Saint Petersburg State University

Krainev Nikita

Graduate qualification work
**Cybersecurity issues in US-Russian relations**

Academic Degree: Master’s Degree
Major: 41.04.05 «International Relations»
Program BM.5566. «Strategic and Arms Control Studies»

**Academic supervisor: Tsvetkova N.A.**

Doctor of Science in History

PhD in Behavioral and Social Sciences Professor

**Reviewer: Khokhlov A.R.**

Deputy Chief Editor of the All-Russian State Television

and Radio Broadcasting Company "Mir"

Saint Petersburg 2022

**Content**

[INTRODUCTION 3](file:///C%3A%5CUsers%5Cn-i-k%5CDesktop%5CCHAPTER%20I.docx#_Toc104739959)

[CHAPTER I: OBAMA’S GOVERNMENT ACTIONS TO STRENGTHEN THE USA CYBERSECURITY](file:///C%3A%5CUsers%5Cn-i-k%5CDesktop%5CCHAPTER%20I.docx#_Toc104739960) 7

[1.1 Initiatives conducted in the field of cybersecurity under Obama presidency and their impact 7](file:///C%3A%5CUsers%5Cn-i-k%5CDesktop%5CCHAPTER%20I.docx#_Toc104739961)

[1.2 Interaction in the field of cybersecurity between Russia and the United States under Obama’s presidency 20](file:///C%3A%5CUsers%5Cn-i-k%5CDesktop%5CCHAPTER%20I.docx#_Toc104739962)

[1.3 Evaluating the effectiveness and results of the Obama’s government cybersecurity policy 26](file:///C%3A%5CUsers%5Cn-i-k%5CDesktop%5CCHAPTER%20I.docx#_Toc104739961)

[CHAPTER II: US GOVERNMENT ACTIONS UNDER TRUMP TO STRENGTHEN CYBERSECURITY 30](file:///C%3A%5CUsers%5Cn-i-k%5CDesktop%5CCHAPTER%20I.docx#_Toc104739963)

[2.1 Trump's administration actions to strengthen cybersecurity 30](file:///C%3A%5CUsers%5Cn-i-k%5CDesktop%5CCHAPTER%20I.docx#_Toc104739964)

[2.2 Issues of relations between Russia and the United States in the field of cybersecurity under Trump 37](file:///C%3A%5CUsers%5Cn-i-k%5CDesktop%5CCHAPTER%20I.docx#_Toc104739965)

[2.3 Evaluation of the results devoted to cybersecurity policy under Trump administration 45](file:///C%3A%5CUsers%5Cn-i-k%5CDesktop%5CCHAPTER%20I.docx#_Toc104739961)

[CHAPTER III: Documents and initiatives created within the framework of cybersecurity policy of Biden Administration and their impact. 49](file:///C%3A%5CUsers%5Cn-i-k%5CDesktop%5CCHAPTER%20I.docx#_Toc104739966)

[3.1 Biden administration initiatives to enhance national cybersecurity defense 49](file:///C%3A%5CUsers%5Cn-i-k%5CDesktop%5CCHAPTER%20I.docx#_Toc104739967)

[3.2 Government under Biden presidency cyber policy in the framework of Russia-US relations. 57](file:///C%3A%5CUsers%5Cn-i-k%5CDesktop%5CCHAPTER%20I.docx#_Toc104739968)

[CONCLUSION 63](file:///C%3A%5CUsers%5Cn-i-k%5CDesktop%5CCHAPTER%20I.docx#_Toc104739969)

[LIST OF SOURCES 66](file:///C%3A%5CUsers%5Cn-i-k%5CDesktop%5CCHAPTER%20I.docx#_Toc104739970)

**INTRODUCTION**

Russia and the United States have a rich history of bilateral relations in various fields. For the most part, these relationships have always been accompanied by tension, and the field of cybersecurity is no exception.

The definition of cybersecurity is a controversial term in general. The US Cybersecurity Infrastructure Security Agency defines cybersecurity as, “The art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.”

In Russia, cybersecurity is often translated as information security, and cybersecurity itself is perceived as a US concept. The Doctrine of Information Security of the Russian Federation defines information security as, “The state of protection of the individual, society and the State against internal and external information threats, allowing to ensure the constitutional human and civil rights and freedoms, the decent quality and standard of living for citizens, the sovereignty, the territorial integrity and sustainable socio-economic development of the Russian Federation, as well as defense and security of the State.”

These different perspectives on cybersecurity have evolved over time along with the cybersecurity doctrine and technological development of each country.

The digital sphere nowadays occupies a crucial role not only for ordinary citizens, but also for states and other actors. In this regard, cybersecurity is actually an integral part of the national interests of states. Since George W. Bush, US cybersecurity has taken on a special role in its policy. Obama has reinforced understanding of the need to develop and maintain the required level of cybersecurity as the main tool for protecting against cyber threats from rival states, cyberterrorists and other intruders.

For Russia, however, cybersecurity has not played such an important role as for America for quite a long time in comparison, and its role has increased relatively recently. However, Russia does not spend as much budget on developing and strengthening cybersecurity as the United States does.

**The aim of the work** – to define the role of US presidential administrations’ policy in solving cybersecurity issues with Russia.

**The object** of the work is actions and issues between the USA and Russia in the field of cybersecurity.

**The subject** is the USA cybersecurity policy under different American presidents.

In order to achieve this aim, the following tasks were set during the work:

1. To study initiatives conducted in the field of cybersecurity under Obama presidency;
2. To analyze issues and cooperation level between Russia and USA governments under Obama;
3. To explore results of the Obama cybersecurity policy;
4. To study initiatives conducted in the field of cybersecurity under Trump presidency;
5. To analyze issues between Russia and USA governments under Trump;
6. To identify results of the Obama cybersecurity policy;
7. To study initiatives conducted in the field of cybersecurity under Biden presidency;
8. To analyze issues between Russia and USA governments under Biden.

The issue of the struggle between Russia and the United States in the field of cybersecurity has been studied quite well.

As for Russian scholars, the memorable work in this field was made by Demidov O. and Angmar M., “US Cyber Strategy 2018. Implications for the Global Dialogue on ICT Behavior and U.S.-Russian Relations”[[1]](#footnote-1). Their work was dedicated to the information policy during Trump’s presidency, and there are also references to Obama’s presidency as well. In their study they also have explored in detail US National Cyber Strategy and showed how important this document is.

Among other Russian scholars the following can be identified: Smekalova M.[[2]](#footnote-2), Smirnov A.[[3]](#footnote-3), Shakirov O.[[4]](#footnote-4), Stadnik I.[[5]](#footnote-5), and others.

The most memorable foreign scholars work was Powers G. “U.S. National Cybersecurity: Strategic Challenges and Opportunities”[[6]](#footnote-6). It is a book which describes challenges faced by the federal government in addressing a strategic approach to cybersecurity and shows what steps were made by Obama’s government to avoid problems and create stable situation.

Among the most important foreign scholars can be identified the following: D’ambrosio A.[[7]](#footnote-7), La Fleur C.[[8]](#footnote-8), Boussios E.[[9]](#footnote-9) and others.

The source base of this master thesis work is:

1. USA national documents;
2. Documents of the Congress;
3. Sources of executive authority;
4. Reports of Mass-Media;
5. Sources of international organizations.

According to the analyses of the literature we can conclude that still no one among scholars tried to consider three USA presidents at one time and to compare their efforts in the field of cybersecurity, as well as no one earlier has studied Biden impact in this field. Most works are also out of date. All this causes **academic novelty** of this research.

This master thesis consists of the introduction, three chapters, conclusion and bibliography. In the first chapter, the author analyzes actions of government under Obama presidency to strengthen USA cybersecurity, issues in the realtions between USA and Russia in this field and results of Obama presidency in this sphere. In the second chapter the author analyze Donald Trump efforts to preserve and enhance cybersecurity of the USA and to solve issues in bilateral relations with Russia. The third chapter focuses on the analyses of the Joseph Biden administration, its efforts to strengthen USA cybersecurity and to solve issues in US-Russian relations.

**CHAPTER I: OBAMA’S GOVERNMENT ACTIONS TO STRENGTHEN THE USA CYBERSECURITY**

The chapter is devoted to reviewing and further analyzing the actions of the government under Obama to strengthen cybersecurity. The main idea is to show the efforts made by the government in strengthening cybersecurity, as well as to identify problems in this area related to bilateral relations between the US and Russia. The results and criticism of the policy pursued by Obama in this field are also considered in the end of the chapter.

***1.1 Initiatives conducted in the field of cybersecurity under Obama presidency and their impact***

On January 20, 2009, Barack Obama assumed the presidency of the American state. He served as president for two whole presidential terms, leaving the post on January 20, 2017. His policy was flexible, but quite aggressive, especially in relation to Russia, in particular in the field of cybersecurity. Some of his initiatives met with approval, others with criticism, but when he left the presidency his approval rating was 60%[[10]](#footnote-10) - a fairly high figure compared to other US presidents.

Obama and his government launched an active cybersecurity policy in May 2009. The official statement said the executive branch was instructed to work closely with all key players in the field of US cybersecurity, including state and local governments, as well as the private sector, to ensure an organized and uniform response to future cyber incidents; strengthen public-private partnerships to find technological solutions that keep the United States safe and prosperous; invest in the cutting-edge research and development needed to innovate and discover to meet the digital challenges of our time; and start a campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms and start building the digital workforce of the 21st century[[11]](#footnote-11).

As the basis of its policy, the government under Obama decided to choose the Cyberspace Policy Review build on the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23) in January 8th, 2008[[12]](#footnote-12).

In particular, in the document were indicated the following goals, designed to help secure the United States in cyberspace: **“To establish a front line of defense against today’s immediate threats** by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government—and ultimately with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions.”, “To defend against the full spectrum of threats by enhancing U.S. counter intelligence capabilities and increasing the security of the supply chain for key information technologies.” and “To strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.”[[13]](#footnote-13)

Another important cybersecurity policy framework introduced shortly after Obama and the new government took office was the GPRA Modernization Act of 2010 and the Cross-Agency Priority (CAP) Goals it established. It was a tool used to accelerate progress in a limited number of priority areas where implementation requires active collaboration across multiple agencies, overcoming organizational barriers to achieve more than one agency alone can achieve.

Established or reviewed at least every four years, CAP objectives include results-based objectives that cover a limited number of cross-cutting policy areas, as well as management objectives aimed at improving management within the Federal Government in the areas of financial management, information technology management, strategic human capital management, procurement and acquisition management, and real property management.

In the 2015 budget, a set of 16 CAP targets were announced with clear views of reporting entities, data-driven reviews, discovery of a wide range of quantitative and observed data, and reports for general websites as a framework to drive performance improvements on cross-government collaboration and tackle nationwide management challenges affecting most agencies.

The Continuous Diagnostics and Mitigation (CDM)[[14]](#footnote-14) Program was developed in 2012 to support government and specific institutions efforts to provide risk-based, consistent, and cost-effective cybersecurity solutions to protect federal civilian networks across all organizational levels.

The CDM Program provides a energetic approach to enhancing the cybersecurity of government networks and systems. The CDM Program ensures cybersecurity instruments, integration services, and dashboards that assist participating agencies improve their security situation.

The CDM program provides a dynamic approach to strengthening the cybersecurity of government networks and systems. The CDM program provides cybersecurity tools, integration services, and dashboards to help participating agencies increase their level of security.

Later in December 2014, Obama signed five new cybersecurity laws. It was the first time in 12 years that cybersecurity laws actually went into effect, passed Congress, and were signed into law. The previous such law was the E-Government Act of 2002[[15]](#footnote-15).

The first of these laws was Federal Information Security Modernization Act of 2014 (FISMA)[[16]](#footnote-16), and in essence it was a modernization of the E-Government Act of 2002. Under the new guidelines, agencies are required on an ongoing basis to monitor the status and vulnerabilities within their systems, as well as provide an assessment of the effectiveness of such checks and protective procedures. The document also clarified the responsibilities and tasks of several positions whose activities are directly related to the threats of information leaks or countering cyber attacks, especially in comparison with the previous law. In general, with this document, Obama was able to achieve a more transparent policy in the field of cybersecurity. Expected activities to protect against cyber threats have become more specific, and some approaches have been changed.

The second document which was also signed in 2014 was Border Patrol Agent Pay Reform Act of 2014[[17]](#footnote-17). This act is mainly concerned with the activities of the Department of Homeland Security (DHS)[[18]](#footnote-18). The organization was created in 2002 after the events of September 11, and at the moment its main goals are the following: combat all forms of terrorism and targeted violence; increase cybersecurity; secure our borders and modernize ports of entry; build a fair, orderly, and humane immigration system; ready the nation to respond to and recover from disasters and combat the climate crisis; combat human trafficking, labor exploitation, and child exploitation[[19]](#footnote-19).

The act helps to determine the necessary IT security skills that staff should have. It was understood that the act will help increase the competitiveness of the DHS within the US cybersecurity framework, as well as simplify the selection of highly qualified personnel in the field of cybersecurity.

The third document was Cybersecurity Workforce Assessment Act of 2014[[20]](#footnote-20). The key provision of the documents sounds as the following: “Not later than 180 days after the date of enactment of this Act, and annually thereafter for 3 years, the Secretary shall assess the cybersecurity workforce of the Department.” The idea of this act was to improve DHS performance by conducting ongoing reviews of the performance of the cybersecurity workforce, and by creating alternative ways to improve the skills, readiness, recruitment, and retention of cybersecurity employees.

The fourth act was National Cybersecurity Protection Act of 2014[[21]](#footnote-21), and it creates National Cybersecurity and Communications Integration Center (NCCIC). NCCIC is a key tool for responding to cyberthreat situations, as well as a key cybersecurity and communications link for the federal government, intelligence and law enforcement agencies. The main activity of the organization is the monitoring of intrusions, vulnerabilities, the exchange of information between sectors of the state and the mitigation of the consequences of cyber attacks and various cyber incidents. NCCIC became a part of DHS.

The fifth act was Cybersecurity Enhancement Act of 2014[[22]](#footnote-22). According to this law, the Department of Commerce acquired the ability to sponsor structures critical to the state in the field of cybersecurity using one of its divisions, the National Institute of Standards and Technology. Moreover, according to the new act, the Office of Science and Technology Policy was ordered to develop a new plan at the federal level regarding research, development and innovation in the field of cybersecurity.

The Obama administration then decided to reinforce its cybersecurity policy by implementing the Cybersecurity Strategy and Implementation Plan (CSIP)[[23]](#footnote-23) for the Federal Civilian Government (October 30, 2015 as a result of the 2015 comprehensive review of the Federal Government's cybersecurity policies, procedures, as well as practices by the Cybersecurity Sprint Team. Its intention was to identify and address critical cybersecurity gaps and emerging priorities, and give particular suggestions to address those gaps and priorities. The five objectives of CSIP are: Prioritized Identification and Protection of high value information and assets; Timely Detection of and Rapid Response to cyber incidents; Rapid Recovery from incidents when they occur and Accelerated Adoption of lessons learned from the [Cybersecurity] Sprint assessment; Recruitment and Retention of the most highly-qualified Cybersecurity Workforce talent the Federal Government can bring to bear; and Efficient and Effective Acquisition and Deployment of Existing and Emerging Technology.

