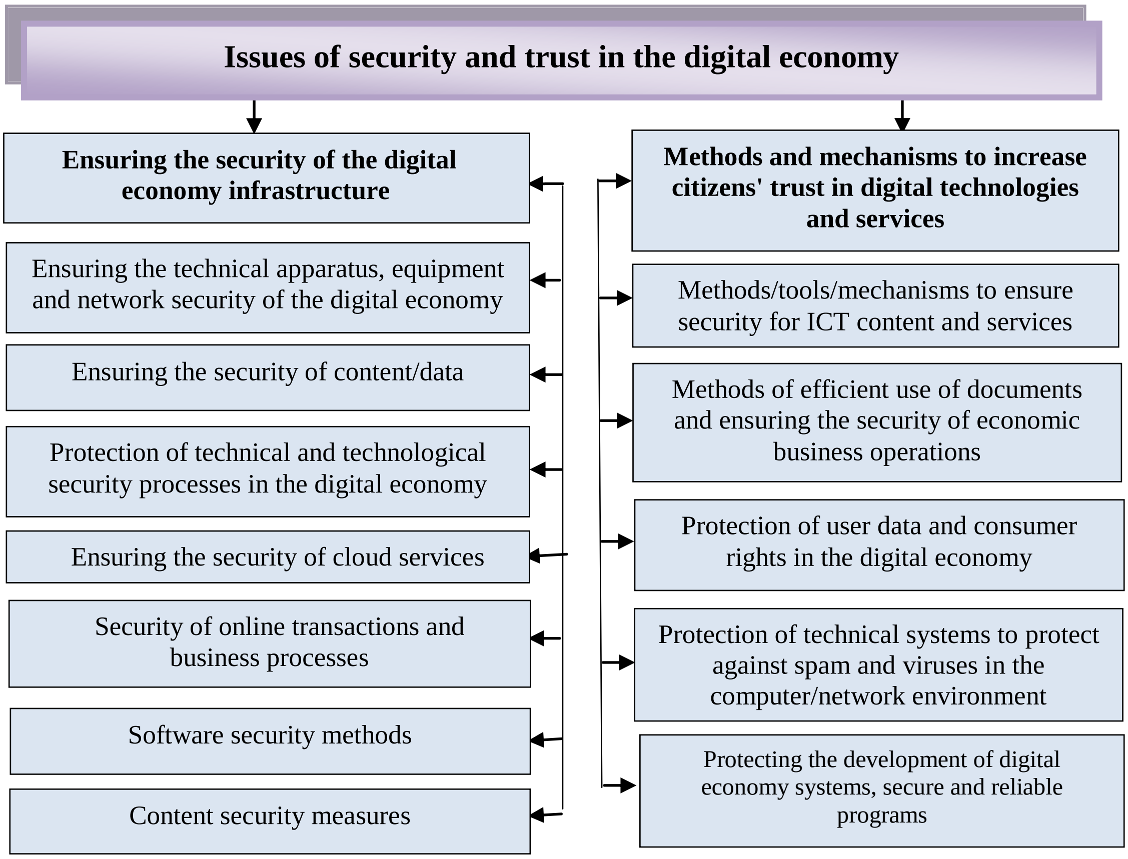

Issues of security and trust in the digital economy
Ensuring the security of the digital economy infrastructure
Ensuring the technical apparatus, equipment and network security of the digital economy
Ensuring the security of content/data
Protection of technical and technological security processes in the digital economy
Ensuring the security of cloud services
Security of online transactions and business processes
Software security methods
Content security measures
Methods and mechanisms to increase citizens' trust in digital technologies and services
Methods/tools/mechanisms to ensure security for ICT content and services
Methods of efficient use of documents and ensuring the security of economic business operations
Protection of user data and consumer rights in the digital economy
Protection of technical systems to protect against spam and viruses in the computer/network environment
Protecting the development of digital economy systems, secure and reliable programs

Fig. 9. Directions of ensuring security and increasing confidence in the digital economy (suggested by the author)

14. Universal base Technologies Commonly Used in the Digital Economy Sectors

In the digital economy, it is advisable to acquire or develop special hardware and software to prevent existing threats in a timely manner. However, since the development of such special technologies is very difficult and requires large financial resources, it is necessary to apply at least standard, basic, universal technologies that can be used in all areas of the digital economy [31].

