УДК 338.2:351.863
DOI https://doi.org/10.32837/apdp.v0i87.2809

Т. С. Перун

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЗОНІ БОЙОВОГО КОНФЛІКТУ

Постановка проблеми. Значні темпи розвитку інформаційних систем різного призначення, комп'ютерних мереж типу Інтернет та електронних засобів масової інформації зумовили формування глобального інформаційного простору. Поряд із сухопутним, морським, повітряним та космічним простором у збройних силах найбільш розвинених країн стали активно використовувати інформаційний простір для вирішення широкого кола військових завдань. Унаслідок вразливості інформаційно-телекомунікаційних систем до радіоелектронних та програмно-апаратних впливів у світі виникла і набула неабиякого поширення інформаційна зброя, що володіє транскордонними вражаючими факторами, а також різко зросла загроза інформаційної війни. Україна стрімко просувається по шляху інформатизації всіх сфер життєдіяльності суспільства, проте незаконна окупація Донецької та Луганської областей, а також АР Крим, принесла із собою серйозні загрози національної безпеки, що походять із глобального інформаційного простору.

Крім того, внаслідок широкого застосування в системах управління військами і зброєю комп'ютерної техніки цей перелік доповнився завданням захисту інформаційної інфраструктури Збройних Сил України від комп'ютерних атак. Досвід збройних конфліктів останніх років, а також практика оперативної підготовки військ і штабів дозволяють констатувати, що зараз у Збройних Силах України сформовано окремий напрям діяльності, покликаний забезпечити ефективне стримування, запобігання і вирішення військових конфліктів у інформаційному просторі, що зумовлює актуальність зазначеного наукового дослідження.

Аналіз останніх досліджень і публікацій. Інформаційна безпека збройних сил через її визначальну роль у забезпеченні національної безпеки знаходиться у фокусі досліджень учених-юристів, економістів та політологів. Теоретичні проблеми, пов'язані з різними аспектами економічних інтересів і їхньої взаємодії, досліджувались у роботах зарубіжних авторів: М. Вебера, А. Маршалла, С. Нілсона, А. Сміта, І. Фішера, Д. Коатса та ін.

У національній науці досі залишається дискусійним питання про сутність інформаційної безпеки. Результатом аналізу наукових праць фахівців різних галузей наукових досліджень стало виокремлення не менше двох десятків визначень, різних за своїм смисловим навантаженням. Серед вітчизняних авторів, які приділяли значну увагу у своїх наукових пошуках дослідженню інформаційної безпеки, можна виділити М.А. Бендікова, Г. Гулака, Я.Д. Вишнякова, Л.П. Гончаренко, А.А. Драга, Г.Б. Клейнера, В. Костицького, Е.А. Олейникова, В.Л. Тамбовцева, М. Єрмошенко, В. Мунтіян, С.А. Харченко, В.В. Черкасова та інших.

Формулювання цілей статті (постановка завдання). Метою проведення наукового дослідження є аналіз еволюції, детермінування та визначення основних ознак поняття інформаційної безпеки в зоні військового конфлікту та визначення перспективних напрямів її формування в сучасних політичних умовах.

Виклад основного матеріалу дослідження. Перманентний розвиток інформаційних технологій та системи електронних послуг, інформатизація органів державної влади та місцевого самоврядування, глобалізація інформаційного простору та інформаційної інфраструктури змушують ставитися до забезпечення інформаційної безпеки як до комплексного, багатоаспектного напряму діяльності. Адже інформаційна безпека давно вийшла за межі окремого виду безпеки, її вже не можна ставити в один ряд, наприклад, з економічною або продовольчою безпекою.

Надзвичайна важливість протидії актам агресивної інформаційної війни вперше була відзначена в Доктрині інформаційної безпеки України, затвердженій Указом Президента України від 25 лютого 2017 року № 47/2017 [1]. У ній, зокрема, визначено, що «до актуальних загроз національної інформаційної безпеки України належать: проведення спеціальних інформаційних операцій, спрямованих на ослаблення національних оборонних можливостей та пригнічення морального стану особового складу українських збройних сил та інших військових формувань, пропаганда екстремізму, посилення соціальної паніки, дестабілізація соціально-політичної та соціально-економічної ситуації, розпалювання міжетнічних та міжконфесійних конфліктів в Україні; спеціальні інформаційні операції, що проводяться державою-агресором в інших державах для створення негативного іміджу України у світі; інформаційна експансія країни-агресора та її контрольної структури, особливо через розширення власної інформаційної інфраструктури на території України та інших країн; інформаційна перевага Російської Федерації на тимчасово окупованих територіях; низький рівень розвитку національної інформаційної інфраструктури, що обмежує можливості України у сфері ефективної протидії інформаційній агресії; низька ефективність реалізації інформаційної політики, недосконалість інформаційного законодавства, низький рівень медіа-культури суспільства; поширення закликів до порушення територіальної цілісності, пропаганда ізоляціоністських та автономістських концепцій розвитку України».