The next step of Obama’s government was adoption and signing of the Cybersecurity Act of 2015[[24]](#footnote-24). The Cybersecurity Act creates a web-portal which helps to DHS and its National Cybersecurity and Communications Integration Center to facilitate the exchange of cyber threat information between the private and public sectors, and explains the NCCIC's statutory logic in assessing and responding to cybersecurity threats and indicators. The web-portal named Automated Indicator Sharing (AIS)[[25]](#footnote-25) was created and adopted in March 2016 by the Cybersecurity and Infrastructure Security Agency[[26]](#footnote-26). The Cyber ​​and Infrastructure Security Agency (CISA) was tasked with providing a common security baseline for the Federal Civil Executive Branch (FCEB) and helping agencies manage their cyber risks. This common baseline is given in part through the EINSTEIN framework[[27]](#footnote-27). EINSTEIN serves two key roles in FCEB cybersecurity. Firstly, EINSTEIN identifies and squares cyberattacks aimed at compromising federal agencies. Secondly, EINSTEIN provides CISA with the situational mindfulness to utilize threat intelligence found in one agency to protect the rest of the government and to assist the private segment protect itself.

CISA has also created a guide to help non-government organizations share cyber threat indicators with the federal government. In addition, the organization explained the policy and required procedures regarding the receipt and use of cyber threat indicators by federal agencies, as well as all the privacy and civil liberties principles associated with the exchange of cyber security threat indicators. Special guidance was also created and adapted for federal agencies on the exchange of information as part of the functioning of government information mechanisms.

The Cybersecurity Act of 2015 allows the President to transfer authority and responsibility for the collection and dissemination of information about cybersecurity threats to organizations other than the NCCIC, including outside of DHS. However, this role cannot be transferred to the US Department of Defense. The law gives DHS the right, at its discretion, to disclose information related to cybersecurity threats obtained through the information portal to other organizations, including various agencies and the private sector. However, it is also DHS's responsibility to remove any personal information that could put the whistleblower at risk. The law also exempts generic cyber threat indicators from disclosure under the Freedom of Information Act (FOIA)[[28]](#footnote-28) and open government laws. FOIA is a federal law that gives the public the right to request documents from a federal agency. Agencies can withhold information in accordance with nine exceptions contained in the law. The FOIA applies only to federal agencies. This does not apply to records held by Congress, the courts, state or local government agencies. Each state has its own public access laws which should be reviewed to gain access to state and local records. FOIA was updated in 2016 to the FOIA Improvement Act of 2016[[29]](#footnote-29).

According to the wording of the law emphasizes, participation in the information exchange system is exclusively voluntary. However, the Law notes that participation may be required due to changes in industry standards or by contract.

In some circumstances, it is possible that threat indicators may be intertwined with personal information. As such, the law requires individuals who directly share information to delete all personal information before submitting it for review, and DHS itself must also delete personal information upon review, preventing further disclosure. Another function of this act is that it restricts the use of information about threats in the field of cybersecurity, and also exempts it from the FOIA, while imposing requirements for the protection of information about threats that contains personal information.

Section 104 of the Cybersecurity Act of 2015 specifies a requirement that individuals must identify and delete such personal information that is not directly related to a cybersecurity threat before sharing information under the Act. There is also Section 103, which describes the requirement to develop procedures to identify and delete information that is not directly related to a cybersecurity threat that a federal agency recognizes during a review as personal information that identifies a specific individual. There are also procedures in place to notify those individuals whose personal information has been disseminated and disclosed in violation of the law. All this is a tool, created within a single act, that allows you to clean up information, report problems, and prevent the dissemination of information, in particular personal information that is not valuable in achieving cybersecurity goals. Section 107 of this act stipulates several oversight mechanisms, including those for the protection of confidentiality, related to the control and deletion of personal information.

On February 9, 2016, Obama instructed the government to implement Cybersecurity National Action Plan (CNAP)[[30]](#footnote-30). The plan included actions in the short and long term regarding raising awareness and increasing protection in the field of cybersecurity in general. In addition, it affects public security, economic and national. He also had to realize the opportunity for Americans to better control their digital space.

The government under the leadership of Obama has been developing this document for 7 years. According to the US government, they took into account all the mistakes and all the experience accumulated during this period of time, and even took into account all the experience of past years. The document is entirely devoted to cybersecurity, in particular, trends, threats and intrusions in this area. The plan itself was intended as a guideline for the federal government, and outlined actions that were supposed to help create and improve the cybersecurity environment not only for the federal government, but also for the private sector and the privacy of citizens.

As part of the CNAP President Obama set up the Commission on strengthening National Cybersecurity[[31]](#footnote-31). The Commission completed its presentation on December 1, 2016, submitting detailed short term and long term recommendations for strengthening cybersecurity in both the state and private sectors while protecting privacy, stimulating innovation and providing economic and national security. To build on their recommendations, the Commissioners sought advice with technical and policy experts, solicited public contribution through public consultations and requests for information, and reviewed the existing literature. The report highlights the need for public-private partnerships as well as international participation. It also discusses the role consumers in enhancing our digital security. The report divides recommendations into six overarching imperatives focused on investment, infrastructure, consumer education, workforce opportunities, government operations, and demands for a fair and open global digital economy.

The report emphasizes the require for organizations between the open and private divisions, as well as worldwide engagement. It too talks about the part buyers must play in improving our advanced security. The report categorizes its suggestions inside six overarching goals centered on foundation, venture, buyer instruction, workforce capabilities, government operations and prerequisites for a reasonable and open worldwide computerized economy.

Another imperative arrangement within the system of the CNAP was to modernize Government IT and change how the Government oversees cybersecurity through the proposition of a $3.1 billion Information Technology Modernization Support, which is able empower the retirement, substitution, and modernization of bequest IT that's troublesome to secure and costly to preserve, as well as the arrangement of a modern position – the Government Chief Information Security Officer – to drive these changes over the Government.

The Technology Modernization Fund (TMF)[[32]](#footnote-32) was authorized by the Modernizing Government Technology Act of 2017. The TMF is directed by the Technology Modernization Board, comprised of Government IT pioneers speaking to demonstrated ability in innovation, transformation, and operations. Agencies submit IT-related project proposition for the Board to review and consider. Agencies yield technology modernization proposals to the Board through a two-phased endorsement process.

 In CNAP was also proposed to empower Americans to secure their online accounts by moving past fair passwords and including an additional layer of securit. By judiciously combining a solid secret word with extra variables, such as a unique finger impression or a single utilize code conveyed in a content message, Americans can make their accounts indeed more secure. This focus on multi-factor verification will be central to a new National Cybersecurity Awareness Campaign propelled by the National Cyber Security Alliance[[33]](#footnote-33) designed to arm customers with straightforward and noteworthy data to ensure themselves in an progressively computerized world.. The National Cyber Security Alliance will partner with leading technology firms like Google, Facebook, DropBox, and Microsoft to form it simpler for millions of clients to secure their online accounts, and money related administrations companies such as MasterCard, Visa, PayPal, and Venmo that are making transactions more secure. In addition, the Federal Government will take steps to to protect individual information in online exchanges between citizens and the government, counting through a modern activity arrange to drive the Federal Government’s adoption and use of effective identity proofing and strong multi-factor authentication strategies and a systematic review of where the Federal Government can decrease dependence on Social Security Numbers as an identifier of citizens.

Within the CNAP system also appeared the idea to contribute over $19 billion for cybersecurity as part of the President’s Fiscal Year (FY) 2017 Budget. This speaks to a more than 35 percent increase from FY 2016 in overall Federal resources for cybersecurity, a fundamental investment to secure our Nation in the future.

The Administration has created the position of Federal Chief Information Security Officer to drive cybersecurity policy, arranging, and execution across the Federal Government. The primary time that there will be a committed senior official who is exclusively centered on developing, overseeing, and planning cybersecurity procedure, approach, and operations over the whole Government space.

The Administration is requiring agencies to identify and prioritize their highest value and most at-risk IT resources and after that take extra concrete steps to move forward their security.

The Department of Homeland Security, the General Services Administration, and other Federal agencies will increment the availability of government-wide shared services for IT and cybersecurity, with the objective of taking each individual agency out of the commerce of building, owning, and working their claim IT when more proficient, viable, and secure alternatives are accessible, as well as guaranteeing that individual agencies are not cleared out on their possess to protect themselves against the foremost modern dangers.

The Federal Government, through endeavors such as the National Initiative for Cybersecurity Education, will improve cybersecurity education and preparing across the nation and enlist more cybersecurity experts to secure Federal agencies. The National Initiative for Cybersecurity Education (NICE)[[34]](#footnote-34), driven by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, is a partnership between government, the scholarly world, and the private segment centered on cybersecurity instruction, preparing, and workforce improvement. The mission of NICE is to energize, advance, and arrange a vigorous community working together to progress an coordinates biological system of cybersecurity instruction, preparing, and workforce improvement. NICE fulfills this mission by planning with government, academic, and industry accomplices to construct on existing effective programs, encourage alter and advancement, and bring leadership and vision to extend the number of talented cybersecurity experts making a difference to keep our Nation secure.

As part of the President’s Cybersecurity National Action Plan, the Administration also discharged the 2016 Federal Cybersecurity Research and Development Strategic Plan [[35]](#footnote-35), which was facilitated by the National Science and Technology Council. This is often the foremost comprehensive government cybersecurity research and development (R&D) arrange to date. With the objective of making cyberspace inherently more secure, the arrange challenges the cybersecurity R&D community to supply strategies and instruments for discouraging, securing, identifying, and adjusting to malicious cyber exercises. The plan characterizes near-, mid-, and long-term objectives to direct and assess advance. The plan’s objective for the close term is to realize science and technology (S&T) progresses that counter adversaries’ asymmetrical preferences with compelling and productive risk management. To do this, organizations got to better understand the extend of vulnerabilities and threats they confront in cyberspace, and to hone evidence-based risk management, which is the method of identifying, surveying, and reacting to risk, counting the advancement of successful and measurable controls. To make the best choices, organizations require solid information on the viability of security controls and their operational affect in practical situations, reflecting the behavior of users, defenders, and adversaries. Understanding which measures will be viable against pernicious cyber exercises will lower cybersecurity dangers. The plan’s goal for the mid-term is to invert adversaries’ asymmetrical focal points by creating economically secure frameworks and operations. To form malevolent cyber exercises more difficult, organizations must decrease the rewards of such exercises by making strides the efficacy and productivity of their defenses by a few orders of magnitude without setting undue burden on users. The plan’s long-term objective is to attain S&T progresses that discourage pernicious cyber exercises, by expanding adversaries’ costs and dangers, whereas moreover bringing down their gains. Measuring the exertion required and the likely results for malevolent exercises is basic to understanding how to successfully prevent such exercises. This requires unused scientific capacities that dependably distinguish the perpetrator rapidly sufficient to take action, without compromising free discourse, or namelessness for those who are doing nothing off-base. If the probability of their revelation is expanded and it gets to be clear they will endure negative results, numerous potential actors would do without malicious exercises.

In conjunction with CNAP the President also built up the Commission on Enhancing National Cybersecurity[[36]](#footnote-36) to supply proposals on activities that can be taken over the following decade to reinforce cybersecurity, counting encourage ventures in research and development activities. Whereas their work is fair starting, the Federal Cybersecurity Research and Development Strategic Plan will give the Commission a profitable reference point as they consider the challenges and openings in cybersecurity R&D.

***1.2 Interaction in the field of cybersecurity between Russia and the United States under Obama’s presidency***

Russia and USA has long term relations with great tension. The efforts of both sides to build profitable trusting relationships between both countries have not brought visible changes for a long time. The area of cybersecurity for both countries at the beginning of the Obama’s presidency was already recognized as a critical element of their national securities. Therefore, both countries sought to find a common language in this area, seeking neutrality and mutual cooperation in order to strengthen their positions in the international arena.

During Obama's presidency and even after that, with reference to the period of his presidency, Russia was often accused of carrying out cyberattacks and generally violating US cyber security. Moreover, as a rule, there was no hard evidence of Russian intervention and there is still no evidence.

In August 2016, then CIA director John Brennan had a scheduled phone call with Alexander Bortnikov. But Brennan said he confronted Bortnikov that day on a separate, urgent issue: mounting evidence of Russian interference in the upcoming presidential election. By then, media outlets were reporting on growing consensus that Russia was behind the hacking of the Democratic National Committee. “I told him that if they were doing this, this would be a grave mistake,” Brennan recalled. “That it was going to roil the relations between the United States and Russia for many years to come. That all Americans would be outraged over it, even if the Russians were trying to advance the prospects of candidates that some Americans were in favor of, because the American people take very seriously the importance of the integrity and the freedom of our election system.”

On a late July day in 2016, Donald Trump, nominee for president, stood at a lectern in Florida, next to an American flag, and urged a US adversary to become involved in the election campaign and find tens of thousands of emails wiped from the server of his Democratic opponent, Hillary Clinton.

“Russia, if you’re listening,” he said at a news conference at one of his resorts, “I hope you’re able to find the 30,000 emails that are missing.”

That same day, July 27, several Russian government hackers launched an attack against the email accounts of staffers in Clinton’s personal office, according to a sweeping indictment Friday by special counsel Robert S. Mueller III. At or around the same time, the hackers also targeted 76 email addresses used by the Clinton campaign, investigators said[[37]](#footnote-37).

Although the broad outlines of the hacking and influence campaign have been widely reported, the indictment describes for the first time the identities, techniques and tactics of the operation to disrupt American democracy[[38]](#footnote-38).

It includes details on how the Russians, using an encrypted file with instructions, delivered their trove of hacked emails to WikiLeaks, the online anti-secrecy organization led by Julian Assange that became the main platform for the Russians to display their trove of hacked emails.

The hackers worked for the spy agency called the Main Intelligence Directorate of the General Staff, or GRU, the indictment said.

They also allegedly targeted a state election board, identified by U.S. officials as Illinois. The Russians stole information about 500,000 voters, including names, addresses, partial Social Security numbers, dates of birth and driver’s license numbers, according to the indictment.

At the same time, U.S. Attorney General William Barr's report states that, according to Mueller's findings, “the investigation did not establish that members of the Trump campaign conspired with the Russian authorities to interfere in the election, or in any way coordinated with them [[39]](#footnote-39).”

In 2018 there was another statement made by Victoria Nuland, who served as assistant secretary of state for Europe during the Obama administration. She told that she had been briefed as early as December 2015 about the hacking of the Democratic National Committee and that the intrusion had all the hallmarks of a Russian operation[[40]](#footnote-40). Still she couldn’t provide any evidences.

The cybersecurity head for Barack Obama government, Michael Daniel, stated that it is “highly likely”[[41]](#footnote-41) that Russian hackers scanned electoral systems ahead of the 2016 elections for vulnerabilities. Moreover, at first it was claimed that 21 states were subjected to cyberattacks, and then two years later it was believed that all 50 states were attacked. No direct or even indirect evidence was provided, however, according to Michael Daniel “It is more likely that we hadn't detected it than that it didn't occur.”[[42]](#footnote-42)

The official position of the Obama administration on this issue was as follows: “Russia’s cyber activities were intended to influence the election, erode faith in U.S. democratic institutions, sow doubt about the integrity of our electoral process, and undermine confidence in the institutions of the U.S. government. These actions are unacceptable and will not be tolerated.[[43]](#footnote-43)”, and “In addition to holding Russia accountable for what it has done, the United States and friends and allies around the world must work together to oppose Russia’s efforts to undermine established international norms of behavior, and interfere with democratic governance.[[44]](#footnote-44)”

Russian presidential aide Yuri Ushakov commented on the statement of one of Obama's advisers, Ben Rhodes, that Putin could not help but be aware of hacker attacks on the Democratic Party and its candidate in the elections, Hillary Clinton. He confirmed that the presidents of Russia and the United States discussed this topic on the sidelines of the G20 summit in China on September 5, 2016[[45]](#footnote-45). However, in the end, no consensus was reached on this issue, and the parties only expressed their opinions to each other on this issue.

