IRSTI 10.77.21

Atakhanova G.M.[1], Aratuly K.[2], Abitaeva A.K.[3]

[1]Associate professor, e-mail: atakan73@mail.ru
[2]PhD, associate professor, e-mail: kunya8585@mail.ru
[3]Aspirant to PhD, e-mail: ayagoz.92@mail.ru
al-Farabi Kazakh National university, Kazakhstan, Almaty

CRIMINAL POLICY OF KAZAKHSTAN IN THE FIELD OF INFORMATION SECURITY

At present, information security in the Republic of Kazakhstan is at a rather low level, and in connection with this, the issues of this security are very acute. As you know, the development of the state and society as political and legal phenomena is always carried out in clearly defined historical and territorial factors that determine this development. At the same time, threats to the state, society and man are also in constant change, adequate for the development of society and the state. Modern world trends today signal the emergence of new formats of threats to the national security of Kazakhstan in the 21st century and among them the issue of information security is the most acute. The aim of scientific research it is been realization of analysis, orderly arguing the present, past and future state of informative safety of Republic of Kazakhstan in a context with international legal relationships in this sphere. The President of Kazakhstan in his annual message to the people of Kazakhstan on January 31, 2017 designates we must cultivate new industries that are created using digital technologies. This is an important complex task ... It is necessary to adapt our legislation to new realities ... Therefore, the government should keep the issue of IT sphere under special control. And the emphasis on informatization and information technologies is made by the President not one time, which speaks about the importance and information support, as well as information security of all important branches of state activity and high-level state tasks. That in turn explains so high importance and meaningfulness of science research and practical works in this direction. Scientific value the article have direct, because in modern society information and informative safety play if not above all, then one of leading roles and meaningful place, that prove the last events what be going on in the world and virtual the internet space for the last years.

Practical meaningfulness of work is explained by a necessity by such works by society and practical and legal systems of the state.

Key words: Criminal policy, President's message, information, information security, information systems, international security, information technologies, computer crimes.

Атаханова Г.М.[1], Аратулы К.[2], Әбітаева А.Қ.[3]

[1]з.ғ.к., профессор м.а., e-mail: atakan73@mail.ru
[2]PhD докторы, доцент м.а., e-mail: kunya8585@mail.ru
[3]докторант, e-mail: ayagoz.92@mail.ru
әл-Фараби атындағы Қазақ ұлттық университеті, Қазақстан, Алматы қ.

Ақпараттық қауіпсіздік саласындағы Қазақстанның қылмыстық саясаты

Қазіргі таңда ақпараттық сауаттылық пен қауіпсіздік Қазақстанда шынайы түрде төменгі дәрежеде, сол себепті осы саладағы мәселелер аса өзекті болып отыр. Саяси-құқықтық құбылыс ретіндегі мемлекет пен қоғамның дамуы әрқашан белгілі бір тарихи және аумақтық факторларда жүзеге асырылады. Сонымен қатар сол мемлекет, қоғам және адам үшін қауіп төндіретін құбылыстар үнемі өзгеріске ұшырап отырады. Қазіргі заманауи тенденциялар бүгінгі таңда XXI ғасырдағы Қазақстанға, оның ұлттық қауіпсіздігіне жаңа нысандағы қорқыныш туралы еске салады, соның ішінде маңыздылардың бірі болып ақпараттық қауіпсіздіктің мәселелері табылады.

Ғылыми зерттеудің мақсаты аталған саладағы Қазақстан Республикасының ақпараттық қауіпсіздігін халықаралық құқықтық қатынастармен біріктіре отырып, өткені мен болашағын әдістемелік тәсілдермен талдау жүргізу болып табылады.

ҚР Президенті өзінің жыл сайынғы Қазақстан халқына жолдауында сандық технологияны қолдану арқылы құрылатын жаңа өнеркәсіптерді өркендету туралы, оның маңызды кешенді міндет екендігін, сонымен қатар осыған орай заңнаманы жаңа жағдайларға бейімдеу керек екендігін атап өткен болатын. Және де ҚР Үкіметі IT саласын дамыту мәселесіне ерекше көңіл бөлуі және бақылауда ұстауы тиіс екендігіне тоқталып кеткен болатын. Сонымен қатар Елбасы ақпараттандыру мен ақпараттық технологияларға аса үлкен көңіл бөліп, мемлекеттің басты мақсаттарының бірі ретінде ақпараттық қауіпсіздік екенін және ақпараттық қамтамасыз етудің маңыздылығы жөнінде екенін бірнеше рет атап өтеді. Осының барлығы, өз кезегінде, қарастырылып отырған бағыттағы ғылыми-зерттеу және тәжірибелік жұмыстың аса маңыздылығы мен қажеттілігін түсіндіреді.