Таким чином, можна говорити, з одного боку, про особливості забезпечення власної інформаційної безпеки держави, з іншого – про військовий складник забезпечення інформаційної безпеки, тобто як про завдання військово-політичного характеру, що має стратегічне значення для забезпечення національної безпеки та збереження територіальної цілісності.

У зв'язку з цим особливий дослідницький інтерес мають положення документів, що визначають стратегічне планування і відображають офіційну систему поглядів на збройний захист і забезпечення безпеки України.

Так, у межах Воєнної доктрини України [2] встановлено ряд положень, що мають безпосереднє відношення до забезпечення інформаційної безпеки в умовах збройного конфлікту. Зокрема: «головними загрозами, що впливають на воєнно-політичну обстановку в Україні, є: проведення спеціальних інформаційних операцій та провокаційних дій для створення конфліктних ситуацій; зростання політичної

нестабільності в сусідніх державах, зумовленої втручанням з боку інших держав, зниженням соціального рівня життя населення, неефективністю державної влади, спробами поширення сепаратиських настроїв серед етнічних утворень; інтенсивна модернізація та переозброєння збройних сил сусідніх держав, розробка новітніх типів озброєння та військової техніки з покращеними можливостями вогневого ураження; посилення рівня мілітаризації в прикордонних регіонах, збільшення кількості іноземної військової техніки на території сусідніх держав; активна дестабілізуюча інформаційна зовнішня політика і політика оборони Російської Федерації щодо України, а також щодо міжнародних військових організацій НАТО та ЄС; ухилення Російською Федерацією від виконання міжнародних зобов'язань за договорами у сфері контролю над озброєнням; модернізація та вдосконалення систем та технічних розвідувальних комплексів для іноземних спецслужб, збільшення спроб несанкціонованого доступу до інформаційної інфраструктури України; уповільнення процесу укладання договорів та юридичного оформлення державних кордонів, а також розмежування виключної (морської) економічної зони та континентального шельфу між країнами; інформаційна агресія Російської Федерації проти України» [2].

Також варто наголосити, що в майбутньому військові конфлікти будуть відрізнятися непрогнозованістю, вибірковістю і високим ступенем ураження об'єктів, швидкістю маневру військами (силами) і вогнем, застосуванням різних мобільних військових угруповань. Оволодіння стратегічною ініціативою, забезпечення ефективного цивільного та військового управління, забезпечення переваги на суші, в морі та в повітряно-космічному просторі стануть вирішальними факторами для досягнення поставлених цілей.

На жаль, зазначені положення лише відображають ті чи інші моменти, пов'язані з інформаційними технологіями та інформаційною сферою і не пов'язані між собою в складі єдиного комплексу заходів або напрямів діяльності.

Так, наприклад, у визначеннях основних понять, що використовуються у Воєнній доктрині, не враховано загрози застосування інформаційних технологій, відповідних сил і засобів, тобто вони не ототожнюються зі зброєю, а їхнє застосування – зі збройним протистоянням. Такі терміни, як «воєнно-політичний ризик», «воєнно-політичний виклик», «воєнний конфлікт», «збройний конфлікт» тощо, визначені з класичних військових позицій, залишаючи відкритими питання впливу застосування інформаційної зброї та інформаційних атак на інфраструктуру і стратегічні об'єкти держави.

Чи вважати агресивні дії в інформаційному просторі або з інформаційного простору агресією? Як визначити, хто відповідальний за їхнє вчинення – держава-агресор чи терористична група? Чи дозволяє факт постійної інформаційної або кібернетичної атаки реалізувати право на індивідуальну або колективну самооборону із застосуванням сил і засобів збройної боротьби? Зазначені питання потребують детальної законодавчої регламентації.

Серед основних завдань Збройних Сил та інших військових формувань у мирний час можна виділити забезпечення інформаційної безпеки України, проте як самостійне завдання воно не виділено, незважаючи на його визначальне значення.