In response to the threat to U.S. national security posed by Russian interference in US elections, Obama has approved an amendment to Executive Order 13964, Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities[[46]](#footnote-46). As originally issued in April 2015, this Executive Order created a new, targeted authority for the U.S. government to respond more effectively to the most significant of cyber threats, particularly in situations where malicious cyber actors operate beyond the reach of existing authorities. The President has sanctioned nine entities and individuals: two Russian intelligence services (the GRU and the FSB); four individual officers of the GRU; and three companies that provided material support to the GRU’s cyber operations.

Russian officials condemned the decision of US President Barack Obama, but did not say what kind of retaliatory measures would follow. “We consider such decisions and such sanctions unreasonable and illegal from the point of view of international law,” Dmitry Peskov, press secretary of the Russian president, told reporters[[47]](#footnote-47).

The Department of Homeland Security and Federal Bureau of Investigation released a Joint Analysis Report (JAR) in December 29, 2016[[48]](#footnote-48). It contains declassified technical information on Russian civilian and military intelligence services’ malicious cyber activity, to better help network defenders in the United States and abroad identify, detect, and disrupt Russia’s global campaign of malicious cyber activities.

This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. The U.S. Government is referring to this malicious cyber activity by RIS as GRIZZLY STEPPE.

The JAR includes information on computers around the world that Russian intelligence services have co-opted without the knowledge of their owners in order to conduct their malicious activity in a way that makes it difficult to trace back to Russia. In some cases, the cybersecurity community was aware of this infrastructure, in other cases, this information is newly declassified by the U.S. government.

The report also includes data that enables cybersecurity firms and other network defenders to identify certain malware that the Russian intelligence services use. Network defenders can use this information to identify and block Russian malware, forcing the Russian intelligence services to re-engineer their malware. This information is newly de-classified.

 Finally, the JAR includes information on how Russian intelligence services typically conduct their activities. This information can help network defenders better identify new tactics or techniques that a malicious actor might deploy or detect and disrupt an ongoing intrusion.

Such a document cannot be called friendly and aimed at bilateral cooperation. In addition, the absence of direct evidence does not increase the credibility of the accusations and does not inspire respect for American policy, at least in the field of cybersecurity. Such moves look unprofessional, especially against the backdrop of all the efforts that have been made by the Obama administration to strengthen US cybersecurity.

However, the Obama presidency also had a positive event that contributed to the improvement of relations between Russia and the United States in the field of cybersecurity. This is about U.S.-Russian Cooperation on Information and Communications Technology Security[[49]](#footnote-49).

The United States and Russia have signed this landmark agreement to reduce the risk of conflict in cyberspace through real-time communications about incidents of national security concern[[50]](#footnote-50).

The pact, the first of its kind, was announced in a statement issued by both countries Monday at the Group of Eight summit in Northern Ireland. The agreement was cast as part of a broader bilateral effort to improve cooperation, including on counterterrorism and weapons of mass destruction.

The United States and the Russian Federation are creating a new working group, under the auspices of the Bilateral Presidential Commission, dedicated to assessing emerging ICT threats and proposing concrete joint measures to address them.  This group will begin its practical activities within the next month.

The United States and the Russian Federation have also concluded a range of steps designed to increase transparency and reduce the possibility that a misunderstood cyber incident could create instability or a crisis in our bilateral relationship.  Taken together, they represent important progress by our two nations to build confidence and strengthen our relations in cyberspace; expand our shared understanding of threats appearing to emanate from each other’s territory; and prevent unnecessary escalation of ICT security incidents. In particular, were set: Links between Computer Emergency Response Teams; Exchange of Notifications through the Nuclear Risk Reduction Centers; White House-Kremlin Direct Communications Line.

Despite the poor start of bilateral relations between Russia and the United States in the field of cybersecurity under Obama, both sides were not very interested in developing such relations and exchanging experience, as practice shows. At the end of Obama's presidency, the 2016 presidential campaign scandal finally ended the good relationship between the two countries.

***1.3 Evaluating the effectiveness and results of the Obama’s government cybersecurity policy***

The Obama administration has made cybersecurity a top priority since the beginning of the Obama presidency and has mentioned its importance in virtually every address to US entities and citizens. Barack Obama, together with his government, developed and approved many acts, bills, initiatives and other documents related to cybersecurity. However, most of the efforts have not found their application in this area.

According to some experts, Obama and his government have done a lot of work, done a lot of useful and important things, including to make cybersecurity a strong area for the United States. But in the end, he failed to achieve either increased security for the government or for the private sector.

One of the most striking cases of failure was the problems associated with hacker attacks, allegedly organized by the Russian side, in order to prevent a fair election of the American president. These events came just at the end of Obama's presidency, and the fact that the leak could not be fixed and chaos ensued shows that all the efforts of the Obama administration in the field of cybersecurity were, if not futile, then insufficient. A big scandal erupted that undermined the credibility of Democratic presidential candidate Hillary Clinton, as well as future Republican President Trump, and the election in general. Moreover, information discrediting the competence of the Obama administration continued to appear even under the current President Trump, undermining his reputation as well[[51]](#footnote-51).

Kevin Murray, director of Murray Associates, said the following after the events: “The government can do as much policy as it wants, but if it doesn't solve the problem, what's the use?”[[52]](#footnote-52)

Paul Rosenzweig, founder of Red Branch Consulting, a former Department of Homeland Security (DHS) official under President George W. Bush, said: “They had the tools but failed to use them.”[[53]](#footnote-53)

The near-total lack of cybersecurity among the organizations and individuals that were the victims of the 2016 US election hacks clearly showed how far the American cybersecurity industry still has a long way to go before achieving excellence. The election story also fits well with the infiltration of the Office of Personnel Management[[54]](#footnote-54) as embarrassing symbol of public and private failures to protect against cyber threats, even years after improved cybersecurity became a cybersecurity key point[[55]](#footnote-55).

Several former federal government officials have been mixed in their assessment of the efforts and results of the Obama administration in the area of ​​cybersecurity. According to them, his administration has done a decent job of making cybersecurity more relevant to senior officials of related departments, but it would be better if such responsibility began to be inculcated sooner. In this case, the results, in their opinion, would be obtained much earlier and with increased efficiency.[[56]](#footnote-56)

Other very important cybersecurity missteps made by the Obama administration include the leak of several million classified documents belonging to US Army soldier Bradley Manning[[57]](#footnote-57) and former NSA contractor Edward Snowden[[58]](#footnote-58). These events undermined the credibility of the US government, which stated that it does not spy on its citizens, in addition, they showed that the US government is not able to protect itself even from internal threats.

Another failure of Obama and his administration, experts recognize two attempts to pass the law, in 2011 and 2015, respectively. Both times there was an attempt to pass legislation that was intended to improve cybersecurity for the American people, critical infrastructure, and the federal government's own networks and computers[[59]](#footnote-59). However, the proposal has never been implemented, in large part due to divergent views in Congress about its passage, as well as opposition from civil rights and privacy groups.

Another problem was the implementation of a project called EINSTEIN. EINSTEIN is a federal system which purpose is to detect and prevent cyber threats. It was later upgraded to EINSTEIN 3 Accelerated by DHS in 2015. But experts criticized the system, which by the time of its modernization was already very outdated, and its implementation deadline ended years before the modernization. Greg Touhill, deputy assistant secretary of cybersecurity operations and programs at DHS, famously said in November 2015 that, “Einstein 3 is really where we needed to be 15 years ago.”[[60]](#footnote-60)

In general, one of the most important problems of the Obama administration, which has gone further and passed on to the Trump and Biden administrations, became the need to balance between better cybersecurity and other needs such as privacy, civil rights, legitimate business and economic interests.

**CHAPTER II: US GOVERNMENT ACTIONS UNDER TRUMP TO STRENGTHEN CYBERSECURITY**

The chapter examines the activities of Donald Trump as President of the United States in the cyber field. In particular, documents are considered that were changed or created under his leadership, and the policy of the American president in relation to Russia in the field of cyber security is analyzed. In addition, the purpose of the chapter is also to disclose the results of Trump's cybersecurity activities throughout his presidency.

***2.1 Trump's administration actions to strengthen cybersecurity***

Donald John Trump is the 45th President of the United States from January 20, 2017 to January 20, 2021. During the years of Barack Obama's presidency, much has been done to develop cybersecurity. Therefore, Donald Trump had to deal with the system built by the previous administration. The period of his presidency is considered controversial in many issues, although he made a great contribution to the development of USA cybersecurity. It is also worth mentioning that with the advent of the Trump administration, the negative trends that manifested themselves in Russian-American relations reached an unprecedented level.

From the very beginning, the actions of the new American president showed his interest in the development of the cyber sphere. On May 11, 2017, Donald Trump signed legislation to strengthen the federal government's cybersecurity and protect the country's critical infrastructure from cyber attacks[[61]](#footnote-61).

Then the new president refused the results of the meeting held in Hamburg on July 7, 2017 between the presidents of the United States and Russia. Instead, the President of the United States on March 23 2018 signed a law clarifying the legal use of data abroad (Clarifying Lawful Overseas Use of Data Act - CLOUD Act[[62]](#footnote-62)), which made it easier for national intelligence agencies to obtain data from technological equipment supplied by American firms to any country[[63]](#footnote-63). In particular, the new law allowed American law enforcement agencies to gain access to the servers of American companies located outside the United States without notifying the state authorities and obtaining official permission from them. It follows from the text of the law that law enforcement agencies of other countries will also be able to access information posted on American servers by sending a request directly to the company, bypassing the standard procedure for political inquiry and actions under mutual legal assistance treaties. It is important that in this case we are talking exclusively about data provided by electronic communication or placed on cloud services. Other types of personal or corporate information are not covered by this law.

US Deputy Secretary of Justice R. Downing called the Act a model for international cooperation, standing above bilateral treaties on mutual legal assistance[[64]](#footnote-64). He also pointed out that the purpose of the law is to form a community of like-minded states respecting each other's rights, acting on the basis of the rule of law. According to the minister, the use of the CLOUD Act will reduce the number of conflict points in the laws of states. The adoption of this law is intended to contribute to the protection of citizens' data.

In December 2017, the US National Security Strategy was adopted[[65]](#footnote-65). It used the term “cyber” many times. The document also highlighted that revisionist forces such as China and Russia are using technology, propaganda and coercion to shape a world order that is contrary to the interests and values ​​of the United States.

On May 15, 2018, the US Department of Homeland Security Cybersecurity Strategy was published, spanning five years, listing the key goals and objectives facing the department until 2023[[66]](#footnote-66).

Moreover, the document identified five main areas of activity:

1) identification and assessment of risks;

2) reduction of vulnerabilities (within the framework of this area, the goal is set to protect the information systems of the federal government and other facilities);

3) reduction of threats, including prevention and termination of the use of cyberspace for illegal (criminal) purposes;

4) minimization of consequences - effective response to incidents;

5) increasing the overall level of cybersecurity through risk management and competent actions by the Ministry.

Not the last place in the document is taken by the issues of financing and international cooperation. The authors of the Strategy believe that the implementation of state tasks in the field of cybersecurity requires active interaction of states. Over the past 20 years, the UN has been the main international platform for discussing issues in this area[[67]](#footnote-67). Against the background of high-profile investigations of the alleged Russian interference in the internal affairs of the United States using ICT, this issue faded into the background, however, in the fall of 2018, Washington again put the issue of international cooperation on the agenda, proposing its own resolution on Promoting Responsible State Behavior in Cyberspace in the Context of International Security[[68]](#footnote-68).

On August 15, 2018, Donald Trump canceled the Presidential Policy Directive 20, which regulated the actions of American intelligence services and federal agencies in cyberspace[[69]](#footnote-69). It was about offensive cyberattacks, not defensive measures. This directive was canceled as a result of regular accusations against Russia of interference in the US presidential election and is justified by preventive measures to ensure the safety of the midterm elections to Congress, which took place on November 6, 2018.

On September 20, 2018, US President Donald Trump signed and approved a new United States National Cybersecurity Strategy[[70]](#footnote-70). The key threat highlighted in the document is the threat to freedom and democracy in the United States. The authors of the strategy referred to the sources of risks such as Russia, China, Iran, North Korea and international terrorism. The policy outlined in the document rests on four pillars: protecting American citizens, the country, and the American way of life; promoting American prosperity; keeping the peace by force; spread of American influence.

The new Strategy states that American private and public cybersecurity actors have been constantly exposed to external threats that have become more dangerous and frequent in recent times. Therefore, this new document (Strategy) was created to overcome these and new challenges, as well as to ensure technological excellence in the field of cybersecurity and improve the effectiveness of the community in the information technology field. The strategy allows the federal government to take any action to improve the state of cybersecurity in the United States.

Also in the US National Cyber Strategy, special attention was paid to the protection of transport and maritime infrastructure and operations in space, which was an important addition to the classic list of objects of critical importance. It seems that previous efforts to strengthen the area have been insufficient, as some sources indicate. This was an order approved by Trump in May 2017 “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure[[71]](#footnote-71)”. According to this document, government agencies must use all the measures available to them to ensure the protection of various areas, including those listed above.

Another important policy element identified in the new Strategy was the modernization of legislation in the field of electronic surveillance and computer crimes. It was planned to update the legislation on electronic surveillance and computer crimes to expand the ability of law enforcement agencies to legally collect the necessary evidence of criminal activity and conduct further operational investigative and judicial procedural actions. The collection of the necessary information could also take place outside the United States.

Significant emphasis in the Strategy was placed on actions that should contribute to the expansion of American influence in the world. One of these areas was the development of the capabilities of partner countries to counter cybercrime. When requested to assist US law enforcement agencies, states must have the appropriate technical capacity. To develop international cooperation in the field of countering cybercrime, the United States, according to the document, is ready to take a leading role in the development of compatible and mutually beneficial mechanisms that will facilitate effective cross-border exchange of information related to law enforcement and lower barriers to cooperation. The use of existing international instruments – the UN Convention on Combating Transnational Organized Crime and the G7 Network of 24-hour Contact Centers – would be promoted.

Under Trump’s presidency, the status of US Cyber ​​Command (US Cybercom) was raised to the status of an independent “command unit.” Thus, for the first time, it became on a par with nine other strategic combat units of the United States[[72]](#footnote-72). In November 2018, the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency Act No. 115-278 was passed[[73]](#footnote-73). According to this document, the US Department of Homeland Security's National Defense and Cybersecurity Directorate was reorganized into the Cybersecurity and Infrastructure Security Agency. The functionality of the new department has not changed: its sphere of responsibility includes issues related to the provision of general and cybersecurity of information infrastructure facilities, as well as federal programs in this area. But it is very important to note that the formed agency got out of the control of the Ministry, becoming an independent executive body. Thus, the status of the US Cyber Command in the military hierarchy was increased. Prior to that, it was subordinate to the Strategic Command of the US Armed Forces, which also operates nuclear weapons, missile defense and space forces. In early September 2020, it became known that Fortitude Hall, located in Fort Gordon near Augusta, Georgia, had become the headquarters of the US Army Cyber Command. Fort Gordon has also hosted the Army Liaison Corps, Cyber Center of Excellence, and other programs focused on network security, allowing the command to collaborate with mission partners. All this further strengthened the position of the US Cybercom in the military sphere.

It is also worth mentioning that following this event in 2018, the National Risk Management Center was created, the purpose of which is to protect information infrastructure facilities, including banking systems and power grids, from attacks.

