МІЖНАРОДНИЙ ДОСВІД

UDC 351.817:004.946.5.056(73)(477) doi: https://doi.org/10.33270/01191134.119

Shemchuk V. – Ph.D in Law, Associate Professor of the Department of Constitutional and International Law of the V. I. Vernadsky Taurida National University, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-7969-6589

National Cyber Strategy of the United States of America: Experience for Ukraine

*The **purpose** of the article is to investigate the positive practice of securing the US cybersecurity in the context of its possible implementation in Ukraine. For its achievement the following tasks were formed: to describe the National cybersecurity strategy of the USA as a political and legal document – to research the institutional mechanism of cybersecurity; to uncover perspective possibilities for introducing positive experience of the USA and Counting negative experience in this area. **Methodology.** Methodological instruments are defined based on the specified purpose, objectives and specifics of the study. In the fundamentals of nom The comparative-legal and historical methods were used to determine the peculiarities of the development and adoption of the national strategy of the USA and other states; system and gnoseological methods – to establish the contents of the so-called categories and phenomena as cyberspace, cybersecurity; dialectical and Formal-Legal – in the process of and scientific provisions; modeling and Forecasting methods – to determine the promising directions of improvement of national practice in this field. **Scientific novelty** consists in figuring out the nature and the US cyber strategy, their significance for National and international law. Paid attention to the structural characteristics of the latest National strategies of 2017 and 2018, their importance for the national security of the USA. Thus the key areas are the protection of the American people, America and American lifestyle, ensuring the prosperity of America, preserving the peace by promotion of American influence. The fundamental principle enshrined freedom of the Internet, prosperity, security and openness of the network world. In our opinion, Ukraine has the appropriate definition of relevant foreign policy landmarks in this area aimed at preventing and eliminating cyber threats. **Conclusions.** The National Cyber strategy of the United States since 2018 is focused on preserving leadership, enhancing the impact and promotion of U.S. interests in the international arena. Security of cyberspace is a part of their national security, which is confirmed by the correlation of areas of the eponymous strategies. The priorities recognize the development and introduction of a multilateral Internet governance model, the need to prevent the use of freedom online to create political threats. As the development and resilience of the digital economy is regarded as the basis of American prosperity, the primary steps are: developing innovations and investing in the infrastructure of recent generations with the involvement of the private sector and civil society; Development of international cooperation; Creation of personnel reserve, improvement of the potential of specialists in the field of cyber defense.*

Keywords: cyberarea; cybersecurity; information security state; USA; ensuring.

Introduction

The United States was one of the first to realize the strategic importance of cyberspace security. The development of the information sphere, its increasing role in the life of society and the state, and the associated increase in threats in an increasingly dependent economy on information and communication technologies, and the terrorist acts of 2001, led to the adoption of the National Strategy to Secure Cyberspace of 2003.

The purpose

The purpose of the article is to investigate the positive practice of securing the US cybersecurity in the context of its possible implementation in Ukraine. For its achievement the following tasks were formed: – to describe the National cybersecurity strategy of the USA as a political and legal document – to research the institutional mechanism of cybersecurity security; – to uncover perspective possibilities for introducing positive experience of the USA and Counting negative experience in this area.

Theoretical bases of the research in the basis of the research methodology are the general theoretical and special methods of scientific knowledge, principles and approaches regarding the definition of concepts «cybersecurity», «cyberarea», «information security» ect. Some aspects problem of achieving cybersecurity are devoted to the work of such scholars as: E. Beling, E. M. Brunner, M. O'Connell, N. Kaminska (Kaminska, 2014), O. Kiriluik, M. Mueller, A. Pazuik, R. Suter, M. Tarnogyrski, S. Watts etc.

Presentation of the main material

In National Strategy to Secure Cyberspace of 2003 the responsibility for cyberspace security was shared between agencies and federal ministries, and the coordinating body was established a year earlier by the Department of Homeland Security. At the same time, more than 50 points of the Cyber Threat Prevention and Information Network were launched.

