US GOVERNMENT INFORMATION SECURITY POLICY DEVELOPMENT PROCESS

Aliyev Olimbek Aybekovich
Researcher of Andijan State University.

Annotation: From the second half of the last century, a period of radical change in the field of information security began in the United States. Since then, serious efforts have been made in the field of state computer and information security. In particular, legal-regulatory documents and legislation related to the field have been improved. The article discusses and analyzes the same issues.

Keywords: information, information security, computer security, cyber security, information attack, cyber terrorism, cyber crime, cyber space, cyber threat, cyber security, information confidentiality

From the second half of the 20th century, a period of radical change began in the field of information security in the United States. During this period, the development of a special communication system designed to ensure the confidentiality, integrity, and ease of obtaining information in emergency situations has intensified. The National Communications System, established in 1963, began to perform the task of providing uninterrupted communications under all conditions, including emergency situations and various international crises[24]. Initially, it covered voice communications. Later, he began to perform the task of ensuring the continuous operation of computer networks and Internet networks. It was terminated in 2012, its functions were divided between state agencies, and maintenance of government communication networks was transferred to the Ministry of Internal Security (ISM) and the Ministry of Defense[29].

During this period, the IXV began to deal with the activities of state authorities, emergency preparedness systems, non-military communications, security of important infrastructures, and communication networks. The Ministry of Defense began to perform the function of ensuring the functioning and security of the system of interaction between the president, vice president, heads of state and government of other countries, the management system of nuclear forces, as well as the executive, judicial and legislative bodies.

With the increase of information threats, the need to improve and strengthen the information security system began to appear. Also, the need to facilitate access to information, to ensure its confidentiality and integrity in new conditions opened the way for the creation of a new and high-quality system of communications. In 1958, the Advanced Research and Development Agency (ARPA) was established by the directive of the US Department of Defense. It was rebuilt in 1972 and renamed the Defense Advanced Research and Development Agency (DARDA).[5]

The main task of this new structure was to create promising projects in the field of completely new future technology. One of the directions of DARPA's activities was to carry out research on the creation of new types of computer and network technologies, their development and their introduction into the field of telecommunications. ARPANT (the ancestor of today's Internet) formed by this agency was created to provide stable distributed communications, which had the ability to continue to operate even if part of the network went down.

During this period, only the concept of "information protection" had just appeared. Therefore, the issue of forming a separate structure responsible for cyber security has begun to be resolved. That is why the US Congress has developed separate legislation on computers and information systems.

Passed in 1965, the Brooks Act gave the National Bureau of Standards (now called the National Institute of Standards and Technology (NIST) under the Department of Commerce) the authority to develop processing standards and thereby protect information in government computer systems. By 1987, the Brooks Act had been replaced and supplemented by the Computer Security Act. Accordingly, NIST was assigned to coordinate the production of security standards for systems

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 12 Issue: 01 in January-2023
https://www.gejournal.net/index.php/IJSSIR

not yet connected to national security support[15]. At the same time, it was decided that NIST would cooperate with the National Security Agency, which has extensive experience in the protection of information systems and cryptography.

With the development and improvement of ICT, as a result of the introduction of computers and networks, the processes have been expanding and improving year by year, and they have started to be considered as sources of various threats. Although the concept of "cyber security" did not exist since the 80s of the XX century, approaches to information security in computer networks and systems began to change seriously. In 1984, the regulatory document "National Policy on Telecommunications and Automated Information Systems" was adopted, which called for the following security: "With the introduction of new technologies, the traditional boundaries between telecommunications and automated information systems are disappearing. Nevertheless, these principles will greatly improve efficiency, productivity, and safety in the future.

Telecommunications and automated information systems are not resistant to information theft, illegal access to the information system, its destruction, intelligence by hostile countries. Hacking technologies are widely used and spread by other countries, terrorist groups and criminal elements. Government and corporate information systems that store information about US citizens and businesses may become targets of hostile countries" [26]. The document identified three threats recognized by the international community in this area: cyberterrorism, cybercrime, and the use of ICT by states for hostile purposes. A new policy in this area was formalized in the Computer Security Act of 1987. The law set the goals of developing and implementing computer security standards to ensure the security of computer systems used by state enterprises[19].

