УДК 004.056.5:351.861(477)
DOI https://doi.org/10.32782/2524-0374/2022-10/123

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ ЯК ПРОБЛЕМАТИКА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

ABSTRACT THREATS TO UKRAINE'S INFORMATION SECURITY AS A NATIONAL SECURITY PROBLEM

Ткаченко В.В., к.ю.н.,
доцент кафедри адміністративного та інформаційного права
Сумський національний аграрний університет

Паливода В.В., студент ІІ курсу магістратури юридичного факультету
Сумський національний аграрний університет

На сьогодні, російсько-український конфлікт переріс в повномасштабну війну, при якій країна-агресор намагається переконати світову спільному в тому, що на території України відбувається громадське протистояння, а тому фактично розгортає проти українського населення не лише військовий (який відбувається вже в умовах сучасності), а й інформаційний фронт, однак, російська федерації потерпає невдачі як і першому плані, так і в другому. Також, з приводу вищевикладеного слід додати, що така війна також має певні ознаки гібридної, адже, висвітлюється те, що держави частіше використовують недержавних дійових осіб та інформаційні технології задля досягнення перемоги над своїми супротивниками за відсутності прямого збройного конфлікту (однак, як показують умови сьогодення, то і під час збройного конфлікту) маючи на меті досягнення певних політичних цілей.

Зауважимо на тому, що аналізуючи стан інформаційної безпеки на рівні держави саме в перспективі протидії кіберзлочинності, слід звернути увага на те, що зазначений пріоритетний напрямок діяльності перебуває на стадії формування, напрацювання необхідного досвіду і практики, створення ефективних інструментів і методики.

Протягом останніх років і на сьогоднішній день простежується високий рівень латентності та неочевидності кримінальних правопорушень у сфері кіберзлочинності. За винятком окремих масштабних кібератак, більшість кіберзлочинів залишаються невиявленими, або не повідомляються жертвами в правоохоронні органи.

У цій статті ми дослідили актуальні питання, що стосуються загроз інформаційній безпеці України, як певного елементу національної безпеки нашої країни, а також знаходження напрямків вирішення зазначених проблем та шляхів, які направлені на протидію загрозам інформаційній безпеці України.

Ключові слова: інформаційна безпека, гібридна війна, загрози національній безпеці України, кібербезпека, суспільство, захист.

Today, the Russian-Ukrainian conflict is a full-scale war, where Russia is an aggressor country, which trying to convince the world community that there is a conflict between citizens of Ukraine, and therefore Russia actually deploys not only military front (which is already happening), but the information front, however, the Russian Federation fails both in the first plan and in the second plan too. Also, it should be added that such a war also has certain signs of a hybrid war, due to states often use non-state actors and information technologies to achieve victory over their opponents in the absence of a direct armed conflict (however, as the current conditions show, even during an armed conflict) for achieving certain political goals.

I must add that a threat to information security is a set of conditions and factors that create a danger to the vital interests of the individual, society and the state in the information sphere. Domestic experts point out that the main threats to information security in our country are the restriction of freedom of speech and citizens' access to information, the destruction of the value system, the spiritual and physical health of individuals and society, the manipulation of public opinion by the government, the low level of Ukraine's integration into the world information space etc.

In this article, we considered current issues which concern with threats to the information security of Ukraine, as a one of elements of the national security of our country/ Also we have offered directions for solving the specified problems and ways that are aimed at countering threats to the information security of Ukraine.

Key words: information security, hybrid warfare, threats to the national security of Ukraine, cyber security, society, defense.

Забезпечення безпеки держави в інформаційній сфері є одним із пріоритетів державної політики України. Указом Президента України від 25.02.2017 № 47 було введено в дію рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», згідно з положеннями якої основними суб'єктами забезпечення інформаційної безпеки є Міністерство інформаційної політики України та Служба безпеки України.

Незважаючи на те, що захист інформації, державних інформаційних ресурсів, інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем є необхідною складовою забезпечення інформаційної безпеки, діяльність з вирішення цих питань, перш всього шляхом формування державної політики, слід розглядати як основу для забезпечення захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через негативні наслідки застосування інформаційних технологій, а також порушення цілісності, конфіденційності та доступності інформації, циркулюючої в інформаційних і технологічних системах.

Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку) відповідно до законодавства в рамках забезпечення інформаційної безпеки забезпечує формування і реалізацію державної політики у сферах криптографічного та технічного захисту інформації, інформаційно-телекомунікаційних систем, захисту державних інформаційних ресурсів у кіберпросторі.

Серед актуальних проблем інформаційної безпеки, від вирішення яких безпосередньо залежить ефективність діяльності у сфері захисту інформації і кіберзахисту державних інформаційних ресурсів в умовах сучасних викликів та загроз у кіберпросторі-проблема підготовки та перепідготовки кадрів, насамперед у сфері кібербезпеки та інформаційної безпеки.

Зусилля, що вживаються на національному рівні з метою посилення інформаційної безпеки та сприяння міжнародному співробітництву в цій сфері.

У 2016 році в Україні затверджено Стратегію кібербезпеки України. В травні 2018 року набув чинності Закон України «Про основні засади забезпечення кібербезпеки України» далі-Кіберзакон), яким на законодавчому рівні закріплені основні цілі, напрямки і принципи державної

політики у сфері кібербезпеки, а також повноваження та обов'язки державних органів, підприємств, установ, організацій, осіб і громадян в цій сфері, що дає можливість розвивати в Україні сучасну цілісну національну систему кібербезпеки.

Прийняття Кіберзакону стало потужним поштовхом до впровадження таких сучасних європейських практик, як управління інформаційною безпекою і її аудит, застосування галузевих стандартизованих вимог до кіберзахисту об'єктів критичної інфраструктури. Вперше в правове поле України введено базовий понятійно-термінологічний апарат сфери кібербезпеки, в зокрема визначення понять критичної інфраструктури та її комунікаційних / технологічних систем; кіберзагрози, кібератаки, кіберзахист, кібертероризм, кібероборона і т. п.

Хотілось би зазначити, що до повномасштабного вторгнення окупаційних військ країни-агресора на територію нашої незалежної країни, дане питання досліджувалось багатьма вітчизняними науковцями, які в своїх наукових працях відображали можливі негативні наслідки гібридної війни та пропонували шляхи щодо її вирішення. Зокрема, хотілось би визначити, що дану проблему досить, в аспекті забезпечення національної безпеки, глобально досліджували такі науковці, як: О. Бандурка, Р. Калюжний, В. Ліпкан, В. Горбулін, М. Стрельбицький, В. Пилипчук, А. Качинський, І. Івченко, А. Марущак, В. Петрик, В. Почецов та інші.

Стосовно організації протидії загрозам інформаційній безпеці, зазначимо, що вона стала предметом досліджень таких вчинених, як: В. Домарєв, М. Живко, В. Бут, В. Цимбалюк, М. Танцюра та інші. Проблемні питання забезпечення кібернетичної безпеки досліджувати такі науковці: В. Бурячок, А. Бабенко, Д. Дубов, М. Погорецький, Р. Лук'янчук, В. Номоконов, В. Шеломенцев та інші. Дослідження зазначених науковців безпосередньо ґрунтується на тому, що інформаційна безпека є певної складовою національної безпеки, її невід'ємним компонентом, однак, поза їх увагою залишились досить актуальні питання стосовно проблеми чіткого окреслення саме інформаційних загроз, всебічне дослідження певних технологій ведення інформаційно-психологічних війн та операцій, а також відповідного визначення та обґрунтування методів протидії інформаційно-психологічними негативним впливам в цілому.

Взагалі, інтенсивна інформатизація всіх сфер життєдіяльності суспільства виступає одним із визначальних масштабних чинників подальшого соціально-економічного, інтелектуального та духовного розвитку людства в цілому. Так, в сучасному світі людство зазнає досить стрімкого розвитку, що тягне за собою збільшення випадків інформаційних війн. Саме тому, в епоху побудови глобального інформаційного суспільства, в якому майже щодня з'являються нові чи удосконалені інформаційні технології, використовуються надсучасні засоби зв'язку та передачі різноманітної інформації тощо, нашій державі необхідно передусім визначити сукупність зовнішніх загроз, встановити, яким із них треба приділити більшу увагу як потенційно найнебезпечнішим, виявити місця, які є найбільш уразливими.

