

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО  
ЗАХИСТУ УКРАЇНИ**

**ДОМБРОВСЬКА С.М.**

**ПОМАЗА-ПОНОМАРЕНКО А.Л.**

**КРЮКОВ О.І.**

**ПОРОКА С.Г.**

***МОНОГРАФІЯ***

**ІНФОРМАЦІЙНІ ЗАГРОЗИ ТА КОМУНІКАТИВНА  
ІНФРАСТРУКТУРА В ДЕРЖАВНОМУ СЕКТОРІ**

Харків – 2024

УДК 351.74 + 342.95

*Монографію розглянуто та рекомендовано до друку Вченою Радою  
Національного університету цивільного захисту України  
Протокол № 8 від 28.03.2024 року*

**Авторський колектив:**

*Домбровська С.М.*, д-р. наук держ. упр., проф. (розділ 1);  
*Крюков О.І.*, д-р. наук держ. упр., проф. (вступ, розділ 2);  
*Помаза-Пономаренко А.Л.*, д-р. наук держ. упр., с.д. (розділ 4, висновки);  
*Порока С.Г.*, доктор філософії (розділ 3).

**Рецензенти:**

*Ажажа Марина Андріївна* доктор наук з державного управління, професор, професор кафедри управління та адміністрування, Запорізький національний університет;

*Мороз Світлана Анатоліївна* доктор наук з державного управління, старший дослідник, провідний науковий співробітник наукового відділу з проблем управління у сфері цивільного захисту, Національний університет цивільного захисту України

**Д23 Домбровська С.М., Помаза-Пономаренко А.Л., Крюков О.І., Порока С.Г. Інформаційні загрози та комунікативна інфраструктура в державному секторі : монографія. Харків: НУЦЗУ, 2024. 244 с.**

У монографії викладено погляди авторів на визначення сутності понять «гібридна війна», «інформаційна безпека», «інформаційно-комунікативна діяльність державного сектору», «токсичний інфопростір» тощо. Досліджено генезис розвитку системи державного управління в умовах інформаційних загроз і гібридної війни в Україні. Особлива увага зосереджена на напрямках удосконалення цієї системи державного управління України в умовах зовнішньої агресії РФ. Крім того, визначено особливості використання РФ зі стратегічною метою відповідної комунікативної інфраструктури під час «невійськової» операції в ЄС. Акцентовано, що ця мета полягає в дестабілізації діяльності державного сектора й унеможливлення формування його інституційної спроможності. Визначено нові інтенції розвитку безпекової політики України в інформаційній сфері. Серед них однією з пріоритетних визнано розробку та прийняття Концепції інформаційної безпеки України з урахуванням напрацьованої позитивної практики стратегування в безпековій сфері держав-членів ЄС. Табл. 1. Іл. 4. Додатків 2. Бібліогр. 225 назв.

УДК 351.74 + 342.95

© С.М. Домбровська, А.Л. Помаза-Пономаренко, О.І. Крюков, С.Г. Порока  
© НУЦЗУ, 2024

**ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ**

ВРУ – Верховна Рада України.

ЄЦПГЗ – Європейський центр з протидії гібридним загрозам.

ЄС – Європейський Союз.

КМУ – Кабінет Міністрів України.

КНР – Китайська Народна Республіка.

ЗМІ – Засоби масової інформації.

ІКТ – Інформаційно-комунікаційні технології.

МВС України – Міністерство внутрішніх справ України.

МЗС України – Міністерство закордонних справ України.

НКО – некомерційні організації.

НУО – неурядові організації.

ООН – Організація Об'єднаних Націй.

ОМС – органи місцевого самоврядування.

ПАРЄ – Парламентська Асамблея Ради Європи.

СБУ – Служба безпеки України.

СУАР – Сіньцзян-Уйгурський автономний район.

США – Сполучені Штати Америки.

ЦОВВ – Центральні органи виконавчої влади.

HRW – Human Rights Watch.

HWRB – Hybrid warfare resistance Bureau.

NIC – National Intelligence Council.

RAND – research and development.

StratCom – Strategic Communications Centre of Excellence.

UCC – United Cyber Caliphate.

**ВСТУП**

*«Інформаційна доба змінила все: і війну, і мир. До нас прийшло майбутнє, до якого ми виявилися не дуже готовими... Світ охопила невизначеність, що постійно зростає, тож ми потребуємо нетрадиційних методів для відновлення впевненості»*

Г. Поцепцов [108, с. 5, 9]

У XXI столітті засоби інформаційної війни почали відігравати значну роль у військових і невійськових конфліктах, та впливати на уряди й населення країн. Цей вплив здійснюється через засоби стратегічної комунікації й інформаційно-комунікативну діяльність державного сектора. Гібридні війни, які розпочала та веде рф є яскравим прикладом цього, адже їхній базис значною мірою становлять дезінформація, пропаганда й ідеологія, що поширюються за допомогою різних технологій і каналів на всіх рівнях управління.

