НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

НОВІКОВ Владислав Олександрович

УДК 351.74+342.95

ІНСТИТУЦІЙНІ МЕХАНІЗМИ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ІНФОРМАЦІЙНО-ГІБРИДНИХ ВІЙН

25.00.05 – державне управління у сфері державної безпеки
та охорони громадського порядку

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата наук з державного управління

Харків –2024

Дисертацією є рукопис.

Робота виконана в Національному університеті цивільного захисту України.

Науковий керівник: доктор наук з державного управління, старший дослідник,
ПОМАЗА-ПОНОМАРЕНКО Аліна Леонідівна,
Національний університет цивільного захисту України, начальник наукового відділу проблем державної безпеки навчально-науково-виробничого центру.

Офіційні опоненти: доктор наук з державного управління, доцент
БОНДАРЕНКО Олександр Геннадійович,
Національна академія Національної гвардії України, начальник кафедри державної безпеки та оперативного мистецтва оперативного факультету;

доктор наук з державного управління, професор
ЩЕПАНСЬКИЙ Едуард Валерійович,
Хмельницький університет управління та права імені Леоніда Юзькова, завідувач кафедри публічного управління та адміністрування.

Захист відбудеться «15» березня 2024 р. о 14.00 годині на засіданні спеціалізованої вченої ради Д 64.707.03 Національного університету цивільного захисту України за адресою: 61024, м. Харків, вул. Лермонтовська, 28, зал засідань (1-й поверх).

З дисертацією можна ознайомитись у бібліотеці Національного університету цивільного захисту України за адресою: 61023, м. Харків, вул. Чернишевська, 94.

Автореферат розісланий «15» лютого 2024 р.

Учений секретар
спеціалізованої вченої ради С.А. Мороз

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Актуальність дослідження обумовлена постійно зростаючою роллю інформації для суспільства та системи публічного управління. У сучасних умовах цифрового простору інформація та відповідні комунікації набули комплексного характеру, передбачаючи їх вплив на виникнення, ведення та характер війн нового типу – інформаційно-гібридних. Зважаючи на це, увага до забезпечення 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.

У той же час, наукове осмислення як самого феномену інформаційно-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 XX 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.

Отже, 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 інформаційно-гібридні загрози. Тому одним із найбільш важливих завдань для нашої держави є створення дієвої інституційної системи публічного управління, із визначенням координуючого суб’єкта. 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 інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни.

Питання дослідження змісту системи публічного управління та вплив її на

національну й інформаційну безпеку неодноразово порушувались у працях зарубіжних і вітчизняних науковців У. Бека, С. Бєлая, З. Бжезінського, О. Бондаренка, У. Вакко, Т. Воропаєвої, А. Гідденса, В. Горбуліна, М. Девідсона, Д. Деннінг, О. Довганя, С. Домбровської, А. Едельштайн, І. Кекіш, А. Кларк, О. Копанчук, О. Кравчука, О. Крюкова, Є. Магди, Ф. Майлза, О. Машкова, О. Мережко, Дж. Найа, Н. Нижник, Г. Ортіної, О. Пархоменко-Куцевіл, А. Помази-Пономаренко, Г. Почепцова, О. Радченка, І. Рущенко, Г. Ситника, В. Скуратівського, В. Торічного, Е. Тоффлера, Ф. Хоффмана, Е. Щепанського, Т. Ярового та ін. В аналізованих наукових працях основна увага зосереджена на організаційних, правових, економічних, ресурсних та інших аспектах державної політики у сфері національної безпеки загалом й інформаційної зокрема.

У той же час, вимагають комплексного відображення питання формування та функціонування інституційної системи публічного управління України в умовах інформаційно-гібридних війн. Це можливо зреалізувати за допомогою дослідження інструментарію «м'якої сили» і «жорсткої сили», виважене та вчасне реагування на які дозволяє унеможливити трансформацію інформаційних загроз у базис для виникнення та поширення інформаційно-гібридної війни. Отже, потреба у теоретичному, методичному та практико орієнтованому вирішенні окреслених завдань підтверджує актуальність дисертаційної роботи, її важливість, наукову новизну, зумовлює мету, завдання, предмет й об'єкт дослідження, а також апробацію та практичне впровадження.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження проведено в межах науково-дослідних робіт, які виконувались Національним університетом цивільного захисту України, а саме: за темою «Розробка наукових основ державного управління у сфері безпеки ринку соціально-економічних послуг України з точки зору цивільного захисту» (ДР № 0115U002035), у межах якої здобувачем визначено формування інституційних механізмів публічного управління невизначеностями в умовах інформаційно-гібридних війн.