Under Trump, one of the most common forms of the United States' fight against cybercrimes against information infrastructure facilities and the response to the actions of other states in the cybersphere has become sanctions. These sanctions were also often aimed at condemning the country for the actions it had already taken.

With the February 2019 “Defending American Security from Kremlin Aggression Act[[74]](#footnote-74)”, the Department of State created a cyberspace and digital economy policy department. This law aims to support international cybersecurity and ensure access to the Internet. It also covered the fight against cybercrime extensively. The Act specifies that the department must cooperate with other divisions of the Department of State in opposing actions carried out by or on behalf of Russia and aimed at undermining US cybersecurity or state democracy. The head of the department should act as a leading link in the fight against the use of cybertools by terrorists, make recommendations to the Secretary of State, jointly with other departments to respond to cyber incidents of a nationwide scale, and analyze cyber threats. In addition, American diplomats should also be involved in strengthening cybersecurity.

In March 2019, US President Donald Trump ordered the federal authorities to determine the format for responding to threats to critical information infrastructures emanating from electromagnetic pulses, intense sound waves provoked, among other things, by cyberattacks[[75]](#footnote-75). A large-scale electromagnetic pulse can seriously harm the economy, suspend the operation of thermal power plants, transport infrastructure, etc., and also threaten with large human losses.

During his presidency, Donald Trump managed to change a lot in the field of US cybersecurity and directed America on a new, as it will become clear later, more aggressive course. Despite the controversial effectiveness of many documents, ultimately the efforts and funds that have been invested in this area are well tracked, and it is safe to say that cybersecurity has become one of the key areas of Donald Trump's policy.

***2.2 Issues of relations between Russia and the United States in the field of cybersecurity under Trump***

Until the end of Obama's presidency, there remained a bilateral format of interaction, where nothing constructive had happened since 2014, when the Russian-American agreements on confidence-building measures in the field of cybersecurity, signed by Vladimir Putin and Barack Obama just a year earlier, in June 2013, were frozen. Trying to restore the 2013 mechanism now is a hopeless project for Donald Trump, primarily because both party wings of the American Congress are putting serious pressure on the White House and forcing Trump to follow a hard line with respect to Russia, including on countering the “Russian threat in cyberspace”[[76]](#footnote-76).

On July 7, 2017, during the G20 meeting, a meeting was also held between US President Donald Trump and Russian President Vladimir Putin. They discussed the possibility of creating a joint working group on cybersecurity. After the meeting, the Russian President said that agreements in this area had been reached, but soon the American President also announced that no specific agreements had been reached. “The fact that President Putin and I discussed the cybersecurity working group does not mean that I believe it can be created. It cannot”, Trump wrote on his Twitter microblog[[77]](#footnote-77). This clearly shows the difference between Trump's own intentions and what he is forced to do in connection with the pressure from the Congress. Probably returning to his homeland and consulting with his supporters, he decided to withdraw his consent to create a joint Russian-US working group in the field of cybersecurity. If he accepted such an offer, he could again be accused of aiding Russian politics, etc.

The most scandalous event during the entire period of Trump's rule for Russia was the creation of the US National Cyber Strategy. The document has become a unique tool in the 15 years preceding its signing and has presented the US cyber industry with many special opportunities.

Ever since the Obama administration, Russia has been identified by America as one of the main threats to US national security in many areas, including cyberspace. In September 2018, this course was reaffirmed both in the new Cyber Strategy and in official statements[[78]](#footnote-78). The US National Cyber ​​Strategy, which was signed by Trump in 2018, is very similar to its predecessor, the 2015 US Department of Defense Cyber ​​Strategies issued under Obama. Thus, the course of confronting Russia has not so much remained the same as it has intensified, despite all the speeches in the direction of Trump, who was often accused of being soft on Russia.

US National Security Adviser John Bolton, speaking at a press conference in Washington to mark the unveiling of a new cyber strategy, said the White House «has authorized offensive cyber operations ... to create deterrent structures that will demonstrate to the adversaries that the cost of their participation in operations against us is higher than they expect[[79]](#footnote-79).»

The 2018 U.S. National Cyber Strategy states that «Russia, Iran, and North Korea conducted reckless cyber attacks that harmed American and international businesses and our allies and partners without paying costs likely to deter future cyber aggression[[80]](#footnote-80).» A similar message can be found in the Pentagon's 2018 cyber strategy[[81]](#footnote-81): «Russia has used cyber-enabled information operations to influence our population and challenge our democratic processes. Other actors, such as North Korea and Iran, have similarly employed malicious cyber activities to harm U.S. citizens and threaten U.S. interests ... Our focus will be on the States that can pose strategic threats to U.S. prosperity and security, particularly China and Russia.» It is significant that this is not the first time that the United States has officially called Russia an adversary in its doctrinal documents.

With regard to the Pentagon's cyber strategy, this document emphasizes the need to “create more deadly forces (lethal force)[[82]](#footnote-82).” Thus, this is already an open expression of aggressive intentions, and the Trump administration is giving the Pentagon the green light for cyberattacks around the world. Considering that there is no clear definition of “malicious acts in cyberspace” in international law, anything can be summed up under such operations[[83]](#footnote-83).

After the release of the US National Cyber ​​Strategy, the US Department of Homeland Security issued a statement that “it used its powers to get government agencies to remove Kaspersky Lab's[[84]](#footnote-84) antivirus products from their systems.” This was considered a temporary restriction that came into effect on October 1, 2018, but later the Governing Council for Federal Procurement, which includes the US Department of Defense, the US General Services Administration and the National Aeronautics and Space Administration (NASA), introduced a permanent ban on the purchase of products «Kaspersky Labs» for American government agencies. The document entered into force on September 10, 2019[[85]](#footnote-85). The event once again highlighted distrust in relation to the Russian cyber sphere, and also showed that the tension only continues to grow.

In general, the degree of aggressiveness of the US cybersecurity policy, in particular with respect to Russia, is well traced. Despite all the efforts on the part of Russia and its willingness to have a dialogue and discuss many issues, the United States under Trump tended to ignore any requests and statements[[86]](#footnote-86).

Another scandal during the Trump presidency was the «possible» interference of Russian hackers in US domestic politics, including elections. The first reports of Russian interference in the US electoral process appeared at the height of the presidential campaign in July 2016, after the hacking of the correspondence of the leadership of the US Democratic Party, which was published on the WikiLeaks website[[87]](#footnote-87). Then it turned out that during the primaries, the National Committee of the party supported ex-Secretary of State Hillary Clinton, acting to the detriment of Bernie Sanders. Clinton then claimed that Russian hackers were involved in the hacking of the mail and that she had "reliable information" about Moscow's intention to influence the course of the presidential elections. According to WikiLeaks, the documents were obtained from insiders in the Democratic Party[[88]](#footnote-88).

On January 6, 2017, the Office of the Director of National Intelligence (which coordinates the work of the US intelligence community, which includes 17 departments) published a report, which stated "with a high degree of certainty" that hacker attacks on computer systems in the United States were undertaken at the personal direction of President Vladimir Putin with the aim of «undermine public confidence in the US democratic process» and discredit Clinton to boost Trump's chances. There is no direct evidence in favor of this version in the report. The refusal to publish them was explained by the need to protect the sources of information[[89]](#footnote-89).

On June 5, 2017, The Intercept published excerpts from a report by the National Security Agency (NSA), which claimed that the GRU of the General Staff of the Russian Armed Forces carried out a cyberattack on a software provider used in voting in the United States. The portal did not provide information confirming the involvement of Russian intelligence in the hacker attacks[[90]](#footnote-90).

An investigation into Russia's alleged election interference began almost immediately after Trump's election on November 8, 2016. It was chaired by the Justice Department, intelligence agencies and both houses of Congress. In addition, in May 2017, the US Department of Justice appointed a special attorney. Several congressional hearings were devoted to the progress of the investigation. So, on March 20, 2017, the FBI Director James Comey and the head of the NSA, Michael Rogers, addressed the House Intelligence Committee. When asked if there was direct evidence that Russia had manipulated voting results in vacillating states, both responded that they had no such data. On May 3, a similar hearing was held by the Senate Judiciary Committee, where Komi was also unable to provide evidence of Russia's involvement in the US election campaign[[91]](#footnote-91).

But it didn't end there. On October 28, 2019, there was a wave of hacker attacks on Georgian state institutions and the media. The Foreign Ministries of the United Kingdom, the United States and Georgia have blamed the Russian military's intelligence unit known as the GRU for this massive cyber attack. "The cyberattack was directed against the national security of Georgia," the Georgian Foreign Ministry said in a statement. Tbilisi believes that Russian hackers, at the direction of the Russian command, deliberately tried to paralyze the activities of many institutions, cause panic among the people and thus harm Georgian citizens. Washington and London made their statements at the same time as the Georgian Foreign Ministry – and they also blamed Moscow for the attacks[[92]](#footnote-92).

On April 20, 2020, a large-scale cyberattack took place on the subjects of healthcare in the Czech Republic. According to the Lidové noviny newspaper, a foreign state may be behind the cyberattacks, and hacker groups from Russia may be involved. «The organizer is a foreign country. It is beginning to become clear that Russia may be behind this. IP addresses lead there», a high-ranking officer who is part of the team of investigators told the newspaper[[93]](#footnote-93). His words were confirmed by a member of the Czech Security Council. America supported the Czech Republic and US Secretary Mike Pompeo warned that such attacks will not go unpunished. The Russian Embassy on its Facebook page called the publications «fake news».

On December 13, 2020, the New York Times reported that The Treasury Department was one of the agencies targeted by the hackers. «The Trump administration acknowledged on Sunday that hackers acting on behalf of a foreign government - almost certainly a Russian intelligence agency, according to federal and private experts - broke into a range of key government networks, including in the Treasury and Commerce Departments, and had free access to their email systems[[94]](#footnote-94).»

On July 16, 2020, The Wall Street Journal wrote: «A prominent state-backed Russian hacking group was blamed Thursday by US, UK and Canadian government officials for ongoing cyber espionage against organizations involved in the development of coronavirus vaccines and other health-care-related work.» The Western officials identified the hacking group as Russia-supported APT29, which is also known as Cozy Bear. «Throughout 2020, APT 29 has targeted various organizations involved in Covid-19 vaccine development in Canada, the United States and the United Kingdom, highly likely with the intention of stealing information and intellectual property relating to the development and testing of Covid-19 vaccines», British, American and Canadian security agencies said in a technical report[[95]](#footnote-95). Russian government again denied any involvement.

At the end of February 2019, American publications reported that on the day of the midterm congressional elections in November 2018, Pentagon specialists disconnected the St. Petersburg Internet Research Agency from the power grids and access to the Internet. This organization in the United States is considered to be connected with businessman Yevgeny Prigozhin and is accused of spreading disinformation during the last presidential elections. As it turned out, the attack was part of Operation Russia Small Group, approved by US Cyber ​​Command Chief Paul Nakasone in August 2018. During this operation, four targets in Russia were to be attacked[[96]](#footnote-96).

On June 15, 2019, The New York Times reported on the intensification of US attempts to hack into computer networks in the Russian energy system. According to the newspaper's sources, the hacker attacks should warn Moscow against interfering in the 2020 presidential elections, and in the event of a conflict between the two countries - become the basis for a full-scale attack in cyberspace. The New York Times reported on the details of the new strategy of the US military command with reference to unnamed former and current employees of the American administration. According to them, in recent years, the cyber command of the US Armed Forces has increased the number of hacks on the computer networks of Russia's power systems. At the same time, as the newspaper's sources make it clear, so far it is only a matter of collecting information and demonstrating opportunities[[97]](#footnote-97).

It seems that Western media and officials do not have any direct evidence, but nevertheless tend to point in the direction of Russia in any cyberattack. The main arguments in such cases are the words that cyberattacks, judging by the IP address, originate from the territory of Russia, however, the Russian government quite rightly answers this by confirming the possibility of the existence of some hacker groups operating from the territory of the Russian Federation, but this is not a factor indicating the direct participle of the Russian government. It is also important to note that the activity that the American government, in particular, shows when the slightest opportunity to accuse Russia of violating someone's cyberspace shows the real intentions of the United States in this area, and this is by no means a desire for cooperation, but for hegemony and control.

However, contact between Russia and the United States in the field of cybersecurity still remains, albeit weak. Theoretically, there is still hope for further cooperation even today, under Biden, but more on that later. This is what the Deputy Secretary of the Russian Security Council Oleg Khramov said even during the Trump presidency: «Mechanisms of interaction on the security of the use of information and communication technologies were formed back in 2013. We are ready for constructive cooperation in bilateral and multilateral formats, including the UN and regional platforms, in particular the OSCE. All the necessary mechanisms for this exist[[98]](#footnote-98).»

It is noteworthy that against the background of continuing attempts to build a dialogue with the United States, Russia is following the same path of forming a group of states adhering to a similar point of view. The idea of ​​creating an international information security system is being promoted, which is designed to preserve the entire positive potential of the information space while maintaining a balance between security and ensuring the rights and freedoms of citizens. Significant success in consolidating views has been achieved within the framework of the Shanghai Cooperation Organization and the BRICS. At the SCO level, an agreement on cooperation in the information space has existed since 2009[[99]](#footnote-99).

A picture is being formed that clearly shows that America simply does not intend to conduct a constructive dialogue at this stage, this is not part of its real interests. The fact is that we are not even talking about disagreement with any specific positions of one of the parties. The US government under Donald Trump did not even consider such a possibility. In fact, it is quite typical for American politics to look for an external enemy on many issues, and it also happened in the case of cybersecurity under Trump. The result of artificially escalating confrontation in the information sphere is tension in international relations, the slowdown in the development of the world economy due to sanctions, as well as undermining confidence in the digitalization processes in general.

***2.3 Evaluation of the results devoted to cybersecurity policy under Trump administration***

Donald Trump found it difficult to defend his position throughout his presidency. In the previous paragraph, I have already cited examples of pressure from Congress, where Trump on several occasions was forced to act against his will. However, Trump had problems not only with Congress, but in general with the support of the people. Not all projects were successful and well received by the public.

On February 28, 2019, an official document was released on the assessment of the activities of the Ministry of Homeland Security in the field of cybersecurity, and this assessment was quite critical[[100]](#footnote-100). In particular, it was noted that the department does not make due efforts to ensure the protection of voting equipment. In addition, it was pointed out that among the reasons for this state of affairs is the lack of staff in the Agency for Cyber and Infrastructure Security.

On March 5, 2019, The Washington Post wrote: «the country's critical infrastructure is no safer from cyberattacks today than in May 2017 when President Trump signed an executive order pledging to better protect it, according to more than three-fourths of digital security experts surveyed by The Cybersecurity 202.» The results of The Network survey are a sharp rebuke to the Trump administration, which has made protecting critical infrastructure such as airports, hospitals and energy plants a cornerstone of its cybersecurity policy. Yet many also said it wasn’t just the Trump administration’s fault. Any improvements the United States had made in protecting critical infrastructure, several experts said, were simply outpaced by adversaries who were able to improve their digital attacks even more[[101]](#footnote-101).

According to the majority of experts interviewed by The Cybersecurity 202, Trump and his administration made a lot of wrong steps in terms of domestic and foreign policy, and this sent the country in the wrong direction[[102]](#footnote-102).

According to 71 out of 100 experts surveyed by The Network[[103]](#footnote-103), over the past four years, Trump has not been able to achieve results in bringing to justice the opponents of the American government, including those responsible for hacking US government agencies and facilities, in particular Russia. Trump, in the course of his policies, removed the most experienced cybersecurity experts from their posts, and for this reason undermined the most trusted US cybersecurity sector, and the reasons for the removals were minor.