The principles of coordination of the ICT sector of the economy were embodied in the Law "On Telecommunications" adopted in 1996[22]. In accordance with it, the goal of strengthening competition between them was envisaged in order to encourage consumers who are widely using ICT and communication infrastructures. US economist Dale Jorgenson noted in his book Pushing the Speed Limit: US Economic Growth in the Information Age that “computers accounted for one-tenth of the percentage growth of the US economy from 1959 to 1973”. At the same time, from 1995 to 1998, the price of computers decreased by 28 percent[6].

By this time, "cyberspace" emerged, globally connected to the digital information communication infrastructure. The rapid development of the commercial environment, the increase in the total amount of digital transactions and the increase in the volume of confidential information have led to the increase of organized criminal structures in the networks.

If in the 90s of the 20th century ICT was considered as some kind of auxiliary tools, by the beginning of the 21st century it has become a separate field of activity. The boundaries between telecommunication and automated information systems have disappeared and they have merged. The concept of cyber security has been formalized and it began to mean "the ability to protect or secure against cyber attacks in the use of cyber space"[14]. Cyber security has been differentiated from protecting information on systems and networks since before the advent of computers and computer security. The cyberspace is a unique environment, characterized by a number of features: networks and systems are interconnected and interconnected, and there are no boundaries between them - therefore, the issue of cyber security does not fall within the scope of information protection in an isolated system. The characteristics of the cyberspace create new dangers and threats through the virtual world, which affect the objects of natural existence.

The United States is the first country to consider cyber security as an important strategic task. The terrorist attacks of September 11, 2001, as well as the growing threats to the economy related to ICT, have put the task of modernizing the security of cyber security and critical infrastructure facilities. The order of the President of the USA on October 16, 2001 (PATRIOT ACT), in 2003, the order on the "National Strategy for the Defense of the Cyberspace" was announced. They were expressed more widely in the adopted "National Security Strategy" [13].

In line with this strategy, cyber security has been divided between agencies and federal ministries[25]. It has been established that each institution has common interests in information protection, and another part of them deals with the protection of their own information infrastructure. An important aspect of such approaches has been the establishment of a coordinating body for cyber security. This task was assigned to the US Department of Homeland Security. Its main tasks were defined as follows:

- assumes special responsibility for elimination of damages, detection of illegal access to the network and failure of infrastructures;
- solves the issues of ensuring confidentiality, integrity, ease of obtaining information and restoration of information networks and systems;
- Participates in international negotiations, procedures, and information exchanges with the US State Department and other ministries and agencies, as well as the private sector, to develop solutions to cyber security issues in different countries.

The National Cyber Security Department of the Department of Information Analysis and Infrastructure Protection of the Ministry of National Security was established. He heads the Monitoring Center, which performs the tasks of researching cyber threats and vulnerabilities in the system, pre-detecting potential cyber threats, responding to them, and restoring damaged parts of the infrastructure. In addition, cyber threat warning and information networks have been launched at 50 points in the country [3].

In January 2004, the National Cyber Security Office launched the National Cyber Attack Alert System, a network where subscribers receive up-to-date information on new vulnerabilities and cyber threats.

The US Intelligence Community and the Federal Bureau of Investigation (FBI) are tasked with developing counterintelligence doctrine to counter the illegal and unauthorized access to confidential information of federal government, commercial, and educational institutions.

The Department of Defense and law enforcement agencies develop a system to find the sources of threats and attacks to ensure a timely and effective response. At the same time, the task of the US Department of Defense includes conducting information warfare and radio-electronic warfare. It is run by the Joint Information Processing Center, which is managed by the US Strategic Command. The US State Department is tasked with promoting international cooperation on all cybersecurity issues.

The next stage of the development of the cyber security system in the USA began in 2008, and from this period, the document "National initiative of cyber security" began to be implemented [27]. It defined a number of measures to solve the problems that arose in the cyber security system:

1. In order to eliminate damage to the computer system and to take timely measures to counter the enemy's capabilities, it was proposed to establish "lines of defense" to protect the data banks of American bases from attacks by enemies and to provide the specialists of the federal government with the necessary information.
2. Ensuring information security on all possible fronts by expanding the technical and operational capabilities of counter-intelligence agencies.
3. Implementation of a comprehensive expansion of the system of training specialists in information security, coordinating and objectively directing research in this area, as well as developing the necessary strategic approaches in order to ensure an effective fight against hostility or criminality in the US cyberspace.

By 2009, US President Barack Obama declared cyber security as the most important state task. At the same time, the task of implementing new developments related to ensuring security in the cyberspace and using them effectively for national interests has also risen to the level of state policy.