Мақаланың ғылыми құндылығы тікелей және айқын, себебі қазіргі қоғамда ақпарат пен ақпараттық қауіпсіздік ең маңызды болмаса да, маңыздылардың бірі болып саналады, оның дәлелі ретінде әлемде әрі виртуалды ғаламторда соңғы онжылдықтардың ішінде болып жатқан көптеген оқиғалар мен ғылыми жетістіктер сипаттап келеді.

Жұмыстың тәжірибелік маңыздылығы қоғам мен мемлекеттің тәжірибелік құқықтық жүйесінің осындай зерттеу жұмыстарына сұранысы мен қажеттілігі болып келеді.

Түйін сөздер: қылмыстық саясат, ҚР Президентінің жолдауы, ақпарат, ақпараттық қауіпсіздік, ақпараттық жүйелер, халықаралық қауіпсіздік, ақпараттық технологиялар, компьютерлік қылмыстар.

Атаханова Г.М.[1], Аратулы К.[2], Абитаева А.К.[3]

[1]к.ю.н., и.о. профессора, e-mail: atakan73@mail.ru
[2]доктор PhD, и.о. доцента, e-mail: kunya8585@mail.ru
[3]докторант, e-mail: ayagoz.92@mail.ru
Казахский национальный университет имени аль-Фараби, Казахстан, г. Алматы

Уголовная политика Казахстана в сфере информационной безопасности

В настоящее время информационная безопасность в Республике Казахстан находится на достаточно низком уровне, и в связи с этим вопросы данной безопасности стоят очень остро. Как известно, развитие государства и общества как политико-правовых явлений осуществляется всегда в четко определенных исторических и территориальных факторах, которые обусловливают это развитие. При этом угрозы для государства, общества и человека также находятся в постоянном изменении, адекватном развитию общества и государства. Современные мировые тенденции сегодня сигнализируют о возникновении новых форматов угроз для национальной безопасности Казахстана в XXI в. и в их числе наиболее остро как раз таки стоит вопрос информационной безопасности.

Целью научного исследования является проведение анализа, методично аргументируя нынешнее, прошлое и будущее состояния информационной безопасности Республики Казахстан в контексте с медународными правоотношениями в данной сфере.

Президент РК в своем ежегодном послании народу Казахстана указывает важность культивирования новых индустрий, которые создаются с применением цифровых технологий. Он отмечает, что это важная коплексная задача, и что следует адаптировать законодательство под новые реалии. Поэтому вопрос IT-сферы Правительство должно держать на особом контроле. И акцент на информатизацию и информационные технологий Президент делает ни один раз, что говорит о важности и информационной поддержке, а также информационной безопасности всех важных отраслей деятельности государства и высокопоставленных государственных задач, что, в свою очередь, объясняет столь высокую важность и значимость научно-исследовательских и практических работ в данном направлении.

Научную ценность статья имеют непосредственную, так как в современном обществе информация и информационная безопасность играют, если не самую главную, то одну из главных ролей и значимое место, что доказывают последние события, происходящие в мире и виртуальном интернет-пространстве за последние три десятка лет.

Практическая значимость работы объясняется потребностью такими работами самим обществом и практико-правовой системой государства.

Ключевые слова: уголовная политика, Послание Президента РК, информация, информационная безопасность, информационные системы, международная безопасность, информационные технологий, компьютерные преступления.

Introduction

In the advanced study on a theme «Criminal policy of Kazakhstan in the field of information security» theoretical questions are investigated on the base of operating and forecasting norms of criminal statute of Republic of Kazakhstan, practical questions touching informative criminality, description is given to the state of politics of the state in the field of counteraction to the cyber crimes, the comparative analysis of home legislation is conducted with the legislation of foreign countries about informative safety.

The scientific novelty of research consists of that complex research of criminal and law problems is in-process carried out in a theory, so in practice, related to the information crimes. The comparative analysis of home legislation and practice is produced with a legislation and experience of foreign countries about cyber crimes.