The survey was conducted ahead of what has since been cited as probably the most serious cybersecurity breach[[104]](#footnote-104) by Trump and his administration. This is a hack related to the Russian Foreign Intelligence Service, or SVR. After that, the hack went further and affected the Commerce, Treasury, Homeland Security and State Department, as well as the National Institutes of Health[[105]](#footnote-105). Other foreign governments and companies around the world may have been affected as well.

However, the respondents’ comments reflect Trump’s widespread concern that he is disinterested in the damage the hack has done to national security, unwilling to challenge Russia, and instead preoccupied with his own efforts to sow baseless doubts about his electoral defeat. “Much of the work done … during the Trump administration, was weakened by a president who did not prioritize cyber issues and who in many cases actively undermined any action or message against our adversaries,” said Chris Painter, the State Department cyber-coordinator under President Obama who also served for several months under Trump until his post was eliminated[[106]](#footnote-106).

Trump fired Krebs by tweet after his agency, and it was met by the expert community really bad. The Cybersecurity and Infrastructure Security Agency, signed on to a statement vouching for the integrity of the 2020 election, despite Trump’s baseless claims it was riddled with fraud. Krebs also launched a CISA “Rumor Control” page that knocked back phony election fraud claims, including some propagated by the president.

“Krebs was one of those individuals that was widely trusted outside the government. His firing is likely to reduce the trust shown by the private sector to the government regarding cybersecurity,” said Jake Williams, a former National Security Agency hacker and the founder of Rendition Infosec[[107]](#footnote-107).

Despite all the negativity directed at the American president, most of the initiatives developed and adopted during his reign were well received in American society and they were quite effective. The most effective tool in his hands was the US National Cyber ​​Strategy. Supporters of hard power appreciated it especially warmly, because it «untied the hands» of the power structures of the Americans. The creation and adoption of the CLOUD Act also essentially increased the powers of the security forces and made the same realists happy. Driven by pressure from the side, Trump was unable to pursue the policies he would like to pursue, but he did not stop fighting, and the resulting hybrid of his own actions and actions dictated by Congress strengthened the American position in the field of cybersecurity in terms of hard power, but removed possible options for cooperation with a number of states, including Russia.

**CHAPTER III: Documents and initiatives created within the framework of cybersecurity policy of Biden Administration and their impact**

The chapter is devoted to the analysis of the activities of Biden and his administration as President of the United States, aimed at strengthening cybersecurity and preventing cyber threats from intruders. At the end of the chapter, the problems in the relationship that have arisen between Russia and the United States in the field of cybersecurity are also considered in more detail.

**3.1 Biden administration initiatives to enhance national cybersecurity defense**

Joseph Biden has been elected President of the United States in January 20, 2021. The legacy of the Obama administration has been refined by the Trump administration. Joseph Biden is the current president of the United States and has already taken several steps in the field of cybersecurity policy. Biden got a lot of unresolved problems from Trump, including problems in relations with the Russian side, including in the field of cybersecurity.

From the very beginning of taking office, Biden and his administration have made cyber security is a part of the national security and economic security imperative. New government promised to prioritize cyber security and try to increase its importance in every possible way, like it was never done before.

One of the first steps as a new president for Biden became signing the Executive Order dated May 12, 2021 to improve national cybersecurity and protect the federal government's networks. The recent cyber attacks associated with SolarWinds[[108]](#footnote-108), Microsoft Exchange[[109]](#footnote-109), and the Colonial Pipeline[[110]](#footnote-110) are important reminders that US public and private sectors are still vulnerable to cybersecurity and are increasingly being targeted by cyberattacks from other countries and cyberterrorists. Each of these developments is similar to each other, for example, they all share a low level of protection in the field of cybersecurity, which makes organizations in different sectors more vulnerable to external influences in general. The purpose of this Executive Order is to make a significant contribution to modernizing cybersecurity defenses while protecting federal networks and raising the level of information sharing within the US government system, as well as with the private sector. In addition, the decree is designed to improve the speed of the US government's response to ongoing incidents. Biden called it the first of many steps towards raising the level of national cybersecurity.

At the same time, the Colonial Pipeline incident serves as a reminder that federal action alone is not enough. In fact, the bulk of the internal critical infrastructure of the United States today belongs to the private sector, and is also managed by it. Therefore, it is private companies that determine the quality and quantity of investment in private sector cybersecurity. The executive order encourages private companies to follow the example of the federal government and do more to harmonize and raise the level of investment in cybersecurity, which aims to reduce the number of possible incidents in this area.

The first point of the Executive Order is to remove barriers to the free flow of information between the federal government and the private sector regarding cyber threats. The executive order provides assurances that IT service providers can and must share information about the various violations identified in the order, without harming their own freedom and security. There was a problem where IT providers were often unable or unwilling to voluntarily share information about a compromise. Sometimes this is due to contractual obligations, sometimes they are simply afraid to point out their own security breaches. In this regard, the removal of all barriers in this area is necessary and would help achieve greater protection for federal agencies, as well as improve the overall level of cybersecurity for the entire country as a whole.

The second point is the modernization and implementation of more stringent cybersecurity standards in the Federal Government. An executive order can help governments start using more secure cloud services as well as zero-trust architectures. In addition, this decree implies that the federal government will begin to pay more attention to the use of multi-factor authentication along with encryption from a certain period of time. Outdated security models have become unreliable, and together with the presence of unencrypted data, have led to the compromise of systems in the private and public sectors. A sustainable cyber defense system requires the federal government to continuously expand its security best practices and be a leader in the field, including through a zero-trust security model, accelerating the transition to secure cloud services, and progressive deployment of core security tools such as multi-factor authentication and encryption.

The third point of the Executive Order is to improve the security of the logistical component of software deliveries. The Executive Order should improve software security by dictating basic security standards for developing software that is then sold to government agencies, also requiring software developers to be transparent about their products and making data on this subject publicly available. The Order was also created to support a parallel process of development between the public and private sectors of new innovative approaches to creating software and to use federal procurement opportunities to stimulate the market in this area. Finally, it creates a pilot program to create an “energy star” type of label so the government – and the public at large – can quickly determine whether software was developed securely. Much of our software, including critical pieces, tends to ship with vulnerabilities that can be exploited by attackers. This is an old problem that we have turned a blind eye to for too long. We need to take advantage of the federal government's ability to push the software market to raise the software security baseline from the ground up.

The fourth point under the Executive Order was the creation of a Cyber ​​Security Review Board. The idea is to establish a special body, the Council, which will be in charge of the cybersecurity security review, chaired jointly by leaders of government and the private sector, which can meet after a major cyber incident to analyze the consequences and understand and take further actions to eliminate the problems that have arisen. Very often, organizations repeat the mistakes of the past and turn a blind eye to the experience gained from cyber incidents. When things don't go according to plan, the federal government, together with the private sector, must ask the tough questions and together propose and implement improvements to the system. This board is modeled after the National Transportation Safety Board used after plane crashes and other accidents.

**The fifth point was creation of a book of standards and actions for the fastest response to cyber incidents. The Executive Order provides for the creation of a collection of possible scenarios, as well as a set of definitions that can help federal governments and agencies respond to cyber incidents. Organizations cannot wait until they are compromised to figure out how to respond to an attack. Recent cybersecurity incidents have shown that the response system in each individual government agency varies in quality. The new scenario, in turn, will provide all authorities with a single action plan and will allow taking common steps to identify threats to cybersecurity. In addition, the playbook can serve as an example for the private sector.**

 **The sixth point was to Improve Detection of Cybersecurity Incidents on Federal Government Networks**. The Executive Order improves the ability to detect malicious cyber activity on federal networks by enabling a government-wide endpoint detection and response system and improved information sharing within the Federal government. Slow and inconsistent deployment of foundational cybersecurity tools and practices leaves an organization exposed to adversaries. The Federal government should lead in cybersecurity, and strong, Government-wide Endpoint Detection and Response (EDR) deployment coupled with robust intra-governmental information sharing are essential.
**Then seventh is to Improve Investigative and Remediation Capabilities.** The Executive Order creates cybersecurity event log requirements for federal departments and agencies. Poor logging hampers an organization’s ability to detect intrusions, mitigate those in progress, and determine the extent of an incident after the fact.  Robust and consistent logging practices will solve much of this problem.

On August 25, 2021, President Biden met with private sector and education leaders to discuss the whole-of-nation effort needed to address cybersecurity threats[[111]](#footnote-111). During this meeting the Biden Administration announced that the National Institute of Standards and Technology (NIST) will collaborate with industry and other partners to develop a new framework to improve the security and integrity of the technology supply chain. The approach will serve as a guideline to public and private entities on how to build secure technology and assess the security of technology, including open source software. Microsoft, Google, IBM, Travelers, and Coalition committed to participating in this NIST-led initiative.

The Biden Administration also announced the formal expansion of the Industrial Control Systems Cybersecurity Initiative to a second major sector: natural gas pipelines. The Initiative has already improved the cybersecurity of more than 150 electric utilities that serve 90 million Americans.

The Biden Administration continues to take steps to safeguard U.S. critical infrastructure from growing, persistent, and sophisticated cyber threats[[112]](#footnote-112). Recent high-profile attacks on critical infrastructure around the world, including the ransomware attacks on the Colonial Pipeline and JBS Foods in the United States, demonstrate that significant cyber vulnerabilities exist across U.S. critical infrastructure, which is largely owned and operated by the private sector. As we have seen, the degradation, destruction, or malfunction of systems that control this infrastructure can have cascading physical consequences that could have a debilitating effect on national security, economic security, and the public health and safety of the American people.

President Biden signed a National Security Memorandum (NSM) on “Improving Cybersecurity for Critical Infrastructure Control Systems,” which addresses cybersecurity for critical infrastructure and implements long overdue efforts to meet the threats we face. The NSM:

 Directs the Department of Homeland Security’s Cybersecurity & Infrastructure Security Agency (CISA) and the Department of Commerce’s National Institute of Standards and Technology (NIST), in collaboration with other agencies, to develop cybersecurity performance goals for critical infrastructure. We expect those standards will assist companies responsible for providing essential services like power, water, and transportation to strengthen their cybersecurity.

 Formally establishes the President’s Industrial Control System Cybersecurity (ICS) Initiative. The ICS initiative is a voluntary, collaborative effort between the federal government and the critical infrastructure community to facilitate the deployment of technology and systems that provide threat visibility, indicators, detections, and warnings. The Initiative began in mid-April with an Electricity Subsector pilot, and already over 150 electricity utilities representing almost 90 million residential customers are either deploying or have agreed to deploy control system cybersecurity technologies. The action plan for natural gas pipelines is underway, and additional initiatives for other sectors will follow later this year.

The Department of Homeland Security’s Transportation Security Administration (TSA) announced a second Security Directive for critical pipeline owners and operators. Following the ransomware attack on a major petroleum pipeline in May 2021, TSA issued an initial Security Directive[[113]](#footnote-113) requiring critical pipeline owners and operators to report cybersecurity incidents, designate a Cybersecurity Coordinator, and conduct a review of their current cybersecurity practices. This second Security Directive will require owners and operators of pipelines that transport hazardous liquids and natural gas to implement a number of urgently needed protections, including: “Implementing specific mitigation measures to protect against ransomware attacks and other known threats to information technology and operational technology systems within prescribed timeframes; Developing and implementing a cybersecurity contingency and recovery plan; Conducting an annual cybersecurity architecture design review; The Federal Government cannot do this alone and securing our critical infrastructure requires a whole-of-nation effort. This NSM, the ICS Cybersecurity Initiative, TSA’s Security Directives and the President’s Executive Order on Improving the Nation’s Cybersecurity are parts of a focused and aggressive continuing effort to address these significant threats to our nation.”

On October 13 and 14, the White House National Security Council facilitated an international counter-ransomware virtual event with over 30 countries and the European Union, with the goal of accelerating cooperation to counter ransomware[[114]](#footnote-114). Countries recognized that ransomware is an escalating global security threat with serious economic and security consequences. Governments recognize the need for urgent action, common priorities, and complementary efforts to reduce the risk of ransomware. Efforts will include improving network resilience to prevent incidents when possible and respond effectively when incidents do occur; addressing the abuse of financial mechanisms to launder ransom payments or conduct other activities that make ransomware profitable; and disrupting the ransomware ecosystem via law enforcement collaboration to investigate and prosecute ransomware actors, addressing safe havens for ransomware criminals, and continued diplomatic engagement. However, several universal cybersecurity best practices can dramatically reduce the likelihood of a ransomware incident and mitigate the risk from a host of other cyber threats. These basic steps include maintaining offline data backups, use of strong passwords and multi-factor authentication, ensuring software patches are up to date, and education against clicking suspicious links or opening untrusted documents. We are committed to working together and with the private sector to promote improvements in basic cyber hygiene to boost network resilience and mitigate the risk of ransomware. Nations should also consider appropriate steps to promote incident information sharing between ransomware victims and relevant law enforcement and cyber emergency response teams (CERTs), with protection for privacy and human rights. Such sharing enables cybercrime investigations and prosecutions, and facilitates broad distribution of cyber threat mitigation steps[[115]](#footnote-115).

On January 19, 2022, President Biden signed a National Security Memorandum (NSM) to improve the cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, as required in his Executive Order (E.O) 14028, Improving the Nation’s Cybersecurity. This NSM requires that, at minimum, National Security Systems employ the same network cybersecurity measures as those required of federal civilian networks in Executive Order 14028. The NSM builds on the Biden Administration’s work to protect our Nation from sophisticated malicious cyber activity, from both nation-state actors and cyber criminals[[116]](#footnote-116).

This NSM to improve the cybersecurity of National Security: Specifies how the provisions of EO 14028 apply to National Security Systems. The President’s May 2021 Executive Order required that the government “shall adopt National Security Systems requirements that are equivalent to or exceed the cybersecurity requirements set forth in this order.” Consistent with that mandate, this NSM to improve the cybersecurity of National Security establishes timelines and guidance for how these cybersecurity requirements will be implemented, including multifactor authentication, encryption, cloud technologies, and endpoint detection services; Improves the visibility of cybersecurity incidents that occur on these systems. It requires agencies to identify their national security systems and report cyber incidents that occur on them to the National Security Agency, which by prior policy is the “National Manager” for the U.S. government’s classified systems. This will improve the government’s ability to identify, understand, and mitigate cyber risk across all National Security Systems; Requires agencies to act to protect or mitigate a cyber threat to National Security Systems. The NSM authorizes the National Security Agency, through its role as National Manager for National Security Systems, to create Binding Operational Directives requiring agencies to take specific actions against known or suspected cybersecurity threats and vulnerabilities. This directive is modeled on the Department of Homeland Security’s Binding Operational Directive authority for civilian government networks. The NSM to improve the cybersecurity of National Security directs NSA and DHS to share directives and to learn from each other to determine if any of the requirements from one agency’s directive should be adopted by the other; Requires agencies to secure cross domain solutions – tools that transfer data between classified and unclassified systems. Adversaries can seek to leverage these tools to get access to our classified networks, and the NSM to improve the cybersecurity of National Security directs decisive action to mitigate this threat. The NSM requires agencies to inventory their cross-domain solutions and directs NSA to establish security standards and testing requirements to better protect these critical systems.

***3.2 Government under Biden presidency cyber policy in the framework of Russia-US relations***

Most of the laws and documents approved by Biden were protective measures. Biden builds a barrier around himself in order to be able to defend himself against any threat, including the threat of a cyber attack from Russia. It is noteworthy that Biden did not correct the documents left after Trump in the field of cybersecurity, and accepted everything as it is.