By 2009, the "Cyberspace Policy Review" was developed. It included not only an analysis of the existing system in the field of cyber security, but also a plan for the comprehensive development and transformation of US cyber security[20]. By J. Bush's presidency, the state policy in this area was further improved and developed based on the "National Cyber Security Initiative" document.

The infamous terrorist acts of September 11, 2001 in the USA, as well as the growing threats to the ICT-connected economy, forced the J. Bush administration to reconsider the tasks of ensuring the security of sensitive and critical infrastructures. There is a need for integrated approaches to this area. Therefore, in 2003, the "National Strategy for the Protection of the Cyberspace" was adopted. In accordance with this strategy, ensuring the security of the cyberspace was divided between agencies and federal ministries, and the coordination of all directions was entrusted to the US Department of Homeland Security (DHS), which was established in 2002. IXV was determined to participate in international negotiations on the development of principles of international relations with the ministry, agencies and the private sector, as well as on the elimination of unauthorized intrusion into networks and infrastructure failures [7]. (Meaning of abbreviations in the table: IXA - Internal Security Agency; MV - Ministry of Defense; MXA - National Security Agency; MRB - Central Intelligence Bureau; FVV - Ministry of Emergency Situations; NASA - US National Aerospace Agency; AIC - Information Storage System)

Further development of the US government's strategy in the field of cyber security was expressed in the US President's Secret Security Directive No. 54 of January 8, 2008, and Homeland Security Directive No. 23. These directives announced the "Comprehensive National Cybersecurity Initiative" (Comprehensive National Cybersecurity Initiative), and also set priorities in the cyberspace.

The "Comprehensive National Initiative on Ensuring Cyber Security" has united the main areas related to ensuring cyber security, 20 decisions have been adopted to implement urgent tasks[28].

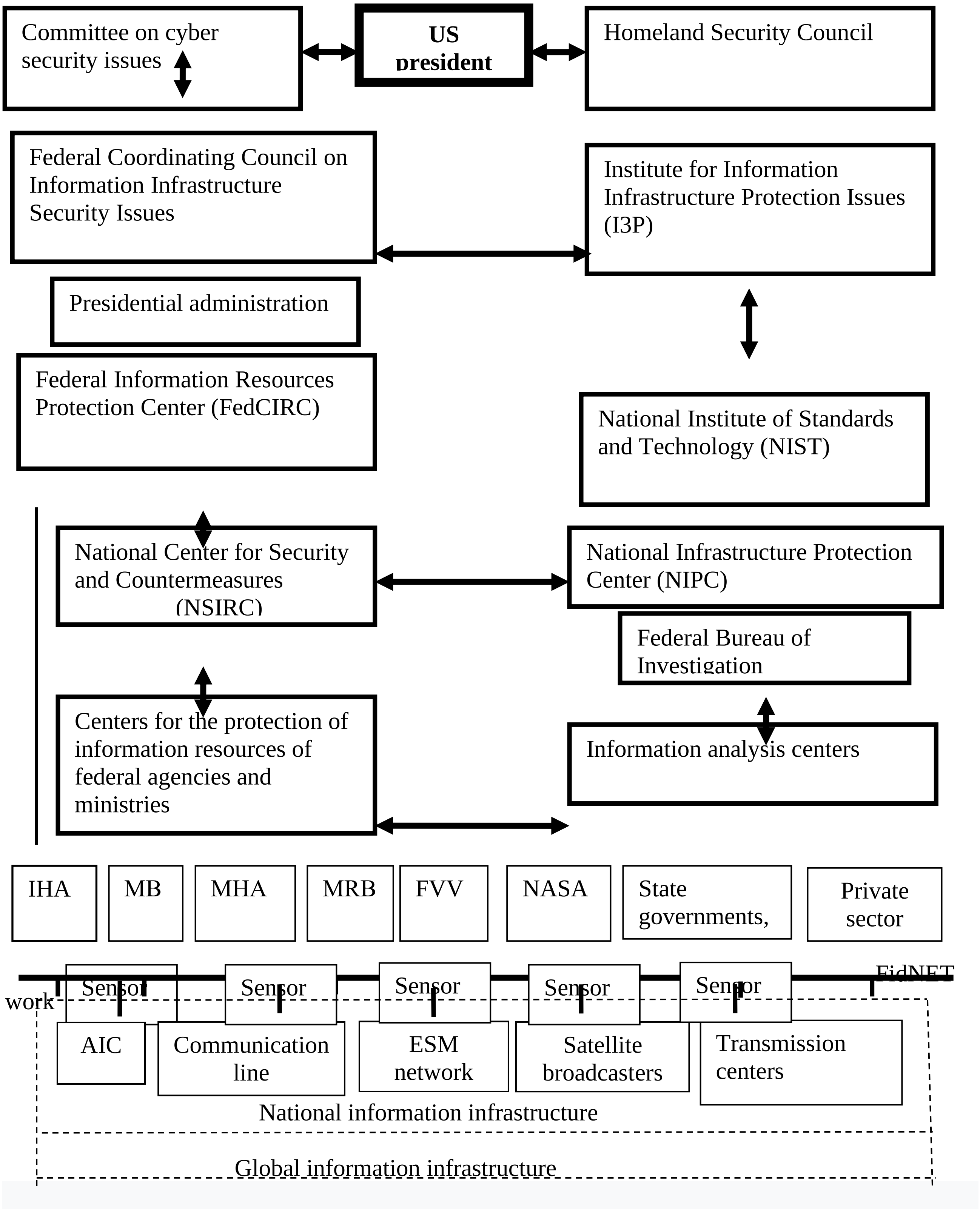
The President's directive redefined the functions of law enforcement agencies in ensuring the cybersecurity of federal systems and networks. In particular, the National Security Agency (NSA) is responsible for monitoring the computer systems of all federal ministries and institutions, the Ministry of Internal Security (ISV) is responsible for ensuring the security of federal information networks, and the Ministry of Defense (MV) is responsible for developing a strategy to combat cyberattacks[4].

