ISSN 2518-1521 (Online), ISSN 2226-2830 (Print)
ВІСНИК МАРІУПОЛЬСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ
СЕРІЯ: ІСТОРІЯ. ПОЛІТОЛОГІЯ, 2018, ВИП. 21

УДК 327.8.019.51

P. Katerynchuk

CHALLENGES AND THREATS OF UKRAINE'S NATIONAL CYBER SECURITY IN HYBRID WAR

Cyber space of Ukraine for a long time remained out of attention of domestic researchers and, therefore, state officials. For more than 20 years, the young Ukrainian state did not waste its efforts on the formation of not only effective and reliable troops, but also information security. The government did not endeavoured to strengthen the country's defence, and only weakened its lack of progress in fighting corruption and the dominance of Russian media and intelligence. As a result, in the spring of 2014, after a long confrontation between the regime of Viktor Yanukovych and the citizens of Ukraine, Russia failed to conduct special operations with the aim of annexing the Crimea and facilitate the war in Donbas. Not the least role in this played a raid for information and factors cyber Russian hackers for the purpose of paralysing government agencies and influence on public opinion in Ukraine through Russian-controlled media.

As a result of prolonged and massive cyberattacks, Ukrainian state structures, the banking system, industrial facilities and private business suffered significant material and reputational losses. At the same time in Ukraine began to realize the seriousness of cyber security as a component of national security and contribute to creating cyber police, national cybersecurity strategy, acceptance of a number of regulations on cyber security, strengthening public defense for the protection of domestic cyber space. At the moment, Ukraine is on the way to rethinking the role of cyber security and the formation of a national system of protection against cyber threats.

Key words: *cyberspace, cybersecurity, hacker attacks, information security.*

Introduction. The hybrid war in the East of Ukraine and the information confrontation with Russia as a state that systematically uses the media space and the Internet to achieve its political goals, necessitates the study of the issue of protecting the cyberspace of Ukraine as an integral part of the state's information security. For the first time, Russian cyber threats and possible cyber attacks began to speak during the 2016 US election campaign, when, according to many researchers, the intervention of Russian hackers and the hacking of the electronic mailbox of the Democratic Party, Hillary Clinton, influenced the electoral campaign and electoral sympathies of Americans. However, these were only echoes of a long and purposeful campaign of Russian intelligence services, which increasingly involve cyberspace and electronic media of mass communication for espionage and undermining the interests of the Kremlin. At the same time, hacker attacks on government structures and industrial facilities occurred earlier, and not only within the same continent.

Analysis of recent research and publications. The study of the security of cyberspace as a component of information security has become the subject of scientific research by foreign and Ukrainian scientists, in particular D. Dubov, A. Gor, M. Ozhevan, V. Butuzova, C. Borys, E. Nakashima, P. Polityuk etc.

However, despite a fairly large number of studies and publications on the topic of information and cyber security, their analysis shows that researchers have considered only general issues of developing a national system of cybernetic security as an integral element of the information security system.

Therefore, the aim of this article is to study the protection of the cyberspace as a component of Ukraine's information security.

Presentation of the main research material. The United States reacted to Russia's hacking attacks by introducing new sanctions against companies and individuals that prohibited any operations within the US financial system. In addition, sanctions prohibit American companies and citizens from having business related to companies and sanctioned individuals. Persons included in the sanction list - Alexander Tribun, Oleg Chirikov and Volodymyr Kagansky - are believed to have a relationship with «Divetechnoservis», a company specializing in hacking attacks on underwater communications systems [23]. Among the examples of «malicious and destabilizing activity» of the US Department of the Treasury calls the NotPetya virus and an attack on power distribution networks. In February 2018, the White House said that the damage caused by the NotPetya virus in Europe, Asia, and America was calculated in billions of dollars. The NotPetya attack in the White House was named part of the Kremlin's efforts to destabilize the situation in Ukraine, which is increasingly demonstrating Russia's participation in the ongoing conflict [21].