Мета та завдання дослідження. *Метою* дисертаційної роботи є визначення науково-теоретичних засад формування інституційних механізмів публічного управління в умовах інформаційно-гібридних війн і розроблення практичних рекомендацій щодо вдосконалення таких механізмів в Україні.

Зважаючи на поставлену мету дисертаційного дослідження, визначено такі науково-теоретичні та практико орієнтовані *завдання*:

– узагальнити теоретичні засади інформаційно-гібридних війн як інструменту соціогуманітарного протиборства в системі публічного управління;

– дослідити особливості функціонування структурно-функціонального механізму виникнення інформаційних війн та механізми формування інформаційних технологій в умовах інформаційно-гібридних війн;

– структуризувати інституційні механізми публічного управління України в умовах інформаційно-гібридної війни;

– охарактеризувати особливості та ризики функціонування інституційних

механізмів публічного управління України в умовах інформаційно-гібридної війни;

– проаналізувати інструменти дисфукнціоналізації інституційних механізмів публічного управління в умовах інформаційно-гібридної війни;

– обґрунтувати ризик-орієнтовані підходи до вдосконалення інституційної системи публічного управління України в умовах інформаційно-гібридної війни;

– запропонувати шляхи розвитку інституційної системи публічного управління України в умовах інформаційно-гібридних війн;

– визначити концептуальні засади прогнозування інформаційно-гібридних війн у контексті розвитку інституційних механізмів публічного управління.

Об'єкт дослідження – публічне управління у сфері забезпечення інформаційної безпеки.

Предмет дослідження – інституційні механізми публічного управління в умовах інформаційно-гібридних війн.

Методи дослідження. Методологічну основою дисертаційного дослідження становить сукупність способів наукового пізнання та загальнонаукових принципів проведення дослідження, що враховують фундаментальні положення й праці вчених щодо аспектів публічного врядування й адміністрування, інституціоналізму, конфліктології тощо.

Дисертаційне дослідження побудовано на *концептуальному, системному, синергетичному й інституціональному підходах*, а також сукупності методів, а саме:

– *логічного узагальнення, синтезу й абстрагування* (під час розкриття сутності феномену інформаційно-гібридної війни як інструмент соціогуманітарного протиборства в системі публічного управління);

– *теоретизування й історичної формалізації* (для визначення механізмів формування інформаційної реальності як чинника забезпечення безпеки);

– *системного аналізу, порівняння, вибірки й опису* (з метою дослідження особливостей і ризиків функціонування інституційних механізмів публічного управління в Україні в умовах інформаційно-гібридної війни);

– *індукції та дедукції* (під час визначення концептуальних засад формування інституційних механізмів публічного управління невизначеностями в умовах інформаційно-гібридних війн);

– *групування та прогнозування* (з метою обґрунтування шляхів удосконалення інституційної системи публічного управління України в умовах інформаційно-гібридних війн).

Інформаційно-фактологічною базою дослідження є закони України, укази Президента України, нормативні акти Кабінету Міністрів України, статистична інформація Державної служби статистики України тощо.

Наукова новизна одержаних результатів полягає у визначенні науково-теоретичних засад формування інституційних механізмів публічного управління в умовах інформаційно-гібридних війн і розробленні практичних рекомендацій щодо вдосконалення таких механізмів в Україні.

