ISSN 2518-170X (Online),
ISSN 2224-5278 (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

Х А Б А Р Л А Р Ы

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

ГЕОЛОГИЯ ЖӘНЕ ТЕХНИКАЛЫҚ ҒЫЛЫМДАР СЕРИЯСЫ

♦

СЕРИЯ ГЕОЛОГИИ И ТЕХНИЧЕСКИХ НАУК

♦

SERIES OF GEOLOGY AND TECHNICAL SCIENCES

6 (426)

ҚАРАША – ЖЕЛТОҚСАН 2017 ж.
НОЯБРЬ – ДЕКАБРЬ 2017 г.
NOVEMBER – DECEMBER 2017

ЖУРНАЛ 1940 ЖЫЛДАН ШЫҒА БАСТАҒАН
ЖУРНАЛ ИЗДАЕТСЯ С 1940 г.
THE JOURNAL WAS FOUNDED IN 1940.

ЖЫЛЫНА 6 РЕТ ШЫҒАДЫ
ВЫХОДИТ 6 РАЗ В ГОД
PUBLISHED 6 TIMES A YEAR

АЛМАТЫ, ҚР ҰҒА
АЛМАТЫ, НАН РК
ALMATY, NAS RK

«ҚР ҰҒА Хабарлары. Геология мен техникалық ғылымдар сериясы».
ISSN 2518-170X (Online),
ISSN 2224-5278 (Print)
Меншіктенуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.).
Қазақстан республикасының Мәдениет пен ақпарат министрлігінің Ақпарат және мұрағат комитетінде 30.04.2010 ж. берілген **№10892-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.

Мерзімділігі: жылына 6 рет.
Тиражы: 300 дана.

Редакцияның мекенжайы: 050010, Алматы қ., Шевченко көш., 28, 219 бөл., 220, тел.: 272-13-19, 272-13-18, http://nauka-nanrk.kz /geology-technical.kz

---

Редакцияның мекенжайы: Қазақстан, 050010, Алматы қ., Қабанбай батыра көш., 69а.
Қ. И. Сәтбаев атындағы геология ғылымдар институты, 334 бөлме. Тел.: 291-59-38.

Типографияның мекенжайы: «Аруна» ЖК, Алматы қ., Муратбаева көш., 75.

«Известия НАН РК. Серия геологии и технических наук».
ISSN 2518-170X (Online),
ISSN 2224-5278 (Print)
Собственник: Республиканское общественное объединение «Национальная академия наук Республики Казахстан (г. Алматы)
Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан **№10892-Ж,** выданное 30.04.2010 г.

Периодичность: 6 раз в год
Тираж: 300 экземпляров

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, ком. 219, 220, тел.: 272-13-19, 272-13-18,
http://nauka-nanrk.kz /geology-technical.kz

Адрес редакции: Казахстан, 050010, г. Алматы, ул. Кабанбай батыра, 69а.
Институт геологических наук им. К. И. Сатпаева, комната 334. Тел.: 291-59-38.

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75

News of the National Academy of Sciences of the Republic of Kazakhstan. Series of geology and technology sciences.
ISSN 2518-170X (Online),
ISSN 2224-5278 (Print)
Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)
The certificate of registration of a periodic printed publication in the Committee of information and archives of the Ministry of culture and information of the Republic of Kazakhstan N 10892-Ж, issued 30.04.2010

Periodicity: 6 times a year
Circulation: 300 copies

Editorial address: 28, Shevchenko str., of. 219, 220, Almaty, 050010, tel. 272-13-19, 272-13-18,
http://nauka-nanrk.kz/geology-technical.kz

Editorial address: Institute of Geological Sciences named after K.I. Satpayev
69a, Kabanbai batyr str., of. 334, Almaty, 050010, Kazakhstan, tel.: 291-59-38.

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

N E W S
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
SERIES OF GEOLOGY AND TECHNICAL SCIENCES
ISSN 2224-5278
Volume 6, Number 426 (2017), 264 – 272

UDK 004.056.5

E. Zh. Aytkhozhaeva, N. A. Seilova

Kazakh national research technical university named after K. I. Satpayev, Almaty, Kazakhstan.
E-mail: ait_djam@mail.ru seilova_na@mail.ru

INFORMATION SECURITY OF THE ELECTRONIC SOCIETY AND THE INTERNET OF THINGS

Abstract. Cyberspace of the electronic society of any state is available for public opinion manipulating, for computer espionage and surveillance, for organizing targeted attacks on state systems, businesses, individuals, for monitoring by all interested persons and states which have special monitoring systems. There are given statistics on the goals and types of cyberattacks (for 2017). New information and communication technologies that contribute to the formation and development of electronic society lead to new risks and threats. The most destructive and difficult to identify are threats of using advanced technologies of Internet of things. There are statistical data of computer security testing of Internet of things devices that show their practical insecurity from cyberattacks. There are not only technical, organizational and legal, but also moral, ethical, sociological, psychological and environmental problems of information security ensuring. The problem of information security of the individual, connected with the human factor, requires the integration of specialists from various fields of knowledge. There are shown statistical data on the development of the information security market in the world. Were given examples of interstate interaction in the field of information security, necessary in connection with the global nature of cyberthreats.
Keywords: electronic society, Internet of Things, threats of cyberspace.

