Черновол Ілля

ІНФОРМАЦІЙНА БЕЗПЕКА США В КОНТЕКСТІ АКТУАЛЬНИХ ЗАГРОЗ І ВИКЛИКІВ

Анотація. *Зосереджено увагу на актуальних проблемах, загрозах та викликах інформаційній безпеці США в добу Дональда Трампа. Надано стислу інформацію про наявні суперечки між двома основними політичними партіями США щодо реалізації інформаційної безпеки, російського втручання в американський електоральний процес та вплив коронавірусної інфекції COVID-19 на інформаційну безпеку Сполучених Штатів. На основі системного підходу з використанням методу критичного аналізу досліджено основні проблеми, загрози та виклики інформаційній безпеці США, окреслено шляхи їхнього вирішення.*

Ключові слова: *інформаційна безпека США, Д. Трамп, міжпартійні суперечки, російське втручання, COVID-19.*

Abstract. *This study focuses on the current problems and challenges of the US information security in the time of Donald Trump. In particular, brief information is provided regarding the existing disputes between the two American main political forces regarding the implementation of information security, the Russian interference in the American electoral process and the impact of COVID-19 coronavirus infection on the US information security. Based on a systematic approach, using the method of critical analysis, the main problems, threats and challenges of the US information security are investigated, possible ways to solve them are identified.*

Keywords: *the U.S. information security, D. Trump, cross-party disputes, Russian intervention, COVID-19.*

Сполучені Штати Америки – один з найбільш могутніх політичних, економічних, технологічних і військових акторів сучасних міжнародних відносин. Внаслідок активного використання інформаційних технологій США раніше за інші країни зіткнулися із негативними наслідками інформаційних загроз. Виявилися потенційно вразливі місця інформаційної сфери, а саме: небезпечний когнітивний вплив у негативній конотації з боку певних засобів масової інформації та соціальних мереж на суспільну думку всередині країни, а також прогалини у сфері захисту персональних даних, державних та приватних комп'ютерних мереж. Сполученим Штатам бракує наявності єдиної візії в контексті протиборства інформаційним атакам та рішучості у реалізації політики інформаційної безпеки, а сучасні загрози та виклики, такі як постійні міжпартійні суперечки, російське втручання та вплив коронавірусної інфекції COVID-19, не наближають американців до цього.

Проблема інформаційної безпеки США широко досліджується в американських та вітчизняних науково-концептуальних та суспільно-політичних колах. Д. Альперович, Е. Накашіма, П. А. Афанасьєва, Н. Б. Бєлоусова, О. Ю. Бусол, О. В. Олійник, О. А. Собко, І. Р. Боднар, О. П. Дзьобань, В. Жуган, В. Пашков, О. М. Косогов, М. Маззетті, Дж. Маркс та інші присвятили свої дослідження проблемам реалізації інформаційної безпеки у США в умовах глобалізації та зростання інформаційних загроз. Проте, відсутність достатньоого усвідомлення глибини та багатогранності

цієї проблеми з погляду існування вищезазначених загроз та викликів дає можливість вивчати її в різних ракурсах та обумовлює актуальність.

Особливістю політики захисту інформаційної безпеки в США є брак наступності та послідовності. Кожна нова президентська адміністрація пропонувала і реалізовувала свої власні тактичні і стратегічні дії. Після опублікування Стратегії національної безпеки у грудні 2017 р. [5] адміністрація Дональда Трампа була розкритикована демократами, оскільки документ, хоч і визначав інформаційну безпеку одним із головних пріоритетів країни, не передбачав реальних заходів для її досягнення [1]. В рамках розпорядження президента від 11 травня 2017 р. № 13800 «Посилення кібербезпеки федеральних мереж і критичної інфраструктури» було розроблено нову Національну кіберстратегію (The National Cyber Strategy of the USA – далі NCS), яка була опублікована у вересні 2018 р. [6]. Цей документ містить цілі, подібні до тих, що поставлені у попередніх схожих документах: політикою у сфері кіберпростору адміністрації Б. Обами 2009 [7] та Національною стратегію безпеки Дж. Буша 2002 [8] щодо безпеки кіберпростору. Однак, незважаючи на схожість з планами попередніх адміністрацій, NCS Д. Трампа знову викликала критичні відгуки з боку його опонентів, оскільки замість того, щоб продовжувати концепцію зміцнення захисних технологій і мінімізувати вплив інформаційних загроз, адміністрація Д. Трампа планує посилити наступальні попереджувальні кібероперації та змусити інші країни боятися притягнення до відповідальності за свої дії у відповідь на такі кібератаки з боку США. Критики звернули увагу на той факт, що ця стратегія не вказує на можливості захисту виборів від інформаційних загроз, що є надзвичайно актуальним у світлі подій 2016 р. [9].