Russia denies involvement in the attack and indicates that Russian companies have also suffered from it. However, the British ministers also said that Russian cyberattacks are NotPetya [22]. The British Foreign Ministry says: «The cyberattack looked like extortion, but the true purpose of the virus was not to get a ransom, but to break the work of the Ukrainian state institutions, the financial and energy sectors of the economy». On the first day of the spread of the virus, June 27, it struck 2,000 organizations, 75% of the victims fell to Ukraine. Ukrainian ministries, police, banks, Boryspil airport, Kyiv metro, media, mobile operators, medical companies have suffered. The virus blocked computers and demanded money in exchange for restoring access to locked programs. British prime minister Theresa May has blamed President Putin in November last year for trying to «sow discord» in the west - through interference in elections, dissemination of misinformation and cyberwar.

Theresa May has accused Russia of meddling in elections and planting fake stories in the media in an extraordinary attack on its attempts to «weaponise information» in order to sow discord in the west. Listing Russia’s attempts to undermine western institutions in recent years, she said: «I have a very simple message for Russia. We know what you are doing. And you will not succeed» [9]. Since Russia’s annexation of Crimea from Ukraine, May said Russia had «fomented conflict in the Donbass [eastern Ukraine], repeatedly violated the national airspace of several European countries, and mounted a sustained campaign of cyber-espionage and disruption» [7].

American and British officials said that the attacks disclosed on Monday affected a wide range of organizations including internet service providers, private businesses and critical infrastructure providers. They did not identify victims or provide details on the impact of the attacks. «When we see malicious cyber activity, whether it be from the Kremlin or other malicious nation-state actors, we are going to push back», said Rob Joyce, the White House cyber security coordinator.

Earlier, in February 2018, German officials also accused Russia of hacking attacks on government sites. In particular, according to media reports, hackers from the grouping of APT28, also known as Fancy Bears, at the end of February successfully attacked the German Foreign and Defence Ministries, entered the so-called Berlin-Bonn Information Network (IVBB), which is used by the Federal Chancellery of Germany, the federal ministries and services security, as well as the Bundestag and the Bundesrat [17].

Along with the statements of the official agencies of the United States, Great Britain and Germany, NATO has adopted a consolidated decision on Russia's destabilizing role in the modern world, which is expressed in «a long illegal and illegitimate annexation of the Crimea, violations of sovereign borders with the use of force; intentional destabilization of the situation in eastern Ukraine; the sudden launch of large-scale military exercises contrary to the spirit of the Vienna Document and provocative military action at NATO's borders, including in the

regions of the Baltic and Black Seas and the Eastern Mediterranean; irresponsible and aggressive nuclear rhetoric, as well as repeated violations of Russia's airspace by Allies» [15].

In communiqué after the Warsaw summit NATO has clearly noted that cyber attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. «We agreed in Wales that cyber defence is part of NATO's core task of collective defence. Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognize cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. It will support NATO's broader deterrence and defence: cyber defence will continue to be integrated into operational planning and Alliance operations and missions, and we will work together to contribute to their success. Furthermore, it will ensure more effective organization of NATO's cyber defence and better management of resources, skills, and capabilities» [15].

However, these examples of violations of the national cyberspace of the Western powers are just the tip of the iceberg, which hides years of agency activity and attempts to control the media from Russia.

Undoubtedly, Ukraine is the main base for cyber crime and cyber attacks on Russia. This is the meaning of the hybrid nature of the war, which, besides the military component itself, also includes powerful information campaigns, misinformation, fake news and hacking activities.

Purposeful cyber attacks against Ukraine began simultaneously with the events of March 2014, when Russia virtually annexed the Crimea by bringing its troops into the peninsula [8]. At the same time with the annexation of the Crimea in Ukraine began massive DDoS attacks by the so-called CyberBerkut. CyberBerkut is a modern organized group of pro-Russian hacktivists. The group became locally known for a series of publicity stunts and distributed denial-of-service (DDoS) attacks on Ukrainian government, and western or Ukrainian corporate websites [13].

