Smoliar L.O. Mynule zarady maibutnoho. Zhinochyi rukh Naddniprianskoi Ukrainy druhoi polovyny XIX – poch. XX: storinky istorii [The past for the sake of the future. Women's movement of the Dnieper Ukraine in the second half of the 19th century – beginning 20-th century: pages of history] / L. O. Smoliar. Odesa, 1998. 408 s. [in Ukrainian]

8. Шведова Н. А. Жіночий рух в Росії: проблеми сучасного етапу // Жіночий рух Росії: вчора, сьогодні, завтра / Н.А. Шведова. М.: РОДП "Яблуко", КМК, 2010.120 с.

Shvedova N. A. Zhinochyi rukh v Rosii: problemy suchasnoho etapu // Zhinochyi rukh Rosii: vchora, sohodni, zavtra [Women's Movement in Russia: Problems of the Modern Stage // Women's Movement of Russia: Yesterday, Today, Tomorrow] / N. A. Shvedova. M.: RODP "Iabluko", KMK, 2010.120 s. [in Ukrainian]

Illia Chernovol
Vasyl' Stus Donetsk National University
Vinnytsia
Research Supervisor: I.Yu. Charskykh, PhD in History, Assoc. Prof.
Language Advisor: V.I. Kalinichenko, PhD in Philology, Ass. Prof.

THE PROBLEMS OF IMPLEMENTATION OF INFORMATION SECURITY IN POLITICAL DISPUTES OF DONALD TRUMP'S SUPPORTERS AND OPPONENTS

Introduction. The most advanced countries use the information potential to achieve military, political and economic goals. Information resources such as information and technology, accordingly, become tools of information influence. The role of the United States of America as one of the most powerful political, economic and military actors in modern international relations should be noted. The power of the United States has largely been caused by the active development and implementation of information technology in various spheres of public life. However, due to the active use of information technology, the US earlier than other countries had faced the negative consequences of information threats and cyber attacks and gained considerable experience in counteracting them.

Review of recent publications. The problem of US information security has been topical for a large number of American and international researchers**.** I. R. Bodnar, O. P. Dzoban, V. Zhugan, V. Pashkov, A. M. Kosogov, M. Mazzetti**,** J. Marks and others have devoted their papers to the problems of information security implementation in the USA under conditions of globalization of society and information threats growth. However, information security researches in terms of different approaches to it by contemporary republicans and democrats have not yet been carried out.

The objective of the paper is to analyze the controversy of Donald Trump's supporters and opponents regarding the implementation of information security, as a component of the US national security, in the context of the issue of Russian interference in the USA election 2016.

Results of the research. Despite the wide-ranging organizational and legal support of information security in the United States, during the last election campaign, the country faced information threats from Russia which reportedly sabotaged the election. This situation drew immediate attention of both proponents and opponents of the administration of acting president.

After the publication of the National Security Strategy, the Trump's Administration was criticized, since the document, though defined information security a country's major priority, did not predict real measures to achieve this. Thereby the new National Cyber Strategy was developed and published in September 2018 [1]. This document contains goals similar to previous compatible documents: B. Obama's cyberspace policy 2009 and J. Bush's National Strategy to Secure Cyberspace, February 2003. However, despite the resemblance to previous administration plans, Donald Trump's National Cyber Strategy caused criticism from its opponents, because instead of continuing the concept of strengthening security technologies and minimizing the impact of information threats, D. Trump's administration plans to reinforce offensive warning cyber-operations and forcing other countries to fear accountability for their actions in response to such cyber attacks from the United States [2]. However, the greatest criticism was that D. Trump's strategy did not in any way indicate the possibility of protecting the election from information threats, which is extremely urgent in the light of the recent events [3].

Among the main problems that the United States are currently facing in the sphere of information security, the following can be distinguished: an increase of installing malware (viruses) on mobile devices, the spread of viruses through the distribution of unlicensed software stores, stealing of accounts and personal data (Fig. 1) [4].

In addition, the US government have directly faced significant information security issues. Among such problems the following can be discussed: the penetration into the government network; the theft of intelligence data; the kidnapping of personal data of the US citizens, government officials and military personnel; wiretapping to telephone conversations and communications; interference in the US elections (Fig. 2) [5].

Representatives of the American authorities and intelligence services have repeatedly stated that Russia was trying to influence the election of the US president in 2016 [6]. Thereby, in 2017, an investigation into the facts of Russian interference in the elections was initiated, according to which it was found out that Russian interference in the elections had been carried out in three directions: the abduction and disclosure the documents of D. Trump's main opponents; massive fraud on Facebook and Twitter with accounts for anti-propaganda of G. Clinton; the cooperation with Trump’s campaign [7]. The last statement has not been confirmed, according to the so-called "Müller Report" [8].