Theoretical and practical meaningfulness of research consists of that her positions and conclusions can be used in legislation activity, and similarly for perfection of criminal statute of Republic of Kazakhstan and more effective achievement of aim of Law defence of computer information as, to the component of interests of providing of public safety.

The results of the real research can be drawn on also in an educational process and scientific researches on those questions of criminal law and process, that is attended with the problems related to the informative crimes.

Object and article of research. The object of this research is criminal activity at the feasance of informative offences.

The norms of Constitution of Republic of Kazakhstan, criminal law, criminal process legislation, other normative legal acts of Republic of Kazakhstan, regulating questions warning, come forward the article of research, opening and investigation of cyber crimes, and also foreign legal system and practical experience.

Aims and tasks of work. The aim of the real research work is: determination of law problems of fight against computer criminality.

The achievement of the adopted aim is related to the necessity of decision of next tasks:

– to expose essence and maintenance, maybe and concepts of criminal politics of counteraction to information offences;

– to expose a role and politics of the state in the field of counteraction to informative offences;

– to conduct the comparative analysis of home legislation with the legislation of foreign countries about cyber crimes;

– to produce legal description of cyber crimes;

– to produce the measures of warning and counteraction to information offences.

Methods and research methodology

Methodological basis of research is presented by totality of the scientific and special methods based on the criteria of objectivity and accordance to truth. Basic accents in the conducted research are placed on a base: empiric, legal-historical, comparatively-legal and formally-logical methods. In addition, during work such research receptions of empiric and theoretical level, as abstracting, analysis and synthesis, were used, legal design of and other In full the methods of certainly-sociological research were applied: study of documents, statistics and etc.

For criminal law science and for legislation a new subject of scientific and political discussions and developments appears. And what is the subject of crimes in the field of computer information on the criminal legislation of Kazakhstan. These are the positions that are based in the norms of the Criminal Code of the Republic of Kazakhstan, regulating relations related to the use of information and information technologies, the analysis of these standards reveals the entire scope of possible criminal acts in the field of new communication technologies. It would seem that every user distributes computer information, also protects at the household level, however, in accordance with the Criminal Code of the Republic of Kazakhstan, computer information is subject to criminal law protection, although in a limited form (Uranbaev N.T., 2012: 1).

The main requirement for such information, in relation to the norms of the criminal law, is that such information should be in the order of limited access. All the secrets that make up information with limited access, relying on the triad “person, society, state”, can be divided into three categories: personal secret; family secret, commercial secret, professional secrets; state and official secrets (Zinina, 2007: 2).

Security is a state in which there is no danger or effective measures are available to eliminate potential dangers and threats. One of the important trends of the modern stage of human development is the information revolution. The rapid changes caused by this process lead to serious shifts in all spheres of public life. The most important sphere, currently undergoing a significant transformation, is the information sphere. In this regard, today one of the urgent problems of any state is the task related to ensuring information security. At present, the problems of considering the basic aspects

of the consideration of information security are characterized by insufficient knowledge and the lack of clearly defined definitions. At the same time, it can be said that the criminal policy of the Republic of Kazakhstan is aware of the attendant threat caused by the rapid development of information technologies and the need to ensure information security (Zhmyhov, 2003: 3).

Information security today has become a strategic category, consisting of such complex concepts as "international security" and "national security". It can be viewed in the aspect of socio-economic development as a policy pursued to preserve and protect technical and linguistic information, the influence of information flows on the mass and individual consciousness, monitoring and classifying computer and network threats and preventing information wars. Understanding and researching these phenomena, developing countermeasures are the main tasks to be addressed by criminal policy in this area. The urgency of the problem of ensuring information security is due, first of all, to the fact that in the modern world information has become a strategic national resource. In recent years, a number of measures have been implemented in the Republic of Kazakhstan to improve the information security system of the state. In accordance with the National Security Strategy of the Republic of Kazakhstan, the Concept of Information Security was developed and adopted providing for the implementation of a set of legal, organizational and scientific and technical measures aimed at forecasting, identifying, preventing and suppressing threats in the field of information security (Nazarbaev, 2006: 4).

«It is necessary to work to prevent the propaganda of religious extremism, including on the Internet and social networks. ... All these measures should be taken into account in the State Program on Countering Religious Extremism and Terrorism for the period 2017-2020, which is being developed on my behalf.