During the period of 2014-2017, about 6,000 hacker attacks were committed against Ukraine [18]. Undoubtedly, the most powerful of the famous cyber attacks took place on June 27, 2017 [3]. A series of powerful cyberattacks using the Petya malware began on 27 June 2017 that swamped websites of Ukrainian organizations, including banks, ministries, newspapers and electricity firms. Similar infections were reported in France, Germany, Italy, Poland, Russia, United Kingdom, the United States and Australia. ESET estimated on 28 June 2017 that 80% of all infections were in Ukraine, with Germany second hardest hit with about 9% (Cyber-attack was about data and not money, say experts, 2017) [5]. On 28 June 2017, the Ukrainian government stated that the attack was halted. On 30 June 2017, the Associated Press reported experts agreed that Petya was masquerading as ransomware, while it was actually designed to cause maximum damage, with Ukraine being the main target [1].

The cyberattack was based on a modified version of the Petya ransomware. Like the WannaCry ransomware attack in May 2017, Petya uses the EternalBlue exploit previously discovered in older versions of the Microsoft Windows operating system. When Petya is executed, it encrypts the Master File Table of the hard drive and forces the computer to restart. It then displays a message to the user, telling them their files are now encrypted and to send US$300 in bitcoin to one of three wallets to receive instructions to decrypt their computer. At the same time, the software exploits the Server Message Block protocol in Windows to infect local computers on the same network, and any remote computers it can find.

Security experts found that the version of Petya used in the Ukraine cyberattacks had been modified, and subsequently has been named NotPetya or Nyetna to distinguish it from the original malware. NotPetya encrypted all of the files on the infected computers, not just the Master File Table, and in some cases the computer's files were completely wiped or rewritten in a manner that could not be undone through decryption. Some security experts saw that the

software could intercept passwords and perform administrator-level actions that could further ruin computer files. They also noted that the software could identify specific computer systems and bypass infection of those systems, suggesting the attack was more surgical in its goal. There also has yet to be discovery of a «kill switch» as there was with the WannaCry software, which would immediately stop its spread. According to Nicholas Weaver of the University of California the hackers had previously compromised MeDoc «made it into a remote-control Trojan, and then they were willing to burn this asset to launch this attack» [2].

During the attack the radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant went offline. Several Ukrainian ministries, banks, metro systems and state-owned enterprises (Boryspil International Airport, Ukrtelecom, Ukrposhta, State Savings Bank of Ukraine, Ukrainian Railways) were affected. In the infected computers, important computer files were overwritten and thus permanently damaged, despite the malware's displayed message to the user indicating that all files could be recovered «safely and easily» by meeting the attackers' demands and making the requested payment in Bitcoin currency.

The attack came on the eve of the Ukrainian public holiday, Constitution Day (celebrating the anniversary of the approval by the Verkhovna Rada (Ukraine's parliament) of the Constitution of Ukraine on 28 June 1996). Most government offices would be empty, allowing the cyberattack to spread without interference. In addition, some security experts saw the ransomware engage in wiping the affected hard drives rather than encrypting them, which would be a further disaster for companies affected by this. A short time before the cyberattack began, it was reported that an intelligence officer and head of a special forces unit, Maksym Shapoval, was killed in Kiev by a car bomb. Former government adviser in Georgia and Moldova Molly K. McKew believed this assassination was related to the cyberattack [10].