Завдання, на які спрямована інформаційна політика визначається надзвичайно важливими. Зокрема, створення розвиненого інформаційного середовища, ефективне формування та використання національних інформаційних ресурсів, стимулювання інновацій та забезпечення всебічного розвитку та захисту національної інформаційної інфраструктури. Водночас, сьогодні одним із найважливіших можна визначити уникнення ризиків (наприклад, несанкціонованого використання інформації) та запобігання загрозам заподіяння в процесі інформаційної діяльності шкоди життєво важливим інтересам особи, суспільства, держави [1, с. 1].

При аналізуванні літератури, можливим стало визначити, що існує два аспекти трактування інформаційної безпеки саме у контексті національної безпеки. Так, з одного боку, інформаційну безпеку розглянуто як самостійний елемент національної безпеки будь-якої країни світу, а з іншого вона виступає як інтегрована складова будь-якої іншої безпеки, а саме: економічної, військової, політичної тощо. Найповнішим виступає таке визначення, що інформаційна безпека являє собою певний стан захищеності життєво важливих інтересів особистості, суспільства та держави, за якого зводиться до мінімуму завдання збитків через неповноту, невчасність та недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [2, с. 4].

На сьогодні, російсько-український конфлікт переріс в повномасштабну війну, при якій країна-агресор намагається переконати світову спільному в тому, що на території України відбувається громадське протистояння, а тому фактично розгортає проти українського населення не лише військовий (який відбувається вже в умовах сучасності), а й інформаційний фронт, однак, російська федерації потерпає невдачі як і першому плані, так і в другому. Також, з приводу вищевикладеного слід додати, що така війна також має певні ознаки гібридної, адже, висвітлюється те, що держави частіше використовують недержавних дійових осіб та інформаційні технології задля досягнення перемоги над своїми супротивниками за відсутності прямого збройного конфлікту (однак, як показують умови сьогодення, то і під час збройного конфлікту) маючи на меті досягнення певних політичних цілей. У свою чергу, на думку українських істориків практично всі інструменти (спроба закріплення свого впливу на українських теренах через підтримку лояльних українських політичних середовищ, внутрішньополітичний розкол українського суспільства засобами пропаганди, відкрите військове втручання, намагання представити агресію як внутрішній громадянський конфлікт) випробовувала російська влада ще з XVII-XVIII століттях. Найбільш яскраво подібний сценарій застосовували більшовики проти Української Народної Республіки під час Української революції ще у 1917-1921 роках [3, с. 3].

Загалом, певні загрози національній безпеці України в інформаційній сфері являють собою сукупність умов та чинників, які становлять небезпеку життєво важливим інтересам держави, суспільства та особи через можливість негативного інформаційного впливу на свідомість та поведінку громадян, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру [4, с. 2]. Так, загрози інформаційній безпеці визначаються як сукупність умов та факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства та держави в інформаційній сфері. До основних загроз інформаційній безпеці нашій державі, як зазначать вітчизняні експерти, можуть бути віднесені обмеження свободи слова та доступу громадян до інформації, руйнування системи цінностей, духовного та фізичного здоров'я особи, суспільства, негативні зміни їх цільових настанов, маніпулювання громадською думкою з боку державної влади, фінансово-політичних кіл, низький рівень інтегрованості України в світовій інформаційній простір тощо.

В сучасній літературі прийнято вирізняти такі фактори, що безпосередньо призводять до створення причин, які сприяють певні загрози інформаційній безпеці: 1) загрози шкідливого впливу відповідної інформації (дезінформації, недостовірної чи шкідливої) на особистість, суспільство, державні інтереси; 2) загрози несанкціонованого чи неправомірного впливу сторонніх осіб до інформації та інформаційних ресурсів фізичних та юридичних осіб, органів державної влади та місцевого

самоврядування; 3) загрози обмеженню інформаційних прав особистості, механізмам їх реалізації [5, с. 1]. Відповідно до Указу Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки», була створена Стратегія інформаційної безпеки, в змісті положень якої чітко визначаються глобальні виклики та загрози інформаційній безпеці, національні виклики та загрози, стратегічні цілі та напрямки реалізації цієї Стратегії, механізми реалізації її мети та завдань, а також очікувані результати від проведеної роботи [6].