Relevant digital economic information technologies can be grouped as follows:

- high and very high-performance supercomputer technologies;
- technologies for creating cyber-physical systems, hardware and technical means of complexes;
- technologies for creating cyber-biological human-machine systems;
- quantum technologies for fast data collection, processing, transmission;
- unmanned systems and robotics technologies;
- Industrial Internet and Internet of Things technologies;
- economic-mathematical and imitation modeling, resource and queue management technologies;
- neural network, genetic and other cognitive technologies;
- fog-cloud computing technologies;
- big data collection and processing technologies;
- virtual environment and reality technologies;
- distributed computing and data technologies;
- blockchain and other financial technologies;
- software engineering technologies, etc.

The analysis and research show that technologies such as big data, neurotechnology and artificial intelligence, blockchain technology, quantum technology, new production, logistics, sales, management technology, Industrial Internet, robotics, sensor technology, wireless communication technology, virtual reality technology, soft-computing technology, cryptographic technology, complex large computing technologies, cloud-fog technologies, etc. are among the main advanced technologies used for the dynamic development of the emerging information economy and its digital sectors in general [32]. These complex directions can be expressed by the implementation of the following measures: ensuring the security and technological independence of the operation of the infrastructure and hardware of data processing centers; Ensuring the safe operation of the country segment of the Internet; development of mechanisms of operation of cyber-physical systems in the new economic conditions and ensuring their safe implementation; creation of necessary bases for formation of trust environment for operation of cyber-physical systems; ensuring security and sustainability of information systems and technologies of different levels and purposes; ensuring international relations on information security in the new economic conditions; ensuring security of information resources, systems integrated with international economic information spaces, etc.

These measures require the development of new security concepts for information security systems, interfaces, inter-element interaction protocols, hardware [33, 34].

In addition, a number of information security technologies are very important for this purpose: cyberspace control, cognitive technologies used to prevent computer attacks; automated modeling and forecasting technologies of competitors; intellectual technologies for information security of big data-based processes; architectural-adaptive security technologies; software configuration network and network function virtualization technologies; cryptographic module technologies; industrial and Internet of Things security technologies; secure cloud-fog and mobile technologies.

15. Conclusion

The digital transformation of the economy and society is one of the main priorities facing the country. In order to achieve faster development of the economy in modern times, to ensure its development on the basis of digital technologies, development of high-tech sectors such as artificial intelligence and robotics, information and communication, Big Data, IoT, space, etc. are essential. Improving the infrastructure of the digitalization of the economy and increasing the potential of the country's ICT industry is directly aimed at fulfilling these tasks. Today, the world's leading nations are working to increase efficiency and transparency through the expansion of digital services and the development of e-government. The solution of the problems of infrastructure and institutional formation of the ICT sector, the formation of innovative directions of its development potential can also lead to positive results in solving this problem. In order to achieve the development of the digital economy, increase its share in GDP, conditions must be created for the formation of appropriate infrastructure, effective management, and the comprehensive application of digital technologies. The explained methodology for the integrated assessment of the damage to IS in the digital economy sectors is based on an expert approach to the construction of the membership function of the initial fuzzy sets. In this case, the algebraic summation of the initial fuzzy sets is used to create a generalized fuzzy set of damage to the IS as a result of all kinds of threats.

It should be noted that as the scientific and technical basis of ICT development and its scope expands, the nature and scale of possible threats to IS in the sectors of the digital economy also change. This automatically changes the form and content of the damage that can be inflicted on the IS and the relevant organization. Therefore, there is a constant need to regularly update, rework and create new methods and tools to calculate these losses.

Usefulness of the obtained result and application in practice. Scientific and methodological bases of complex assessment of threats and damage to information systems of the digital economy and their assessment on the basis of fuzzy approaches can be applied in information systems of relevant ICT structures in other regional economies. The results of a comprehensive assessment of the proposed criteria for a comprehensive assessment of threats and damage to information systems in the digital economy with a fuzzy approach can serve as a platform for a comprehensive assessment of threats and damage to economic information systems in general. In this direction, the study of the security aspects of the abundance and excess of information in the context of sustainable development of the digital economy also reveals additional opportunities.