Introduction. Nowadays almost all countries are involved in the process of formation and development of electronic society as a part of the global information society. The components of electronic society (ES) are information resources in electronic form, organizational structures, means of information interaction. These components ensure the viability of the ES and prior to the 1980s they determined the indicator of the development and maturity of the ES, but the most important thing was not taken into account - the level of use of these components. The current indicator of the development and maturity of ES is focused on the level of use of these components in various areas of society. In ES there can be distinguished different domains: e-polity, e-finance, e-economy, e-city, etc. But the development of electronic society is mainly determined by the development of four key domains: e-government, e-commerce, e-networking, e-working. Depending on the level of development of these domains, the stage of development of the country's ES is determined: the initial stage is a formative stage, the stage of development is the developmental stage and the mature stage [1].

Kazakhstan is at a formative stage, despite the fact that some of the reached indicators correspond to the developmental stage. In the International rating of 2016 of the e-government development Kazakhstan is on 33rd place from 193 with the EGDI (UN-E-Government Development Index) at 0.725, with a "high" level of development [2].

The development of information and communication technologies leads to the development of ES cyberspace. New technologies such as Virtualization, Cloud Computing, Internet of Things (IoT), Machine-to-Machine (M2M), Cyber-Physical Systems (CPS), etc. contribute to the development of ES, providing comfort and efficiency of its use.

In article [3] there is presented the dynamics of changes of the basic bibliometric indicators (the number of articles and citations) on the promising directions of information and communication technologies is presented. Were used the data of the scientific publications databases EBSCO and

ScienceDirect. The dynamism of publications reflects the accelerated dynamism of the development of new information and communication technologies. But these new technologies bring not only new opportunities with them, but also new problems of ensuring information security.

Problems of security ensuring of ES cyberspace. ES cyberspace is actively used for criminal purposes to violate the privacy of citizens, for public opinion manipulating, for computer espionage and surveillance, for organizing targeted attacks on state systems, businesses, individuals.

Attackers moved the focus of their attacks from ordinary users to corporations (since 2016). Figure 1 presents statistics of the cyberattacks targets in 2017 (April) [4].

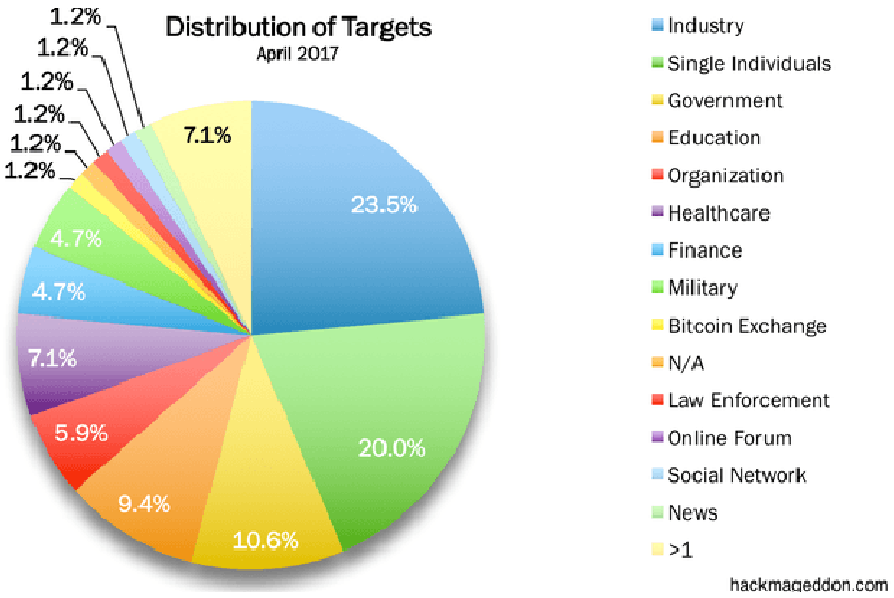

Figure 1 – Distribution of cyberattacks targets

Statistics show that the dominant targets of cyberattacks were industrial systems (23.5%), then ordinary users (20.0%) and state systems (10.6%).

According to the reports of Group-IB (one of the leading international companies for the prevention and investigation of cybercrime) the amount of thefts caused by targeted attacks on banks increased three times in 2016 in comparison with the previous year [5]. Increased the risk of attacks on a critical infrastructure in the industrial sector. Were activated DDoS attacks, including the use of IoT-devices. Very popular are cyber espionage and interception of traffic at the level of mobile operators and Internet providers.