The fight against cybercrime is becoming increasingly important.

I instruct the Government and the National Security Committee to take measures to create a Cybershield of Kazakhstan system» – from the Address of the President of the Republic of Kazakhstan to the people of Kazakhstan. Never before has the state, including the President of the Republic of Kazakhstan, been so particularly important both in the legal and in the strategic plan since the establishment of Kazakhstan by an independent state.

The National Security Committee, in cooperation with relevant state structures, participates in the development of a number of normative legal acts on the creation and development of a single information telecommunications system of state bodies. Thus, information security should be considered as a state of protection of the information space of the Republic of Kazakhstan in the first place. Secondly, it is the protection of the rights and interests of the individual and citizen, society and the state in the information sphere from real and potential threats, when sustainable development and information independence of the country is ensured. Legal provision of the state of security and activities to counter and prevent threats is the main condition for the activities of the modern state and criminal policy in general.

If we compare US policy in the field of information security for comparison, we can come to the following remarks or conclusions. The US Administration at the official level views information as a strategic resource that arises from the processing of data using specialized analysis systems. With the use of modern information technologies (IT), such as computer networks and databases, the value of information (from the point of view of resolving the tasks of conducting combat operations) increases, as they enable to increase the level of awareness, improve the interaction between the command of various levels, military command and control agencies and thereby realize their information superiority. The same IT, when used in the civil sphere, increases the efficiency of life support systems, social services, financial institutions and government (Melik, 1998: 5).

Thus, the task of providing cyber security for computer systems, involving operations in computer networks, requires a high level of interagency interaction. Moreover, in this context, it is not only about protecting our own information systems, but also about offensive operations in enemy networks (Dmitrienko, 2003: 6).

For conducting offensive and defensive operations in computer networks within the Ministry of Defense, the command of joint information operations (Joint Information Warfare Command – JIOWC) and command of military operations in cyberspace (US Cyber command), part of the united strategic command (USC) of the US Armed Forces. The real opportunities and specific activities of these structures are classified, however, according to foreign sources, they closely cooperate with the special services of the United States, and also attract civil and military specialists from allies.

Conducting operations in computer networks involves three main areas of activity: the protection of their own information systems, the collection of intelligence data in computer systems of the enemy and, finally, network computer attacks. Although these directions were initially formulated in the MO, at the same time, many other United States departments are also implementing them. The protection of computer networks covers activities aimed at protecting information, computers and networks from penetration, damage or destruction by the enemy. The most vulnerable elements of the national information infrastructure include the following: equipment, including peripheral and communication equipment; computers, tele-, video- and audio equipment; software; network standards and data transmission codes; information as such, presented in the form of databases, audio and video recordings, archives, etc.; specialists working in the information field (Chemiyakin, 2008: 7).

Realizing that the sustainable functioning of the state and all its institutions increasingly depends on the stable operation of key supply systems, including information systems, the US government, by decree No. 13010 of July 15, 1996, established the presidential commission for the protection of critical infrastructures (Presidential Commission for Critical Infrastructure Protection – PC-CIP). This commission in October 1997 published a report "Critical foundations. Protection of American infrastructure. " Guided by his recommendations, in May 1998, the US president signed two directives – No. 62 "Combating terrorism" and No. 63 "Protecting critical infrastructure", in which the main lines of action were taken to protect national critical infrastructure facilities, in particular information.

Directive No. 63 specifies among other things the agencies responsible for priority areas of activity, one way or another related to the protection of critical infrastructure facilities, including for national defense – MO, international relations – the State Department, intelligence – the CIA and legislative support of this activity – the Ministry of Justice and the FBI. Taking into account the recommendations of leading agencies and the national economic council, the US president was to form a national council on infrastructure security (National Infrastructure Assurance Council – NIAC), called to improve interaction in this area between the public and private sectors. However, in spite of these measures, the immediate task of ensuring the safety of critical infrastructure facilities remained unsolved.

In accordance with the Law on Uniting and Rallying the United States for the purpose of taking measures to combat terrorism (Uniting and strengthening America by Providing Appropriate Tools, Required to Intercept and Obstruct Terrorism – USA PATRIOT Act), adopted by Congress on October 26, 2001, a critical infrastructure is defined as «a collection of physical or virtual systems and means that are important for the country in such a way that their failure or destruction can lead to disastrous consequences in the field of defense, economy, health and the security of the nation» Washington DC, White House.