Increasing the level of security and confidence in the digital economy provides a basis for making appropriate management decisions on the activities of ICT, information systems and resource security structures. As a result of the research, the main directions of information security in the digital economy were identified, the directions of ensuring its security and increasing its confidence were identified. The proposed methodological approach to the comprehensive assessment of threats and damage in the digital economy can be applied in other regional-sectoral economies. In this case, more effective results can be achieved by applying the proposed generalized criteria in the assessment of damage. Implementation of complex risk and damage assessment in the digital economy can be characterized as scientific support for management decisions in the increase of economic cyber resilience, economic diversification issues, investment in real economic sectors, and ensuring regional technological sovereignty.

References

[1] Decree of the President of the Republic of Azerbaijan on Improving Governance in the Field of Digital Transformation. Baku, april 27, 2021. https://president.az/articles/51299.

[2] Decree of the President of the Republic of Azerbaijan on some measures to improve governance in the field of digitalization, innovation, high technologies and communications in the Republic of Azerbaijan. Baku, october 11, 2021. https://president.az/articles/53407.

[3] Nevmyvako V.P. Tsifrovaya ekonomika i Industriya 4.0: novyye vyzovy dlya malogo i srednego predprinimatel'stva. *Problemy rynochnoy ekonomiki*. 2021, №1, s.96-109.

[4] Uspayeva M.G., Gachayev A.M. Razvitiye struktury tsifrovoy ekonomiki v usloviyakh globalizatsii mirovoy ekonomiki. *Economics: Yesterday, Today and Tomorrow*, 2021, vol. 11, Is. 3A, pp. 92-101.

[5] Alguliyev R.M., İmamverdiyev Y.N., Mahmudov R.Sh. Information security as a national security component. *Problems of Information Society,* 2020, №1, pp.3-25.

[6] Grigor'yeva V.V., Strukov G.N., Slepokurova YU.I., Slepokurova A.A. Ekonomicheskaya bezopasnost' Rossiyskoy Federatsii: sovremennoye sostoyaniye, uroven' i ugrozy. *Vestnik VGUIT*. 2017, T.79, №3, s.238-252.

[7] Aliyev A.G. Directions and technologies to ensure cyber security in the information economy. *IV Republican conference "Actual multidisciplinary scientific-practical problems of information security"*. Baku, december 14, 2018, pp.150-154.

[8] Aliyev A.G. Methodological aspects of estimation of ICT-based economic development. *International Journal Management Dynamics in the Knowledge Economy*. 2018, vol.6 no.2, pp.227-245

[9] Sidorov A., Senchenko P. Regional digital economy: Assessment of development levels. *Mathematics* 2020, 8(12), pp.21-43.

[10] Sarygulov A.I., Rapgof V.B. Problemy modernizatsii i perekhoda k innovatsionnoy ekonomike. *Problemy sovremennoy ekonomiki,* 2020, №2(74), s.1-4.

[11] Aliyev A.G., Shahverdiyeva R.O. Formation of technological innovation sectors of ICT-based economy and the aspects of their impact on socio-economic processes. *Problems of Information Society,* 2021, №1, рр.94-110.

[12] Tsifrovaya ekonomika: osnovnyye napravleniya razvitiya. *Monografiya/Pod nauchnoy redaktsiyey N.V.Apatovoy. Simferopol'*, 2018.

[13] Vinze Ajay S., Raghu T. Information security in the knowledge economy. Int. J. Human-Computer Studies, 2007, 65, pp.1-2.

[14] Kargina L.A., Lebedeva S.L. Rol' informatsionnoy bezopasnosti v tsifrovoy ekonomike. Avtomatika, svyaz', informatika, 2021, №4, s.28-30.

[15] Boban, Marija. Information security and the right to privacy in digital economy- the case of republic of Croatia. *Conference: 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).*Croatia, may 26-30, 2014, pp.1503-1508.