In 2009, a «Cyberspace Policy Review» was presented, which, based on an analysis of the cyber

security system in place, proposed a plan to improve it to better provide US cyber security. This review was based on the Comprehensive National Cybersecurity Initiative of 2008. Key changes in the cyberspace security system were to create a position of state cybersecurity policy coordinator responsible for interagency engagement, overall development of policy and policy, and reducing the role of government in protection of infrastructure. From now on, private companies had to provide their own security in cyberspace, and the state retained the function of general guidance and standardization.

The development of international cyber defense cooperation has led to acceptance «International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World» of 2011 ("International Strategy").

This Strategy, by its very nature, was the first political and strategic document that enshrined a comprehensive regulatory approach on a wide range of issues in cyberspace, and defined cyberspace itself as an independent subject area of regulation requiring international cooperation. The purpose of this strategy was to create a unified platform for international cyberspace engagement based on US approaches to cybersecurity. To implement US cyberspace policy, the position of Coordinator for Cyber Issues at the US Department of State was created.

An important direction of the US International Cyberspace Strategy was capacity building through provided assistance to developing countries by providing them with the necessary knowledge, resources, and professionals, including developing national cybersecurity strategies ("International Strategy").

An example of US cooperation with other countries in the field of cyber defense is the signing in 2013 of the Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building, which spelled out cooperation in the field of protection of critical information systems and mechanisms reducing the level of danger in cyberspace. To date, these agreements have been halted because of Russia's aggression against Ukraine.

In September 2018, the new US Administration presented its vision for cyberspace protection policies in the National Cyber Strategy of the US (hereinafter – US Cyber Strategy). This document is based on the Executive Order, «Strengthening of Federal Networks and Critical Infrastructure» ("President Executive") and on the National Security Strategy of the United States of America of 2017 ("National Cyber Strategy", 2017). The US Cyber Strategy structurally consists of the following pillars: «Pillar I: Protect the American People, the Homeland, and the American way of life», «Pillar II: Promote American Prosperity», «Pillar III: Preserve peace through strength», «Pillar IV: Advance American influence». Each pillar establishes areas, defined objective and relevant priority actions.

Named pillars of the US Cyber Strategy are correlated with the tasks of the US Presidential Administration in the field of cyber defense, namely:

– Defend the homeland by protecting networks, systems, functions, and data;

– Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation;

– Preserve peace and security by strengthening the ability of the United States – in concert with allies and partners – to deter and, if necessary, punish those who use cyber tools for malicious purposes; and Expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet ("National Cyber Strategy", 2018, p. 14).

Any strategy is developed on the basis of an assessment of risks, threats, trends, potential, etc., that is, an analysis of the situation. In the US Cyber Strategy, the analysis of the current situation is presented in the following directions:

1. Statement of increasing influence of cyberspace on all spheres of public life of the modern world in general, and on the political, social, economic, public life of America in particular.

2. Supporting and promoting the American vision of an open, interoperable, reliable, and secure Internet.

3. Recognition the facts of the use of the adversaries and competitors of the benefits of free Internet to harm the economic, military and political interests of the United States, their partners and allies.

It is noticeable that the Russian Federation, Iran and North Korea are directly accused of a series of hacking attacks against US and multinational companies and their partners. China is accused of using cyberspace to conduct economic espionage and theft of intellectual property worth trillions of dollars.

It also notes threats from non-governmental organizations, including terrorist and criminal groups, which use cyberspace to profit, recruit new members, promote their ideas, and attack the United States, their allies and partners.

It is advisable to look more closely at the main elements of the US Cyber Strategy, the objectives, and the content units that define priority actions.

Pillar I: Protect the American People, the Homeland, and the American way of life formulates a key objective – manage cybersecurity risks to increase the security and resilience of the Nation's information and information systems. This basic element comprises of three units.

Unit 1.Secure federal networks and information provides for such priority actions: further centralize

management and oversight of federal civilian cybersecurity; align risk management and information technology activities; improve federal supply chain risk management; strengthen federal contractor cybersecurity; ensure the government leads in best and innovative practices.

