УДК 004.056.5

Ю.Д Щур
Н.Р. Кондратенко

АНАЛІЗ ДАНИХ ВІДКРИТИХ ДЖЕРЕЛ ДЛЯ ПЕРЕДБАЧЕННЯ ХВИЛЬ ФІШИНГУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Вінницький національний технічний університет

Анотація. *У роботі проаналізовано новітні форми ведення гібридної війни, що поєднують високотехнологічні, інформаційні та кіберкомпоненти. Висвітлено приклади таких дій в Україні з 2014-20205 року, включаючи анексію Криму та конфлікт на Донбасі. Автори доводять, що сучасні конфлікти зміщуються у бік інтеграції асиметричних впливів на ключові державні та соціальні системи без обов'язкового використання регулярних військ.*

Ключові слова: гібридна війна, кібербезпека, інформаційна боротьба, високі технології, Україна.

Abstract. *The paper analyzes the latest forms of hybrid warfare that combine high-tech, information and cyber components. Examples of such actions in Ukraine since 2014-2025, including the annexation of Crimea and the conflict in Donbas, are highlighted. The authors argue that modern conflicts are shifting towards the integration of asymmetric influences on key state and social systems without the mandatory use of regular troops.*

Keywords: hybrid warfare, cybersecurity, information warfare, high technology, Ukraine.

Вступ

У сучасних умовах трансформації глобальної безпекової архітектури та стрімкого розвитку цифрових технологій відбувається докорінна зміна філософії, концепції й практики ведення війни. Сучасні конфлікти дедалі більше виходять за межі класичного бойового протистояння, набуваючи багатовимірного характеру та охоплюючи одночасно військові, економічні, політичні, дипломатичні, інформаційні, кібернетичні та психологічні сфери. У цьому контексті ключовим поняттям стає «гібридна війна», що описує явище, за якого застосовуються як звичайні, так і незвичайні засоби впливу — від військових операцій до маніпуляцій суспільною думкою та деструктивної діяльності в кіберпросторі. Проблематика дослідження гібридних воєн є надзвичайно актуальною в контексті збройної агресії російської федерації проти України, яка триває з 2014 року та має яскраво виражений гібридний характер.

Результати дослідження

У сучасних умовах трансформації глобальної безпекової архітектури та стрімкого розвитку цифрових технологій відбувається докорінна зміна філософії, концепції й практики ведення війни. Сучасні конфлікти дедалі більше виходять за межі класичного бойового протистояння, набуваючи багатовимірного характеру та охоплюючи одночасно військові, економічні, політичні, дипломатичні, інформаційні, кібернетичні та психологічні сфери [1]. У цьому контексті ключовим поняттям стає «гібридна війна», що описує явище, за якого застосовуються як звичайні, так і незвичайні засоби впливу — від військових операцій до маніпуляцій суспільною думкою та деструктивної діяльності в кіберпросторі [1], [2]. Проблематика дослідження гібридних воєн є надзвичайно актуальною в контексті збройної агресії проти України, яка триває з 2014 року та має яскраво виражений гібридний характер [1], [3].

Аналіз матеріалів дослідження дозволяє стверджувати, що гібридна війна є цілеспрямованим і координованим процесом системного впливу на критичні елементи державної, суспільної, економічної, інформаційної та оборонної інфраструктури супротивника [1], [4]. На відміну від традиційних воєн, у гібридних конфліктах акцент переноситься на досягнення стратегічних цілей шляхом створення довготривалого деструктивного впливу без необхідності безпосереднього контролю території. Такий вплив досягається за рахунок точкового використання кібероперацій, інформаційно-психологічних атак, дезінформації, соціального розколу, підтримки протестних рухів і дискредитації влади [5].

Досвід України демонструє масштабність, скоординованість та інноваційність сучасних гібридних агресивних дій. Починаючи з анексії Криму та військових дій на Донбасі, було зафіксовано систематичне використання Росією високотехнологічних засобів радіоелектронної боротьби, безпілотних літальних апаратів, комплексів розвідки та ураження, інструментів інформаційно-психологічного впливу, а також кібератак проти урядових установ, об'єктів критичної інфраструктури та інформаційного простору держави [1], [3]. Кібероперації

супроводжуються інформаційними кампаніями, що спрямовані на підрив легітимності влади, деморалізацію збройних сил, поширення паніки, зневіри та апатії серед населення. В умовах війни з Росією в Україні проявляється новий тип протистояння — війна за свідомість, ідентичність та довіру суспільства [2].

З огляду на стрімке поширення технологічних засобів впливу, зокрема соціальних мереж, бот-мереж, алгоритмічного просування контенту та штучного інтелекту, гібридна війна дедалі більше стає змаганням за домінування в інформаційному середовищі. Протягом бойових дій було зафіксовано різке зростання інформаційної активності в кіберпросторі перед початком активної фази бойових дій, що свідчить про цілеспрямоване використання інформаційного простору як інструмента підготовки до військових операцій [1]. Паралельно з цим, противник активно впроваджував методи прихованої дезінформації, фейкових новин, фальшивих акаунтів і створення штучних протестних рухів, які імітували внутрішнє невдоволення владою [4].