Figure 2, which shows the ratio of different types of attacks in 2017 (April), clearly demonstrates the diversity and frequency of various types of attacks use [4].

The first detailed instructions how to infiltrate in computer systems and manage them appeared 30 years ago. These were the first issues of the Phrack magazines in the US and The Hackers Handbook in the UK. Nowadays the information resources of the ES include a variety of instructions for attacks organization, all possible means of attacks implementation.

Cybercriminals for communication use closed networks and forums. There are hacking magazines, teleconferences and hacking websites where hacker conferences are held. The annual conference of hackers (Def Con) in Las Vegas in 2016 gathered more than 12 thousand participants, experts of the highest class. There was performed a demonstration of hacking and remote opening of smart locks via a Bluetooth connection. Before that, hackers specializing in hacking of computer databases organized their Black Hat conference. We can talk about an actively developing cybercrime industry, which continuously improves threats, increases the rate of their spread and is actively looking for ways to expand the working space.

More than 200 thousand users in 150 countries of the world suffered from the virus WannaCry on May 12, 2017. Among them were state institutions, hospitals, energy and transport infrastructure facilities around the world. On May 25, 2017 appeared information about a new class of vulnerabilities in programs for video viewing. Experts estimate the number of potential victims in more than 200 million.

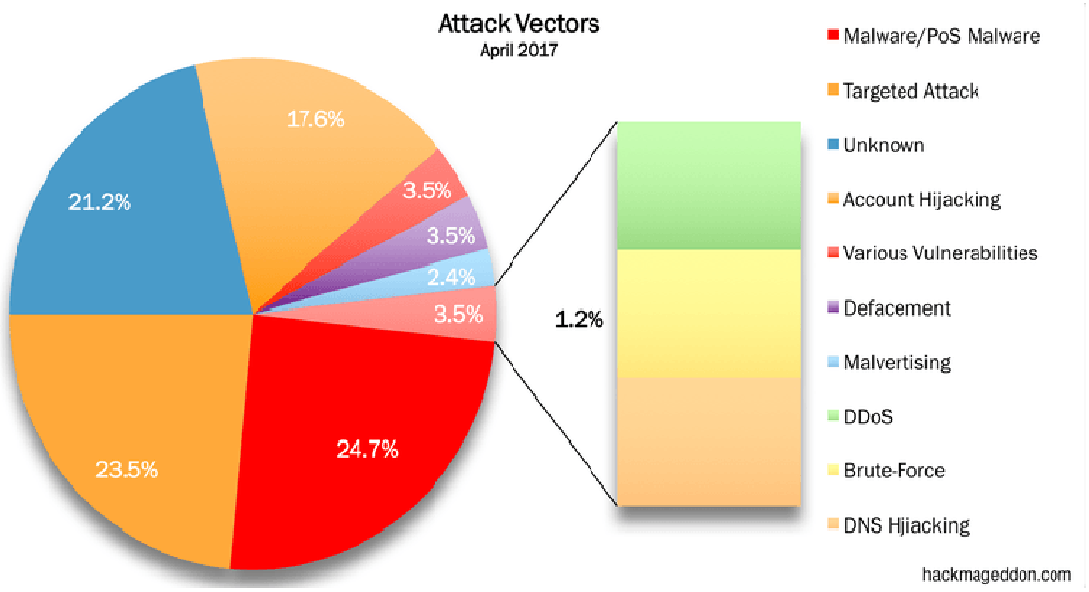

Figure 2 – Cyberattack types usage

In March 2017 Wikileaks web-site started the publication of confidential US CIA documents obtained from a highly-protected network in the CIA Cyber Intelligence Center [6]. Highly qualified specialists of this center have developed many computer programs for computer espionage and surveillance. Among them are password collectors, modules for capturing images and sound from web cameras, exploits for various types of operating systems and mobile devices, various malicious programs for stealing information, tools for intercepting messages (before encryption) and much more. Among the confidential CIA documents there are instructions on the camouflage and concealment of traces of cybercrime. Thanks to the leak and to the publication of the CIA's hacking information, anyone can take advantage of opportunities that were formerly available only to American specialists. Including for criminal activity, which poses a threat to the security of citizens, enterprises and state in the electronic society.

The hacker group "Shadow intermediaries" published on April 14, 2017 documents about the infiltration of the US National Security Agency (NSA) into the society of the interbank SWIFT system. This group, which appeared in 2016, put for sale programs of the NSA that were in their hands. Some of these programs were distributed free of charge by the hackers in the Internet.

The concept and threats of Internet of Things. According to the review prepared for the International Economic Forum in 2016 in Davos, the top 5 technological drivers of the fourth industrial revolution are the Internet of Things [7]. IoT (concept of 1999) is one of the most promising and demanded technologies.