On 30 June, the Security Service of Ukraine (SBU) reported it had seized the equipment that had been used to launch the cyberattack, claiming it to have belonged to Russian agents responsible for launching the attack. On 1 July 2017 the SBU claimed that available data showed that the same perpetrators who in Ukraine in December 2016 attacked the financial system, transport and energy facilities of Ukraine (using TeleBots and BlackEnergy) were the same hacking groups who attacked Ukraine on 27 June 2017. «This testifies to the involvement of the special services of Russian Federation in this attack» it concluded [14]. Ukraine claims that hacking Ukrainian state institutions is part of what they describe as a «hybrid war» by Russia on Ukraine [12].

According to reports cited in January 2018 the United States Central Intelligence Agency claimed Russia was behind the cyberattack, with Russia's Main Intelligence Directorate (GRU) having designed NotPetya [11]. Similarly, the United Kingdom Ministry of Defence accused Russia in February 2018 of launching the cyberattack, that by attacking systems in the Ukraine, the cyberattack would spread and affect major systems in the United Kingdom and elsewhere. Russia had denied its involvement, pointing out that Russian systems were also impacted by the attack [8].

The reaction of the Ukrainian state to such actions by the northern neighbour was predictable. First of all, the role of the Department of Cyberpolice of the National Police of Ukraine was strengthened - the interregional territorial body of the National Police of Ukraine, which is part of the structure of the criminal police of the National Police and in accordance with the legislation of Ukraine, ensures the implementation of state policy in the field of combating cybercrime. This division specializes in the prevention, detection, termination and disclosure of criminal offenses, the mechanisms of preparation, execution or concealment of which, involves the use of electronic computers (computers), telecommunication and computer Internet networks and systems [20]. On July 19, 2017, within the framework of the project «Capacity building for cyberpolice», representatives of the OSCE Project Coordination in

Ukraine transferred 194 units of specialized equipment to the units of the cyberpolice of the National Police of Ukraine [16].

In addition, repeated cyber attacks have prompted accelerated adoption of the law of Ukraine on protection of cyberspace, which was adopted on October 5, 2017, but came into force only on May 9, 2018 [19].

This Law defines the legal and organizational foundations for ensuring the protection of vital interests of a person and a citizen, society and the state, the national interests of Ukraine in cyberspace, the main goals, directions and principles of state policy in the field of cybersecurity, the powers of state bodies, enterprises, institutions, organizations, persons and citizens in this area, the main principles of coordination of their work on the provision of cyber security.

The law explicitly interprets the meaning of the notion of cyberspace - the environment (virtual space), which provides opportunities for communication and / or implementation of social relations, formed as a result of the operation of compatible (connected) communication systems and the provision of electronic communications using the Internet and / or other networks global data networks [19]; and cyber defense - a set of organizational, legal, engineering and technical measures, as well as measures of cryptographic and technical protection of information aimed at preventing cyber incidents, detecting and protecting against cyber attacks, eliminating their consequences, restoring the sustainability and reliability of the functioning of communication and technological systems.

The law also stipulates that the main subjects of the national system of cyber security are the State Service for Special Communications and Information Protection of Ukraine, the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Defence of Ukraine and the General Staff of the Armed Forces of Ukraine, intelligence agencies, the National Bank of Ukraine [19].

The objects of critical infrastructure are enterprises and organizations that provide services in the economic sphere, in the energy and chemical industry, transport and information and communication industries, utility companies, healthcare, or objects of potentially dangerous technologies and industries. Coordination of activities is carried out by the President of Ukraine with the help of the National Security and Defence Council of Ukraine, which he heads. The Cabinet of Ministers of Ukraine ensures the formation and implementation of state policy in the field of cyber security [19].

Thus, the Ukrainian authorities have taken a number of steps to protect the national cyberspace, both normative and practical. However, this does not reduce the level of threats that cyber attacks carry. After all, after the adoption and the enactment of the law on the protection of domestic cyberspace, the creation of the Department of Cyberpolice and a number of other actions by Ukraine, attempts at cyberattacks for our country have not been stopped.