В американському політикумі головним показником зростання проблеми захисту інформаційної безпеки Сполучених Штатів та символічною точкою відліку при її сучасному описі вважається російське втручання в американські президентські вибори 2016 р. Це безпрецедентне явище, оскільки така масштабна кампанія з боку Росії, що була з успіхом проведена, мала місце вперше в контексті історії інформаційної безпеки США. Це був болісний удар не тільки для інформаційної сфери та національної безпеки країни, але й для американської ідеології та іміджу. Так, у червні 2016 р. в американських мас-медіа з’явилася інформація про несанкціоноване втручання в інформаційну систему Національного комітету Демократичної Партії США, особливо було згадано російське «Агенство інтернет-досліджень» (далі – IRA), яке фінансувалося Євгеном Пригожиним (російський бізнесмен, засновник «фабрики тролів» з Ольгіна, одна з ключових фігур в російсько-українській інформаційній війні), скандально відомим як «кухар Путіна» [2]. У 2017 р. було розпочато розслідування фактів російського втручання у вибори, яке очолив спеціальний прокурор Роберт Мюллер. За результатами майже дворічного розслідування було виявлено, що російське втручання у вибори здійснювалося за трьома основними напрямами: викрадення та оприлюднення документів основних

опонентів Д. Трампа; масове шахрайство з акаунтами популярних соціальних мереж для анти-пропаганди Г. Клінтон; хакерське проникнення до державних та приватних комп'ютерних мереж для отримання важливої конфіденційної інформації державного значення, що містила дані стосовно американського електорального процесу [4].

Провальна реакція Сполучених Штатів на загрозу коронавірусної інфекції COVID-19 завдала значного удару по американській позиції міжнародного лідера у суперництві з Китаєм, а також знайшла своє негативне відбиття у сфері інформаційної безпеки. Йдеться про нещодавню заяву посадовців Держдепу стосовно чергового використання вищезгаданим російським IRA тисячі фейкових акаунтів у соціальних мережах, зокрема Facebook, Instagram та Twitter, для поширення фейкової інформації про Covid-19. Мовляв, нібито Covid-2019 є біологічною зброєю, розробленою Центральним розвідувальним управлінням США (ЦРУ) задля економічної війни з Китаєм [3].

Актуальні загрози та виклики мають значний дестабілізуючий вплив на критично важливу американську інформаційну інфраструктуру, а отже, складають серйозну загрозу національній безпеці США. Основним завданням уряду за таких умов має бути вироблення та розвиток єдиного (двопартійного) бачення державної політики щодо сфери інформаційної безпеки з формуванням потужної системи захисту та постійним удосконаленням останньої для протидії зовнішнім та внутрішнім загрозам. Такі кроки унеможливили б інформаційні атаки та когнітивний зовнішній вплив на громадськість у подальшій перспективі, за умови досягнення консенсусу між основними політичними силами США.

Джерела та література

1. Довгопол Я. Трамп ігнорує серйозні загрози для національної безпеки з боку Росії. URL: https://www.ukrinform.ua/rubric-world/2184991-so-i-ak-skazav-tramp-kongresu.html
2. Жигалкин Ю. Доказательства вмешательства России в выборы президента США. URL: https://www.svoboda.org/a/usa-russia-indictment/29044968.html
3. Macmillan A., Shaun Tandon. Russia-linked disinformation campaign fueling coronavirus alarm, US says // AFP. February 22, 2020. URL: https://news.yahoo.com/russia-linked-disinformation-campaign-fueling-coronavirus-alarm-us-134401587.html
4. Mazzetti M., Bennet K. Mueller report summary. URL: https://www.nytimes.com/2019/03/24/us/politics/mueller-report-summary.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking.html
5. The White House. National Security Strategy of the United States of America. Washington DC, December 2017. 56 p. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf
6. The White House. National Cyber Strategy of the United States of America. Washington DC, September 2018, 29 p. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
7. The White House. Cyber Security Review. Washington DC, March 2009, 47 p. URL: https://obamawhitehouse.archives.gov/cyberreview/documents/
8. The White House. The National Security Strategy, Washington DC, September 2002. URL: https://georgewbush-whitehouse.archives.gov/nsc/nss/2002/
9. Wolff J. Trump's Reckless Cybersecurity Strategy. URL: https://www.nytimes.com/2018/10/02/opinion/trumps-reckless-cybersecurity-strategy.html