In the direction of IoT such world famous companies as Intel, Samsung Electronics, Dell, Broadcom are actively working. All things in our life will be interconnected by a network like the Internet. Microsoft Corporation has developed a free version of its operating system for the IoT distribution support program, is developing a whole set of Azure tools for IoT. Today IoT sensors are used everywhere, from fitness trackers to sophisticated electronics in industry and agriculture. According to the forecasts of analysts of International Data Corporation (IDC - an international research and consulting company engaged in the study of the world market of information technologies and telecommunications) by 2020 the volume of the IoT market will be 3 trillion dollars and 30 billion autonomous devices will be connected to the Internet of things. Many IoT-devices become symbols of prestige, fashion.

IoT-devices are digital intelligent devices with built-in means of interaction through network technologies. One of the foundations of the IoT concept is M2M, which allows IoT devices to communicate with each other.

You can distinguish between different segments of the IoT-devices application: smart city, smart transportation, smart business, smart manufacturing, smart airport, smart home, etc.

IoT-devices are an integral part of smart home. The smart home systems allow providing comfortable living conditions, while reducing the consumption of consumed resources (electricity, gas, water). These intelligent systems allow you to control various devices, monitor the operation of such subsystems as heating, lighting, security, ventilation, air conditioning, etc. Management is performed remotely using network technologies. In this case, control devices are IoT-devices, with a built-in chip, which allows you to control the device also from a mobile phone, using special software. This is an intelligent environment and pervasive computer systems.

Threats carried out by IoT-devices can not be noticed by users for a long time and lead to dangerous situations. Recent computer tests of computer security of the smart home systems by different companies showed their practical insecurity from cyberattacks. In 2015 Hewlett Packard Enterprise (HP) published a report about the found 25 vulnerabilities tested by 10 home devices of the IoT class: Smart TV, webcams, smart thermostats, intelligent electrical outlets, locks, home alarms, garage opening devices, control hubs, smart scales, etc. Figure 3 shows the results of the researches [8].

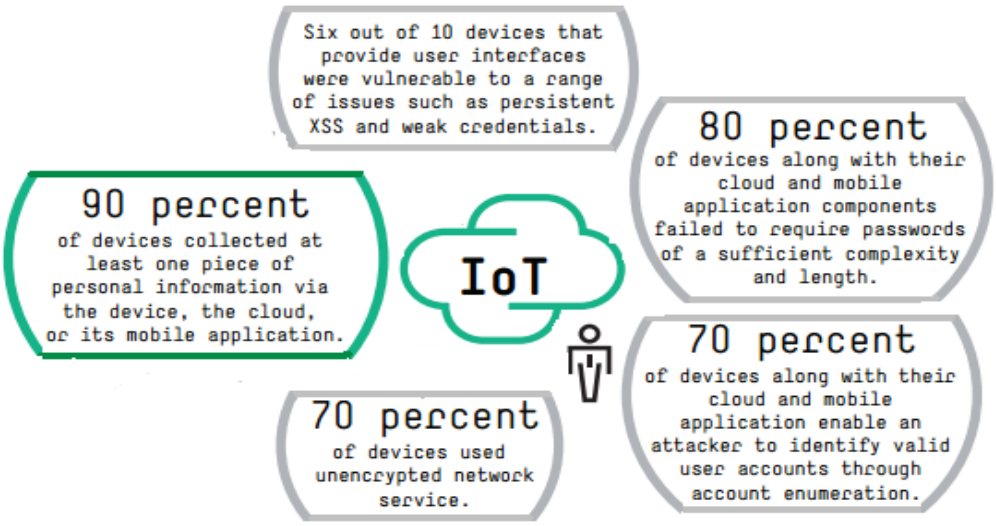

Figure 3 – IoT-devices vulnerabilities

It turned out that 70% of devices use unencrypted network services, 70% of mobile and cloud applications of IoT-devices are available to attackers for receiving accounts, 90% of devices allow receiving partial personal data of users, 80% of devices use passwords of insufficient complexity and length and etc. The HP Fortify methodology was used to test the Internet of things on demand, combining manual and automatic checks. Then there was the HP report on the study of the security parameters of the 10 most popular security systems of the smart home. The company's specialists easily cracked all ten systems, using a number of vulnerabilities (weak password policy, no account lockout, easily selectable user names, incorrectly configured data transfer encryption, incorrect SSL/TLS encryption protocol implementation). 70% of the systems allowed unlimited transfer of account data through an unprotected cloud interface. Only in one system there was used two-factor authentication. The found vulnerabilities allowed to collect information about the home remotely, including information from video cameras.

Synack Company tested 16 smart devices, which (except one - a smoke detector) were cracked in less than 20 minutes.

Symantec Company has tested the security of fifty IoT devices for smart homes [9]. All of them were vulnerable. None of them used mutual authentication, complex passwords, it was not protected from bruteforce (password selection by search). Moreover, one-fifth of all devices did not encrypt data transmitting them to the cloud.

At one of the world's largest mobile industry exhibitions Mobile World Congress 2017 in Barcelona there were demonstrated the results of experiments by Avast specialists, which showed that almost 5.3 million IoT devices in Spain connected to the Internet can be hacked [10].