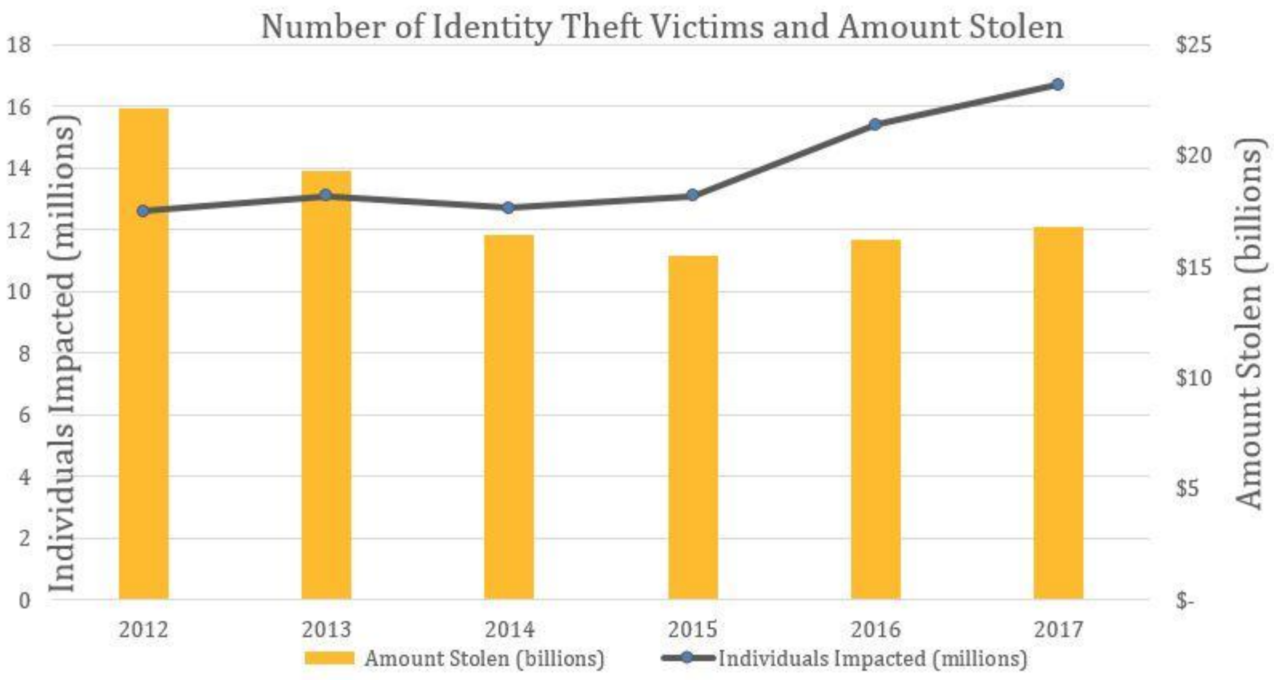

Fig. 1 Number of Identity Theft Victims and Amount Stolen.
Source: [4]

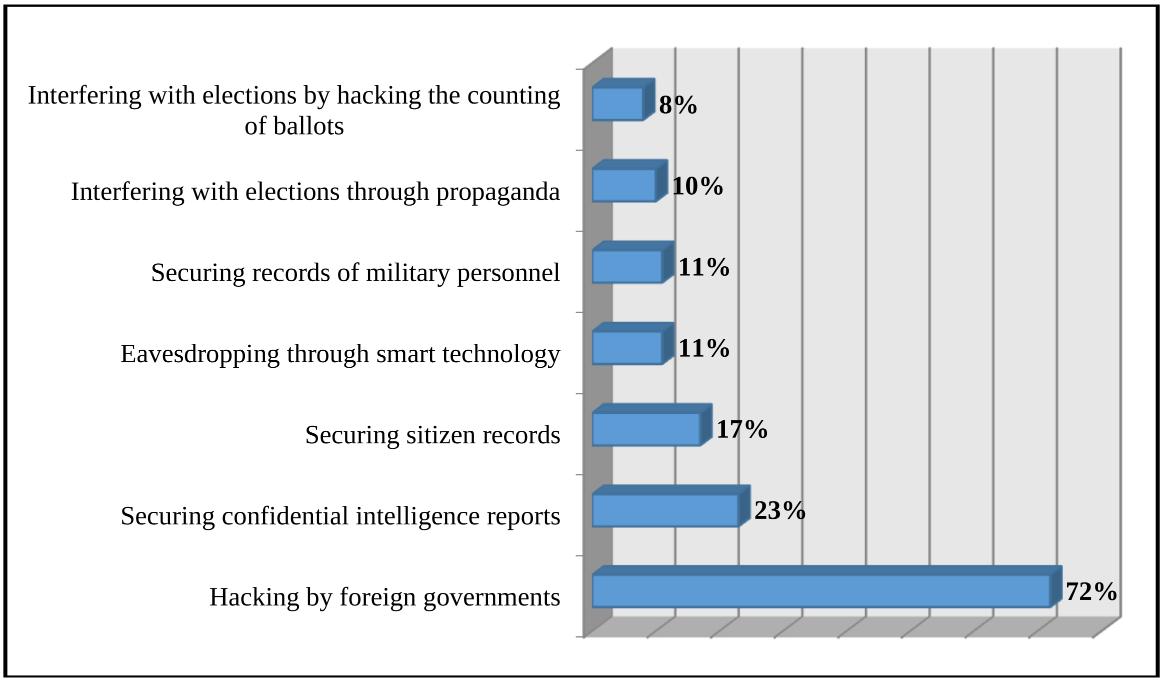

Fig. 2 Biggest cyber security problems facing the U.S. government.
Source: [5]