[16] Varfolomeyev A.A.Osnovy informatsionnoy bezopasnosti. Moskva, 2008.

[17] Koroleva N.SH., Topunova I.R. Informatsionnaya bezopasnost' kak usloviye razvitiya tsifrovoy ekonomiki. *Modern Economy Success,* 2019, №3, s.110-116.

[18] Global Cybersecurity Index, 2020. *International Telecommunication Union. ITUPublications*. 172 p. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

[19] Ahmet Ali Süzen. A risk-assessment of cyber attacks and defense strategies in Industry 4.0 ecosystem. *I.J.Computer Network and Information Security,* 2020, 1, pp.1-12. DOI: 10.5815/ijcnis.2020.01.01

[20] Golovenchik G.G. Problemy kiberbezopasnosti v usloviyakh tsifrovoy transformatsii ekonomiki i obshchestva. *Ekonomika. Upravleniye. Innovatsii,* 2018, №2(4), s.23-33.

[21] Klimov S.M. Metodika otsenki vozmozhnogo ushcherba ot narusheniya bezopasnosti informatsii avtomatizirovannoy sistemy. *Izvestiya YUFU. Tekhnicheskiye Nauki,* 2003, №4, s.27-31.

[22] Aliyev A.G. Issues of complex assessment of damage to the security of information systems. *I Republican Scientific-Practical Conference "Problems of Information Security".* Baku, may 16-17, 2013, pp.71-74.

[23] Yazov YU.K., Grigor'yeva T.V. K voprosu o postroyenii yedinoy kolichestvennoy shkaly otsenok raznorodnykh ushcherbov ot realizatsii ugroz bezopasnosti informatsii v komp'yuternykh sistemakh. *Informatsiya i bezopasnost',* 2008, №1.

[24] Dzhabrailova L.KH. Informatsionnaya bezopasnost' kak prioritetnoye napravleniye razvitiya tsifrovoy ekonomiki. *Monografiya,* 2020, 118 s.

[25] Dubinin Ye.A., Kopytov V.V., Tebuyeva F.B. Obrabotka rezul'tatov ekspertnoy otsenki ushcherba informatsionnoy sisteme dlya vyvoda integral'noy funktsii prinadlezhnosti. *Infokommunikatsionnyye tekhnologii*, 2012, №1, s.89-96.

[26] Rosenko A.P., Avetisov R.S. Metodika otsenki velichiny ushcherba ot vozdeystviya na avtomatizirovannuyu informatsionnuyu sistemu vnutrennikh ugroz. *Izvestiya SGU*. 2006, №8, str.113-118.

[27] Grusho A.A., Grusho N.A., Zabezhaylo M.I., Timonina Ye.Ye. Metody otsenki zashchishchennosti komp'yuternykh sistem informatsionnoy podderzhki tsifrovoy ekonomiki. *International Journal of Open Information Technologies,* 2019, T.7, №4, s.61-66.

[28] Soshina O.N. Osnovnyye problemy obespecheniya urovnya ekonomicheskoy bezopasnosti regiona v tsifrovoy ekonomike. *Ekonomika. Informatika*, 2020, Tom 47, №1, pp.31-39.

[29] Modenov A.K., Vlasov M.P. Osobennosti ekonomicheskoy bezopasnosti v tsifrovoy ekonomike. *Peterburgskiy ekonomicheskiy zhurnal*, 2020, №2, s.121-134.

[30] Olad'ko V.S. Intsidenty setevoy bezopasnosti v sisteme tsifrovoy ekonomiki. Nauchnyy rezul'tat. *Informatsionnyye tekhnologii,* 2019, T.4, №4, s.19-30.

[31] Minzov A.S., Nevskiy A.YU., Baranov O.YU. Informatsionnaya bezopasnost' v tsifrovoy ekonomike. *ZH., ITNOU,* 2018, №3, s.52-59.

[32] Mamayeva L.N. Kharakternyye problemy informatsionnoy bezopasnosti v sovremennoy ekonomike. *Nauchno-prakticheskiy zhurnal Informatsionnaya bezopasnost' regionov*, 2016, №1(22), s.21-24.