The presence of vulnerabilities of IoT-devices is the mistake of both companies-developers, and those companies that are engaged in the introduction of "smart technologies". Due to technical difficulties, many companies-developers simply can not release devices with built-in protection functions, so cybercriminals are increasingly using IoT-devices. In addition, many users do not think about their security using IoT-devices.

Nowadays Industrial Internet of Things (IIoT) is actively developing. This is a multi-level system of production facilities with sensors, controllers and software for collecting and exchanging data, united by computer networks for remote monitoring and control in automated mode. IIoT opens new opportunities for increasing the efficiency of production processes at a qualitatively new level. This is an automated digital production - Smart Manufacturing. The problems of IIoT security have their own peculiarities.

Trend Micro Company's report indicates that from 83 000 industrial robots currently available from the Internet around the world 5 000 do not have authentication mechanisms. In the robots there were found 65 vulnerabilities, which allow to bypass authentication mechanisms, to modify key settings and to change the operation mode of the device [11]. During the hacking of industrial routers, an access to those devices that are not connected to the Internet is also available.

Using IIoT it is necessary to solve the problems of ensuring security in a comprehensive manner. In the development and implementation of complex IIoT infrastructure protection the participation of various specialists in thesphere of production, development and deployment of IIoT devices and infrastructure is required: IIoT manufacturers and integrators, IIoT solution developers, IIoT solution deployment specialists, IIoT solution operators.

The threats brought by IoT devices are noticed by many specialists working in the field of information security (IS). IoT technology appears in the Disruptive Civil Technologies (2008) report of the US National Intelligence Council, as one of six potentially destructive technologies of the future [12]. There is also a forecast that by 2025 all the objects surrounding modern man can be equipped with IoT nodes.

Analysts predict that one of the main trends of 2017 in cybersecurity will be increasing attacks on the IoT sector. Gartner Company in its review of key areas of information security for 2017 as one of the five main areas identifies the safety of IoT. By 2020, Gartner predicts, more than 25% of known attacks on enterprises will be conducted through IoT devices, but the IoT security budget will be only 10% of the total IS budget. There is also a forecast that until 2018 more than 50% of IoT device manufacturers will not be able to eliminate threats due to weak authentication methods [13].

The malicious and abusive use of IoT to carry out attacks, taking into account their wide distribution, can lead to global catastrophes. The director of the US National Security Agency said that a number of countries have sufficient capabilities for the implementation of cyber attacks that could cause the US electricity network components disconnection (using M2M).

Nowadays there are created special worms and viruses which are introduced into IoT devices. These malicious programs allow to attack millions devices connected to the network. Using M2M they can propagate from device to device. The destructiveness of the potential lies in a wide range of targets for attacks: from smart watch to medical equipment, including pacemakers, cardio defibrillators, insulin pumps. In general, any devices connected to the Internet are vulnerable: televisions, kitchen appliances, cameras, computer systems of cars, various devices, production facilities, etc. For example, there are developed special programs for installation in vehicle control systems. They can be used to organize planned accidents and for killing people. The US CIA together with british secret service MI5/BTSS has developed an exploit for Samsung TVs (with microphones) called Weeping Angel. The program records conversations in the room and sends them through the Internet to a specific server, even when the TV looks turned off. In 2016 the botnet Mirai consisting of IoT-devices participated in the organization of DDoS-attacks, which by their power broke all records and led to the denial of service to the whole region. In open access to the ES there are the source codes of this botnet. They can be used by anyone for their criminal purposes.

Measures to ensure the safety of the use of IoT-devices are implemented only on the state level. The European Commission plans to introduce mandatory certification of all devices related to IoT-devices. Not only the devices are needed to be controlled, but also the networks to which they are connected, as well as the used cloud storages. The basis of cloud storages is the technology of virtualization, which is characterized by new little-studied and little-researched risks and threats to information security [14].

Ensuring with information security of ES. Existence in an electronic society, high risk of cyberattacks forces to give priority to information security issues. Using information and communication technologies the legal, organizational and technical problems of information security ensuring of society and the state come to the fore.

First of all, it connects with the creation of a legal basis for ES. In different countries, this process is at different levels of development. In legislation of all countries, including in the legislation of developed countries, a large class of relations related to the turnover of information (and its use) still falls out from the scope of legal regulation. No country can approve the completion of the creation of a legal basis for ES, because the process of the electronic society development is a natural process of human development.

The appearance of new cyberthreats, their diversity leads to the need to improve technical facilities, to the development of new methods and means of information protection, to new services of information security ensuring.

To moral, ethical, sociological, psychological and environmental problems of information security ensuring in ES there are paid much less attention. But these problems are more complex, because they are related to the human factor. In modern cyberspace the problem of information security of a person is especially urgent. Widely used for illegal purposes social engineering, based on a set of approaches of the applied social sciences. According to statistics of 2016 27% of all cyber attacks used social engineering methods [15]. Social engineering is used in the implementation of mass attacks and at the initial stage of the targeted attack. This is a method for human actions control without the use of technical means, in order to perform the actions required by the attacker.