A new trend in cyber defense policy is the development of a federal-level supply chain risk management system that includes, inter alia, defining clear authority to exclude (in some cases) from the supply and procurement process of those suppliers of products and services that are considered risky. These actions will be combined with risk management efforts across supply chains related to the nation's infrastructure ("National Cyber Strategy", 2018). It seems that the degree of risk of using products of the supplier's must be determined on a case-by-case basis.

An example of cyberspace security in this area is the information campaign against Chinese hardware manufacturer Supermicro. Recent media reports, citing an investigation by Bloomberg Businessweek, have referred to the introduction of hardware bookmarks by the Chinese government into server boards used by many US companies, including Amazon and Apple ("The Big Hack", 2018).

The bookmark chips were reportedly inserted during the production process at Supermicro plants by operative agents from the People's Liberation Army of China.

Unit 2. Secure critical infrastructure covers the following priority actions: refine roles and responsibilities; prioritize actions according to identified national risks; leverage information and communications technology providers as cybersecurity enablers; protect our democracy; incentivize cybersecurity investments; prioritize national research and development investments; improve transportation and maritime cybersecurity; improve space cybersecurity.

It is necessary to note that the US considers unimpeded access and freedom of action in space a vital element of ensuring their security and economic prosperity. Considered these assets are critical to functions such as positioning, navigation, and timing (PNT); intelligence, surveillance, and reconnaissance (ISR); satellite communications; and weather monitoring. In connection with what Administration intends to intensify efforts to protect current and future space assets and support infrastructure against cyber threats through interaction with industry and international partners ("National Cyber Strategy", 2018, p. 10).

Space troops are already being created in the United States, with China and the Russian Federation being the main opponents in this area.

Unit 3. Combat cybercrime and improve incident reporting includes the following priority actions: improve incident reporting and response; modernize electronic surveillance and computer crime laws; reduce threats from transnational criminal organizations in cyberspace; improve apprehension of criminals located abroad; strengthen partner Nations' law enforcement capacity to combat criminal cyber activity.

Improvement of the computer crime legislation provides for the expansion of law enforcement agencies' ability to lawfully gather the necessary evidence of criminal activity and to carry out further investigative and judicial proceedings. Gathering the necessary information may also occur outside the United States. Previously, the so-called mutual legal assistance agreements implemented, including within the framework of the Budapest Convention on Cybercrime, were used to carry out such activities, then the «CLOUD Act» S2383 ("Clarifying Lawful", 2018) adopted this year gives law enforcement authorities considerable powers to obtain information that stored on those servers of US companies located outside the United States. Thus, the conclusion of agreements and the corresponding notification of States on the conduct of investigative measures in their territory is no longer required.

Threat Reduction Activities from Transnational Crime Organizations in Cyberspace are envisaged to be carried out by giving federal ministries and agencies necessary legal authorities and resources to combat transnational cybercriminal activity, including identifying and dismantling botnets, dark markets, and other infrastructure used to enable cybercrime, and combatting economic espionage. To effectively deter, disrupt, and prevent cyber threats, law enforcement will work with private industry to confront challenges presented by technological barriers, such as anonymization and encryption technologies, to obtain time-sensitive evidence pursuant to appropriate legal process. Law enforcement actions to combat criminal cyber activity serve as an instrument of national power by, among other things, deterring those activities ("National Cyber Strategy", 2018, p. 10).

Pillar II: Promote American Prosperity defines the key objective: preserve United States influence in the technological ecosystem and the development of cyberspace as an open engine of economic growth, innovation, and efficiency. This pillar consists of three units.

Unit 1. Foster a vibrant and resilient digital economy focuses on priority actions such as: incentivize an adaptable and secure technology marketplace; prioritize innovation; invest in next generation infrastructure; promote the free flow of data across borders; maintain United States leadership in emerging technologies; promote full-lifecycle cybersecurity.

Fostering and protecting American invention and innovation is critical to maintaining the United States' strategic advantage in cyberspace. The United States Government will nurture innovation by

promoting institutions and programs that drive United States competitiveness. The United States Government will counter predatory mergers and acquisitions and counter intellectual property theft. It will also catalyze United States leadership in emerging technologies and promote government identification and support to these technologies, which include artificial intelligence, quantum information science, and next-generation telecommunication infrastructure ("National Cyber Strategy", 2018, p. 16).