Розв'язана рф гібридна війна на території України засвідчила, наскільки скоординовані дії органів державного сектору загалом і сил правопорядку в економічній сфері, дипломатії, кіберпросторі, інформаційному просторі та соціальній сфері класичними методами ведення війни можуть бути вигідними для держави-агресора. У цьому контексті варто наполягати на важливості вчасного застосування дієвих засобів протистояння та попередження інформаційно-гібридній війні, зокрема неklasичних. Оскільки інформаційний вплив рф спрямований на унеможливлення формування в українського населення власної самоідентичності, а в Україні – її інституційної спроможності та державності.

Після захоплення рф українського Кримського півострова та російської військової агресії на сході України, розпочатої у 2014 році, уся система регіональної та глобальної безпеки була деформована – усі міжнародні гарантії України, включно з тими, що містяться в Будапештському меморандумі від

05 грудня 1994 року, підписаному між Україною, США, росією та Великою Британією, виявилися неактуальними, оскільки агресором виступала російська федерація – держава-гарант, а також постійний член Ради Безпеки ООН. Безперечно, агресія рф проти України не залишилася непоміченою як у світі, так і в самій рф, тому держава-агресор безпрецедентно використала всі можливі інструменти інформаційної війни, застосовуючи пропаганду та дезінформацію, стратегічні канали комунікації та інші елементи комунікативної інфраструктури для виправдання протиправної агресії. Такі ж канали і методи стратегічного зв'язку росія використовувала в інших військових, військово-політичних та інших конфліктах, як із військовим, так і з невійськовим елементом.

Вкладаючи значні кошти в інформаційну війну, яка є невід'ємною частиною гібридної війни, російська влада переслідує свої політичні та військові інтереси, використовуючи стратегічні комунікації та відповідну інфраструктуру як зброю проти України та інших країн. Завдяки засобам стратегічної комунікації ця російська влада спотворює існуючу реальність і створює свою – паралельну.

Отже, актуальність цього дослідження зумовлена постійно зростаючою роллю інформації для суспільства та системи публічного управління, що включає державний сектор. У сучасних умовах цифрового простору інформація та відповідні комунікації набули комплексного характеру, передбачаючи їхній вплив на виникнення, ведення та характер війн нового типу – інформаційно-гібридних. Зважаючи на це, увага до забезпечення державним сектором безпековості інформаційного простору набуває все більш важливого значення для національної безпеки загалом і для інституційної системи України. Ці зміни знайшли відповідний практико орієнтований відгук на найвищому рівні, зокрема, у межах указу Президента України від 25.02.2017 р. № 47/2017, що затвердив Доктрину інформаційної безпеки. Цей правовий документ передбачає створення єдиної системи забезпечення контролю та безпеки, а також протидії загрозам на всіх рівнях управління. Розробці цієї доктрини передувало

схвалення Стратегії розвитку інформаційного суспільства в Україні (розпорядження Уряду України від 15.05.2013 р. № 386-р). Така стратегія передбачала гарантування законності та розумної достатності при зборі, накопиченні та поширенні інформації про громадян й організацій, а також забезпечення державного захисту інтересів українських громадян в інформаційній сфері. Однак дана стратегія так і не була зреалізована повною мірою, як і Стратегія інформаційної безпеки, затверджена указом Президента України № 685/2021 [96].

У той же час, наукове осмислення як самого феномену гібридної війни, так і його впливу на всі аспекти життєдіяльності соціуму та функціонування інституційної системи публічного управління за умов цієї війни продовжує змінюватися, набуваючи ознак парадигмальності. Відзначимо, що теоретичні основи визначення інформаційної війни були закладені на початку ХХ ст., а з 2000-х років розпочався новий етап її дослідження – через сутнісні зміни цього феномену в умовах сучасних локальних конфліктів, а також трансформації світових війн у гібридні. Дане ж дослідження передбачає, що через збільшення викликів і загроз, зумовлених цими змінами, інституційна система публічного управління потребує розвитку з урахуванням появи нових концепцій і стратегій ведення глобальних інформаційно-гібридних війн.

Таким чином, сучасне положення міжнародної безпеки є нестабільним, що зумовлює збільшення кількості конфліктів і зміну підходів до ведення війни нетрадиційними засобами. Останніми роками Україна та її населення змушені відчувати на собі всі ці зміни, а також інформаційні загрози. Тому одним із найбільш важливих завдань для нашої держави є створення дієвої інституційної системи публічного управління, із визначенням координуючого суб'єкта в межах державного сектора. Гарантування безпеки для населення – це підтримка на належному рівні безпеки, яка виходить від нього. Такий рівень відображає стан задоволення соціальних інтересів, і тому важливо забезпечувати безпечний розвиток інформаційного суспільства. Зважаючи на це, актуальним є визначення теоретичних й організаційно-правових засад дієвого

функціонування державного сектора із використанням комунікативної інфраструктури в умовах інформаційних загроз і гібридної війни.