Authorities in the United States said they broke up a potential digital attack called VPNFilter that affected half a million internet routers and could have caused widespread havoc in Ukraine. The US Justice Department said this was the most recent attack programmed by the Sofacy Group, the Russian hackers – also known as Fancy Bear – are suspected of being behind cyberattacks on several governments, international agencies and infrastructure providers. The largest number of infections was in Ukraine but affected routers in 54 countries, according to technology company Cisco Systems and antivirus company Symantec, which cooperated with the FBI during the operation [6].

Conclusion. The study of cyberspace as a component of Ukraine's information security gives a number of important conclusions. Cyber security and cyber space of Ukraine remained for a long time out of the attention of domestic researchers and, therefore, civil servants. For more than 20 years, the young Ukrainian state did not waste its efforts on the formation of not only effective and reliable troops, but also information security. The government did not

endeavoured to strengthen the country's defence, and probably only weakened its lack of progress in fighting corruption and the dominance of Russian media and intelligence. As a result, in the spring of 2014, after a long confrontation between the regime and the citizens of Ukraine Viktor Yanukovych, Russia failed to conduct special operations with the aim of annexing the Crimea and facilitate the war in Donbas. Not the least role in this played a raid for information and factors cyber Russian hackers for the purpose of paralysing government agencies and influence on public opinion in Ukraine through Russian-controlled media.

As a result of prolonged and massive cyberattacks, Ukrainian state structures, the banking system, industrial facilities and private business suffered significant material and reputational losses. At the same time in Ukraine began to realize the seriousness of cyber security as a component of national security and contributed to creating cyber police, national cybersecurity strategy, acceptance of a number of regulations on cyber security, strengthening public defence for the protection of domestic cyber space. At the moment, Ukraine is on the way to rethinking the role of cyber security and the formation of a national system of protection against cyber threats.

References

1. Bajak F. Companies still hobbled from fearsome cyberattack [Electronic resource] / F. Bajak, R. Satter // USnews. - 2017. - June 30. – Mode of access: https://www.usnews.com/news/business/articles/2017-06-30/companies-still-hobbled-from-fearsome-cyberattack

2. Borys C. Ukraine braces for further cyber-attacks [Electronic resource] / C. Borys // BBCNews. - 26 July. - 2017. - Mode of access: https://www.bbc.com/news/technology-40706093

3. Borys C. The day a mysterious cyber attack crippled Ukraine [Electronic resource] / C. Borys // BBCNews. - 2017. – 4 July. - Mode of access: http://www.bbc.com/future/story/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine

4. Countering Hybrid Threats: Lessons Learned from Ukraine [Electronic resource] / ed. byN. Iancu, A. Fortuna, C. Barna. – Amsterdam, Berlin, Washington: OIS Press, 2015. – Mode of access: https://books.google.ee/books?id=Uwy3DAAAQBAJ&printsec=frontcover&hl=uk#v=onepage&q&f=false

5. Cyber-attack was about data and not money, say experts [Electronic resource] // BBCNews. - 2017. - 29 June. – Mode of access: https://www.bbc.com/news/technology-40442578

6. FBI thwarts potential cyberattack on Ukraine [Electronic resource] // Deutsche Welle. - 2018. – 24 May. - Mode of access: http://www.dw.com/en/fbi-thwarts-potential-cyberattack-on-ukraine/a-43905916

7. Finkle J. U.S., Britain blame Russia for global cyber attack [Electronic resource] / J. Finkle, D. Chiacu // Reuters. - 2018. – 16 April. – Mode of access: https://www.reuters.com/article/us-usa-britain-cyber/u-s-britain-blame-russia-for-global-cyber-attack-idUSKBN1HN2CK ;

8. MarshS. US joins UK in blaming Russia for NotPetya cyber-attack [Electronic resource] / S. Marsh // The Guardian. – 2018. - 15 Feb. - Mode of access: https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine

9. Mason R. Theresa May accuses Russia of interfering in elections and fake news [Electronic resource] / R. Mason // The Guardian. – 2017. - November 13. - Mode of access: https://www.theguardian.com/politics/2017/nov/13/theresa-may-accuses-russia-of-interfering-in-elections-and-fake-news

10. McKew M. A killing in Kiev shows how the West continues to fail Ukraine [Electronic resource] / M. McKew // The WashingtonPost. – 2017. - June 27. - Mode of access: https://www.washingtonpost.com/news/democracy-post/wp/2017/06/27/a-killing-in-kiev-shows-how-the-west-continues-to-fail-ukraine/?noredirect=on&utm_term=.9d530a2446a4

11. Nakashima E.Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes [Electronic resource] / E. Nakashima // The Washington Post. – 2018. - January 12. - Mode of access: https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?utm_term=.4be7c7c50230

12. Polityuk P. Ukraine points finger at Russian security services in recent cyber attack [Electronic resource] / P. Polityuk // Reuters. – 2017. - July 1. - Mode of acces: https://www.reuters.com/article/us-cyber-attack-ukraine/ukraine-points-finger-at-russian-security-services-in-recent-cyber-attack-idUSKBN19M39P

13. Soshnikov A. Inside a pro-Russia propaganda machine in Ukraine [Electronic resource] / A. Soshnikov // BBC Russian. – 2017. - 13 November. - Mode of access: https://www.bbc.com/news/blogs-trending-41915295

14. Ukraine Security Service Blames Russia For Recent Cyberattack. [Electronic resource] // Radio Free Europe. – 2017. - July 01.- Mode of access:https://www.rferl.org/a/cyberattack-ukraine-blames-russia/28589606.html

15. Warsaw Summit Communiqué. NATO[Electronic resource] : Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. – 2017. - March 29. - Mode of access:https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

16. Кіберполіція отримала 194 одиниці спеціального обладнання для протидії кіберзагрозам [Електронний ресурс] // Міністерство внутрішніх справ України. - 2017. – 19 липня. – Режим доступу: http://mvs.gov.ua/ua/news/9208_Kiberpoliciya_otrimala_194_odinic_specialnogo_obladnannya_dlya_protidii_kiberzagrozam_FOTO_VIDEO.htm; Kiberpolitsiia otrymala 194 odynytsi spetsialnoho obladnannia dlia protydii kiberzahrozam [Elektronnyi resurs] // Ministerstvo vnutrishnikh sprav Ukrainy. - 2017. – 19 lypnia.– Rezhym dostupu : http://mvs.gov.ua/ua/news/9208_Kiberpoliciya_otrimala_194_odinic_specialnogo_obladnannya_dlya_protidii_kiberzagrozam_FOTO_VIDEO.htm

17. Німеччина звинуватила Росію в кібератаці на урядові мережі [Електронний ресурс] // ТСН. – 2018. -11 квітня. – Режим доступу: https://tsn.ua/svit/nimechchina-zvinuvatila-rosiyu-v-kiberataci-na-uryadovi-merezhi-1138362.html; Nimechchyna zvynuvatyla Rosiiu v kiberatatsi na uriadovi merezhi [Elektronnyi resurs] // TSN. – 2018. – 11 kvitnia. – Rezhym dostupu: https://tsn.ua/svit/nimechchina-zvinuvatila-rosiyu-v-kiberataci-na-uryadovi-merezhi-1138362.html

18. Президент затвердив Стратегію кібербезпеки України. 16 березня 2016[Електронний ресурс] // Президент України : офіційне інтернет-представництво. – Режим доступу :http://www.president.gov.ua/news/prezident-zatverdiv-strategiyu-kiberbezpeki-ukrayini-36856; Prezydent zatverdyv Stratehiiu kiberbezpeky Ukrainy. 16 bereznia 2016 [Elektronnyi resurs] // Prezydent Ukrainy : ofitsiine internet-predstavnytstvo. – Rezhym dostupu : http://www.president.gov.ua/news/prezident-zatverdiv-strategiyu-kiberbezpeki-ukrayini-36856