Despite the fact that D. Trump’s both supporters and opponents agree that information security is a top priority of national security, there is no unanimity on its implementation. Accordingly, D. Trump’s supporters have focused on external threats and believe that it is worth struggling with it by initiating their own information attacks. However, in D. Trump’s opponents opinion, such policy will not bring the desired results and, first of all, it is necessary to introduce violations of information security to American companies that do not have the appropriate security systems and establish strict control over them. The key issue for which there is a discrepancy is protecting the election from information threats [9].

Conclusion. Finally, despite the disagreements between democrats and republicans on the issue of implementing information security, both parties focus their attention on intensifying efforts for its maintenance and implementation in order to protect the United States of America from globalization challenges and information attacks. Donald Trump’s supporters and opponents have realized that as a top priority of national security.

References

1. National Cyber Strategy of the United States of America [Electronic resource]. September 2018. Washington D.C.: The White House, 2018. 26 p. Retrieved from: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

2. Wolff J. Trump’s Reckless Cybersecurity Strategy [Electronic resource] / J. Wolff. Retrieved from: https://www.nytimes.com/2018/10/02/opinion/trumps-reckless-cybersecurity-strategy.html

3. Grisby A. The White House National Cyber Strategy: Continuity with a Hint of Hyperbole [Electronic resource] / A. Grisby. Retrieved from: https://www.cfr.org/blog/white-house-national-cyber-strategy-continuity-hint-hyperbole

4. Symantec Corporation. 10 cyber security facts and statistics for 2018 [Electronic resource]. Retrieved from: https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html

5. The Statistic Portal. Biggest cyber security problems facing the U.S. government according to adults in the United States as of January 2017 [Electronic resource]. Retrieved from: https://www.statista.com/statistics/676601/biggest-us-government-cyber-security-problems/

6. Жигалкин Ю. Доказательства вмешательства России в выборы президента США [Электронный ресурс] / Ю. Жигалкин. Режим доступа: https://www.svoboda.org/a/usa-russia-indictment/29044968.html

Zhigalkin Yu. Dokazatelstva vmeshatelstva Rossii v vibori prezidenta SShA [Evidence of Russia's intervention in the US presidential election] [Electronic resource] / Yu. Zhigalkin. Retrieved from: https://www.svoboda.org/a/usa-russia-indictment/29044968.html

7. CNN. 2016 Presidential Election Investigation Fast Facts [Electronic resource]. Retrieved from: https://edition.cnn.com/2017/10/12/us/2016-presidential-election-investigation-fast-facts/index.html

8. Barr W.P. (Attoney General). Letter to Congress on Special Councel's Report [Electronic resource] / W.P. Barr. Retrieved from: https://games-cdn.washingtonpost.com/notes/prod/default/documents/9048a12b-2332-4645-a1be-d645db216eb5/note/6f3248a4-4d94-4d5f-ad42-8ff6ccb1a89e.pdf#page=1

9. Kolbasiuk M. White House National Cyber Strategy: An Analysis [Electronic resource] / M. Kolbasiuk. Retrieved from: https://www.bankinfosecurity.com/white-house-national-cyber-strategy-analysis-a-11558

Mariia Dakaliuk
University of Prešov,
Prešov, Slovakia
Research Supervisor: M.M. Kasianova, Doc. of Political Science, Prof.
Language Advisor: V.I. Kalinichenko, PhD in Philology, Ass. Prof.

NATO INFORMATION POLICY

Introduction. Today informatization is not just a local sphere of public life, it currently covers all spheres, and its consequences affect the life of a person, society, state, this influence becomes more and more significant. Society, using modern opportunities in the field of information, has acquired mechanisms, which allow to take control over the activities of the state and influence political decision-making. NATO is an organization which actively uses information technology, and therefore there is a need to consider it as an example of the effective use of information as a weapon. In our opinion, Ukraine needs to use the experience of NATO in the information war, which the Russian Federation is waging against it.

Review of recent publications. Aspects of the NATO information policy are increasingly being covered in the media around the world, especially over the last decade. Primary sources have become valuable for research, for example, the strategic concept of NATO [6]. The NATO Strategic Concept, adopted at the Lisbon summit in November 2010, reflected the perception of cyber threats [4]. This document also became one of the primary sources for researching the problem. Among the periodicals, we can single out an article in the BBC news edition "Ukraine-Russia clash: NATO's dilemma in the Black Sea" [1].

The objective of the paper is to discuss the basic features of NATO information policy, methods of the Alliance for providing security in cyberspace, as well as to analyze the applicability of these methods for Ukraine.

Results of the research. Recently, NATO has paid considerable attention to the role of technology, information weapons and psycho-propaganda operations in the wars of the 21st century, which significantly change the nature of the use of various