Supporting US leadership in cutting-edge technology also involves promoting US cybersecurity innovations around the world in the following ways:

1) utilizing trading operations;

2) raising awareness of innovative tools and services in the field of American origin and manufacturing cybersecurity;

3) exposing and countering repressive regimes that use such tools and services to violate human rights;

4) Removing barriers to creating a single global cybersecurity market.

Unit 2. Foster and protect United States ingenuity provides for such priority actions: update mechanisms to review foreign investment and operation in the United States; maintain a strong and balanced intellectual property protection system; protect the confidentiality and integrity of American ideas.

Unit 3. Develop a superior cybersecurity workforce consists of such priority actions: build and sustain the talent pipeline; expand re-skilling and educational opportunities for America's workers; enhance the federal cybersecurity workforce; use executive authority to highlight and reward talent.

Pillar III: Preserve peace through strength there an objective is: identify, counter, disrupt, degrade, and deter behavior in cyberspace that is destabilizing and contrary to national interests, while preserving United States overmatch in and through cyberspace. This pillar has two units.

Unit 1. Enhance cyber stability through norms of responsible state behavior provides for priority actions as encourage universal adherence to cyber norms.

Unit 2. Attribute and deter unacceptable behavior in cyberspace aims at the need for such priority actions as: lead with objective, collaborative intelligence; impose consequences; build a cyber-deterrence initiative; counter malign cyber influence and information operations.

Pillar IV: Advance American influence as an objective formulates: preserve the long-term openness, interoperability, security, and reliability of the Internet, which supports and is reinforced by United States interests.

Unit 1. Promote an open, interoperable, reliable, and secure Internet includes such priority actions: protect and promote Internet freedom; work with like-minded countries, industry, academia, and civil society; promote a multi-stakeholder model of Internet governance; promote interoperable and reliable communications infrastructure and Internet connectivity; promote and maintain markets for United States ingenuity worldwide.

The principle of Internet freedom is at the heart of the American Cyber Strategy. The United States declares its intention to promote this principle as an international standard. At the same time, any attempt by other states to restrict this freedom, even under the pretext of combating terrorism and security, is recognized as a political threat and a sign of authoritarianism.

The Internet is seen as an area of freedom of expression, the right to peaceful assembly and privacy, and, accordingly, the principle of Internet freedom is a guarantee of these rights and a component of national security.

At the same time, the freedom of expression on the Internet is also seen in the context of the free dissemination of information on the Internet, which promotes the development of international trade and commerce, the development and implementation of innovations, and enhances both national and international security. Online freedom of expression is also seen as an important aspect of US foreign policy, including the fight against cybercrime and terrorism.

The United States emphasizes its assistance to other countries in promoting freedom of expression on the Internet through venues such as the Freedom Online Coalition, of which the United States is a founding member.

In this direction, the United States is planning to introduce a multilateral Internet governance model internationally. The essence of which is transparency and equal participation of the state, the private sector, civil society, academia and the technical community in Internet governance.

Unit 2. Build international cyber capacity relates to priority actions to enhance cyber capacity building efforts.

Thus, it is expected to step up efforts to share automated and actionable cyber threat information, enhance cybersecurity coordination, and promote analytical and technical exchanges. In addition, the United States will work to reduce the impact and influence of transnational cybercrime and terrorist activities by partnering with and strengthening the security and law enforcement capabilities of our partners to build their cyber capacity ("National Cyber Strategy", 2018, p. 26).

Scientific novelty

The scientific novelty is to find out the nature and nature of US cyber strategies, their importance for national and international law and order. The structural features and content of the latest national strategies for 2017 and 2018 underscore the

importance of the following key areas for US national security: protecting the American people, America and the American way of life, ensuring America's prosperity, keeping the peace by coercion, and promoting American influence.