У монографії досліджено питання формування та функціонування інституційної системи державного управління України в умовах інформаційних загроз і гібридних війн. Це можливо зrealізувати за допомогою дослідження особливостей застосування комунікативної інфраструктури й інструментарію «м'якої сили». У монографії визначено механізми реагування на інформаційні загрози, упровадження яких (механізмів) державним сектором дозволяє унеможливити трансформацію цих загроз у базис, необхідний для виникнення та поширення гібридних війн. Рекомендовано закріпити ці механізми в Концепції інформаційної безпеки України, її (концепції) положення наведені в даній монографії, що, у свою чергу, визначає оригінальність і наукову новизну проведеного дослідження.

Теоретичні положення монографії застосовані під час проведення лекцій і практичних занять із навчальних дисциплін «Інформаційна політика в Україні» і «Сучасні геополітичні процеси: світ і Україна» за програмою підготовки здобувачів вищої освіти за другим рівнем вищої освіти (магістерським) у Національному університеті цивільного захисту України (акт 22-27 від 28.11.2023 р.).

Монографія складається із вступу, 4 розділів, загальних висновків, додатків, а також списку використаних джерел. Вона буде корисною для наукових і науково-педагогічних працівників, здобувачів вищої освіти, а також практичних працівників-фахівців, які досліджують питання формування та реалізації безпекової політики за кордоном і в Україні.

## ЗМІСТ

<b>ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ</b>	<b>3</b>
<b>ВСТУП</b>	<b>4</b>
<b>РОЗДІЛ I. ТЕОРЕТИЧНІ ЗАСАДИ СОЦІОГУМАНІТАРНИХ І КОМУТАТИВНИХ ТЕХНОЛОГІЙ СУЧАСНИХ ІНФОРМАЦІЙНО-ГІБРИДНИХ ВІЙН У СИСТЕМІ ДЕРЖАВНОГО УПРАВЛІННЯ</b>	<b>8</b>
1.1. Феномен інформаційно-гібридної війни як інструмент протиборства в системі державного управління	8
1.2. Структурно-функціональний і комунікативний механізми виникнення інформаційних війн у глобалізованому світі	20
1.3. Механізми формування інформаційної реальності як чинник забезпечення національної безпеки	34
<b>РОЗДІЛ II. АНАЛІЗ СУЧАСНОГО СТАНУ ФУНКЦІОНУВАННЯ МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ В УМОВАХ ІНФОРМАЦІЙНИХ ЗАГРОЗ І ГІБРИДНИХ ВІЙН</b>	<b>47</b>
2.1. Особливості функціонування механізмів державного управління в Україні в умовах інформаційних загроз і гібридної війни	47
2.2. Концепція інформаційно-гібридної війни: загрози для державного сектору та суспільства	64
2.3. Комунікативна інфраструктура й інструменти дисфункціоналізації державного управління в умовах інформаційно-гібридної війни	79
<b>РОЗДІЛ III. НАПРЯМИ ВДОСКОНАЛЕННЯ МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ В УМОВАХ ІНФОРМАЦІЙНИХ ЗАГРОЗ І ГІБРИДНИХ ВІЙН</b>	<b>99</b>



3.1. Ризик-орієнтовані підходи до забезпечення розвитку комунікативної інфраструктури в державному секторі в умовах інформаційних загроз	99
3.2. Шляхи вдосконалення системи державного управління України в умовах інформаційних загроз і гібридних війн	115
3.3. Прогнозування інформаційних загроз у контексті вдосконалення механізмів державного управління	136
<b>РОЗДІЛ IV. РОЛЬ СТРАТЕГІЧНОЇ КОМУНІКАЦІЇ В ЗАХИСТІ НАЦІОНАЛЬНИХ ІНТЕРЕСІВ ЄС Й УКРАЇНИ</b>	<b>153</b>
4.1. Особливості використання стратегічної комунікації рф під час невійськових операцій у світі	153
4.2. Стратегічні комунікації як зброя рф проти України в гібридній війні	164
4.3. Відбудова стратегічної комунікації в Україні	173
4.4. Вплив інформаційних загроз на ментальне здоров'я населення та шляхи протистояння ним	186
4.5. Віртуальний та інформаційний щити України – засоби унеможливлення формування «вчорашнього» майбутнього	196
<b>ВИСНОВКИ</b>	<b>208</b>
<b>СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ</b>	<b>214</b>
<b>ДОДАТКИ</b>	<b>238</b>

*Наукове видання*

**ДОМБРОВСЬКА Світлана Миколаївна**

**ПОМАЗА-ПОНОМАРЕНКО Аліна Леонідівна**

**КРЮКОВ Олексій Ігорович**

**ПОРОКА Станіслав Григорович**

**ІНФОРМАЦІЙНІ ЗАГРОЗИ ТА КОМУНІКАТИВНА  
ІНФРАСТРУКТУРА В ДЕРЖАВНОМУ СЕКТОРІ**

**М о н о г р а ф і я**

Формат 60x84/16. Папір офсетний. Друк цифровий.

Гарнітура Times New Roman.

Підписано до друку 29.03.2024 р.

Наклад 100. Умовн. друк. арк. 10.

Надруковано в друкарні ФО-П Дуюнова Т.В.

Свідоцтво про державну реєстрацію № 2475418720 від 19.11.2014 р.

61023, м. Харків, вул. Весніна, 12, тел. (057) 717-28-80