It is possible to differentiate information-technical and information-ideological security of a person. Accessibility and activity of information resources of electronic society plays not only a positive role in the development of society. Factors such as direct access to the audience, the breadth of distribution, the lack of verification of the reliability of information, the anonymity of activities in cyberspace are used to devaluate and to replace common human values leading to the degradation of the individual and society as a whole. Leading experts of relevant fields of knowledge should participate in solving these problems.

Electronic society with its risks and threats and the physical world are integrated into a single whole. Solutions to ensure information security are become vital. The information security market is constantly growing. According to IDC global revenue from IS-solutions will grow from $ 73.7 billion (2016) to $ 101.6 billion (2020). The analysis was conducted on 8 regions, 53 countries and 20 industries. The cumulative annual growth rate (CAGR) in this segment of the market will be 8.3%, which exceeds twice the similar equivalent for the total amount of budgets for information and communication technologies in the next five years [16].

Especially high growth rate of the IS market is observed in the countries where ES development started later and goes according to an accelerated schedule. For example, according to IDC forecasts from 2017 the Russian market for information security services will grow by an average of 27.4% over the next five years. The research of cyberthreats is an important component of information security. The service market for cyberthreats research is steadily growing. In 2016 the volume of the Russian service market for the cyberthreats research amounted 14.17 million US dollars, which is 23.1% more than in 2015 (report of IDC Russia Threat Intelligence Security Services 2016 Market Analysis and 2017-2021 Forecast) [17].

There are no state borders in ES. On issues of timely response to information security incidents aimed at the information infrastructure of states, more than 90 countries of the world interact through the CERT system of coordinates. In Kazakhstan since 2011 there is a service for responding to computer incidents - KZ-CERT. In 2012 KZ-CERT joined the international organization FIRST (Forum of Incident Response and Security Teams), which unites the services of CERT around the world. KZ-CERT joined to the Trusted Introducer for Security and Incident Response Teams (TI), and is a member of the APWG antiphishing working group, a member of the CSIRT Assistance Program for security and incident response. In 2016 KZ-CERT joined the alliance of the Services for Responding to Computer Incidents of the Countries Participating in the Organization of Islamic Cooperation "(OIC-CERT).

The issue of harmonizing and adopting standards, laws and other documents in the field of protection against cybercrime, common to the entire international community is topical.

The family of International Standards for Information Security Management Systems 2700X (used a sequential numbering scheme starting from 27 000) includes the International Standards defining

requirements for information security control systems, risk management, metrics and measurements, as well as an implementation guide. The standards are developed by the ISO/IEC Joint Technical Committee 1 (Subcommittee 27) which is a division of the International Organization for Standardization (ISO) and of the International Electrotechnical Commission (IEC) - ISO/IEC JTC 1/SC 27. ISO/IEC JTC 1/SC 27 was created In 1989. The sphere of its activity is the development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines for both security and privacy aspects [18]. Nowadays 55 countries are full members of ISO/IEC JTC 1/SC 27 (including Kazakhstan), 22 countries have observer status. 27 Subcommittee developed and published 164 standards, there are 72 standards for information security in the development. Accepted national standards in the field of information security are harmonized with international standards.

The governments of the states where ES is actively developing accept the agreements on cooperation in the field of international information security ensuring. There is an agreement between the governments – members of the Shanghai Cooperation Organization (on June 2, 2011 it came into force) [19]. The agreement covers the whole spectrum of problems of international information security - from cybercrime and cyberterrorism counteraction to disarmament issues.

In 2013 between the countries-members of OSCE there were accepted Confidence Building Measures in the field of cybersecurity. The countries of the European Union adopted in 2016 common documents in the field of cybersecurity of data protection: Network and Information Security (NIS) Directive) and the General Data Protection Regulation (GDPR) of the European Union. The directive is mandatory for all EU members, it represents the first EU legislation on cybersecurity. It aims to improve the overall security of networks and information systems within the EU on the basis of: improving cybersecurity at the national level; strengthening cooperation in the EU; risk management and reporting obligations in case of incidents for providers and digital service operators. The regulation is aimed at strengthening measures to protect personal data. It is mandatory for all EU countries, as well as companies offering goods and services for the EU, monitoring the citizens of the EU.

Conclusion. Potential catastrophic consequences of crimes in ES cyberspace can be compared with the consequences of the nuclear weapon. Ubiquitous transformation into Internet nodes of common things can damage national information security, it has a potential danger to the lives of people and to organizations.