Наукова новизна результатів конкретизується в таких положеннях:

уперше:

– запропоновано шляхи розвитку інституційної системи публічного управління України в умовах інформаційно-гібридної війни, серед яких основними визнано, зокрема, створення єдиного координаційно-аналітичного центру/ради в Україні, на зразок американського Бюро протидії гібридній війні, яке напрацювало дієві управлінські практики реагування на інформаційні загрози, а також налагодження результативної взаємодії України з іншими державами та міжнародними організаціями в напрямку вчасного протистояння цим загрозам;

удосконалено:

– визначення головної небезпеки інформаційно-гібридної війни як потенційної можливості цільового інформаційного впливу, зокрема негативного, на об'єктивно закладені та наявні суперечності практично на всіх рівнях державного та суспільного устрою в будь-якій країні чи регіоні, з метою примусового прояву цього впливу із заданим рівнем інтенсивності та в завідомо окресленому напрямку;

– ризик-орієнтовані підходи до забезпечення розвитку інституційної системи публічного управління України в умовах інформаційно-гібридної війни, що (підходи) дозволили обґрунтувати сценарії реагування на ці війни – проактивний сценарій, який рекомендовано реалізовувати під час стратегічного планування та поступального забезпечення сталого розвитку, і реактивний сценарій, що передбачає оперативне реагування на інформаційні загрози, зокрема, у межах уточненої концепції протидії ним;

– концептуальні засади щодо прогнозування інформаційно-гібридних війн у контексті розвитку інституційних механізмів публічного управління на пострадянському і вітчизняному просторі, на які впливають зовнішні та внутрішні фактори, серед яких найбільш загрозливими на сучасному етапі визнано соціальні, пов'язані з рівнем міграції громадян, їхнього добробуту, безробіття, демографічного розвитку та ін.;

дістало подальшого розвитку:

– визначення асиметрії як основоположної властивості інформаційно-гібридних війн, що відзначається латентністю та спрямованістю на найбільш вразливі місця в інформаційній обороні противника, наслідки недосконалості якої порівнянні із застосуванням нетрадиційної зброї, покликаної значно зменшити витрати на використання традиційної зброї й отримати інформаційну перевагу над противником;

– структуризація інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни, яка (структуризація) дозволила: 1) виокремити в складі цих механізмів організаційний, правовий і структурно-функціональний, які приводить у рух відповідна суб'єктна підсистема; 2) уточнити визначення поняття інформаційної безпеки як об'єкту державного впливу; 3) обґрунтувати шляхи підвищення результативності функціонування цих підсистем із наведенням конкретних нормотворчих пропозицій щодо усунення дублювання функцій органів державної влади у сфері інформаційної безпеки;

– визначення ризиків функціонування інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни, унеможливлення трансформації яких (ризиків) у небезпеки інформаційного характеру рекомендовано здійснювати шляхом: протидії поширенню неправдивої та видозміненої інформації з боку країни-агресора, що впливає на розвиток українського суспільства й держави; формування цілісної інформаційної концепції й стратегії поширення об'єктивної інформації та протидії загрозам інформаційного характеру; підвищення рівня медіа-культури суспільства та його цифровізованого розвитку тощо;

– класифікація інструментів дисфукнціоналізації інституційних механізмів публічного управління в умовах інформаційно-гібридної війни, серед яких технологіям «м'якої сили» відведено особливе місце, тому що вони передбачають здійснення щодо держави-об'єкта (держави-мішені) неоголошеної гібридної війни з боку держави-актора, нейтралізувати негативний інформаційний вплив якої рекомендовано із застосуванням ризик-орієнтованих підходів, напрацьованих за кордоном.

Практичне значення одержаних результатів полягає в можливості їхнього застосування в діяльності органів публічної влади, що сприятиме підвищенню результативності інституційної реалізації публічного управління у сфері національної й інформаційної безпеки України.

Пропозиції щодо застосування ризик-орієнтованих підходів до забезпечення розвитку інституційної системи публічного управління України в умовах інформаційно-гібридної війни використані в організаційно-аналітичній роботі Управління Служби безпеки України в Харківській області (довідка № 70/4-8859-1 від 14.11.2022 р.) і Черкаської районної ради (довідка № 10/01-13 від 06.02.2024 р.).

Крім того, пропозиції дисертації щодо концептуальних засад прогнозування інформаційно-гібридних війн на пострадянському та вітчизняному просторі використовувалися в навчальному процесі Національного університету цивільного захисту України, зокрема, при викладанні здобувачам вищої освіти другого (магістерського) рівня вищої освіти (спеціальність 281 «Публічне управління та адміністрування») таких дисциплін, як «Інформаційна політика в Україні» і «Сучасні геополітичні процеси: світ і Україна» (акт № 22-20 від 28.11.2023 р.).