In January 2001, a report of the National Security Commission (the Hart-Rudman Commission) was published, which referred to "the need for fundamental changes in the structure and activities of US agencies that provide national security." In particular, it was suggested to make the issue of "internal security" a priority and create an independent internal security agency (ISA).

Back in March 2001, US President George W. Bush, speaking at the CIA headquarters in Langley, listed the main threats to the security of the United States. The second place after terrorism in this list is information warfare and already after it – the proliferation of weapons of mass destruction and their means of delivery.

After the terrorist attacks of September 11, 2001, at the end of 2001 – early 2002, the US took a number of organizational and legislative measures to improve the security of the national territory. President George W. Bush appointed T. Ridge, a former Pennsylvania governor and personal friend, to the newly created position of an internal security adviser, and shortly thereafter established the ISA, in which the council for internal security was established. The body included: the president (chairman), vice president, finance, defense, justice, health and transport ministers, the director of the federal emergency agency, the FBI and the CIA, the president's assistant for internal security and other officials of the executive branch, which the head of state can invite to meetings of the council if necessary. The heads of the administrations of the president and vice president, as well as the presidential assistant for national security, have free access to any council meetings. The Secretary of State, the Ministers of Agriculture, the Interior, Energy, Labor and Trade, the Secretary for Veterans Affairs, the Head of the Environmental Protection Agency, the Presidential Assistants for Economic and Domestic Politics are invited only to those meetings that consider issues related to their competence.

In the course of a radical restructuring and strengthening of the executive branch, on November 25, 2002, George W. Bush signed the Law on Homeland Security, according to which in January 2003, ISA was transformed into the Ministry of Internal Security (MIS). The ministry was headed by T. Ridge, and his deputy was the US Navy Minister G. England.

On March 1, 2003 the staff were transferred to DHS and began his duties by a decision of "information analysis and infrastructure protection tasks following divisions of ministries and departments of the US government: critical infrastructure security department of the Ministry of Commerce (Infrastructure Assurance Office – CIAO), National Infrastructure Protection Center under the FBI of the Ministry of Justice (National Infrastructure Protection Center-NIPC), National Center for Modeling and Analysis of Infrastructure at the Institute for Information Security Problems of the Ministry of Energy (National Infrastructure Simulation and Analysis Center – NISAC), Federal Center for Information Resources Protection of the Administration of Common Services (Federal Computer Incident Response Center of the General Services Administration – Fed CIRC), Security management Energy Ministry of Energy Systems (Energy Assurance Office of the Department of Energy – EAO), national communication system (National Communication System – NCS). In preparing the war in Iraq, the US administration adopted three new directive documents in the interests of ensuring internal security: the "National Strategy for Combating Terrorism" (The National Strategy for Combating Terrorism), "National Strategy for the Protection of Cyberspace" (The National Strategy to Secure Cyberspace) and "National Strategy for the Physical Protection of Critical Infrastructure". In them for the first time officially recognized "the complete dependence of the US infrastructure on information systems and networks" and the vulnerability of the latter. In addition, they target the government, industry, business and society as a whole to create a so-called unified national system for responding to cyberattacks (National Cyberspace Security Response System) as a set of territorial, departmental and private centers for analyzing and distributing information (ISAC) in various sectors of the country's economy.

In the structure of DHS unit was set up cyber security (National Cyber Security Division – NCSD), the main element of which is newly formed by combining three groups (CC/CERT, NCS, NTPC) of immediate response to an emergency response center for computer incidents in the US (U.S. Computer Emergency Response Team – US-CERT). The main tasks of the US-CERT are detection of the fact of an attack (invasion) on the information structure of the United States and issuing a warning (recommendation) to all administrators of the country's information systems within no more than 30 minutes from the time the threat is detected.

The main objectives in the field of information security in accordance with the new strategy are to "prevent cyberattacks on critical infrastructure, reduce the vulnerability of the nation to such attacks, and minimize damage and recovery time". At the same time, under the term "cyberterrorism" in the United States today is meant "the deliberate destruction, interruption or distortion of data in digital form or information flows that have wide-ranging consequences in political, religious or ideological terms." In general, the information security strategy will be implemented according to the classical scheme of the civil defense system: training, prevention, notification and elimination of consequences.