Разом із тим у збройних силах провідних країн світу зазначений напрям діяльності не просто є пріоритетним, а сформовано окремі військові підрозділи, які безпосередньо відповідають за його реалізацію, регулярно проводяться відповідні навчання. Нарощують ударні ІТ-можливості й деякі країни, що розвиваються. Так, за розрахунками американських військових аналітиків, у Північній Кореї зараз є близько 60 000 фахівців, які виконують завдання, пов'язані з ІТ-розвідкою і кібернетичними атаками [5].

Військова діяльність в інформаційній сфері стає новим різновидом збройної боротьби, а сам інформаційний простір – ще одним полем бойових дій і спеціальних операцій [6, с. 40]. Багато країн вже не приховують не тільки наявність спеціальних сил подібного призначення, але й факти розроблення інформаційної зброї.

Крім того, в країнах НАТО з метою комплексного забезпечення інформаційної безпеки зміцнюється і порядок взаємодії між військовими підрозділами, науково-дослідними інститутами, спеціальними службами, правоохоронними органами, державними установами, організаціями фінансово-економічного сектору, а також розробляються нормативно-правові основи цієї діяльності [8]. У складі спеціальних служб на додаток до існуючих відділів інформаційної безпеки створюються підрозділи розвідувального та спеціального призначення для дій в інформаційній сфері.

Таким чином, підрозділи інформаційної безпеки збройних сил низки іноземних держав постійно забезпечують захист не тільки військової, але також державної цивільної інформаційної інфраструктури. Крім того, формується тенденція розвитку єдиної системи забезпечення інформаційної безпеки в усіх стратегічно важливих державних і суспільних сферах, її орієнтування на постійний моніторинг і попередження інформаційних загроз.

На жаль, офіційна система поглядів на збройний захист і забезпечення безпеки України навіть у перспективному плані подібних підходів не передбачає. Не є більш змістовними в контексті розглянутого питання і положення Стратегії національної безпеки України [9].

У Стратегії наголошується, що «основними її цілями є: мінімізувати загрози національному суверенітету та створити умови для відновлення територіальної цілісності України в межах міжнародно визнаних національних кордонів та забезпечити гарантію мирного майбутнього України, що стає суверенною, незалежною, демократичною, соціальною та правовою державою; забезпечити реалізацію прав та свобод людини і громадянина, забезпечити нову якість економічного, соціального та гуманітарного розвитку, забезпечити інтеграцію України до Європейського Союзу та створити умови для вступу до НАТО» [9].

Разом із тим у рамках докладного опису основних пріоритетів і цілей сталого розвитку, а також серед численних видів безпеки, таких як військова, економічна, продовольча, енергетична і технологічна, інформаційна безпека чомусь не вказана. Згадка про неї зустрічається тільки в самому кінці документа, в розділі, присвяченому організаційним, нормативно-правовим та інформаційним основам реалізації стратегії.

У свою чергу в нашій країні популяризується державна програма «Держава в смартфоні», Міністерство цифрової трансформації презентувало мобільний додаток «Дія», а також онлайн-платформу «Дія. Цифрова грамотність» [4], тобто вже зараз необхідна єдина комплексна політика щодо забезпечення інформаційної безпеки, а не просто облік окремих концептуальних рекомендацій.

Однак Доктрина інформаційної безпеки України була прийнята понад п'ять років тому і вже не відповідає сучасним політичним реаліям, не враховує нові загрози в інформаційній сфері, рівень розвитку і проникнення інформаційних технологій у державне і суспільне життя, критично важливі галузі економіки та народного господарства країни. У свою чергу недооцінка таких ризиків у формуванні інформаційного суспільства в Україні може негативно позначитися на забезпеченні державної безпеки.

Відсутність міжнародних домовленостей і взаємних зобов'язань держав із питань заборони інформаційної зброї і демілітаризації світової інформаційної сфери відкривають широкі можливості перед спеціальними службами і збройними силами щодо використання потенціалу інформаційних технологій на шкоду інтересам миру, стабільності й міжнародної безпеки [13]. Специфіка інформаційної сфери дозволяє віддалено і приховано впливати на критично важливу інформаційну інфраструктуру, порушити роботу систем управління енергетикою, транспортом, зв'язком, фінансовою сферою, викликати техногенні аварії, завдати серйозної шкоди підприємствам і установам, а також підірвати основи обороноздатності країни.

Розуміючи складність ситуації, окремі країни проводять агресивну політику щодо вдосконалення правового, організаційного та технічного складників забезпечення інформаційної безпеки. У травні 2011 року США прийняли Міжнародну стратегію щодо кіберпростору. Зазначений документ, з одного боку, розкриває підхід керівництва цієї країни до проблем забезпечення безпеки світового інформаційного простору і містить заклики до розвитку міжнародного співробітництва в цій галузі [15]. З іншого боку – досить чітко визначає позицію США щодо оперативного реагування на різні інциденти, пов'язані з посяганням на національну інформаційну інфраструктуру та її окремі елементи. Зокрема, в цьому документі кібернетична атака прирівнюється до акту агресії, з усіма його наслідками [16].

