Ігор ХМИРОВ,
доктор наук з державного управління, доцент,
доцент кафедри управління у сфері цивільного захисту
навчально-наукового інституту цивільного захисту
Національного університету цивільного захисту України,
ORCID: https://orcid.org/0000-0002-7958-463X
e-mail: khmyrov7771@gmail.com.ua

Анастасія ХМИРОВА,
кандидат наук з державного управління,
старший викладач-методист навчально-наукового інституту
оперативно-рятувальних сил
Національного університету цивільного захисту України,
ORCID: https://orcid.org/0000-0002-0680-7505
e-mail: khmyrova.anast@gmail.com

Михайло БИРНЯК,
здобувач другого (магістерського)
рівня вищої освіти групи ЗМУЦЗ-24
Національного університету цивільного захисту України,
e-mail: khmyrov7771@gmail.com.ua

DOI: https://doi.org/10.32620/pls.2025.8.79

МЕТОДОЛОГІЧНІ ЗАСАДИ ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Анотація. *Гібридні загрози є комплексною проблемою сучасності, яка характеризується використанням широкого спектру інструментів впливу для досягнення стратегічних цілей агресора при збереженні можливості правдоподібного заперечення своєї участі. На сьогодні необхідно розробити рекомендації щодо вдосконалення нормативно-правового забезпечення інформаційної політики в умовах гібридних загроз, розвитку інституційної спроможності органів державної влади у сфері інформаційної безпеки. Також розробити методологічні та концептуальні засади формування національної стратегії інформаційної безпеки в умовах гібридних загроз, яка передбачає комплексний підхід до розвитку інформаційної стійкості на індивідуальному, організаційному та загальнодержавному рівнях.*

Ключові слова: *державна інформаційна політика, гібридні загрози, інформаційна безпека, стратегічні комунікації, публічне управління, інформаційна держава, гібридність, інформаційне середовище.*

Стрімкий розвиток інформаційно-комунікаційних технологій створює нові можливості для підвищення ефективності державного управління, але водночас породжує нові вразливості. Зростання складності та масштабності інформаційних атак, використання штучного інтелекту для створення дезінформації, розвиток технологій глибинних фейків – усе це формує новий ландшафт загроз для національної безпеки, який вимагає постійного вдосконалення системи інформаційної безпеки у державі. В таких умовах розробка теоретико-методологічних засад формування та реалізації державної інформаційної політики стає не просто актуальним науковим завданням, а нагальною потребою забезпечення національної безпеки та сталого розвитку держави.

Ефективна протидія сучасним гібридним загрозам вимагає комплексного підходу, який би враховував як глобальний характер інформаційних викликів, так і специфіку національного контексту. Необхідність захисту критичної інформаційної інфраструктури, забезпечення інформаційного суверенітету та протидія деструктивним інформаційним впливам стають пріоритетними завданнями державної політики. При цьому важливо розуміти, що успішність цих зусиль залежить від здатності держави мобілізувати та координувати ресурси всіх зацікавлених сторін, створюючи ефективну екосистему інформаційної безпеки.

Питання формування та реалізації державної політики щодо забезпечення інформаційної безпеки розглянуто у працях таких зарубіжних дослідників, як М. Данн, К. Зеттер, Дж. Карр, С. Кемпбелл, Р. Кларк, Е. Клімбург.

Серед вітчизняних науковців проблеми

забезпечення інформаційної та національної безпеки у публічному секторі досліджували такі науковці як С. Гончар, Ю. Даник, П. Воробієнко, В. Дзюндзюк, Д. Дубов, В. Карпенко, Б. Корнієнко, О. Курбан, Р. Лук'янчук, О. Рижук, А. Семенченко, А. Хряпинський, І. Хмиров, А. Хмирова та ін.

Гібридні загрози, як явище та концепція, дуже швидко опинились у центрі дискурсу державної політики після російської агресії проти України в 2014 році. Тому виникла потреба краще зрозуміти це явище, щоб мати можливість виявити та ідентифікувати його, створити стійкість проти нього та, нарешті, протистояти йому. Зрозуміло, що сіра межа між миром і війною значно розширилася, а тому зросла потреба визначити та зрозуміти, як впоратися з усім спектром гібридних загроз, які можуть виникнути.