The fundamental principle enshrined freedom of the Internet, prosperity, security and openness of the network world. In our opinion, Ukraine has the appropriate definition of relevant foreign policy landmarks in this area aimed at preventing and eliminating cyber threats.

In view of the assetsofne reforming different spheres of social and state life in Ukraine, entering the world and European information spaces, development of information-communication and other technologies, national legislation of Ukraine demonstrates some progress. Thus, a number of laws and by-laws regulations of Ukraine have been adopted, in particular, the Laws of «Basic principles of cybersecurity of Ukraine» dated October 5, 2017 No. 2163-VIII; «On the national security of Ukraine» June 21, 2018 No. 2469-VIII, Strategy of the Information society development in Ukraine, approved by the Decree of the Cabinet of Ministers of Ukraine on May 15, 2013 No. 386-p. etc.

In our opinion, it is possible to borrowings taking into account national peculiarities in part of legislative consolidation of the advancement of Ukrainian influence, protection of Ukrainians, way of life, ensuring prosperity of Ukraine, restoration and preservation of peace, along with the consolidation of the principle of freedom of the Internet, prosperity, security and openness of the network world. For Ukraine, it is reasonable to define relevant foreign policy landmarks in Cyber threats. Proposals regarding the improvement of the potential of cyber defence professionals, development of innovations and investment in the infrastructure of recent generations with the involvement of private sector and civil society are noteworthy.

Conclusions

The US Cyber Strategy of 2018 is focused on maintaining leadership, leveraging and promoting US interests internationally. US cyberspace security is a component of their national security, as evidenced by the correlation of the directions of the eponymous strategies. The protection of online space in the United States is based on the principles of Internet freedom. In this aspect, the development and implementation of a multilateral internet governance model is a priority. At the same time, it recognizes the need to prevent the use of freedom on the Internet to create political threats.

The development and sustainability of the digital economy is seen as the cornerstone of American prosperity. In this vector, the following are the priority steps: development of innovation and investment in the latest generation of infrastructure with the involvement of the private sector and civil society; development of international cooperation; creation of personnel reserve, which provides training, development, improvement of the capacity of specialists in the field of cyber defense. It is important moment that exactly highly qualified cybersecurity personnel are recognized by the US as its strategic asset for national security, so that the search for young talents and professionals is carried out by government around the world through a variety of government programs.

REFERENCES

Clarifying Lawful Overseas Use of Data Act. (2018). CLOUD Act S2383. (n.d.). *www.congress.gov.* Retrieved from https://www.congress.gov/bill/115th-congress/senate-bill/2383/all-info.

Demchenko, P. (2018). Kibernetychna bezpeka yak novitnii napriam informatsiinoi skladovoi natsionalnoi bezpeky Ukrainy: konstytutsiino-pravovyi aspekt [Cyber security as a new trend in the information component of Ukraine's national security: constitutional and legal aspects]. *Visnyk Lvivskoho natsionalnoho universytetu imeni I. Franka, Bulletin of Lviv National University named after I. Franko, 67.* doi: http://dx.doi.org/10.30970/vla.2018.67.170 [in Ukrainian].

International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World. (n.d.). *www.whitehouse.gov.* Retrieved from http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Kaminska, N., & Bondar, I. (2018). Protydiia kiberzlochynnosti: mizhnarodnyi dosvid ta novely natsionalnoho zakonodavstva [Cybercrime: International experience and national legislation]. *Pravovi reformy v Ukrainy: realii sohodennia, Legal reforms in Ukraine: the realities of today:* Proceedings of the Interstitial Scientific Practical Conference. Kyiv: NAVS [in Ukrainian].

Kaminskaia, N.V. (2014). Vliianie globalizatsionnykh tendentsiy na stanovlenie regionalnykh pravovykh sistem [The impact of globalization trends on the formation of regional legal systems]. *Mezndunarodnoe pravo, International law, 2.* 20-33. Retrieved from http://e-notabene.ru/wl/article.10941.html. doi: 10.7256/2306-899.2014.2.10941 [in Russian].