У зв'язку з цим положення про можливе застосування класичних сил і засобів збройної боротьби у відповідь на інформаційну атаку варто сприймати, радше, як декларативне попередження, а не реальний хід у відповідь. Водночас вони можуть бути використані як формальний привід для розв'язання збройного конфлікту.

Саме тому необхідно розвивати міжнародне співробітництво за цими напрямками. Також із метою забезпечення міжнародної інформаційної безпеки, запобігання і припинення атак в інформаційному просторі, спрямованих на розв'язання збройних конфліктів, а також захисту критично важливих об'єктів держав та інформаційної інфраструктури, необхідно створити міжнародний центр моніторингу інформаційної сфери. За посередництвом такої структури держави могли б обмінюватися актуальною інформацією, формувати й розвивати міжнародно-правову основу забезпечення інформаційної безпеки, повідомляти про всі інциденти

та загрози, пов'язані з інформаційною сферою, оперативно реагувати на них, спільно боротися з ІТ-злочинністю, брати на себе зобов'язання й іншими способами зміцнювати взаємну довіру і розвивати співпрацю.

Висновки. Отже, на основі аналізу документів, що відображають офіційну систему поглядів на збройний захист і забезпечення безпеки України в контексті забезпечення інформаційної безпеки, можна зробити декілька висновків.

Забезпечення інформаційної безпеки в рамках Воєнної доктрини України і Стратегії національної безпеки України як окремий і самостійний напрям діяльності не розглядається. Незважаючи на визнання інформаційних загроз, відображені лише окремі питання, пов'язані з інформаційною сферою та застосуванням інформаційних технологій.

Доктрина інформаційної безпеки України вже не відповідає сучасним політичним реаліям, не враховує нові загрози в інформаційній сфері, рівень розвитку й проникнення інформаційних технологій у державне та суспільне життя, критично важливі галузі економіки та народного господарства країни, а також потребує оновлення.

Для захисту критично важливих об'єктів держав та інформаційної інфраструктури необхідно створити міжнародний центр моніторингу інформаційної сфери.

Література

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лютого 2017 року № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 29.07.2020).

2. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України» : Указ Президента України від 24 вересня 2015 року № 555/2015. URL: https https://zakon.rada.gov.ua/laws/show/555/2015#Text (дата звернення: 29.07.2020).

3. Костицький В.В. Інформаційна війна проти України – виклик світовому порядку. URL: http://oksamyt.org/2015/02/02/0202201511 (дата звернення: 10.06.2017).

4. Лещенко О.Я. «Гібридна війна» як науковий конструкт: проблеми пошуку термінологічної та концептуальної сутності. *Гілея: науковий вісник :* зб. наук. праць. Київ, 2017. Вип. 117. С. 262–267.

5. Security Strategy for Society. URL: https://turvallisuuskomitea.-fi/en/security-strategy-for-society (дата звернення: 05.01.2020).

6. Nilsson S.C. Swedish National Security: Challenges and Opportunities beyond 2014. The Royal Swedish Academy of War Sciences, 2013. 57 p.

7. Resilience: a core element of collective defence. URL: http://www.-nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.-htm (дата звернення: 29.07.2020).

8. The Three Ages of NATO: An Evolving Alliance. Speech by NATO Secretary General Jens Stoltenberg at the Harvard Kennedy School. URL: https://www.nato.int/cps/en/natohq/opinions_135317.htm (дата звернення 29.07.2020).

9. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» : Указ Президента України 26 травня 2015 року № 287/2015 URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text (дата звернення: 29.07.2020).

10. Розробка форм і способів інформаційної боротьби при виконанні внутрішніми Міністерства внутрішніх справ України службово-бойових завдань (шифр «Концепт») : звіт про НДР (заключ.) 02.12.09 р. / Акад. ВВ МВС України ; кер. В.І. Воробйов ; викон. : О.Д. Черкашин та ін. Харків, 2009. 312 с.

11. Konstadinides T. Civil Protection in Europe and the Lisbon solidarity clause: A genuine legal concept or a paper exercise. URL: https://www.-jur.uu.se/digitalAssets/585/c_585476-l_3-k_wps2011_3.pdf (дата звернення: 29.07.2020).