Особистий внесок здобувача. Дисертація є самостійною науковою працею, теоретичні та прикладні результати якої отримано особисто здобувачем. Конкретний внесок здобувача в наукових працях, підготовлених у співавторстві, зазначений у списку опублікованих праць за темою дисертації [6].

Апробація результатів дисертації. Основні теоретичні положення та висновки дисертації були апробовані на міжнародних і всеукраїнських науково-практичних конференціях, зокрема, тези було опубліковано за результатами: Всеукраїнської науково-практичної конференції «Публічне управління в системі координат: демократія, децентралізація, місцеве самоврядування» (м. Мелітополь, 2019 р.); I Міжнародної науково-практичної «Modern research in science and education» (м. Київ, 2023 р.); XXXII Міжнародної наукової

конференції здобувачів вищої освіти і молодих учених «Наука і вища освіта» (м. Запоріжжя, 2023 р.), Всеукраїнської науково-практичної конференції «Національна безпека в умовах війни, післявоєнної відбудови та глобальних викликів XXI століття» (м. Житомир, 2023 р.).

Публікації. Основні положення дисертаційної роботи опубліковано у 11 наукових працях, із них: 6 статей у вітчизняних наукових фахових виданнях, включених до категорії Б; 1 стаття у закордонному науковому виданні за напрямком дослідження; 4 тез доповідей на конференціях. Загальний обсяг публікацій автора відповідно до теми дослідження становить 4,86 друк. арк.

Структура дисертації. Дисертація складається зі вступу, трьох розділів, висновків, списку використаних джерел (225 найменувань на 24 стор.) і 5 додатків. Загальний обсяг роботи становить 218 стор., із них 186 стор. – це основний текст. Дисертація містить 4 рисунки і 1 таблицю.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми дослідження, визначено стан її наукової розробленості, з'ясовано зв'язок із науковими програмами, планами, темами, визначено мету, завдання, об'єкт, предмет і методи дослідження, розкрито наукову новизну та практичне значення одержаних результатів, наведено відомості про їхню апробацію й оприлюднення.

У першому розділі – «*Теоретичні засади соціогуманітарних технологій сучасних інформаційно-гібридних війн у системі публічного управління*» – досліджено феномен інформаційно-гібридної війни як інструменту соціогуманітарного протиборства в системі публічного управління, визначено особливості структурно-функціонального механізму виникнення інформаційних війн у глобалізованому світі, а також механізм формування інформаційної реальності як чинника забезпечення національної безпеки.

Обґрунтовано, що інформаційно-гібридна війна – це вища форма міждержавного інформаційного протистояння, що передбачає виникнення конфлікту інтересів суб'єктів геополітичної/геоекономічної конкуренції (протиборства) в інформаційному просторі з метою вирішення протиріч щодо влади та здійснення політичного керівництва, а також щодо перерозподілу їх ролі, місця та функцій у політико-управлінській системі сучасного суспільства, в якому зіткнення конфліктуючих сторін відбувається у формі інформаційних та інформаційно-психологічних операцій із застосуванням інформаційної зброї.

Визначено, що сутність інформаційно-гібридної війни полягає в нанесенні військової поразки противнику шляхом досягнення та використання інформаційної переваги над ним.

При цьому наголошено, що інформаційно-гібридна війна може здійснюватися й в умовах відсутності силового конфлікту. Даний факт дозволяє віднести цей різновид війни до числа найбільш поширених, популярних та універсальних засобів щодо забезпечення реалізації зовнішніх (геополітичних/геоекономічних) інтересів. Акцентовано, що за відносно мирних умов інформаційно-гібридні війни цього типу можуть передбачати

застосування як спеціальних механізмів управління кризами, так і провокування вчинення правопорушень на території противника. Уважаємо, що ця обставина визначає асиметричний характер інформаційно-гібридних війн, але не унеможливлює наявності потенційних можливостей у країни-мішені щодо протистояння цілеспрямованими точковими ударами держави-актора шляхом нанесення шкоди менш технологічно розвиненому противнику.