Despite public statements that U.S. talks with Russia are pressing forward on cyber attacks, some of President Joe Biden’s own aides are skeptical that President Vladimir Putin will act to rein in cyber criminals based there. “He’s not going to,” says one Biden Administration official, speaking about Putin taking steps to crack down on hacks originating in Russia and on Russian networks. The official says several members of Biden’s team are doubtful. Without Putin intervening, “the criminal groups will keep doing what they’re doing” the official says. “He’s wreaking havoc.”[[117]](#footnote-117)

When the two leaders met in Geneva in June, Biden asked Putin to help crack down on criminal hackers working in Russia that have been targeting American institutions and businesses. Less than a month later, Russian hackers allegedly broke into computers used by a contractor for Republican National Committee, and a Russian cyber criminal network activated another massive international ransomware attack that targeted an estimated 1,500 businesses, some in the U.S.

U.S. intelligence officials have watched ransomware attacks escalate in scale and sophistication as relations between Washington and Moscow grew increasingly strained in recent years. Russia’s invasion of Ukraine, Putin’s meddling in U.S. elections, the Congressional investigation into links between President Donald Trump’s campaign and the Kremlin, and Trump’s unpredictable public statements about Russia put the countries on adversarial footing, preventing high-level discussions to outline rules of the road and clear consequences for aggressive hacking.

The presidents of Russia and the United States had a phone conversation on Friday. It was the first phone talk between Putin and Biden after their summit meeting in Geneva on June 16, when they spoke for nearly 3.5 hours. Before that, the two leaders spoke over the phone two times, on January 26 and on April 13[[118]](#footnote-118).

The president continued dialogue on issues of information security and the fight against cybercrime that began at the Russian-US summit in Geneva, the Kremlin said. "In the context of the recent reports about a series of cyberattacks allegedly originating from Russia, Vladimir Putin noted that despite the Russian side’s readiness for joint efforts to stop crimes in the information space, no inquiries on these matters came from the United States’ security agencies in the past month," the Kremlin said.

The Russian-American relationship, overall, remains a “mixed picture,” with sharp disagreements and suspicions on many issues, a senior State Department official said in an interview Tuesday. But the administration feels it’s making slow progress in some parts of the security agenda that President Biden and Russian President Vladimir Putin set in their summit in Geneva in June[[119]](#footnote-119).

The joint cybersecurity initiative was packaged in a resolution submitted to the U.N. General Assembly last Friday. The language is mostly diplomatic boilerplate, but it commits the two countries to support two U.N. cyber efforts, one Russian-backed and the other American, that a year ago were on a collision course. The resolution has been co-sponsored by 55 countries and will likely pass overwhelmingly before year-end.

Russia and the United States, in essence, have agreed to seek a common set of “rules of the road” to prevent malicious cyberattacks. The two nations differ sharply about what those standards should be — and intense competition will continue in the trenches of the organizations that oversee global telecommunications. But in principle, there’s now a shared commitment to cybersecurity.

Andrei Krutskikh, a top cyber adviser to Putin, recently hailed the joint resolution as a “historic moment,” which termed the resolution “a real diplomatic breakthrough.” U.S. officials say that overstates the significance of the resolution, which State hasn’t announced formally.

“What we are doing is to lean into setting norms, standards and rules of the road for cyberspace through the U.N. and other international bodies,” said the senior State official. A year ago, Washington had been pressing its cybersecurity agenda through a report by the U.N.’s Group of Governmental Experts, while Russia had backed recommendations of a rival forum known as the “Open-ended Working Group.” The joint resolution embraces both.

Vladimir Putin and Joseph Biden during a video conference announced their readiness to continue cooperation in the field of cybersecurity, kremlin.ru reported on Tuesday. “When exchanging views on information security, both sides emphasized the importance of an actively ongoing dialogue on this topic,” the message says. “Readiness was expressed to continue practical cooperation in the criminal procedural and operational-technical areas of combating cybercrime.”[[120]](#footnote-120)

According to the White House website [[121]](#footnote-121), the presidents, among other things, “discussed the Russian-American dialogue on strategic stability and separately discussed the issue of cyber extortion.

On March 21, 2022, the official Biden statement was the following: “I have previously warned about the potential that Russia could conduct malicious cyber activity against the United States, including as a response to the unprecedented economic costs we’ve imposed on Russia alongside our allies and partners. It’s part of Russia’s playbook. Today, my Administration is reiterating those warnings based on evolving intelligence that the Russian Government is exploring options for potential cyberattacks.”[[122]](#footnote-122) Press Secretary of the President of Russia Dmitry Peskov responded to Biden's statements that the Russian Federation, unlike Western countries and the United States, is not engaged in banditry.[[123]](#footnote-123)

Also in his statement, the current American president called on the government's private sector partners to strengthen their cyber defenses, using all the experience that America has accumulated in recent years. He noted that most of America's critical infrastructure is in the hands of the private sector, which is why it is so important to protect the private sector. “You have the power, the capacity, and the responsibility to strengthen the cybersecurity and resilience of the critical services and technologies on which Americans rely.”[[124]](#footnote-124)

Against the background of the Special Military Operation on Ukraine, the United States began to claim that they were receiving intelligence, according to which the Russian government was considering the possibility of carrying out cyberattacks against the United States and its allies. In this regard, as part of the activities of the current US administration under the leadership of Biden, the need to create a new initiative was indicated. This initiative was named Shields Up, and it was implemented and ensured by the Cybersecurity and Infrastructure Security Agency (CISA)[[125]](#footnote-125). The initiative implies the need to strengthen the cyber defense of the private sector, and the task of CISA is to help to prepare for cyberattacks. This is mainly about advising and providing instructions on how to install the most effective protection in the field of cybersecurity.

At the moment, it is difficult to draw conclusions about the long-term outlook for the development of Biden and his administration's policy in the field of cybersecurity. Especially considering how dramatically the slightest progress in this area can be lost and forgotten, as was the case, for example, with the progress achieved after the recent events in Ukraine took place. However, some conclusions can be drawn even taking into account the above.

In general, from the very beginning, Biden was wary of Russia and constantly prepared those around him for a possible attack in the cyber sphere. He even took many protective measures to be able to cope in the event of a digital intrusion.

Also, despite the tense relationship that the new Biden government inherited from Trump, the United States was ready for bilateral dialogue with Russia on several issues, including cybersecurity. However, the events in Ukraine completely cut off all progress and relations again acquired an isolationist character.

In the short term, relations will only get worse, and there can no longer be any talk of any joint initiatives. Probably until the end of Biden's presidential term, US policy towards Russia will no longer change, at least because otherwise Biden and the government will be misunderstood.

**CONCLUSION**

As our analysis in the first chapter illustrates the poor start to mutual cybersecurity relations between Russia and the United States under Obama, both sides have not been particularly keen on building such a relationship and trading participation. At the end of Obama's presidency, the 2016 presidential campaign scandal finally ended the imperfect relationship between the two countries.

In summary, one of the most significant concerns of the Obama administration, which has gone further and taken over by the Trump and Biden administrations, has been the need to balance better cybersecurity with other needs such as privacy, civil rights, legitimate business, and economic interests.

During Donald Trump’s presidency, much has been changed regarding US cybersecurity, and America has been steered on a new, as practice has shown, more aggressive course. Given the controversial effectiveness of many adopted documents, in the end, the efforts and funds that were invested in this field are well monitored, and it is safe to say that cybersecurity has become one of the key areas of Donald Trump's policy.

In spite of all the negativity directed at the American president, most of the initiatives developed and adopted during his reign were well perceived in American society and proved to be quite effective. The most efficient tool in his hands was the US National Cyber Strategy. Supporters of hard power especially warmly appreciated it, since it "untied the hands" of the American power structures. The development and implementation of the CLOUD Act also significantly increased the powers of the security forces and had a positive effect on the same realists. Trump's susceptibility to outside pressure led to an inability to implement the policies he wanted to pursue, but he did not stop the course of inadmissibility, the result is a hybrid of his own actions and actions dictated by Congress that driven strengthened the American position in the field of cybersecurity in the face of hard power, but removed the possible options for cooperation with a number of states, including Russia.

Taking into account all the specifics of Donald Trump's political course, the author of the study sees a clearly emerging picture that explicitly demonstrates that American establishment under Trump simply did not intend to conduct a constructive dialogue at this stage, this is not in its real interests. The fact is that there was not even a discourse about disagreeing with any particular position of one of the parties, the US Government did not even consider such a possibility. As a matter of fact, it is quite common for American politics to look for an external enemy on many issues, and this has also happened in the case of cybersecurity under Trump. The result of the artificially induced confrontation in the information sphere was tension in international relations, a slowdown in the development of the world economy due to sanctions, as well as undermining confidence in digitalization processes in general.

A peculiar political course is being pursued by the government under the Biden administration. It is characterized by a crusade of protective measures, which is illustrated by all the approved documents and laws in its term. The main aspect of his policy is to build barriers around himself in order to be able to defend himself against any threat, including the threat of a cyber attack from Russia. It is noteworthy that Biden did not change the documents in the field of cybersecurity adopted by the Trump administration.

At this point, it is difficult to draw long-term conclusions about the evolution of Biden and his administration's cybersecurity policy. Especially when you consider how abruptly the slightest progress in this area can be lost and forgotten, as was the case, for example, with the progress made after the recent events in Ukraine. However, some conclusions can be drawn from the above.

Already at the initial stage, Biden expressed wariness towards Russia and constantly prepared those around him for a possible attack in the cyber sphere, which was followed by many protective measures to combat the digital invasion. Moreover, the strained relationship that the new Biden administration inherited from Trump has not blocked the possibility of bilateral dialogue with Russia on a range of issues, including cybersecurity. However, events in Ukraine completely blocked any progress, and relations again acquired an isolationist character.

In the short term, only a deterioration in relations is foreseen, and there can no longer be any talk of any joint initiatives. Probably, until the end of Biden's presidential term, US policy towards Russia will no longer turn in a positive direction, due to the high probability of misunderstanding the actions of Biden and the government.

**List of sources**

**Documents**

1. S.482 - Defending American Security from Kremlin Aggression Act of 2019 (18.12.2019). URL: https://www.congress.gov/bill/116th-congress/senate-bill/482.
2. UN resolution 73/266 (22.12.2018). URL: https://undocs.org/A/RES/73/266.
3. H.R.3359 - Cybersecurity and Infrastructure Security Agency Act of 2018 (16.11.2018). URL: https://www.congress.gov/bill/115th-congress/house-bill/3359.
4. National Cyber Strategy of the United States of America (20.09.2018). URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
5. U.S. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY STRATEGY (15.05.2018). URL: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy\_1.pdf.
6. H.R.4943 - CLOUD Act (02.06.2018) // Official website of the U.S. Congress. URL: https://www.congress.gov/bill/115th-congress/house-bill/4943.
7. DEPARTMENT OF DEFENSE CYBER STRATEGY (2018). URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER\_STRATEGY\_SUMMARY\_FINAL.PDF.
8. National Security Strategy of the United States of America (December 2017). URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.
9. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (11.05.2017). URL: https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.
10. The Comprehensive National Cybersecurity Initiative (2009) // Obama White House official website. URL: https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative.
11. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (16.06.2009). URL: http://base.spinform.ru/show\_doc.fwx?rgn=28340.

**Articles**

1. Демидов О., Ангмар М. Киберстратегия США 2018. Значение для глобального диалога о поведении в сфере использования ИКТ и российско-американских отношений // Индекс Безопасности, Триалог, №1, 2019. с. 24. URL: https://pircenter.org/media/content/files/14/15499609670.pdf.
2. Смекалова М.В. Эволюция доктринальных подходов США к обеспечению кибербезопасности и защите критической инфраструктур // Вестник Московского университета. 25, 2019. с. 47-68.
3. Смирнов А. Новейшие Киберстратегии США – Преамбула войны? // Международные процессы, том 16, №4 (55), 2018. c. 181-192.