The tasks set out in the "Comprehensive National Cyber Security Initiative" became the basis of Barack Obama's cyber policy. He has made cyber security a top policy priority during his campaign. His first step in this field began with an analysis of US cyber security policy. The special commission prepared a report in December 2008. According to it, the development of a comprehensive national security strategy was announced as an urgent task[17].

In May 2009, a group of experts presented the president with the Cyberspace Policy Review, which included proposals for changes in the cyber security system. Based on this view, B.Obama indicated five priority directions in the field of cyber security. As the most important of them, the development of a new nationwide strategy for ensuring security in American information and communication networks initiated by J. Bush was put forward. Based on the legacy of other directions established during the presidency of Bill Clinton and J. Bush, the following were defined in the field of cyber security:

Table 2.1.1

US National Information Security Management Framework[9]


Committee on cyber security issues
US president
Homeland Security Council
Federal Coordinating Council on Information Infrastructure Security Issues
Institute for Information Infrastructure Protection Issues (I3P)
Presidential administration
Federal Information Resources Protection Center (FedCIRC)
National Institute of Standards and Technology (NIST)
National Center for Security and Countermeasures (NSIRC)
National Infrastructure Protection Center (NIPC)
Federal Bureau of Investigation
Centers for the protection of information resources of federal agencies and ministries
Information analysis centers
IHA
MB
MHA
MRB
FVV
NASA
State governments,
Private sector
Sensor
Sensor
Sensor
Sensor
Sensor
FidNET
work
AIC
Communication line
ESM network
Satellite broadcasters
Transmission centers
National information infrastructure
Global information infrastructure

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 12 Issue: 01 in January-2023
https://www.gejournal.net/index.php/IJSSIR

- development of mechanisms for cooperative actions of federal and local authorities, as well as the private sector, in order to ensure uniform and coordinated approaches in response to cyber attacks;
- strengthening the cooperation of the public and private sectors to provide the security sector with technical factors;
- implementation of the most advanced developments and researches in the field of ICT;
- increase the level of information and education of the population, investments in scientific research and test-construction work (ITSKI), programs related to information security in schools and universities[16].

Based on the conclusions and recommendations of experts regarding the activation of mutual cooperation with foreign partners on issues of security in the cyberspace, the "International Strategy for Actions in the Cyberspace" was adopted in May 2011, which embodied the main principles implemented in the cyberspace, the priorities of the US global cyber policy. The document also stated that the main goal of the United States is to provide leadership in the process of creating a peaceful and stable cyber space. In this regard, it was announced that the United States will focus on the implementation of two levels of cooperation: interstate - on the basis of bilateral and multilateral (based on the focus on partnership with developing countries), as well as public-private (network users, Internet providers, software with supply manufacturers and computer hardware manufacturers[32].