National Cyber Strategy of the United States of America. (2017). (n.d.). *www.whitehouse.gov.* Retrieved from https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

National Cyber Strategy of the United States of America. (2018). (n.d.). *www.whitehouse.gov.* Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

President Executive Order 13800 Strengthening of Federal Networks and Critical Infrastructure. (n.d.). *www.dhs.gov.* Retrieved from https://www.dhs.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure.

Shemchuk, V. (2019) Problems of definition freedoms s information and realization on the temporarily occupied territory of Ukraine. *Ukrainian journal of inetnational law*, 2.

Shemchuk, V.V. (2019). Informatsiina bezpeka ta informatsiina oborona v konteksti rozvytku vitchyznianoi doktryny i zakonodavchoi osnovy [Information security and information defense in the context of the development of national doctrine and legislative framework]. *Vcheni zapysky TNU imeni V.I. Vernadskoho, Scientific notes of TNU Vernadsky, 4,* 31-37. doi: https://doi.org/10.32838/1606-3716/2019.4/06 [in Ukrainian].

The Big Hack. (2018): How China Used a Tiny Chip to Infiltrate U.S. *Site "Bloomberg"*. Retrieved from https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

Стаття надійшла до редколегії 19.09.2019

Шемчук В. В. – кандидат юридичних наук, доцент кафедри конституційного та міжнародного права Таврійського національного університету імені В. І. Вернадського, м. Київ
ORCID: https://orcid.org/0000-0001-7969-6589

Національна стратегія кібербезпеки США: досвід для України

Метою *статті є вивчення позитивної практики забезпечення кібербезпеки США в контексті перспектив її можливого запровадження в Україні. Задля її досягнення було сформульовано такі завдання: схарактеризувати Національну стратегію кібербезпеки США як політико-правовий документ; дослідити інституційний механізм забезпечення кібербезпеки; висвітлити перспективні можливості впровадження позитивного досвіду США і необхідність врахування негативного досвіду в цій сфері.* ***Методологія.*** *Методологічний інструментарій визначено відповідно до зазначеної мети, завдань і специфіки дослідження. Було використано порівняльно-правовий та історичний методи для визначення особливостей розроблення та прийняття національної стратегії США, інших держав; системний гносеологічний і структурно-функціональний методи – для встановлення змісту таких категорій та явищ, як кіберпростір, кібербезпека; діалектичний і формально-юридичний – у процесі формулювання основних понять і наукових положень; методи моделювання і прогнозування – для визначення перспективних напрямів удосконалення вітчизняної практики в цій сфері.* ***Наукова новизна*** *полягає в з'ясуванні сутності кіберстратегій США, їх значення для національного й міжнародного правопорядку. Увагу акцентовано на структурних характеристиках національних стратегій 2017-го і 2018 років, їх важливості для національної безпеки цієї країни. Ключовими напрямами визначено захист американського народу, Америки й американського способу життя, забезпечення процвітання, збереження миру методом примусу, поширення американського впливу. Основоположними принципами закріплено свободу Інтернету, процвітання, безпеку й відкритість мережевого світу. Для України доцільно окреслити відповідні зовнішньополітичні орієнтири в цій сфері, спрямовані на попередження та усунення кіберзагроз.* ***Висновки.*** *Національна кіберстратегія США від 2018 року орієнтована на збереження лідерства, посилення впливу й утвердження інтересів США на міжнародній арені. Безпека кіберпростору є складовою їх національної безпеки, що засвідчує кореляція напрямів однойменних стратегій. Пріоритетними визнано розроблення та запровадження багатосторонньої моделі управління Інтернетом, необхідність запобігання використанню свободи в мережі для створення політичних загроз. Оскільки розвиток і стійкість цифрової економіки є основою американського процвітання, першочерговими кроками визначено: розроблення інновацій та інвестування в інфраструктуру останніх поколінь із залученням приватного сектору та громадянського суспільства; розвиток міжнародного співробітництва; створення кадрового резерву, удосконалення потенціалу спеціалістів у сфері кіберзахисту.*

Ключові слова: кіберпростір; стратегія; кібербезпека; інформаційна безпека; США; забезпечення.