Враховуючи описані загрози, автори роботи аргументовано доводять необхідність формування комплексної системи протидії гібридним викликам. Така система має включати створення національних центрів кіберзахисту та протидії інформаційним загрозам, розвиток вітчизняних кластерів передових оборонних технологій, впровадження ситуативного управління в реальному часі, забезпечення належного рівня підготовки спеціалістів у сфері кібербезпеки, електронної розвідки та інформаційної протидії [1].

Узагальнюючи результати дослідження, що гібридна війна є новим етапом еволюції воєнного протистояння, де перемагає не той, хто має більшу кількість збройних сил, а той, хто краще опановує технології, швидше адаптується до змін і вміє системно використовувати як «жорстку», так і «м'яку» силу [2], [5]. Саме тому державна політика в галузі національної безпеки має бути орієнтована на розвиток інновацій, освіти, науки та високотехнологічної оборонної промисловості. Перемога в сучасній війні — це насамперед перемога за інтелектуальну перевагу, здатність до синергетичного мислення та стратегічного планування.

Висновки

У ході дослідження було встановлено, що гібридна війна є складним явищем, у межах якого поєднуються традиційні воєнні дії з кібернетичними, інформаційними, економічними та психологічними інструментами впливу. Основною її метою є не стільки пряме знищення супротивника, скільки підрив його внутрішньої стабільності, деморалізація населення та делегітимізація інститутів державної влади. Особливість сучасних гібридних конфліктів полягає в тому, що противник цілеспрямовано діє на ключові вразливості — інфраструктурні, інформаційні та ідеологічні — використовуючи новітні технології, соціальні мережі, інструменти дезінформації й кібератаки.

На прикладі України автори продемонстрували, що з 2014 року російська агресія має виразно гібридний характер, у якому інформаційні кампанії, операції з впливу на громадську думку, атаки на цифрову інфраструктуру та маніпуляції у медіапросторі стали такими ж важливими, як і бойові дії. Ці дії мають на меті створити у свідомості громадян відчуття безпорадності, невпевненості та втрати контролю, що сприяє посиленню внутрішньої фрагментації суспільства.

Дослідження доводить, що ефективна протидія гібридним загрозам потребує не лише технологічної модернізації системи безпеки, а й розвитку кадрового потенціалу, створення кіберзахисних структур, інституцій стратегічних комунікацій та освітніх програм. Успішна відповідь держави на подібні виклики залежить від здатності адаптуватися до нової логіки конфлікту, що ґрунтується не на фронті, а в інформаційному полі та свідомості людей.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Danyk, Y., Maliarchuk, T., & Briggs, C. (2017). Hybrid War: High-tech, Information and Cyber Conflicts. Connections: The Quarterly Journal, 16(2), 5–24. https://doi.org/10.11610/Connections.16.2.01 (дата звернення: 29.04.2025).
2. Гібридна війна – Вікіпедія. Вікіпедія. [Електронний ресурс] URL: https://uk.wikipedia.org/wiki/Гібридна_війна (дата звернення: 29.04.2025).
   10.Andriyevskyy T. G. Цілі російсько-української гібридної війни. Політичне життя. 2018. № 2. С. 103–108. [Електронний ресурс] URL: https://doi.org/10.31558/2519-2949.2018.2.17 (дата звернення: 29.04..2025)
3. Центр протидії дезінформації. Telegram. [Електронний ресурс]URL: https://t.me/CenterCounteringDisinformation/7744 (дата звернення: 29.04..2025)
4. Як розпізнати фейк? – Міністерство з питань реінтеграції тимчасово окупованих територій України. Just a moment... [Електронний ресурс] URL: https://minre.gov.ua/2023/08/27/yak-rozpiznaty-fejk/ (дата звернення:05.12.2023).
5. Volodymyr. Гібридна війна. ВУЕ. [Електронний ресурс] URL: https://vue.gov.ua/Гібридна_війна (дата звернення: 29.01.2023)

Щур Юлія Дмитрівна– студентка 2 курсу групи 2БС-23б, факультет інформаційної технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email:

scjulia23@gmail.com

Кондратенко Наталія Романівна – к.т.н., проф., професор кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: kondratenko.natalia@vntu.edu.ua

Shchur Yuliia Dmytrivna– second-year student of group 2BS-23b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: scjulia23@gmail.com

Kondratenko Nataliia Romanivna – Phd in Technical Sciences, Professor, Department of Information Security, Vinnytsia National Technical University, Vinnytsia, email: kondratenko.natalia@vntu.edu.ua