By 2012, the "National Strategy for Information Protection and Exchange" was adopted. This document defined three main principles of the US information security policy: information as a national asset; exchange and protection of information as common risks necessitate sharing; making better decisions due to increased flow of information. Of course, the main reason for this was the result of the president's administration trying to find new and innovative ways to protect information security due to the excessive number of information attacks against the United States [12].

On April 24, 2015, the US Department of Defense adopted an updated national cyber security strategy. According to him, the task was to strike against any cyber attacks, to protect the United States as perfectly as possible from any enemy or criminal.

In this strategy, the most powerful adversaries of the United States in the cyber field are clearly shown, and three groups of threats are defined:

1) some countries (Russia, China, North Korea and Iran):

By 2015, Russia and China have achieved great results in the development of cyber capabilities. China's theft of intellectual property for the benefit of Chinese companies has greatly damaged US competitiveness. Russian hackers are distinguished by their stealth, making it impossible to consistently expose them. Although North Korean and Iranian hackers have smaller capabilities, according to US experts, they are in a hostile situation for the US and its interests.

2) non-state actors (Islamic State):

Non-state actors such as the Islamic State are using cyberspace to recruit militants and spread terrorist propaganda. Logically, the US included them in the list of enemy countries.

3) Cybercriminals:

In information networks, many cybercriminals, regardless of the affiliation of any country, have been increasing their behavior year by year, mainly for their own interests. Often, the behavior of criminals in information networks makes it difficult to find the sources of threats, and errors in this area are increasing. Thus, in order to reduce these specified risks and increase the national security of the United States, the following tasks and objectives were announced in the strategy:

- creation of tools necessary for cyberspace management;

- Protection of information networks and information of the Ministry of Defense, reduction of threats to it;
- protecting the country and its vital interests from disruptive and destructive cyberattacks;
- creation and support of strong international alliances and cooperation of partners to increase international security and stability and stop common threats[23].

On December 19, 2017, President Donald Trump's administration released its National Security Strategy. It described China as an opponent of the United States and emphasized that it is trying to change the global distribution of forces in the interests of its interests, to subjugate it to its own interests, and this situation was assessed as a threat to the United States[31].

According to some experts, this strategy was in some sense a return to the Bush doctrine based on the principle of "peace based on strength". However, during the presidency of B.Obama, an attempt was made to use "soft power". When D. Trump came to power, the policy of "Peace through strength" was given priority[10]. According to Michael Salmeyer, a well-known US expert, cyber security is carefully considered in the new strategy, but the main national security problems are that "the new strategy deviates from the established goals, and at the same time, it pays little attention to the retention and sharing of information" [18].

On January 19, 2018, the US Department of Defense announced an updated version of the National Defense Strategy. In it, the strategy of restraining Russia and China in the field of information and cyber security was included in the military plan of the general strategic directions of the ministry [2]. In the fall of 2018, President D. Trump signed the "National Cyber Security Strategy" document. Based on this document, the US cyber security strategy included:
- Strengthening of state security - protection of information, database and system;
- The current digital economy should grow in all aspects of social life, which allows the development of the state;
- strengthening the capabilities of the United States in the field of peace and prosperity support; prevent criminals from using modern cyber weapons;
- Strengthening the US influence in the international arena in the field of information technologies and networks, ensuring stable and safe operation of the Internet[8].

By 2019, the US Department of Defense will increase spending on cyberspace to $8.5 billion. delivered to the dollar. In 2020, the annual budget of the US Ministry of Defense is 750 billion. reached the dollar, the main part of it was directed to the strengthening of national security, and this situation was caused by the strengthening of competition with China and Russia. Also, the US Department of Homeland Security will receive 1 billion dollars to strengthen information security. was provided with funds in the amount of dollars. 12.2 billion to the US Department of Commerce to provide rural areas with high-speed internet. USD amount was allocated[21].

With the election of Joe Biden as president in 2021, the focus on cyber security has increased. In May 2021, he signed an executive order "Strengthening Cybersecurity and Protection of Federal Government Networks." The order aims to address barriers to government and private sector information sharing created by cyber security threats, while providing measures to protect US companies from increased hacking attacks from the outside world.

In accordance with this decree, a special standardized guideline for combating attacks in the cyber sphere was developed for the country's authorities, which included a number of recommendations. It also made a number of recommendations to the private sector [1].