Акцентовано, що в постіндустріальному і очевидно постмодерному інформаційному світі, який формується, найважливішим ресурсом виявляється не традиційний географічний простір із закріпленими в ньому фізичними людьми та виробничими потужностями, а інтелект, інформація та пов'язаним із нею фінансовим, матеріально-технічним та іншим забезпеченням. Відтак, за допомогою високо розвинених технологій інформація, що містить дані про результати інтелектуальної діяльності, оперативно та безперешкодно переміщується в просторі – цифровому й інституційному. Виявлено, що відсутність територіальної «прив'язки» ключових ресурсів до цифрового простору дозволяє країнам-лідерам в інформаційно-комунікаційному середовищі використовувати їх у своїх цілях без будь-якого фізичної сили. Щодо інституційного простору, представленого органами публічного управління, то обстоюється позиція, що він, по-перше, відзначається територіальною «прив'язкою» ключових ресурсів. А по-друге, не може бути абсолютно убезпеченим від застосування проти нього фізичної, кінетичної та іншої сили, для посилення ефекту дії якої може паралельно використовуватися не традиційна зброя (інформаційна).

Отже, ефективне освоєння чужих територій у межах інформаційно-гібридних війн стає можливим без значного застосування кадрового потенціалу країни-актора. Однак у цьому контексті необхідним є врахування рівня добробуту основної частини населення країни-актора, а також держави-мішені (держави-об'єкта), що освоюється для досягнення поставлених цілей шляхом використання інформаційно-технологічної локалізації та фактичного вилучення із соціально-економічного простору носіїв інтелекту та розпорядників фінансових ресурсів. Без належного врахування таких аспектів інформаційно-гібридних війн не можна розраховувати на її успішну реалізацію.

У другому розділі – *«Аналіз сучасного стану функціонування інституційних механізмів публічного управління в умовах інформаційно-гібридних війн»* – визначено особливості та ризики функціонування інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни, проаналізовано сучасну концепцію інформаційно-гібридної війни, а також інструменти дисфукнціоналізації інституційних механізмів публічного управління в умовах такої війни.

Досліджено особливості та ризики функціонування інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни, яка ведеться проти нашої держави. Це здійснено крізь призму визначення ролі суб'єктів державної політики у сфері національної й інформаційної безпеки (рис. 1). Виявлено, що серед науковців публічного

управління відсутній єдиний підхід до групування суб'єктів державної політики у цій сфері. Тому систематизовано класифікацію суб'єктів державної політики у сфері національної й інформаційної безпеки: 1) зважаючи на рівень формування та реалізації державної політики (державні суб'єкти різних рівнів та недержавні); 2) зважаючи на функціональне навантаження та спектр повноважень (суб'єкти, що виконують дослідницько-інформаційні, організуючі та координуючі функції); 3) залежно від статусу суб'єктів (органи публічної влади, що включають державні інституції та організації недержавного сектору, які залучаються до формування державної політики).