In accordance with article 1502 of the Internal Security Law, the head of the IMB presented the president with a plan for the reorganization of this ministry before September 2003. The plan provided for the completion of all necessary organizational and staff activities and fully ensure the work of the IMB as the body responsible for the safety of citizens, land and sea borders, infrastructure facilities, all types of transport and information resources of the United States (by that time the total staff of the IMB already numbered 180,000 employees).

For the first time, the internal security strategy was developed and promulgated as part of the ISA in July 2002. The fact that it was adopted shortly after the September 11 terrorist attack significantly influenced the definition of the concept of "internal security" proposed in the document. As George Bush declared, "the nation is in danger, our society is an almost endless set of potential targets, which can be attacked by various methods". That is why one of the key tasks of the strategy was the protection of critical infrastructures. And one of the main areas of this activity was recognized as the protection of cyberspace.

NCSD was established in June 2003 on the basis of the Security Infrastructure for Critical Infrastructures, the National Center for Infrastructure Protection, the Federal Center for Responding to Computer Malfunctions and a number of other structures. Its tasks include interdepartmental coordination and establishment of interaction with

the private sector and foreign partners in the field of information security. Technical support was provided by US-CERT. The responsibilities of this unit include the analysis and detection of sources of cyber threats and vulnerabilities, as well as the dissemination of information on changes in the level of such a threat. In addition, the US-CERT coordinates actions to restore federal computer networks and systems after failures and cyberattacks.

The collection of intelligence from computer systems of the enemy makes it possible to obtain information about it from a strategic and operational point of view and to identify vulnerabilities in its information systems. In the US, at an official level, they acknowledge that control over the enemy's secret communications while protecting their own provides them with unique opportunities to maintain their leading positions in the world.

In accordance with Presidential Decree No.12333 of December 4, 1981, all issues related to securing access to secret or encrypted data from other states and protecting their information resources from technical intelligence are under the responsibility of the National Security Council / Central Secret Service (NSC/CSS). The NSC is formally working within the Ministry of Defense, but in fact it is one of the key elements of the American intelligence community. The CSS plays the role of coordinator between the agency and those MO structures involved in cryptanalysis. The main tasks of the NSC are: conducting radio technical intelligence, cryptanalysis and protecting federal communication and information systems from threats emanating from other states. Currently, the agency is responsible for protecting computer networks belonging to federal ministries and departments from possible attacks. The work of the National Security Council is concentrated in two directions: conducting radio and electronic reconnaissance (Signal Intelligence – SIGINT), which is engaged in relevant management (Signal Intelligence Directorate – SID), and information security (Informational Assurance – IA), which is managed by the Information Security Department (Information Assurance Directorate – IAD).

Detection, notification and response to emerging cyber threats, as well as the development of encryption systems for secure information exchange between systems within the NSC are entrusted to the management of information security. IAD certifies user security systems (thereby supporting security operations), as well as evaluating commercial software and hardware for compliance with government standards. It also oversees the development of information security systems for the global "information grid" created by the Ministry of Defense.

In this regard, the interest is represented by research work, which in 2009 was planned by the Office of Advanced Studies MO (Defense Advanced Research Projects Agency – DARPA). One of them – the so-called global information grid – the next generation wireless network (The Wireless Network after Next-WnaN, Global Information Grid-GIG).

Planning and implementation of operations in global computer networks are carried out in accordance with the concept of "Net-Centric Operations". The basis for network-centric operations is the global information network (global information grid) of the GIG (Global Information Grid) of the US Department of Defense, which is a set of interconnected high-security local information networks. It optimizes the processes of collecting, processing, storing, distributing and managing information, as well as bringing it to consumers within the Ministry of Defense and beyond. With the help of GIG, both administrative and operational control of the US Armed Forces is carried out. The head office responsible for the operability and protection of the global information network of the military department has appointed a joint strategic command of the US Armed Forces, DARPA, 2010.

