Берегута Віталій
Донецький національний університет імені Василя Стуса

ВДОСКОНАЛЕННЯ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРБЕЗПЕКИ УКРАЇНИ ЯК НАСЛІДОК ТРАНСФОРМАЦІЇ ХАРАКТЕРУ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Ключові слова: інформаційна безпека України, кібербезпека України, російсько-українська війна, характер міжнародного конфлікту, характер війни.
Keywords: information security of Ukraine, cybersecurity of Ukraine, Russian-Ukrainian war, character of international conflict, character of war.

Сучасні міжнародні конфлікти та війни характеризуються комплексним використанням протиборчими сторонами політичних, економічних, військових, технологічних та інформаційно-психологічних інструментів впливу на супротивника з метою максимальної реалізації власних національних інтересів. Не є винятком і російсько-українська війна, в якій воєнна агресія Росії супроводжується активним використанням новітніх інформаційних технологій поза зоною бойових дій. Ідеться, наприклад, про хакерські атаки та кібератаки, інформаційно-психологічні операції та поширення дезінформації через ЗМІ. Такі інструменти традиційно використовуються Росією з метою впливу на політичне керівництво України та українських громадян як для просування російських наративів, поширення недовіри до влади й внутрішньої дестабілізації України, так і для посилення своєї позиції в переговорному процесі щодо врегулювання російсько-української війни.

Кількість кібератак, здійснених Росією на українські органи державної влади та об’єкти критичної інфраструктури, постійно зростає. Державна служба спеціального зв’язку та захисту інформації України повідомляє, що Урядова команда реагування на комп’ютерні надзвичайні події CERT-UA у 2024 р. зафіксувала 4 315 відповідних кіберінцидентів, що на 69,8 % більше, ніж у 2023 р. (2 541 кіберінцидентів) [9] та на 105,4 % більше, ніж у 2022 р. (2 100 кіберінцидентів, з яких понад 1 500 – з 24.02.2022) [8]. Отже, це засвідчує трансформацію характеру російсько-української війни у вигляді формування інформаційного простору та кіберпростору як новітньої повноцінної арени боротьби між двома державами. Відповідно кожна зі сторін додатково застосовує різні інформаційні інструменти впливу на перебіг війни, а відсутність стратегії попередження та протидії деструктивному використанню державою-опонентом інформаційно-комунікаційних технологій створює вразливе місце в системі національної безпеки.

Важливою передумовою гарантування інформаційної безпеки та кібербезпеки України є формування нормативно-правової бази та її оновлення відповідно до актуальних викликів суверенітету, територіальної цілісності та незалежності держави. Так, якщо до початку російської агресії чинною залишалась Доктрина інформаційної безпеки України, що затверджена Указом Президента України від 08.07.2009, то вже під час російсько-української війни були ухвалені два нові документи у сфері інформаційної безпеки, а саме: Доктрина інфор-

маційної безпеки України, що затверджена указом Президента України від 25.02.2017, та Стратегія інформаційної безпеки України, що затверджена Указом Президента України від 28.12.2021.

У Доктрині інформаційної безпеки України 2017 р. визначено, що метою використання Росією інформаційних технологій впливу на громадську свідомість є пропаганда агресивної війни, ідей порушення територіальної цілісності й суверенітету України, насильницької зміни її конституційного ладу, а також посилення ворожнечі на релігійному та національному підґрунті. Одним із пріоритетних завдань державної політики в інформаційній сфері окреслено протидію російській деструктивній пропаганді й дезінформації та захист українських громадян від них в умовах гібридної війни [6].

Порівняно з Доктриною 2017 р., Стратегія інформаційної безпеки України 2021 р. містить більш конкретизовані напрями й форми російських інформаційних впливів. Так, у документі визначені намагання Росії інформаційними засобами посилити панічні настрої в суспільстві й загострити та дестабілізувати соціально-економічну й політичну ситуацію в Україні, а також окреслені російські інформаційні кампанії антиукраїнського характеру на тимчасово окупованих територіях України через ЗМІ. Водночас Україна визнає відсутність ефективної системи реагування та протидії інформаційній агресії Росії через, зокрема, нерозвиненість інформаційної інфраструктури, несформовану систему стратегічних комунікацій між органами державної влади, відповідальних за інформаційну політику, і невисокий рівень інформаційної культури та медіаграмотності населення [4].

Відповідно до таких викликів у 2023 р. було розроблено План заходів з реалізації Стратегії інформаційної безпеки на період до 2025 р., який охоплює сім стратегічних цілей із визначеними завданнями, заходами й термінами їх реалізації: «Протидія дезінформації та інформаційним операціям, насамперед держави-агресора», «Забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності», «Підвищення рівня медіакультури та медіаграмотності суспільства», «Забезпечення дотримання прав особи на збирання, зберігання, використання та поширення інформації», «Інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України, до загальноукраїнського інформаційного простору», «Створення ефективної системи стратегічних комунікацій» та «Розвиток інформаційного суспільства та підвищення рівня культури діалогу» [1].

Розглядаючи кібербезпеку, важливо наголосити, що в довоєнний період вона не була виділена як окремий сектор національної безпеки України. Однак з метою ефективнішої протидії кіберзагрозам під час російсько-української війни були ухвалені дві стратегії кібербезпеки України, що затверджені указами Президента України від 15.03.2016 та від 26.08.2021, і Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017.