President J. Biden expressed the policy in the field of cyber security as follows: "The policy of my administration is to protect the important and critical infrastructures of the nation. Emphasis will be placed on ensuring resilient systems and cyber security that support critical national functions across government and the private sector. Also, mistakes, corruption or improper performance of functions in this area lead to the weakening of national security, economic security, health or safety of the population” [11].

The above analysis shows that the state information security policy and strategy developed by the United States in order to ensure the stability of the society in the next half century is to develop international standards in this field, increase the security of global information networks, strengthen the ability of the armed forces to repel any cyber attacks, and establish effective Internet management structures. , focused on expanding security capabilities, improving the system of rights and freedoms in relation to private property on the Internet.

Most of the world's countries invested in this sector. This situation increased its political and military power and increased its chances of living as a state that determines world politics.

REFERENCES

1. Байден подписал указ о повышении уровня кибербезопасности в стране. 13 мая 2021 г.// https://www.interfax.ru/world/765723.
2. Budget in brief. Fiscal year 2017 // U.S. Department Of Homeland Security 16.02.2016. URL: https://www.dhs. gov/sites/default/files/publications/FY2017_BIB-MASTER.pdf (дата обращения: 01.03.2018).
3. Vaida B. Warning Center for Cyber Attacks is Online, Official Says. National Journal's Technology Daily
June 25, 2003 // Government Executive. [Web-source]. URL:http://www.govexec.com/ story_page.cfm?filepath=/dailyfed /0603/062503td1.htm oref=search (дата обращения 01.05.2014)
4. В связи с тем, что Директива закрытая, информация получена из открытых источников. Nakashima, Ellen. Bush Order Expands Network Monitoring. Intelligence Agencies to Track Intrusions [Электронный ресурс] // The Washington Post. January 26, 2008. – URL: http://www.washingtonpost.com/wpdyn/content/article/2008/01/25/AR2008012503261_pf.html (дата обращения: 24.04.2014).
5. Department of Defence Directive 5105.15: Department of Defence Advanced Research Projects Agency [issued on 07.02.1958] // ARPA. [Official website] Систем. требования: Adobe Acrobat Reader URL: http://www.darpa.mil/Docs/ DARP_Original_Directive_1958_ 200807180942212.pdf (дата обращения 01.05.2014).
6. D.W. Jorgenson and K.J. Stiroh Raising the Speed Limit: U.S. Economic Growth in the Information Age, 2000 // O iLibrary. [Official website] Систем. требования: Adobe Acrobat Reader URL:http://www.oecdilibrary.org/oecd/deliver /fulltext/5lgsjhvj82kf.pdf;jsessionid=1nap0snalfg1l.delta?contentType=/ns/WorkingPaper&itemId=/ content/workingpaper/ 5614 81176503 &containerItemId=/conten t/workingpaperseries/18151973 accessItemIds= mimeType=application/pdf (дата обращения 01.05.2014) p. 46.
7. Карасев П. Дж. Буш мл. - национальная оборона и защита критически важной инфраструктуры// https://russiancouncil.ru/analytics-and-comments/analytics/novye-strategii-ssha-v-oblasti-kiberbezopasnosti/.
8. Кибербезопасность США. Особенности стратегии.// https://spravochnikvs.com/kiberbezopasnost_ssha_osobennosti _strategii.
9. Леваков А. Анатомия информационной безопасности США.//http:// www.jetinfo.ru/2002/6/1/article1.6.2002.html
10. Мухин А. Новая стратегия национальной безопасности США – информационная бомба? / А. Мухин // Международный дискуссионный клуб Валдай. 26.12.2017. URL:http://ru.valdaiclub.com/a/highlights/strategiya-natsbezopa -snosti -ssha/ (дата обращения: 01.03.2018).

ISSN 2277-3630 (online), Published by International journal of Social Sciences & Interdisciplinary Research., under Volume: 12 Issue: 01 in January-2023
https://www.gejournal.net/index.php/IJSSIR