Зазначимо той факт, що після введення воєнного стану на територію нашої незалежної країни, Радою Національної безпеки та оборони України було прийнято рішення від 18 березня 2022 року «Про нейтралізацію загроз інформаційній безпеці держави», в змісті якого влада нашої держави визначила, що адміністрація Державної служби спеціального зв'язку та захисту інформації України разом із іншими службами ЗМІ повинні забезпечити: 1) стале функціонування об'єктів цифрового ефірного мовлення та безперебійну трансляцію телевізійних каналів в МХ -1, -2, -3, -5; 2) цілодобовий моніторинг ефірної мережі, обладнання головної станції мультиплексування, супутникових та наземних каналів зв'язку; 3) резервування супутникових каналів доставки програм та обладнання головної станції мультиплексування; 4) резервну доставку телеканалів до цифрових передавачів із залучення альтернативного оператора супутникового зв'язку [7].

При аналізуванні сучасної юридичної літератури, довелося визначити, що як певна протидія глобальним негативним інформаційним впливам, операціям та війнам, пріоритетними напрямами державної політики та важливими кроками з боку власних органів України мають бути: 1) інтеграція України до світового та регіонального європейського інформаційного просторів; 2) створення власної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства; 2) інтеграція у міжнародні інформаційні та інформаційно-телекомунікаційні системи та організації; 4) впровадження нових та підвищення ефективності вже існуючих сучасних інформаційно-комунікативних технологій у процеси державного управління; 5) ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригуванні державної політики в інформаційній сфері [8, с. 30]. Так, ми погоджуємся з тим, що зазначені напрямки державної політики саме у сфері інформаційної безпеки зможуть в подальшому спонукати державну владу у знаходження й інших можливих напрямків протидії загрозам інформаційної безпеки як певного елементу національної безпеки нашої держави.

Захист та протидія загрозам інформаційної безпеки України, як відповідного елемента національної безпеки нашої країни, в останні роки так і в умовах сучасності набуває все більшої актуальності, у зв'язку із повномасштабним вторгненням окупаційних військ країни-агресора на територію нашої незалежної держави. Дана актуальність підтверджується тим, що країна-агресор намагається переконати світову спільному в тому, що на території України відбувається громадське протистояння, а тому фактично розгортає проти українського населення не лише військовий (який відбувається вже в умовах сучасності), а й інформаційний фронт, однак, російська федерації потерпає невдачі як і першому плані, так і в другому.

Саме через вищевикладене, державна влада України повинна прикласти не малі зусилля задля підтримання захисту своїх громадян, суспільства та держави в цілому, щоб запобігати будь-яким проявам неправдивої інформації в ЗМІ України.

ЛІТЕРАТУРА

1. Глушко А.Д., Пантась В.В., Бабенко С.Р. Інформаційна політика в системі забезпечення фінансової безпеки держави. URL: http://www.economy.nayka.com.ua/pdf/2_2022/97.pdf (дата звернення: 23.09.2022).

2. Захист інформаційної безпеки як функція держави. URL: http://www.mego.info (дата звернення: 23.09.2022).

3. Гібридна війна проти України: історія, інструменти, технології. URL: https://library.vn.ua/news-and-events/novini/gibridna-vijna-proti-ukraiini (дата звернення: 26.09.2022).

4. Petryk V. Sutnist informatsiinoi bezpeky derzhavy, suspilstva ta osoby. Rezhym dostupu. URL: http://www.justinian.com.ua/article.php?id=3222 (дата звернення: 26.09.2022).

5. Основні загрози інформаційній безпеці України. URL: https://sites.google.com/site/bezpekiukraien223/osnovni-zagrozi-informacijnij-bezpreci (дата звернення: 27.09.2022).

6. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 року №685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 29.09.2022).

7. Про нейтралізацію загроз інформаційній безпеці держави: Рішення Ради національної безпеки та оборони України від 18.03.2022 року №n0003525-22. URL: https://zakon.rada.gov.ua/laws/show/n0003525-22#Text (дата звернення: 01.10.2022).

8. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічними впливам. Політичні науки, 2016. 27-32 с.