12. Integrating climate change adaptation into civil protection: comparative lessons from Norway, Sweden and the Netherlands. *Local Environment*. 2012. Vol. 17. Issue 6–7. P. 679–694.

13. Newson, Robert A. Counter-Unconventional Warfare Is the Way of the Future. How Can We Get There? URL: https://smallwarsjournal.com/blog/counter-unconventional-warfare-is-the-way-of-the-future-how-can-we-get-there (дата звернення: 29.07.2020).

14. Luiijf E., Besseling K., Graaf P. (2013). Nineteen National Cyber Security Strategies. International Journal of Critical Infrastructure Protection. 9. 3. 10.1504/IJCIS.2013.051608.

15. Coats, D.R. (2017). Worldwide Threat Assessment of the US Intelligence Community. Washington, DC, USA.

16. International Strategy for Cyberspace. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (дата звернення: 29.07.2020).

Анотація

Перун Т. С. **Забезпечення інформаційної безпеки в зоні бойового конфлікту.** – Стаття.

У статті аналізуються положення нормативно-правових актів, які відображають офіційну систему поглядів на збройний захист і забезпечення безпеки України, що присвячені питанням забезпечення інформаційної безпеки. Обґрунтовується необхідність їхнього подальшого розвитку та формування єдиного підходу до забезпечення інформаційної безпеки як комплексному напряму діяльності.

Метою статті є аналіз еволюції, детермінування та визначення основних ознак поняття інформаційної безпеки в зоні військового конфлікту та визначити перспективні напрями її формування в сучасних політичних умовах.

Автором досліджено положення документів, що визначають стратегічне планування та відображають офіційну систему поглядів на збройний захист і забезпечення безпеки України.

Також проаналізовано генезис наукових поглядів на інформаційну протидію як механізм вирішення міждержавних протиріч. Досліджено сутність засобів забезпечення інформаційної безпеки в умовах збройного конфлікту.

Забезпечення інформаційної безпеки в межах Воєнної доктрини України і Стратегії національної безпеки України як окремого і самостійного напряму діяльності не розглядається. Незважаючи на визнання інформаційних загроз, відображені лише окремі питання, пов'язані з інформаційною сферою та застосуванням інформаційних технологій.

Автор доходить висновку, що забезпечення інформаційної безпеки в рамках Воєнної доктрини України і Стратегії національної безпеки України як окремого і самостійного напряму діяльності не розглядається.

Доктрина інформаційної безпеки України вже не відповідає сучасним політичним реаліям, не враховує нові загрози в інформаційній сфері, рівень розвитку і проникнення інформаційних технологій у державне і суспільне життя, критично важливі галузі економіки та народного господарства країни та потребує оновлення.

Для захисту критично важливих об'єктів держави та інформаційної інфраструктури необхідно створити міжнародний центр моніторингу інформаційної сфери.

Ключові слова: безпека, інформаційна безпека, форми інформаційної безпеки, інформаційна безпека держави, напрями формування інформаційної безпеки, збройний конфлікт.

Summary

Perun T. S. **The ensuring of information security on the combat conflict area.** – Article.

The article analyzes the provisions of normative - legal acts that reflect the official system of views on the armed defense and security of Ukraine, which are devoted to the issues of information security. The necessity of their further development and formation of a unified approach to information security as a complex area of activity is substantiated.

The aim of the article is to analyze the evolution, determination and definition of the main features of the concept of information security in the zone of military conflict and to identify promising areas of its formation in modern political conditions.

The author examines the provisions of documents that define strategic planning and reflect the official system of views on the armed defense and security of Ukraine.

The genesis of scientific views on information counteraction as a mechanism for resolving interstate contradictions is also analyzed. The essence of means of providing information security in the conditions of armed conflict is studied.

Ensuring information security in the framework of the Military Doctrine of Ukraine and the National Security Strategy of Ukraine as a separate and independent area of activity is not considered. Despite

the recognition of information threats, only some issues related to the information sphere and the use of information technology are reflected.

The author concludes that the provision of information security in the framework of the Military Doctrine of Ukraine and the National Security Strategy of Ukraine as a separate and independent area of activity is not considered. Despite the recognition of information threats, only some issues related to the information sphere and the use of information technology are reflected.

The doctrine of information security of Ukraine no longer corresponds to modern political realities, does not take into account new threats in the information sphere, the level of development and penetration of information technologies into state and public life, critical sectors of the economy and the economy and needs updating.

To protect critical objects of states and information infrastructure, it is necessary to create an international monitoring center for the information sphere.

Key words: security, information protection, forms of information security, information security of the state, directions of information security formation, management system.