11. Меморандум Байдена// https://zavtra.ru/blogs/memorandum_bajdena.
12. National Strategy for Information Sharing and Safeguarding / The White House // The White House, 2012. URL:
13. National Security Strategy 2010. // National Security Strategy Archive. [Web-source] Систем. требования: Adobe crobat Reader URL: http://nssarchive.us/NSSR/2002.pdf (дата обращения 01.12.2014).
14. NIST IR 7298 Revision 2, *Glossary of Key Information Security Terms //* NIST [Official website] Систем. требования: Adobe Acrobat Reader URL: http://nvlpubs.nist.gov/ nistpubs /ir/2013/NIST.IR.7298r2.pdf (дата обращения 01.05.2014).
15. Public Law 89-306 (Brooks Act – with amendments) [issued on 30.10.1965] // National Institute of Standards and Technology. [Official website] Систем. требования: Adobe Acrobat Reader URL:http://itl.nist.gov/History%20 Documents /Brooks%20Act.pdf (дата обращения 01.05.2014).
16. Remarks by The President on Securing our Nation's Cyber Infrastructure. May 29, 2009.
17. Securing Cyberspace for the 44th Presidency. A Report of the CSIS Commission on Cybersecurity for the 44th Presidency [Электронный ресурс] / Center for Strategic and International Studies. December 2008. – P. 1. – URL: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf (дата обращения: 27.04.14)
18. Sulmeyer Michael. Cybersecurity in the 2017 National Security Strategy / Michael Sulmeyer. // Lawfare. 19.12.2017. URL: https://www.lawfareblog.com/cybersecurity-2017-national-security-strategy (дата обращения: 01.03.2018).
19. COMPUTER SECURITY ACT OF 1987 Public Law 100-235 // National Institute of Standards and Technology. [Official website] Систем. требования: Adobe Acrobat Reader URL:http://www.nist.gov/cfo/legislation/ Public%20Law% 20100-235.pdf (дата обращения 01.05.2014)
20. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure [issued on 29.05.2009] // The White House. [Official website]. URL: http://www.whitehouse.gov/assets/documents/ yberspace_Policy_Review_ final.pdf (дата обращения 01.05.2014).
21. США увеличит расходы на кибербезопасность.13/03/19// http://www.itsec.ru/ news/ssha-uvelichit-rashodi-na-kiberbezopasnost.
22. Telecommunications Act of 1996 [issued on 01.02.1996] // The Federal Communications ommission. [Official website] Систем. требования: Adobe Acrobat Reader URL: http://www.fcc.gov/Reports/tcom1996.pdf (дата обращения 01.05.2014)
23. The DOD Cyber Strategy // U.S. Department of Defense. April 2015. URL: http://www.defense. gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (дата обращения: 28. 02.2018).
24. The President of the US National Security Action Memorandum Number 252 [released on 11.07.1963] // John F. Kennedy Presidential Library. [Official website]. URL: http://www.jfklibrary.org/Asset-Viewer/mOsd6HP9gkGmqGvJhY1q A.aspx (дата обращения 01.05.2014).
25. The National Strategy to Secure Cyberspace [published 02.2003] // US Department of Homeland Security. [Official website] Систем. требования: Adobe Acrobat Reader URL:иhttp://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (дата обращения 01.05.2014), p. 16-17 «Lead Agencies».
26. The President of the US National Policy on Telecommunications and Automated Information Systems Security NS №145 [issued on 17.09.1984] // ederation of American Scientists. [Official website] URL: http://fas.org/irp/offdocs/nsdd145.htm (дата обращения 01.05.2014).

27. The Comprehensive National Cybersecurity Initiative [2008] // The White House. [Official website] Систем. требования: Adobe Acrobat Reader URL: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (дата обращения 01.05.2014).
28. The Comprehensive National Cybersecurity Initiative. Washington, D.C.: The White House [Электронный ресурс]. – URL:http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (дата обращения:24.04. 2014).
29. Xecutive Order « ASSIGNM NT O NATIONAL S URITY AN M RG N Y PR PAR N SS OMMUNI ATIONS UN TIONS» //The White House [Official website] URL: http://www.whitehouse.gov/the-press-office/2012/07/06/executive-order-assignment -national-securityand-emergency-preparedness- (дата обращения 01.05.2014).
30. https://obamawhitehouse.archives.gov/sites/default/files/docs/2012sharingstrategy_1.pdf (дата обращения: 28.02.2018).
31. Huileng Tan. China to USA: 'Stop deliberately distorting' our global strategy / Tan Huileng // CNBC. 20.12.2017. URL: https://www.cnbc.com/2017/12/20/china-us-beijing-reacts-to-trumps-america-first-policy.html (дата обращения: 01.03.2018).
32. 9 International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World. Washington, D.C.: The White House. May 2011. – P.12 [Электронный ресурс]. – URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (дата обращения: 27.04.2014).