Управління гібридними загрозами є предметом дискурсу, який швидко зростає на національному та міжнародному рівнях. Це вимагає від держав, суспільств і міжнародних організацій розуміння загрози, підвищення стійкості та набуття можливостей для протидії загрозі. Одним із головних викликів у протидії гібридним загрозам є те, що, з одного боку, ми стикаємося з традиційною проблемою безпеки та зовнішньої політики – зовнішнім антагоністичним державним суб'єктом, тобто зовнішньою загрозою, але з іншого боку, загрози часто проявляються у внутрішній сфері безпеки, де також слід вживати багато можливих контрзаходів. Проте політична культура та бюрократичні структури демократичних держав не завжди сприяють подоланню розриву між тим, що традиційно тлумачиться як «внутрішні» та «зовнішні» виклики безпеці. Тому нове гібридне середовище загроз означає, що концепція політики безпеки має бути розширеною та частково переосмисленою.

Міжнародна співпраця та солідарність також є важливими інструментами для посилення стримування, розуміння загрози та формування стійкості. Невипадково ЄС і НАТО розробили нові інструменти для протидії гібридним загрозам, і Україна останнім часом залучається до цього процесу. За словами колишнього міністра оборони США Дональда Рамсфельда, це передбачає пошук «відомих невідомих» – речей, про які ми знаємо, що ми їх не знаємо [5]. Однак у випадку гібридних загроз такі початкові вимоги є дискусійними, і їх часто неможливо визначити. У такому разі і ті, хто попереджає, і ті, хто приймає рішення, опиняються в положенні не знати того, чого вони не знають.

Незважаючи на зусилля держави в напрямку цифровізації та інформатизації, рівень цифрової трансформації та розвитку електронного урядування в Україні все ще залишається недостатнім. Це обумовлено низкою факторів, серед яких ключовими є недостатня розвиненість матеріально-технічної бази органів публічної влади та обмежений доступ до швидкісного Інтернету в багатьох регіонах країни. Підвищення рівня інформаційної безпеки в публічному секторі України вимагає комплексного підходу, що включає як фінансові інвестиції, так і організаційні та кадрові рішення. Перш за все, необхідно збільшити бюджетні асигнування відповідних відомств на заходи з кібербезпеки та модернізації інформаційної інфраструктури. Стратегічні інвестиції мають бути спрямовані на розвиток інформаційної аналітики та впровадження хмарних технологій, які дозволять підвищити ефективність управління даними та забезпечити їх надійний захист.

Розробка просунутого програмного забезпечення соціальних ботів рухається швидкими темпами. Сьогодні автоматичні облікові записи можуть шукати в Інтернеті інформацію, яка потім використовується для створення надійного профілю, незалежно коментувати публікації інших користувачів, поширювати зібрану інформацію в певний час та імітувати створення людського органічного вмісту в темпі, який виглядає реалістичним на перший погляд. Через це зростає важливість покращення обізнаності та знань у демократичних країнах щодо використання соціальних ботів. Таким чином, операції впливу використовують широкий спектр методологій, технологій та інструментів, але всі вони виграють від великої кількості легкодоступних даних, що дає змогу на відстані дізнатися, як працює чуже інформаційне середовище. Здатність оцінювати та переналаштовувати операції також значно зросла останнім часом. Завдяки швидкості, охопленню та можливостям анонімності в сучасних каналах зв'язку також легше залучати або вилучати акторів у цьому середовищі, не розкриваючи свою особу та справжні мотиви. Враховуючи зростаючу стурбованість з приводу зловживання платформами соціальних мереж, компанії самі вживали і вживають ряд заходів, спрямованих на обмеження шкоди від дезінформації. Із зростанням загрози кібератак з боку національних держав, хакерів і злочинних організацій це почало впливати на те, як світ бачить Інтернет. Неадекватне управління кіберзагрозами наражає користувачів на небезпеку, підриває довіру до Інтернету і ставить під загрозу його здатність бути рушієм економічних і соціальних інновацій. Але поряд з цим, дезінформована та непропорційна реакція органів влади може потенційно загрожувати свободі Інтернету та створити атмосферу страху, невпевненості та сумнівів. Тому майбутнє Інтернету та подальше зростання мережі визначатиметься тим, як органи влади та приватні організації колективно реагуватимуть на обсяг і масштаб кібератак, зростає ризик того, що свободи онлайн і глобальне підключення будуть серйозно обмежені на користь національної безпеки. Оскільки Інтернет переплітається з національною безпекою держав, наступальні та оборонні кіберстратегії формуватимуть майбутнє Інтернету як для користувачів, так і для промисловості. Зараз кіберпростір вважається п'ятою сферою ведення

бойових дій, поряд з землею, морем, повітрям та космосом, але на відміну від інших сфер, конфлікти в кіберпросторі не схожі на традиційну війну.