Так, Стратегія кібербезпеки України 2016 р. визначає російську військову агресію одним із ключових факторів виокремлення та розробки національної системи кібербезпеки як частини національної безпеки України [5]. Натомість

Закон України «Про основні засади забезпечення кібербезпеки України» хоча й не містить безпосередніх згадок про Росію, але окреслює принципи, правову основу, суб'єктів та об'єктів гарантування кібербезпеки України й характеризує державно-приватне та міжнародне партнерство в процесі цього [2].

Стратегія кібербезпеки України 2021 р. окреслює російську гібридну агресію проти України в кіберпросторі як загрозу кібербезпеці України, ключовою формою якої як елементу інформаційно-психологічних операцій є кібератаки на інформаційно-комунікаційні системи об'єктів інформаційної інфраструктури й органів державної влади для виведення їх з ладу або отримання несанкціонованого доступу до інформації. Документ також визначає розвідувально-підривну діяльність Росії в українському кіберпросторі із залученням представників міжнародних хакерських угруповань [3]. Як і у випадку зі Стратегією інформаційної безпеки України 2021 р., додатком до Стратегії кібербезпеки України 2021 р. є План її реалізації до 2025 р., який охоплює десять стратегічних цілей із визначеними завданнями, заходами й термінами їх реалізації: «Дієва кібероборона», «Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму», «Ефективна протидія кіберзлочинності», «Розвиток асиметричних інструментів стримування», «Національна кіберготовність та надійний кіберзахист», «Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки», «Безпечні цифрові послуги», «Зміцнення системи координації», «Формування нової моделі відносин у сфері кібербезпеки» та «Прагматичне міжнародне співробітництво» [7].

Отже, активне системне протиборство Росії та України в інформаційній сфері трансформувало характер російсько-української війни так, що можна стверджувати про утворення двох нових її взаємопов'язаних вимірів – інформаційного та кібернетичного, які засвідчують вихід російсько-українського протистояння за межі зони бойових дій. У таких умовах формування системи гнучкого реагування та протидії російським інформаційним та кіберзагрозам є критично необхідним для комплексного гарантування національної безпеки України, а функціонування такої системи має бути визначене стратегіями інформаційної безпеки та кібербезпеки, успішний досвід реалізації яких Україна вже має. Оскільки обидві чинні стратегії були ухвалені до початку повномасштабного російського вторгнення та розраховані на період до 2025 р., то вже на початку 2026 р. Кабінет Міністрів України й Рада Національної безпеки і оборони України повинні розробити, а Президент України – затвердити оновлені стратегії інформаційної безпеки та кібербезпеки і плани дій щодо їх реалізації зі врахуванням досвіду війни з Росією у 2022–2025 рр.

Джерела та література

1. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: Розпорядження Кабінету Міністрів України від 30.03.2023 р. № 272-р. *Урядовий кур'єр.* 2023. № 67. URL: https://zakon.rada.gov.ua/laws/show/272–2023-%D1%80

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. *Голос України.* 2017. № 208. URL: https://zakon.rada.gov.ua/laws/show/2163-19# Text

3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 р. № 447/2021. *Урядовий кур'єр.* 2021. № 165. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

4. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 р. № 685/2021. *Урядовий кур'єр.* 2021. № 251. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

5. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 р. № 96/2016. *Офіс Президента України.* 2016. URL: https://www.president.gov.ua/documents/962016–19836

6. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 р. № 47/2017. *Офіс Президента України.* 2017. URL: https://www.president.gov.ua/documents/472017–21374

7. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України»: Указ Президента України від 01.02.2022 р. № 37/2022. *Офіс Президента України.* 2022. URL: https://www.president.gov.ua/documents/372022–41289

8. CERT-UA від початку року опрацювала більше двох тисяч кібератак на Україну. *Державна служба спеціального зв'язку та захисту інформації України.* 2022. URL: https://cip.gov.ua/ua/news/cert-ua-vid-pochatku-roku-opracyuvala-bilshe-dvokh-tisyach-kiberatak-na-ukrayinu

9. CERT-UA минулого року опрацювала 4 315 кіберінцидентів. *Державна служба спеціального зв'язку та захисту інформації України.* 2025. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv

Затоковенко Максим
Донецький національний університет імені Василя Стуса

ФАКТОР КНДР У РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ

Ключові слова: російсько-українська війна, російсько-північнокорейські відносини.
Keywords: Russian-Ukrainian war, Russia–North Korean relations.

Північна Корея направила військових до України для підтримки російського вторгнення, і цей крок став черговим свідченням поглиблення двосторонньої співпраці після початку повномасштабної війни. Ймовірно, москва прагне використати північнокорейський людський ресурс для посилення своїх наступальних операцій та часткового компенсування нестачі власного особового складу. Втім присутність північнокорейських військових у зоні бойових дій в Україні має ширші геополітичні наслідки. Пхеньян, схоже, розглядає це як можливість надати своїм військовим досвід участі в сучасній війні, який потенційно може бути використаний у майбутніх конфліктах. Поглиблення військово-політичного союзу між КНДР та росією становить серйозну загрозу довготривалій стабільності не лише на Корейському півострові, а й у всьому Азійсько-Тихоокеанському регіоні, що може мати потенційний вплив на стратегічних союзників України – США та Японію.

Тому мета статті – дослідити масштаб залученості КНДР у війну в Україні та підтримку РФ.