19. Про основні засади забезпечення кібербезпеки України [Електронний ресурс]: Закон України № 2163-VIII від 05.10.2017. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/2163-19 ; Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [Electronic resource] : Zakon Ukrainy № 2163-VIII vid 05.10.2017. – Rezhym dostupu : http://zakon5.rada.gov.ua/laws/show/2163-19

20. Про утворення територіального органу Національної поліції : Постанова Кабінету Міністрів України від 13.10.2015 № 831 // Урядовий кур'єр. – 2015. – 21 жовтня (№ 195) ; Pro utvorennia terytorialnoho orhanu Natsionalnoi politsii : Postanova Kabinetu Ministriv Ukrainy vid 13.10.2015 № 831 // Uriadovyi kurier. – 2015. – 21 zhovtnia (№ 195)

21. США також звинуватили у вірусі NotPetya Росію [Електронний ресурс] // BBC. – 2018. – 16 лютого. – Режим доступу :https://www.bbc.com/ukrainian/news-43082212; CShA takozh zvynuvatyly u virusi NotPetya Rosiiu [Elektronnyi resurs] // BBC. – 2018. – 16 liutoho. – Rezhym dostupu : https://www.bbc.com/ukrainian/news-43082212

22. Уряд Британії звинуватив Росію у кібератаці на Україну [Електронний ресурс] // BBC. – 2018. – 15 лютого. – Режим доступу :https://www.bbc.com/ukrainian/news-43069110 ; Uriad Brytanii zvynuvatyv Rosiiu u kiberatatsi na Ukrainu [Electronic resource] // BBC. – 2018. – 15 liutoho. – Rezhym dostupu : https://www.bbc.com/ukrainian/news-43069110

23. Через кібератаки США запровадили щодо Росії нові санкції // BBC. – 2018. – 12 червня. – Режим доступу: https://www.bbc.com/ukrainian/news-44450668; Cherez kiberataky SshA zaprovadyly shchodo Rosii novi sanktsii // BBC. – 2018. – 12 chervnia. – Rezhym dostupu : https://www.bbc.com/ukrainian/news-44450668

Стаття надійшла до редакції 10.05.2018 р.

П.М. Катеринчук

ВИКЛИКИ ТА ЗАГРОЗИ КІБЕКРБЕЗПЕЦІ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Кіберпростір України тривалий час залишався поза увагою вітчизняних дослідників, а відтак і державних службовців. Молода Українська держава понад 20 років не витрачала зусиль на формування не лише дієвого та надійного війська, але й інформаційної безпеки. Керівництво держави не докладало зусиль для зміцнення обороноздатності країни, і швидше лише послаблювали її відсутністю прогресу у боротьбі з корупцію та засиллям російських ЗМІ та спецслужб. Як результат, весною 2014 року, після тривалого протистояння громадян України та режиму В. Януковича, Росія вдалася до проведення спецоперації з метою анексувати Крим і сприяти війні на Донбасі. Не останню роль у цій спецоперації відігравали саме інформаційні чинники та кібератаки російських хакерів з метою паралізувати урядові структури та вплинути на формування громадської думки в Україні через підконтрольні Росії медіа.

Внаслідок тривалих і масованих кібератак українські державні структури, банківська система, промислові об'єкти та приватний бізнес зазнали значних матеріальних та репутаційних втрат. Водночас в Україні почали розуміти усю серйозність безпеки кіберпростору як складової національної безпеки держави і це сприяло створенню кіберполіції, державної стратегії кібербезпеки, прийняття низки нормативних актів щодо кібербезпеки, посилення державного впливу у сфері захисту вітчизняного кібепростору.

Ключові слова: *кіберпростір, кібербезпека, хакерські атаки, інформаційна безпека.*