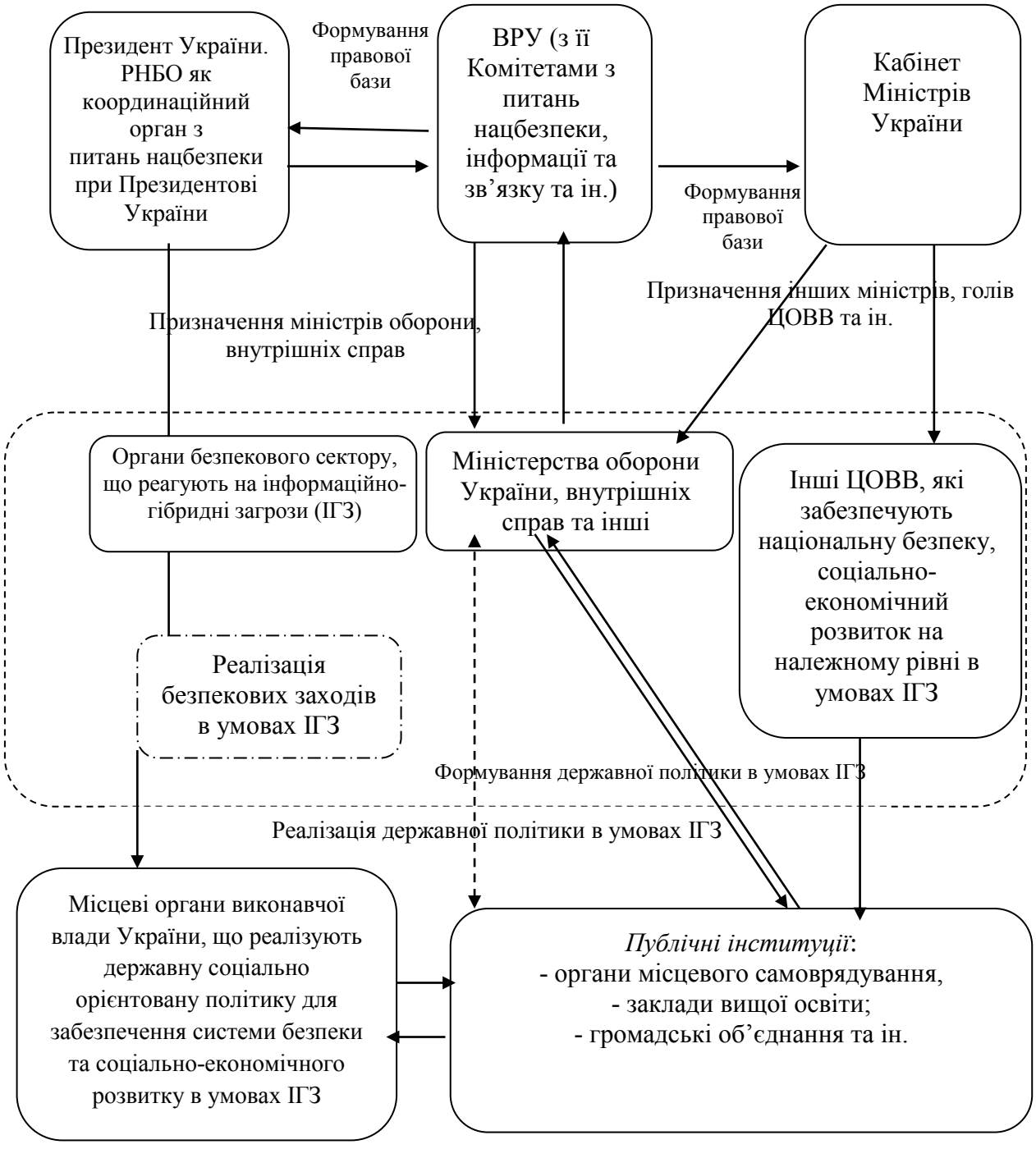

Рис. 1. Особливості функціонування інституційних механізмів публічного управління в умовах інформаційно-гібридних загроз і війн в Україні

З’ясовано, що суб’єктів державної політики у сфері національної й інформаційної безпеки, на яку деструктивно впливає інформаційно-гібридна війна, можна розділити на дві основні категорії: 1) органи державної влади України (різних рівнів управління та сфер суспільної життєдіяльності, на які це управління спрямоване, органи місцевого самоврядування та ін.); 2) суб’єкти, що функціонують поза системою публічного управління: підприємства та організації різних форм власності і господарювання, громадські об’єднання, асоціації та інші організації громадянського суспільства.

Аналіз наукових напрацювань у межах обраної проблематики дав підстави стверджувати про виокремлення у структурі інституційних механізмів публічного управління в умовах інформаційно-гібридної війни організаційної та правової підсистем. Дана гіпотеза висловлена, з одного боку, з огляду на роль правових і соціальних інститутів у забезпеченні належного функціонування всіх сфер суспільної життєдіяльності. А з другого – зважаючи на місце інституцій як органів публічної влади у такому забезпеченні. З’ясовано, в умовах інформаційно-гібридної війни визначальне місце серед таких інституцій займають *координуючі суб’єкти публічного управління*, що формують і реалізують державну політику у сфері національної й інформаційної безпеки. У цьому контексті акцентується, зокрема, на функціях і повноваженнях Ради національної безпеки і оборони України, її апарату та профільного комітету, що здійснюють таке: 1) моніторинг та дослідження рівня інформаційних загроз; 2) вивчення стану та результативності реалізації стратегій і програм щодо гарантування національної й інформаційної безпеки; 3) підвищення її рівня; 4) надають пропозиції щодо нейтралізації інформаційних загроз, кіберзагроз тощо.