The new directives allow the Pentagon to develop plans for conducting cyberattacks against information networks of US opponents. In cases where the NSC establishes a specific fact of the attack and the server of the foreign state from which the attack was launched is identified, Defense Ministry specialists will strike it back to prevent further attacks on the information networks of the US government. In matters of information security / NSC works closely with DHS. So, in 2004, the CSD and the cyber security unit agreed to jointly develop an information security training course for the agency's staff development center. In 2008, in accordance with the presidential directive, the NSC was named the leading organization for monitoring and protecting federal government networks from cyberterrorism. Network computer attacks cover the whole range of activities aimed at breaking or destroying information contained in computers or computer networks of the enemy. At the same time, the information flows themselves are directly used as weapons. For example, the transmission of an information packet with a command to turn off the electricity is an attack of this kind, while the generation of a power surge in the supply network, as a result of which the computer system of the

enemy will be de-energized, already belongs to the category of electronic combat (Streltsov, 2003: 8).

Doubts about the effectiveness and predictability of the consequences of network operations were discussed at a meeting of government officials and experts at the Massachusetts Institute of Technology in January 2003. The concern of politicians was caused by the prospect of a transboundary cascading effect in the implementation of cyberattacks, which could disrupt the functioning of civilian computer systems. In many respects guided by the results of this discussion, the US President in February 2003 issued the National Security Directive No. 16 regulating the conditions under which the United States can launch a network attack against the computer systems of another state. It also identified officials authorized to take decisions on conducting such operations.

According to the Pentagon, in 2007 alone, almost 44,000 incidents were recorded that were classified as cybercrimes committed by foreign armies, intelligence agencies and individual.

In December 2006, the Joint Chiefs of Staff prepared the document «National Military Strategy cyber operations» (currently partially declassified), which among other things has identified the strategic priorities of the US operations to ensure information security:

– the achievement and retention of initiative in the course of operations conducted within the decision-making cycle of the enemy;

– ensuring the protection of its own computer systems and carrying out offensive operations in enemy computer networks;

– the inclusion of operations in cyberspace in the military planning system for the entire range of armed conflicts with a view to developing methods for conducting such operations (taking into account the specificities of the various) in close cooperation with the Armed Forces and MO departments, who in turn must coordinate their actions with other US departments, coalition allies and industrial contractors;

– the creation within the Ministry of Defense of the necessary conditions for cybernetic operations, including organizational arrangements, training of specialists and the creation of an appropriate infrastructure;

– assessing the risks of network operations that may arise due to insufficiently effective selection of funds or counter use by the enemy of vulnerabilities in the cyberspace of the United States, as well as from the side effect of offensive operations.

Obviously, these priorities are of a very general nature and only outline guidelines for future operations in cyberspace.

In early March 2008, the United States held exercises code-named «Cyberstorm-2». They were conducted by the Ministry of the Interior with the participation of 18 federal agencies, including the CIA, the FBI, the USC US Armed Forces and NSC, representatives of nine US states and over three dozen private companies, as well as relevant services of Australia, the United Kingdom, Canada and New Zealand. The command post of the exercises was located, as reported} at the headquarters of the US secret service, which is responsible for the safety of the head of state and is structurally part of the IMF. «Probable enemy» was not indicated, but it was believed that he pursued political and economic goals and to achieve them he undertook a powerful cyberattack against the US and its allies. During the exercises, the participants worked out joint actions designed to repel this attack. The development of cyberspace was one of the main priorities of US President Barack Obama, who came to power in early 2009, who returned to the project of creating a cyber command, having substantially raised its level, but not in the structure of the US Air Force, but within the USC US Armed Forces.

After his election, President Obama was introduced to the report of the US National Intelligence Agency, Global Perspectives-2025, which concluded that «there is an urgent need to take measures to counter information threats», and that these threats must be considered at the national level security of the country.

A similar conclusion was reached by the authors of another report prepared at the Center for Strategic and International Studies and directly devoted to the cybersecurity policy pursued by the White House at the present time. In it, President Barack Obama is recommended to take urgent measures in order to prevent the threat of national security from escalating in this direction. The actions of the new administration show that it classifies information threats to the level of national security. Thus, at the end of February 2009, the president sent a draft federal budget to the congress in 2010, which outlines contingency spending for intelligence (the «National Intelligence Program»), which provides key elements of US national security. In this document, threats to federal information and technology networks are characterized as real, serious and growing, and the task of strengthening cybersecurity at the federal level is in second place.

We can say that the reform of the information security system actually began from the very first days of the new president's tenure. The role of the Ministry of Internal Security, the National Security Agency, the National Intelligence Council, the CIA and other special services has significantly increased. Simultaneously with the reform of the information security system, the Obama administration also adopted other organizational and legislative measures aimed at securing the status of an information superpower for the United States.