The development and acceptance of state cyber security doctrines is topical. In Kazakhstan, although with a delay, the work is also under development and adoption Cybersecurity Concept (Cyber shield of Kazakhstan) [20]. The level of information security in Kazakhstan today does not meet the needs of society and the state. The creation of a cybershield is a complex, resource-consuming, multifaceted, but vitally necessary state matter. Only the joint efforts of the state, business and ordinary users the collapse can be avoided.

Due to the absence of ES boundaries to ensure information security, it is necessary to unite all its members and all states to cybercrime counteract. The accelerated dynamism of the ES development and of the new information and communication technologies, the global nature of cyberthreats require the same dynamic and global interstate interaction. For consideration to the UN General Assembly Russia is preparing to make a resolution on information security. There should be both national and international monitoring of the state of the problem of information security. The issue is very complex, because the military, economic, social and diplomatic interests of various states are closely intertwined in cyberspace.

The famous American sociologist, publicist-futurist E.Toffler in his book "The Third Wave" almost 40 years ago warned that in the society of the third wave of civilization there is a potential danger of control not of technology by people but of people by technologies [21]. These warnings of the former honored associate professor of the University of National Defense in Washington are relevant and deserve attention not only to IS specialists, but to the entire international community.

REFERENCES

[1] Becky P Y Loo (2011) The E-Society. Hauppauge: Nova Science Publishers, ISBN: 978-1-61209-831-9, 266 p.

[2] United Nations E-Government Survey 2016. E-Government in Support of Sustainable Development (2016) New York: United Nations, 242 p.

[3] Abdilmanova A, Aliguliyev R, Muhamedyev R. (2016) Differentsialnye metriki otsenki bibliometricheskikh pokazatelei domenov IKT [Cloud of Science] T. 3. No. 3. 366-379 (in Russian).

[4] Hackmageddon. Information Security Timelines and Statistics [http://www. hackmageddon.com]

[5] Hi-Tech crime trends 2016. Group-IB annual report of cybercrime trends. [http://www.group-ib.com/2016-report.html].

[6] Vault 7: CIA Hacking Tools Revealed [www.wikileaks.org/ciav7p1/cms/ index.html]

[7] The Future of Jobs. Employment, Skills and Workforce strategy for The Fourth Industrial Revolution. January 2016 [http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf]

[8] Internet of things research study: 2015 report. Hewlett Packard Enterprise. [http://h20195.www2.hpe.com/V4/GetDocument.aspx?docname=4AA5-4759ENW]

[9] Barcena MB, Wueest C (2015) Insecurity in the Internet of Things [http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/insecurity-in-the-internet-of-things.pdf]

[10] Mobile World Congress 2017 (2017) Barselona 27 feb - 2 mar [https://www. mobileworldcongress.com]

[11] Quarta D, Pogliani M, Polino M, Zanchettin FM and Zanero S (2017) Rogue Robots: Testing the Limits of an Industrial Robot's Security [Trend Micro Forward-Looking Threat Research] [https://documents.trendmicro. com/assets/wp/wp-industrial-robot-security.pdf]

[12] Disruptive Civil Technologies. Six Technologies With Potential Impacts on US Interests Out to 2025 (2008) [Conference Report CR 2008-07] April 2008. 47 p. [www.fas.org/irp/nic/disruptive.pdf]

[13] Greene T. (2016) Gartner's top 10 security predictions [Network World] [http://www.networkworld.com/article/3088084/security/gartner-s-top-10-security-predictions. html]

[14] Aytkhozhaeva EZh, Ziro AA, Zhaibergenova ZhA (2017) Virtualization safety [Computer Modelling and New Technologies] T. 21. No. 2. 48-53.

[15] Zinenko O (2017) Analiz ugroz informatsionnoy bezopasnosti 2016-2017. [Analiticheskiy tsentr Anti-Malware.ru] [https://www.anti-malware.ru /analytics/Threats_Analysis/Analysis_ information_security_threats_2016_2017] (In Russian).

[16] Worldwide Semiannual Security Spending Guide. [www.idc.com/getdoc.jsp?containerId=IDC_P33461]

[17] Russia Threat Intelligence Security Services 2016 Market Analysis and 2017–2021 Forecast. IDC. [http://www.idc.com/getdoc.jsp?containerId=CEMA42095117]

[18] ISO/IEC JTC 1/SC 27. IT Security techniques. ISO [https://www.iso.org/committee/ 45306.html].

[19] Soglashenie stran SHOS o sotrudnichestve v oblasti informatsionnoy bezopasnosti vstupilo v silu (2011) [InfoSHOS: internet-portal] [http:// www.infoshos.ru/ru/?idn=8381] (In Russian).

[20] Kontsepciya kiberbezopasnosti («Kibershchit Kazakhstana») (2017) [http://mdai.gov.kz/ ru/pages/koncepciya-kiberbezopasnosti-kibershchit-kazahstana] (in Russian)

[21] Toffler A (1980) The Third Wave. New York: William Morrow & Company, ISBN 0688035973, 9780688035976, 544 p.