Установлено, що РНБО України безпосередньо взаємодіє з Президентом і Парламентом України, його Комітетами з питань національної безпеки, інформації та зв’язку. Ця взаємодія відбувається в межах наданих пропозиції щодо внесення законодавчих змін у сферах: електронного обігу, телекомунікацій, розвитку інформаційного суспільства, національної програми інформатизації, захисту системи електронних інформаційних ресурсів тощо. Крім того, наголошується на особливій ролі інших спеціалізованих органів: СБУ, Нацполіції, Державної служби спеціального зв’язку та захисту інформації України тощо. Зважаючи на правову диференціацію у визначенні суб’єктного складу підсистем, що покликані гарантувати та підтримувати систему безпеки України в умовах інформаційно-гібридної війни, запропоновано внести зміни до чинного правового поля з метою усунення такої диференціації. Рекомендується узгодити між собою положення Закону України «Про національну безпеку України», Доктрини інформаційної безпеки України та Закону України «Про основні засади забезпечення кібербезпеки України».

Доведено, що інформаційна безпека України представляє собою сукупність суб’єктно-об’єктних взаємовідносин, що виникають між суб’єктами інформаційного середовища (простору), які здійснюють цілеспрямований, організуючий вплив на різні сфери суспільної життєдіяльності загалом і на об’єкти інформаційної інфраструктури зокрема, що відбувається за допомогою

комплексу правових, організаційних, інформаційних, економічних та інших заходів (під час формування й оновлення правової бази, удосконалення структури та/або форм діяльності органів публічної влади, стратегічних, урядових і кризових комунікацій тощо) з метою унеможливлення трансформації ризиків і загроз інформаційного характеру у небезпеки та війни. Запропоноване визначення поняття «інформаційна безпека» передбачає застосування системного підходу до формування інституційної системи публічного управління в умовах інформаційно-гібридної війни. Ключовим завдання такої системи визнано нейтралізацію негативного впливу інформаційно-психологічної війни, пропаганди щодо нівелювання української мови та культури, унеможливлення формування російськими ЗМІ альтернативної інформаційної дійсності шляхом викривленої справжньої картини світу, підвищення позитивного іміджу України на міжнародній арені.

Дослідження особливостей сучасної концепції інформаційно-гібридної війни дозволило визначити таке: ця концепція не набула ще єдиної загально визнаної характеристики ні в теоретичній, ні в практичній площинах. З’ясовано, що на доктринальному рівні новації у методах визначення нетрадиційної війни пов'язані зі зміною спектру інформаційних загроз та акторів конфлікту, що формують ту якість, яка робить війну вже не просто іррегулярною, а інформаційно-гібридною. Іще однією особливістю інформаційно-гібридних війн визнано їхній тривалий характер, який вимагає превентивної та тривалої політики протидії, організованої на державному рівні. Однак на рівні планування та проведення операцій ключовими залишаються учасники, методи та засоби нетрадиційної війни, що зайвий раз говорить про те, що концепція інформаційно-гібридної війни поки знаходиться на стадії становлення. Відтак, спосіб протидії США інформаційно-гібридним загрозам з боку рф, Ірану та Китаю дослідники пропонують називати «протидією нетрадиційним війнам». З урахуванням того, що інформаційно-гібридні загрози мають складну природу виникнення та відзначаються масштабністю та довготривалістю, можна спрогнозувати, що через кілька десятиліть доктрина протидії нетрадиційним війнам суттєво видозміниться.

Крім того, пропонується застосовувати синергетичний та інституційний підходи до характеристики поняття «інформаційно-гібридна війна». Ці підходи дозволили встановити, що ризики в системі публічного управління чинять істотний вплив на всі сфери суспільної життєдіяльності. На цій підставі рекомендовано розглядати ризик-орієнтоване публічне управління як підвид інституційного публічного управління, що реалізується системою органів державної влади та недержавним сектором у напрямку системної інтеграції (імплементації) концептів, стратегій і механізмів стратегічного та поточного прогностичного оцінювання існуючих ризиків і загроз інформаційного характеру.