Комплексний погляд цих питань, дозволяє акцентувати увагу на природі загроз і супротивників, а також викликах, які вони створюють для демократичних країн. При цьому стає все більш важливим питання спроможності демократій та демократичних державних інституцій безпеки протистояти гібридним загрозам і гібридним війнам, розуміючи конкретні вразливі місця в демократичних суспільствах і ліквідуючи їх, а також розробляючи відповіді на ворожі заходи з боку зовнішніх акторів. Особлива вразливість і обмеження, а також переваги демократій вимагають особливих підходів у цьому середовищі. Відкриті суспільства, побудовані на нормативних засадах верховенства права, прав людини та демократії, обов'язково захищаючи свободу слова, об'єднань і преси, повинні розробити рішення, які не тільки зберігають ці основні свободи, але й спираються на їхні сильні сторони. Як показує досвід багатьох країн, ця робота йде повним ходом, для чого залучаються численні організації, яким доручено аналізувати та вирішувати проблему протидії гібридним загрозам, у тому числі (часто і переважно) в інформаційній сфері.

Враховуючи складний характер наявних загроз, реагування має бути організованим відповідно спільних принципів, інтегруючи різні сектори суспільства, а також взаємодію держав партнерів. Ще один важливий висновок, який випливає з розглянутого вище, це важливість знання свого опонента (противника). У той час як ідентифікація та приписування загроз створює реактивні відповіді, проактивне усунення наявних вразливостей для підвищення стійкості вимагає усвідомлення не лише того, що робить супротивник, але й чому. У зв'язку з цим актуальним стає погляд на світ очима супротивника, щоб визначити стратегічні цілі та шляхи їх досягнення, а також уразливі місця.

Бібліографічні посилання

1. Дубов Д. В. Державна інформаційна політика України в умовах гібридного миру та війни. Стратегічні пріоритети. № 3(40). 2016. С. 86-93.

2. Корнієнко В.О. Державна інформаційна політика в контексті глобальних викликів. Матеріали XLV Науково-технічної конференції ВНТУ, м. Вінниця, 23-24 березня 2016 р.

3. Курбан О. В. Сучасні інформаційні війни в мережевому онлайн просторі: навч. посіб., Київ: ВІКНУ, 2016. 286 с. DOI: https://doi.org/10.28925/2524-2644.2016.2.18.

4. Майстро С.В., Штеба Р.Ю., Хмиров І.М., Тресков А.В., Хмирова А.О., Головко В.В. «Забезпечення національної безпеки як пріоритетний напрям формування та реалізації державної політики сталого розвитку України в умовах існуючих викликів і загроз» :монографія. Х. : НУЦЗУ, 2023. 233 с.

5. UK Government Communication Service. RESIST Counter Disinformation Toolkit. 2019. URL: https://gcs.civilservice.gov.uk/publications/resist-counter-disinformation-toolkit/.

I. Khmyrov, A. Khmyrova, M. Byrnyak

Methodological principles of formation and implementation of state information policy in the conditions of hybrid threats.

Abstract. Hybrid threats are a complex problem of our time, characterized by the use of a wide range of influence tools to achieve the strategic goals of the aggressor while maintaining the possibility of plausible denial of its participation. Today, it is necessary to develop recommendations on improving the regulatory and legal support for information policy in the context of hybrid threats, and developing the institutional capacity of state authorities in the field of information security. Also, develop methodological and conceptual principles for forming a national information security strategy in the context of hybrid threats, which provides for a comprehensive approach to developing information resilience at the individual, organizational, and national levels.

Keywords: state information policy, hybrid threats, information security, strategic communications, public administration, information state, hybridity, information environment.

Зразок для цитування:

Хмиров І., Хмирова А., Бирняк М. Методологічні засади формування та реалізації державної інформаційної політики в умовах гібридних загроз. Пропілеї права та безпеки, 2025. №8. С. 298-300. DOI: https://doi.org/10.32620/pls.2025.8.79.