**Websites**

1. Bastien Inzaurralde. The Cybersecurity 202: Trump's efforts failed to make critical infrastructure safer from cyberattacks, experts say // Official website of the news agency The Washington Post. URL: https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/03/05/the-cybersecurity-202-trump-s-efforts-failed-to-make-critical-infrastructure-safer-from-cyberattacks-experts-say/5c7d6c5b1b326b2d177d5fbd/.
2. Biden firmly believes in top-level cyber security cooperation with Russia — official // Official website of the news agency TASS. URL: https://tass.com/world/1312585?utm\_source=google.com&utm\_medium=organic&utm\_campaign=google.com&utm\_referrer=google.com
3. Biden Administration Says Talks with Russia on Cyber Attacks Are Progressing. Privately, Staffers Are Skeptical. // Official website of the TIME news agency. URL: https://time.com/6078997/biden-cyber-attacks-putin/
4. Dustin Volz. Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive // Official website of the news agency The Wall Street Journal. URL: https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721.
5. DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators // US Government Department of Homeland Security official website. URL: https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators
6. DHS, State and NIH join list of federal agencies — now five — hacked in major Russian cyberespionage campaign // The Washington Post news agency official website. URL: https://www.washingtonpost.com/national-security/dhs-is-third-federal-agency-hacked-in-major-russian-cyberespionage-campaign/2020/12/14/41f8fc98-3e3c-11eb-8bc0-ae155bee4aff\_story.html?wpmk=1&wpisrc=al\_news\_\_alert-national--alert-world--alert-politics&utm\_source=alert&utm\_medium=email&utm\_campaign
7. FACT SHEET: President Biden Signs National Security Memorandum to Improve the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems // Biden White House official website. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/19/fact-sheet-president-biden-signs-national-security-memorandum-to-improve-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
8. FACT SHEET: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure // Biden White House official website. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/
9. FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation’s Cybersecurity // Biden White House official website. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/
10. Hackers Breached Colonial Pipeline Using Compromised Password // Bloomberg news agency official website. URL: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password
11. Jenny Strasburg, Dustin Volz. Russian Hackers Blamed for Attacks on Coronavirus Vaccine-Related Targets // Official website of the news agency The Wall Street Journal. URL: https://www.wsj.com/articles/russian-hackers-blamed-for-attacks-on-coronavirus-vaccine-related-targets-11594906060.
12. Johnson D.B. The CLOUD Act, one year on // Official website of news agency FCW. URL: https://fcw.com/articles/2019/04/08/cloud-act-turns-one.aspx.
13. Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021 // Biden White House official website. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/
14. Matthew Cole, Richard Esposito, Sam Biddle, Ryan Grim. TOP-SECRET NSA REPORT DETAILS RUSSIAN HACKING EFFORT DAYS BEFORE 2016 ELECTION // Official website of the news agency «The Intercept\_». URL: https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.
15. Obama approval hits 60% as end of term approaches // Official CNN website. URL: https://edition.cnn.com/2017/01/18/politics/obama-approval-rating-cnn-orc-poll/index.html.
16. Readout of President Biden’s Video Call with President Vladimir Putin of Russia // Biden White House official website. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/07/readout-of-president-bidens-video-call-with-president-vladimir-putin-of-russia/
17. Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect // Official website of the news agency The New York Times. URL: https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html
18. Shields Up // Official CISA website. URL: https://www.cisa.gov/shields-up.
19. Statement by Secretary Kirstjen M. Nielsen on the Release of the National Cyber Strategy // Official website of the USA Department of Homeland Security. URL: https://www.dhs.gov/news/2018/09/20/statement-secretary-kirstjen-m-nielsen-release-national-cyber-strategy.
20. Statement by President Biden on our Nation’s Cybersecurity // Official website of the Bidan White House. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/
21. Sterling Burnett H. PRESIDENT TRUMP SIGNS EMP ORDER TO PROTECT CRITICAL INFRASTRUCTURE // Official website of the think-tank «The Heartland Institute». URL: https://www.heartland.org/news-opinion/news/president-trump-signs-emp-order-to-protect-critical-infrastructure.
22. The Cybersecurity 202: Trump administration seeks to project tougher stance in cyberspace with new strategy // Official website of the information agency The Washington Post. URL: https://www.washingtonpost.com/news/ powerpost/paloma/the-cybersecurity-202/2018/09/21/the-cybersecurity-202-trump-administrationseeks-to-project-tougher-stance-in-cyberspace-with-new-strategy/5ba3e85d1b326b7c8a8d158a/?nor edirect=on&utm\_term=.a2a77a27737a.
23. The Cybersecurity 202: Trump took the nation in the wrong direction on cybersecurity, experts say // https:// The Washington Post news agency official website. URL: www.washingtonpost.com/politics/2020/12/15/cybersecurity-202-trump-took-nation-wrong-direction-cybersecurity-experts-say/
24. Connecting cybersecurity experts across government and industry in an ongoing survey. // The Washington Post news agency official website. URL: https://www.washingtonpost.com/graphics/2018/politics/powerpost/thenetwork/
25. The Cybersecurity 202: Trump took the nation in the wrong direction on cybersecurity, experts say // The Washington Post news agency official website. URL: https://www.washingtonpost.com/politics/2020/12/15/cybersecurity-202-trump-took-nation-wrong-direction-cybersecurity-experts-say/
26. The Microsoft Exchange Server hack: A timeline // The CSO official website. URL: https://www.csoonline.com/article/3616699/the-microsoft-exchange-server-hack-a-timeline.html
27. The ice between the U.S. and Russia may be thawing — for now // The Washington Post News Agency official website. URL: https://www.washingtonpost.com/opinions/2021/10/19/ice-between-us-russia-may-be-thawing-now/
28. The Cybersecurity 202: A Russian mega-hack is further damaging Trump’s cybersecurity legacy // The Washington Post news agency official website. URL: https://www.washingtonpost.com/politics/2020/12/14/cybersecurity-202-russian-mega-hack-is-further-damaging-trumps-cybersecurity-legacy/
29. Trump fires head of election cybersecurity who debunked conspiracy theories. // NBCNews news agency official website. URL: https://www.nbcnews.com/tech/security/trump-fires-head-u-s-election-cybersecurity-after-he-debunked-n1248063
30. US Cybercom // Official website of the analytical agency TADVISER. URL: https://www.tadviser.ru/index.php/Компания:Киберкомандование\_США\_(US\_Cybercom).
31. U.S. Escalates Online Attacks on Russia’s Power Grid // Official website of the news agency The New York Times. URL: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?action=click&module=Top%20Stories&pgtype=Homepage.
32. Update on the International Counter-Ransomware Initiative // US Department of State official website. URL: https://www.state.gov/briefings-foreign-press-centers/update-on-the-international-counter-ransomware-initiative
33. What is WikiLeaks // Official website of the news agency WikiLeaks. URL: https://wikileaks.org/What-is-WikiLeaks.html.
34. Байден поручил усилить кибербезопасность в США из-за российских хакеров // Официальный сайт новостного агентства Лента. URL: https://lenta.ru/news/2022/03/23/haker/
35. Белый дом: Трамп подписал указ об усилении кибербезопасности не в связи с РФ // Официальный вебсайт информационного агентства «ТАСС». URL: https://tass.ru/mezhdunarodnaya-panorama/4245924.
36. Бовдунов А., Заквасин А., Комарова Е. Погружение в хаос: насколько опасны для России возможные кибератаки со стороны США // Официальный сайт информационного агентства RT. URL: https://russian.rt.com/world/article/643001-kiberbezopasnost-ataka-ugroza-rossiya-ssha.
37. Встреча президентов в киберопасности // Официальный сайт информационного агентства Коммерсантъ. URL: https://www.kommersant.ru/doc/4003491.
38. Как Россию обвиняли во вмешательстве в американские выборы. Досье // Официальный сайт информационного агентства ТАСС. URL: https://tass.ru/info/4324773.
39. "Кибератака ГРУ". Грузия, США и Британия обвинили Россию в нападении на грузинские сайты // Официальный сайт информационного агентства BBC News. URL: https://www.bbc.com/russian/news-51576795.
40. «На страже киберграниц». Замсекретаря Совбеза — о защите интересов страны // Официальный сайт информационного агентства Аргументы и Факты. URL: https://aif.ru/politics/world/na\_strazhe\_kibergranic\_zamglavy\_sovbeza\_-\_o\_zashchite\_interesov\_strany.
41. Официальный аккаунт Посольства Украины в Чехии. Твиттер. URL: https://twitter.com/UKRinCZE?ref\_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1252145767818637312%7Ctwgr%5E%7Ctwcon%5Es1\_&ref\_url=https%3A%2F%2Fwww.lidovky.cz%2Fdomov%2Fkyberutoky-na-ceske-nemocnice-ci-letiste-palbu-ma-organizovat-cizi-velmoc-stopy-vedou-do-ruska.A200419\_211808\_ln\_domov\_sei.
42. Президенты России и США заявили о готовности продолжать сотрудничество в области кибербезопасности // Официальный сайт информационного агентства D.Russia. URL: https://d-russia.ru/prezidenty-rossii-i-ssha-zajavili-o-gotovnosti-prodolzhat-sotrudnichestvo-v-oblasti-kiberbezopasnosti.html
43. При атаке на SolarWinds взломали e-mail ответственных за кибербезопасность США. // Официальный сайт информационного агентства Интерфакс. URL: https://www.interfax.ru/world/758340
44. Раздел «О нас» // Официальный сайт компании Kaspersky. URL: https://www.kaspersky.ru/about.
45. Сухаревская А. Власти США ввели постоянный запрет на госзакупки продукции «Лаборатории Касперского» // Официальный сайт информационного агентства Ведомости. URL: https://www.vedomosti.ru/technology/articles/2019/09/16/811360-zapret?ref=vc.ru.
46. Трамп передумал сотрудничать с Россией по кибербезопасности // Официальный сайт информационной службы BBC News. URL: https://www.bbc.com/russian/news-40545776.
1. Демидов О., Ангмар М. Киберстратегия США 2018. Значение для глобального диалога о поведении в сфере использования ИКТ и российско-американских отношений, 2019 [↑](#footnote-ref-1)
2. Смекалова М.В. Эволюция доктринальных подходов США к обеспечению кибербезопасности и защите критической инфраструктур, 2019 [↑](#footnote-ref-2)
3. Смирнов А. Новейшие Киберстратегии США – Преамбула войны? 2018 [↑](#footnote-ref-3)
4. Shakirov O. Whoever Comes to Us With a Cyber Sword: Russian and U.S. Approaches to Deterrence in Cyberspace, 2021 [↑](#footnote-ref-4)
5. Стадник И. Политика кибербезопасности США, 2018 [↑](#footnote-ref-5)
6. Powers G. U.S. National Cybersecurity: Strategic Challenges and Opportunities, 2014 [↑](#footnote-ref-6)
7. D’ambrosio A. Cybersecurity : Executive Order 13636 and the Critical Infrastructure Framework, 2014 [↑](#footnote-ref-7)
8. La Fleur C. Team performance in a series of regional and national US cybersecurity defense competitions: Generalizable effects of training and functional role specialization, 2021 [↑](#footnote-ref-8)
9. Boussios E. Hacking Back: Trump's "Madman Theory" Approach to Cybersecurity, 2021 [↑](#footnote-ref-9)
10. Obama approval hits 60% as end of term approaches // Official CNN website. URL: https://edition.cnn.com/2017/01/18/politics/obama-approval-rating-cnn-orc-poll/index.html [↑](#footnote-ref-10)
11. The Comprehensive National Cybersecurity Initiative // Obama White House official website. URL: https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative [↑](#footnote-ref-11)
12. Cybersecurity Policy // White House official archive. URL: https://irp.fas.org/offdocs/nspd/nspd-54.pdf [↑](#footnote-ref-12)
13. Ibid [↑](#footnote-ref-13)
14. CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM // CISA official website. URL: https://www.cisa.gov/sites/default/files/publications/cdm-program-overview-fact-sheet-012022-508.pdf [↑](#footnote-ref-14)
15. Obama Signs 5 Cybersecurity Bills // BankInfoSecurity news agency official website. URL: https://www.bankinfosecurity.com/obama-signs-5-cybersecurity-bills-a-7697 [↑](#footnote-ref-15)
16. S. 2521 // USA Congress official website. URL: https://www.congress.gov/113/bills/s2521/BILLS-113s2521enr.pdf [↑](#footnote-ref-16)
17. S. 1691 // USA Congress official website. URL: https://www.congress.gov/113/bills/s1691/BILLS-113s1691es.pdf [↑](#footnote-ref-17)
18. History // Official DHS website. URL: https://www.dhs.gov/history [↑](#footnote-ref-18)
19. Ibid. [↑](#footnote-ref-19)
20. Cybersecurity Workforce Assessment Act // Congress official archive. URL: https://www.govinfo.gov/content/pkg/BILLS-113hr2952enr/pdf/BILLS-113hr2952enr.pdf [↑](#footnote-ref-20)
21. S. 2519 // Congress official archive. URL: https://www.govinfo.gov/content/pkg/BILLS-113s2519es/pdf/BILLS-113s2519es.pdf [↑](#footnote-ref-21)
22. S. 1353 // Congress official archive. URL: https://www.govinfo.gov/content/pkg/BILLS-113s1353es/pdf/BILLS-113s1353es.pdf [↑](#footnote-ref-22)
23. Cybersecurity Strategy and Implementation Plan // NIST official website. URL: https://csrc.nist.gov/Topics/Laws-and-Regulations/executive-documents/CSIP [↑](#footnote-ref-23)
24. Information Sharing // USA Senate official website. URL: https://www.intelligence.senate.gov/sites/default/files/legislation/Cybersecurity-Act-Of-2015.pdf [↑](#footnote-ref-24)
25. Automated Indicator Sharing // CISA Official website. URL: https://www.cisa.gov/ais [↑](#footnote-ref-25)
26. Cybersecurity Information Sharing Act of 2015 Procedures and Guidance // CISA official website. URL: https://www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-and-guidance [↑](#footnote-ref-26)
27. EINSTEIN // CISA official website. URL: https://www.cisa.gov/einstein [↑](#footnote-ref-27)
28. FOIA // FOIA official website. URL: https://foiaonline.gov/foiaonline/action/public/request [↑](#footnote-ref-28)
29. S. 337 // USA Congress official website. URL: https://www.congress.gov/114/bills/s337/BILLS-114s337enr.xml [↑](#footnote-ref-29)
30. FACT SHEET: Cybersecurity National Action Plan // Obama White House official website. URL: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan [↑](#footnote-ref-30)
31. Commission on Enhancing National Cybersecurity // NIST official website. URL: https://www.nist.gov/cybercommission [↑](#footnote-ref-31)
32. The TMF is an innovative funding vehicle that gives agencies additional ways to deliver services to the American public more quickly, better secure sensitive systems and data, and use taxpayer dollars more efficiently. // TMF official website. URL: https://tmf.cio.gov/ [↑](#footnote-ref-32)
33. Empowering a more secure interconnected world. // National Cybersecurity Alliance official website. URL: https://staysafeonline.org/ [↑](#footnote-ref-33)
34. About NIST // NIST official website. URL: https://www.nist.gov/itl/applied-cybersecurity/nice/about [↑](#footnote-ref-34)
35. National Challenges and Goals for Cybersecurity Science and Technology // Obama White House official website. URL: https://obamawhitehouse.archives.gov/blog/2016/02/08/national-challenges-and-goals-cybersecurity-science-and-technology [↑](#footnote-ref-35)
36. Executive Order -- Commission on Enhancing National Cybersecurity // Obama White House official website. URL: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity [↑](#footnote-ref-36)
37. How the Russians hacked the DNC and passed its emails to WikiLeaks // The Washington Post Official Website. URL: https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78\_story.html [↑](#footnote-ref-37)
38. The Indictment. // CNN Official website. URL: http://cdn.cnn.com/cnn/2018/images/07/13/gru.indictment.pdf [↑](#footnote-ref-38)
39. Расследование Мюллера: какими будут последствия для России? // Официальный сайт информационного агентства BBC. URL: https://www.bbc.com/russian/features-47391585 [↑](#footnote-ref-39)
40. Obama cyber chief confirms 'stand down' order against Russian cyberattacks in summer 2016 // Yahoo!News news agency official website. URL: https://news.yahoo.com/obama-cyber-chief-confirms-stand-order-russian-cyberattacks-summer-2016-204935758.html [↑](#footnote-ref-40)
41. Obama cybersecurity czar: Russian hackers likely scanned election systems in all 50 states // USA Today news agency official website. URL: https://www.usatoday.com/story/news/politics/2018/06/20/obama-cyber-czar-russia-likely-scanned-all-50-state-election-systems/717652002/ [↑](#footnote-ref-41)
42. Ibid [↑](#footnote-ref-42)
43. FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment // Obama White House official website. URL https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and [↑](#footnote-ref-43)
44. Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment // Obama White House official website. URL: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity [↑](#footnote-ref-44)
45. Кремль рассказал о беседе Путина и Обамы по поводу хакерских атак // Официальный сайт информационного агентства BBC. URL: https://www.bbc.com/russian/news-38340790 [↑](#footnote-ref-45)
46. Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" // Obama White House official website. URL: https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m [↑](#footnote-ref-46)
47. От Обамы за хакеров: что известно о новых санкциях США // Официальный сайт информационного агентства РБК. URL: https://www.rbc.ru/politics/30/12/2016/58657b4f9a7947e2c896dc3d [↑](#footnote-ref-47)
48. GRIZZLY STEPPE – Russian Malicious Cyber Activity // CISA official website. URL: https://www.cisa.gov/uscert/sites/default/files/publications/JAR\_16-20296A\_GRIZZLY%20STEPPE-2016-1229.pdf [↑](#footnote-ref-48)
49. FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security // Obama White House official Website. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol [↑](#footnote-ref-49)
50. U.S. and Russia sign pact to create communication link on cyber security // The Washington Post news agency official website. URL: https://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788-11e2-9df4-895344c13c30\_story.html [↑](#footnote-ref-50)
51. Obama cyber chief confirms 'stand down' order against Russian cyberattacks in summer 2016 // Yahoo!News news agency official website. URL: https://news.yahoo.com/obama-cyber-chief-confirms-stand-order-russian-cyberattacks-summer-2016-204935758.html [↑](#footnote-ref-51)
52. Obama’s cybersecurity legacy: Good intentions, good efforts, limited results // CSO news agency official website. URL: https://www.csoonline.com/article/3162844/obamas-cybersecurity-legacy-good-intentions-good-efforts-limited-results.html [↑](#footnote-ref-52)
53. Blowing Sources and Public Intelligence Claims // LawFare news agency official website. URL: https://www.lawfareblog.com/blowing-sources-and-public-intelligence-claims [↑](#footnote-ref-53)
54. Inside the Cyberattack That Shocked the US Government // WIRED news agency official website. URL: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ [↑](#footnote-ref-54)
55. President Obama’s Pursuit of Cyber Deterrence Ends in Failure // Council on Foreign Relations official website. URL: https://www.cfr.org/blog/president-obamas-pursuit-cyber-deterrence-ends-failure [↑](#footnote-ref-55)
56. Obama warns of U.S. weaknesses on cybersecurity // FCW news agency official website. URL: https://fcw.com/security/2016/07/obama-warns-of-us-weaknesses-on-cybersecurity/220310/ [↑](#footnote-ref-56)
57. Bradley Manning sentenced to 35 years for classified document leaks // CSO news agency official website. URL: https://www.csoonline.com/article/2133876/bradley-manning-sentenced-to-35-years-for-classified-document-leaks.html [↑](#footnote-ref-57)
58. Two years after Snowden leaks, US tech firms still feel the backlash // CSO news agency official website. URL: https://www.csoonline.com/article/2933475/two-years-after-snowden-leaks-us-tech-firms-still-feel-the-backlash.html [↑](#footnote-ref-58)
59. SECURING CYBERSPACE - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts // Obama White House official website. URL: https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat [↑](#footnote-ref-59)
60. DHS official: Einstein 3A is 15 years behind the times // FEDScoop official website. URL: https://www.fedscoop.com/dhs-official-einstein-3a-is-15-years-behind-the-times/ [↑](#footnote-ref-60)
61. Белый дом: Трамп подписал указ об усилении кибербезопасности не в связи с РФ // Официальный вебсайт информационного агентства «ТАСС». URL: https://tass.ru/mezhdunarodnaya-panorama/4245924 [↑](#footnote-ref-61)
62. H.R.4943 - CLOUD Act (02.06.2018) // Official website of the U.S. Congress. URL: https://www.congress.gov/bill/115th-congress/house-bill/4943 [↑](#footnote-ref-62)
63. Смирнов А. Новейшие Киберстратегии США – Преамбула войны? // Международные процессы, том 16, №4 (55), 2018. C. 182 [↑](#footnote-ref-63)
64. Johnson D.B. The CLOUD Act, one year on // Official website of news agency FCW. URL: https://fcw.com/articles/2019/04/08/cloud-act-turns-one.aspx [↑](#footnote-ref-64)
65. National Security Strategy of the United States of America (December 2017). URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf [↑](#footnote-ref-65)
66. U.S. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY STRATEGY (15.05.2018). URL: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy\_1.pdf [↑](#footnote-ref-66)
67. Смекалова М.В. Эволюция доктринальных подходов США к обеспечению кибербезопасности и защите критической инфраструктур // Вестник Московского университета. 25, 2019. С. 57 [↑](#footnote-ref-67)
68. UN resolution 73/266 (22.12.2018). URL: https://undocs.org/A/RES/73/266 [↑](#footnote-ref-68)
69. Dustin Volz. Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive // Official website of the news agency The Wall Street Journal. URL: https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721 [↑](#footnote-ref-69)
70. National Cyber Strategy of the United States of America (20.09.2018). URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [↑](#footnote-ref-70)
71. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (11.05.2017). URL: https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ [↑](#footnote-ref-71)
72. US Cybercom // Official website of the analytical agency TADVISER. URL: https://www.tadviser.ru/index.php/Компания:Киберкомандование\_США\_(US\_Cybercom) [↑](#footnote-ref-72)
73. H.R.3359 - Cybersecurity and Infrastructure Security Agency Act of 2018 (16.11.2018). URL: https://www.congress.gov/bill/115th-congress/house-bill/3359 [↑](#footnote-ref-73)
74. S.482 - Defending American Security from Kremlin Aggression Act of 2019 (18.12.2019). URL: https://www.congress.gov/bill/116th-congress/senate-bill/482 [↑](#footnote-ref-74)
75. Sterling Burnett H. PRESIDENT TRUMP SIGNS EMP ORDER TO PROTECT CRITICAL INFRASTRUCTURE // Official website of the think-tank «The Heartland Institute». URL: https://www.heartland.org/news-opinion/news/president-trump-signs-emp-order-to-protect-critical-infrastructure [↑](#footnote-ref-75)
76. Демидов О., Ангмар М. Киберстратегия США 2018. Значение для глобального диалога о поведении в сфере использования ИКТ и российско-американских отношений // Индекс Безопасности, Триалог, №1, 2019. с. 24. URL: https://pircenter.org/media/content/files/14/15499609670.pdf [↑](#footnote-ref-76)
77. Трамп передумал сотрудничать с Россией по кибербезопасности // Официальный сайт информационной службы BBC News. URL: https://www.bbc.com/russian/news-40545776 [↑](#footnote-ref-77)
78. Statement by Secretary Kirstjen M. Nielsen on the Release of the National Cyber Strategy // Official website of the USA Department of Homeland Security. URL: https://www.dhs.gov/news/2018/09/20/statement-secretary-kirstjen-m-nielsen-release-national-cyber-strategy [↑](#footnote-ref-78)
79. The Cybersecurity 202: Trump administration seeks to project tougher stance in cyberspace with new strategy // Official website of the information agency The Washington Post. URL: https://www.washingtonpost.com/news/ powerpost/paloma/the-cybersecurity-202/2018/09/21/the-cybersecurity-202-trump-administrationseeks-to-project-tougher-stance-in-cyberspace-with-new-strategy/5ba3e85d1b326b7c8a8d158a/?nor edirect=on&utm\_term=.a2a77a27737a [↑](#footnote-ref-79)
80. National Cyber Strategy of the United States of America (20.09.2018). URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [↑](#footnote-ref-80)
81. DEPARTMENT OF DEFENSE CYBER STRATEGY (2018). URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER\_STRATEGY\_SUMMARY\_FINAL.PDF [↑](#footnote-ref-81)
82. Ibid. [↑](#footnote-ref-82)
83. Смирнов А. Новейшие Киберстратегии США – Преамбула войны? // Международные процессы, том 16, №4 (55), 2018. с. 185 [↑](#footnote-ref-83)
84. Раздел «О нас» // Официальный сайт компании Kaspersky. URL: https://www.kaspersky.ru/about [↑](#footnote-ref-84)
85. Сухаревская А. Власти США ввели постоянный запрет на госзакупки продукции «Лаборатории Касперского» // Официальный сайт информационного агентства Ведомости. URL: https://www.vedomosti.ru/technology/articles/2019/09/16/811360-zapret?ref=vc.ru [↑](#footnote-ref-85)
86. Бовдунов А., Заквасин А., Комарова Е. Погружение в хаос: насколько опасны для России возможные кибератаки со стороны США // Официальный сайт информационного агентства RT. URL: https://russian.rt.com/world/article/643001-kiberbezopasnost-ataka-ugroza-rossiya-ssha [↑](#footnote-ref-86)
87. What is WikiLeaks // Official website of the news agency WikiLeaks. URL: https://wikileaks.org/What-is-WikiLeaks.html [↑](#footnote-ref-87)
88. Как Россию обвиняли во вмешательстве в американские выборы. Досье // Официальный сайт информационного агентства ТАСС. URL: https://tass.ru/info/4324773 [↑](#footnote-ref-88)
89. Ibid. [↑](#footnote-ref-89)
90. Matthew Cole, Richard Esposito, Sam Biddle, Ryan Grim. TOP-SECRET NSA REPORT DETAILS RUSSIAN HACKING EFFORT DAYS BEFORE 2016 ELECTION // Official website of the news agency «The Intercept\_». URL: https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/ [↑](#footnote-ref-90)
91. Как Россию обвиняли во вмешательстве в американские выборы. Досье // Официальный сайт информационного агентства ТАСС. URL: https://tass.ru/info/4324773 [↑](#footnote-ref-91)
92. "Кибератака ГРУ". Грузия, США и Британия обвинили Россию в нападении на грузинские сайты // Официальный сайт информационного агентства BBC News. URL: https://www.bbc.com/russian/news-51576795 [↑](#footnote-ref-92)
93. Официальный аккаунт Посольства Украины в Чехии. Твиттер. URL: https://twitter.com/UKRinCZE?ref\_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1252145767818637312%7Ctwgr%5E%7Ctwcon%5Es1\_&ref\_url=https%3A%2F%2Fwww.lidovky.cz%2Fdomov%2Fkyberutoky-na-ceske-nemocnice-ci-letiste-palbu-ma-organizovat-cizi-velmoc-stopy-vedou-do-ruska.A200419\_211808\_ln\_domov\_sei [↑](#footnote-ref-93)
94. Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect // Official website of the news agency The New York Times. URL: https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html [↑](#footnote-ref-94)
95. Jenny Strasburg, Dustin Volz. Russian Hackers Blamed for Attacks on Coronavirus Vaccine-Related Targets // Official website of the news agency The Wall Street Journal. URL: https://www.wsj.com/articles/russian-hackers-blamed-for-attacks-on-coronavirus-vaccine-related-targets-11594906060 [↑](#footnote-ref-95)
96. Встреча президентов в киберопасности // Официальный сайт информационного агентства Коммерсантъ. URL: https://www.kommersant.ru/doc/4003491 [↑](#footnote-ref-96)
97. U.S. Escalates Online Attacks on Russia’s Power Grid // Official website of the news agency The New York Times. URL: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?action=click&module=Top%20Stories&pgtype=Homepage [↑](#footnote-ref-97)
98. «На страже киберграниц». Замсекретаря Совбеза — о защите интересов страны // Официальный сайт информационного агентства Аргументы и Факты. URL: https://aif.ru/politics/world/na\_strazhe\_kibergranic\_zamglavy\_sovbeza\_-\_o\_zashchite\_interesov\_strany [↑](#footnote-ref-98)
99. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (16.06.2009). URL: http://base.spinform.ru/show\_doc.fwx?rgn=28340 [↑](#footnote-ref-99)
100. «На страже киберграниц». Замсекретаря Совбеза — о защите интересов страны // Официальный сайт информационного агентства Аргументы и Факты. URL: https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-24-Feb19.pdf [↑](#footnote-ref-100)
101. Bastien Inzaurralde. The Cybersecurity 202: Trump's efforts failed to make critical infrastructure safer from cyberattacks, experts say // Official website of the news agency The Washington Post. URL: https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/03/05/the-cybersecurity-202-trump-s-efforts-failed-to-make-critical-infrastructure-safer-from-cyberattacks-experts-say/5c7d6c5b1b326b2d177d5fbd/ [↑](#footnote-ref-101)
102. The Cybersecurity 202: Trump took the nation in the wrong direction on cybersecurity, experts say // https:// The Washington Post news agency official website. URL: www.washingtonpost.com/politics/2020/12/15/cybersecurity-202-trump-took-nation-wrong-direction-cybersecurity-experts-say/ [↑](#footnote-ref-102)
103. Connecting cybersecurity experts across government and industry in an ongoing survey. // The Washington Post news agency official website. URL: https://www.washingtonpost.com/graphics/2018/politics/powerpost/thenetwork/ [↑](#footnote-ref-103)
104. The Cybersecurity 202: A Russian mega-hack is further damaging Trump’s cybersecurity legacy // The Washington Post news agency official website. URL: https://www.washingtonpost.com/politics/2020/12/14/cybersecurity-202-russian-mega-hack-is-further-damaging-trumps-cybersecurity-legacy/ [↑](#footnote-ref-104)
105. DHS, State and NIH join list of federal agencies — now five — hacked in major Russian cyberespionage campaign // The Washington Post news agency official website. URL: https://www.washingtonpost.com/national-security/dhs-is-third-federal-agency-hacked-in-major-russian-cyberespionage-campaign/2020/12/14/41f8fc98-3e3c-11eb-8bc0-ae155bee4aff\_story.html?wpmk=1&wpisrc=al\_news\_\_alert-national--alert-world--alert-politics&utm\_source=alert&utm\_medium=email&utm\_campaign [↑](#footnote-ref-105)
106. The Cybersecurity 202: Trump took the nation in the wrong direction on cybersecurity, experts say // The Washington Post news agency official website. URL: https://www.washingtonpost.com/politics/2020/12/15/cybersecurity-202-trump-took-nation-wrong-direction-cybersecurity-experts-say/ [↑](#footnote-ref-106)
107. Trump fires head of election cybersecurity who debunked conspiracy theories. // NBCNews news agency official website. URL: https://www.nbcnews.com/tech/security/trump-fires-head-u-s-election-cybersecurity-after-he-debunked-n1248063 [↑](#footnote-ref-107)
108. При атаке на SolarWinds взломали e-mail ответственных за кибербезопасность США. // Официальный сайт информационного агентства Интерфакс. URL: https://www.interfax.ru/world/758340 [↑](#footnote-ref-108)
109. The Microsoft Exchange Server hack: A timeline // The CSO official website. URL: https://www.csoonline.com/article/3616699/the-microsoft-exchange-server-hack-a-timeline.html [↑](#footnote-ref-109)
110. Hackers Breached Colonial Pipeline Using Compromised Password // Bloomberg news agency official website. URL: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password [↑](#footnote-ref-110)
111. FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation’s Cybersecurity // Biden White House official website. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/ [↑](#footnote-ref-111)
112. FACT SHEET: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure // Biden White House official website. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/ [↑](#footnote-ref-112)
113. DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators // US Government Department of Homeland Security official website. URL: https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators [↑](#footnote-ref-113)
114. Update on the International Counter-Ransomware Initiative // US Department of State official website. URL: https://www.state.gov/briefings-foreign-press-centers/update-on-the-international-counter-ransomware-initiative [↑](#footnote-ref-114)
115. Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021 // Biden White House official website. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/ [↑](#footnote-ref-115)
116. FACT SHEET: President Biden Signs National Security Memorandum to Improve the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems // Biden White House official website. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/19/fact-sheet-president-biden-signs-national-security-memorandum-to-improve-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/ [↑](#footnote-ref-116)
117. Biden Administration Says Talks with Russia on Cyber Attacks Are Progressing. Privately, Staffers Are Skeptical. // Official website of the TIME news agency. URL: https://time.com/6078997/biden-cyber-attacks-putin/ [↑](#footnote-ref-117)
118. Biden firmly believes in top-level cyber security cooperation with Russia — official // Official website of the news agency TASS. URL: https://tass.com/world/1312585?utm\_source=google.com&utm\_medium=organic&utm\_campaign=google.com&utm\_referrer=google.com [↑](#footnote-ref-118)
119. The ice between the U.S. and Russia may be thawing — for now // The Washington Post News Agency official website. URL: https://www.washingtonpost.com/opinions/2021/10/19/ice-between-us-russia-may-be-thawing-now/ [↑](#footnote-ref-119)
120. Президенты России и США заявили о готовности продолжать сотрудничество в области кибербезопасности // Официальный сайт информационного агентства D.Russia. URL: https://d-russia.ru/prezidenty-rossii-i-ssha-zajavili-o-gotovnosti-prodolzhat-sotrudnichestvo-v-oblasti-kiberbezopasnosti.html [↑](#footnote-ref-120)
121. Readout of President Biden’s Video Call with President Vladimir Putin of Russia // Biden White House official website. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/07/readout-of-president-bidens-video-call-with-president-vladimir-putin-of-russia/ [↑](#footnote-ref-121)
122. Statement by President Biden on our Nation’s Cybersecurity // Official website of the Bidan White House. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/ [↑](#footnote-ref-122)
123. Байден поручил усилить кибербезопасность в США из-за российских хакеров // Официальный сайт новостного агентства Лента. URL: https://lenta.ru/news/2022/03/23/haker/ [↑](#footnote-ref-123)
124. Ibid. [↑](#footnote-ref-124)
125. Shields Up // Official CISA website. URL: https://www.cisa.gov/shields-up [↑](#footnote-ref-125)