[33] Svetlakov A.G., Glotina I.M. Vliyaniye informatsionnogo prostranstva na ekonomicheskuyu bezopasnost' regiona. *Ekonomika regiona,* 2018, T.14, vypusk 2, s.474-484.

[34] Petrenko S.A. Vyzovy i ugrozy bezopasnosti tsifrovoy ekonomiki Rossiyskoy Federatsii. Finansovo-ekonomicheskoye i informatsionnoye obespecheniye innovatsionnogo razvitiya regiona. *Sbornik materialov Vserossiyskoy nauchno-prakticheskoy konferentsii,* 2018, s.74-77.

[35] Mohammadinejad H., Mohammadhoseini F. Privacy protection in smart cities by a personal data management protocol in blockchain. *I. J. Computer Network and Information Security,* 2020, №3, pp.44-52.

[36] Lidong Wanga, Guanghui Wang. Big Data in cyber-physical systems, digital manufacturing and Industry 4.0. *I.J. Engineering and Manufacturing*, 2016, №4, pp.1-8.

[37] Volodymyr Tolubko, Viktor Vyshnivskyi, Vadym Mukhin, et al. Method for determination of cyber threats based on machine learning for real-time information system. *I.J. Intelligent Systems and Applications*, 2018, №8, pp.11-18.

[38] Rida Qayyum, Hina Ejaz. Data security in mobile cloud computing: A state of the art review. *I.J. Modern Education and Computer Science*, 2020, №2, pp.30-35.

[39] Mohamed Nazih Omri, Wafa Mribah. Towards an intelligent machine learning-based business approach. *I.J. Intelligent Systems and Applications,* 2022, №1, pp.1-23.

[40] Petrenko S.A. Kiberustoychivost' tsifrovoy ekonomiki. Kak obespechit' bezopasnost' i nepreryvnost' biznesa. Izdatel'skiy dom" Piter", 2021, s.384.

Authors' Profiles

Alovsat Garaja Aliyev PhD in economic, associate professor Alovsat G.Aliyev (born January 8, 1956). Head of department of the Institute of Information Technology of Azerbaijan National Academy of Sciences. He has a total number of 270 scientific articles and 5 books. It has more than 30 scientific publications indexed in the Web of Sciences (WOS), Scopus and other international databases. Alovsat Aliyev continues to conduct scientificresearch works and deals with issues such as characteristics of ICT application in economical processes and management authorities, information problems in socialeconomical systems, scientific-theoretical basics of formation of information society, information economy, determination of demonstrative systems in ICT field, research of reasons of establishment of digital differences in the society, study economical basics, problems of informatization of humanitarian fields, humanitarian aspects of ICT.

Areas of interest: ICT-based information (digital) and knowledge economy, mobile, cloud, Big Data, artificial intelligence, cryptocurrency and blockchain technologies, sustainable green, inclusive and cybersecurity of economics, Industry 4.0 technologies, innovation management, e-commerce and payment systems, innovation structures, science-industrial technoparks, industrial clusters, science management and commercialization, application of digital twin technologies, smart systems and structures, cyber-sustainable green, inclusive development of the economy, including the oil industry economy, security and cyber sustainability of the non-oil industry potential, increase of the cybersecurity sustainability of information and digital economy.

For more information, please click:
https://science.gov.az/en/institutes/145; https://ict.az/en/content/32/
https://www.facebook.com/alovsat.qaraca.aliyev
https://scholar.google.com/citations?pli=1&authuser=1&user=KMWGTuoAAAAJ

Roza Ordukhan Shahverdiyeva Senior scientist of Institute of Information Technology of Azerbaijan National Academy of Sciences. She has more than 40 scientific articles. Her articles dedicated to actual ICT problems are regularly published in various scientific journals.

Areas of interest: information systems, process of innovation, innovation management, innovation structures, science-industrial technoparks, industrial clusters, Industry 4.0 technologies.

How to cite this paper: Alovsat Garaja Aliyev, Roza Ordukhan Shahverdiyeva, " Scientific and Methodological bases of Complex Assessment of Threats and Damage to Information Systems of the Digital Economy", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.14, No.2, pp. 23-38, 2022. DOI: 10.5815/ijieeb.2022.02.02