Е. Ж. Айтхожаева, Н. А. Сейлова

Қ.И. Сәтпаев атындағы Қазақ ұлттық техникалық зерттеу университеті, Алматы, Қазақстан

ЭЛЕКТРОНДЫҚ ҚОҒАМНЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІ ЖӘНЕ ИНТЕРНЕТ ЗАТТАРДЫҢ

Аннотация. Кез келген мемлекеттің электронды қоғамның киберкеңістігі арнайы мониторингті жүйесі бар барлық тұлғалар мен мемлекеттердің мониторингіне қолжетімді. Ол қоғамдық ойды манипуляциялау үшін, компьютерлік тыңшылық және аңду үшін, мемлекеттік жүйелерге, бизнес, жеке тұрғындарға мақсатты шабуылдарды ұйымдастыру үшін құқыққа қарсы мақсаттарда белсенді қолданылады. Кибер шабуылдар мақсаттары мен түрлері бойынша сараптама келтіріледі (2017 жыл бойынша). Электронды қоғамның қалыптасуына және дамуына үлес қосатын жаңа ақпараттық-коммуникациялық технологиялар жаңа тәукелдер мен қауіптерге акеледі. Ең жойқын және қиын анықталатын қауіптер Интернет заттардың келешек технологияларын пайдалануы болып табылады. Интернет заттар құрылғыларының компьютерлік қауіпсіздіктің тестілеуінің статикалық деректері келтіріледі, алайда олар кибер шабуылдардан олардың тәжірибиелік осалдығын көрсетеді. Ақпараттық қауіпсіздікті қамтамасыз ету техникалық, ұйымдастырушылық және құқықтық проблемаларының шешімінғана талап етпейді, сонымен қатар моральді-этикалық, социологиялық, психологиядық және экологиялық. Адами фактормен байланысты тұлғаның ақпараттық қауіпсіздік проблемасы, білімнің түрлі салаларында мамандар интеграциясын талап етеді. Ақпараттық қаупсіздік нарығының дамуы бойынша статикалық деректер дүние жүзі бойынша келтіріледі. Кибер қатерлердің жаһандық сипаттылығына байланысты талап етілетін ақпараттық қауіпсіздік саласындағы мемлекетаралық ынтымақтастықтың мысалдары келтірілген.

Түйін сөздер: электронды қоғам, интернет заттардың, киберкеңістіктің қауіптері.

Е. Ж. Айтхожаева, Н. А. Сейлова

Казахский национальный исследовательский технический университет им. К. И. Сатпаева,
Алматы, Казахстан

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО ОБЩЕСТВА И ИНТЕРНЕТ ВЕЩЕЙ

Аннотация. Киберпространство электронного общества любого государства доступно для манипулирования общественным мнением, для компьютерного шпионажа и слежки, для организации целевых атак на государственные системы, бизнес, отдельных граждан, для мониторинга всеми заинтересованными лицами и государствами, имеющими специальные мониторинговые системы. Приводится статистика по целям и типам кибератак (по 2017 году). Новые информационно-коммуникационные технологии, способствующие формированию и развитию электронного общества, несут новые риски и угрозы. Самыми разрушительными и трудно выявляемыми являются угрозы использования перспективной технологии интернет вещей. Приводятся статистические данные тестирования компьютерной безопасности устройств интернет вещей, которые показывают их практическую незащищенность от кибератак. Существуют не только технические, организационные и правовые, но и морально-этические, социологические, психологические и экологические проблемы обеспечения информационной безопасности. Проблема информационной безопасности личности, связанная с человеческим фактором, требует интеграции специалистов различных областей знаний. Приводятся статистические данные по развитию рынка информационной безопасности в мире. Приводятся примеры межгосударственного взаимодействия в сфере информационной безопасности, необходимого в связи с глобальным характером киберугроз.

Ключевые слова: электронное общество, интернет вещей, угрозы киберпространства.

Сведения об авторах:

Айтхожаева Евгения Жамалхановна – кандидат технических наук, ассоциированный профессор кафедры Информационной безопасности Казахского национального исследовательского технического университета имени К.И.Сатпаева, Казахстан, e-mail: ait_djam@mail.ru,

Сейлова Нургуль Абадуллаевна – кандидат технических наук, ассистент-профессор кафедры Информационной безопасности Казахского национального исследовательского технического университета имени К.И. Сатпаева, Казахстан, e-mail: seilova_na@mail.ru

Publication Ethics and Publication Malpractice
in the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www:nauka-nanrk.kz

ISSN 2518-170X (Online), ISSN 2224-5278 (Print)

http://geolog-technical.kz/index.php/kz/

Верстка *Д. Н. Калкабековой*

Подписано в печать 08.12.2017.
Формат 70x881/8. Бумага офсетная. Печать – ризограф.
19,0 п.л. Тираж 300. Заказ 6.

Национальная академия наук РК
050010, Алматы, ул. Шевченко 28, т. 272-13-19, 272-13-18