In May 2009, Pentagon officials announced their intention to create a new structure – the command of military operations in cyberspace, which is designed to ensure the security of not only military, but also civilian information systems.

Under its protection, cybernetic command takes the military systems of the United States – 15 thousand electronic networks, about 7 million computers and other information technology services. Other government or private computer networks will remain beyond his responsibility.

The American administration believes that the formation of a single global information infrastructure under US control will enable them to solve the task of strategic use of information weapons «Up to blocking the telecommunications networks of states that do not recognize the realities of the modern international system».

It should be noted that at present the use of information technology for military purposes is not actually regulated by international law. According to foreign experts, these issues should be considered and resolved on a multilateral basis with the participation of all interested parties. At the same time, information space management is necessary to ensure not only the national security of the absolute IT leader-US, but also international security in general. However, on these issues, the United States takes a special position and leaves agreements (Tayley, 2007: 9).

Washington for many years opposed the proposals of Russia on the conclusion of a kind of «treaty on arms control», in which it should be, in particular, about cyber weapons. At the same time, the White House noted that in the framework of international cooperation, it is first necessary to concentrate efforts on combating cybercrime. The Russian Federation sought to secure support for concluding a treaty at the UN on restricting the use of cyber weapons, such as computer programs capable of destroying enemy computer systems.

However, recently the situation is beginning to change. «What Russia has proposed is perhaps the starting point for the start of international debate», said General Keith Alexander, speaking at the Washington Analytical Center for Strategic and International Studies (Alexander, 2014: 10). We must carefully study these proposals and, apparently, we will do it. «Such a statement can be regarded as the beginning of the search for joint approaches to solving the accumulated problems».

Conclusions

On efficiency of counteraction of cybercrime imperfection of the legal providing of informative sphere affects in the state, in this connection, need perfection: legal mechanisms, regulative informative legal relationships, arising up at a search, receipt, consumption of different category of information, informative resources, informative products, informative services; legal mechanisms, regulative the processes of production, transmission and distribution of information, informative resources, informative products, informative services; legal mechanisms, regulative informative legal relationships, arising up at creation and application of the informative systems, their networks, backer-ups, telecommunication infrastructure.

The number of the informative offences registered on territory of Kazakhstan increases with every year. Therefore measures on a fight against these crimes must be conducted systematic. The republic of Kazakhstan for more successful fight against informative crimes cooperates with many countries of the world.

The basic achievements of this advanced study are:

Looking over legislative acts, legal and special literature on the examined question criminal politics is analysed on counteraction of informative criminality;

The concept of politics of the state is exposed in the field of counteraction to the cyber crimes, her principles and forms of realization are certain;

The comparative analysis of home legislation was produced with the legislation of foreign countries about cyber crimes, in particular, the USA, Russian Federation, West Europe, etc.

References

Uranhaev N.T. Introduction of new information technologies and development of communication support in the context of ensuring national security of Kazakhstan. – Astana, 2012.

Zinina U.B. Crimes in the field of computer information in Russian and foreign criminal law. // Thesis for a scientific degree. – Moscow, 2007.

Zhmyhov A.A. Computer crime and computer security software. Crime problems in capitalist countries. – Moscow: Viniti, 2003. – № 6. – p.3.

Nazarbaev N.A. Decree of the President of the Republic of Kazakhstan «On the Concept of Information Security of the Republic of Kazakhstan» dated October 10, 2006 №199 – Astana: AKORDA, 2006. – https://zonakz.net...

Eleonora Melik. Computer crimes. // Information-analytical review. – M., 1998. – http://www.melik.narod.ru/

Dmitrienko T.A. Ensuring Information Security and Development of the Information Infrastructure of the Republic of Kazakhstan // Informational and Analytical Journal «ANALYTIC». – 2003. – № 5.

Chemiyakin Yu.V. Political communications and information security of society. // Tutorial. – Ekaterinburg, 2008.

Streltsov A.A. Actual problems of ensuring information security. – Informational and analytical journal «Fact», 2003. – № 11. – //fact.ru/arhiv11s7.htm.

Ed Tayley. Computer Security. – Minsk: Papourri, 2007.

Kate Alexander Washington analytical center of strategic and international studies. – USA, Center of Strategic and International Studies, 2014.