Порівняльний аналіз досвіду Казахстану, США, України та Франції щодо оцінювання таких ризиків у публічному управлінні дав змогу наполягати на:

1) важливості впровадження нових ризик-орієнтованих підходів у систему публічного управління України, що, по-перше, відбувається на рівні

формування та реалізації державної політики, а, по-друге, повинно відображатися в ключових правових документах стратегічного планування (у т.ч. у рамках побудови так званої «нової моделі» публічного управління);

2) актуалізації питань управління ризиками інформаційного характеру через їхню трансформацію в загрози, що становлять у подальшому базис для виникнення та поширення інформаційно-гібридних війн;

3) постійній реалізації заходів попередження, прогнозування, реагування на вплив інформаційних загроз. Для цього має функціонувати диверсифікована система профільних органів, що реалізують науково-обґрунтоване профільне ризик-орієнтоване публічне управління в конкретних сферах суспільних відносин, за наявності також і централізованої структури, що оцінює якість реалізації ризик-орієнтованого публічного управління в масштабах усієї держави. Зважаючи на положення чинного законодавства України щодо національної безпеки, акцентується на особливі ролі спеціалізованих органів, покликаних гарантувати таку безпеку в умовах впливу інформаційних загроз. Завданням таких інституцій є гарантування інформаційної безпеки України й унеможливлення трансформації інформаційних загроз у небезпеки та війни;

4) проектуванні інструментів ризик-орієнтованого публічного управління України в умовах інформаційно-гібридної війни з урахуванням позитивно верифікованої багаторічної закордонної практики реагування на інструменти «м'якої сили».

Визнано, що інструменти «м'якої сили» представляють собою сукупність інституційних, проектно-ідеологічних, міжнародно-правових, організаційних, фінансових, інформаційно-пропагандистських, розвідувальних та інших механізмів проектування, алгоритмізації, реалізації, забезпечення та контролю процесів дисфункціоналізації, дискредитації або тотальної руйнації іншої суверенної держави (держави-об'єкта) із метою трансформації цієї держави в неспроможну, що веде до повного її знищення або примусової її трансформації у субмісивні форми з редукованим або повністю втраченим суверенітетом, а також для досягнення інших цілей на користь держави-актора. Застосування «м'якої сили» завжди передбачає агресивні дії противника, але не навжди фізичну, кінетичну та іншу зброю. Отже, актуальним завданням для України є визначення заходів із випередження та припинення впливу противника (держави-актора). Ці заходи передбачають захист від очікуваних і не прогнозованих агресивних дій із боку держави-актора. На цій підставі застосування інструментів «м'якої сили» обґрунтовано може інтерпретуватися як здійснення щодо держави-об'єкта (держави-мішені) неоголошеної інформаційно-гібридної війни, як-то відбувається по відношенню до України.

У третьому розділі – «*Напрями вдосконалення інституційних механізмів публічного управління в умовах інформаційно-гібридних війн*» – обґрунтовано ризик-орієнтовані підходи до забезпечення розвитку інституційної системи публічного управління в умовах інформаційно-гібридних війн, запропоновано шляхи вдосконалення інституційної системи публічного управління України в умовах інформаційно-гібридних війн, а також визначено концептуальні засади прогнозування інформаційно-гібридних війн у контексті розвитку

інституційних механізмів публічного управління.

Доведено, що значна частина традиційних війн і військових конфліктів, які відбуваються у світі, сьогодні набули гібридного характеру, передбачаючи вплив інформаційних загроз. Дослідження міжнародного та вітчизняного законодавства дає підстави стверджувати, що в ньому слід закріпити визначення поняття «інформаційно-гібридна війна». Крім того, уважаємо, що розвиток вітчизняного законодавства має відбуватися шляхом прийняття Концепції інформаційної безпеки України. Виявлено, що вона самостійно та спільно з ООН, ОБСЄ та іншими міжнародними організаціями й об'єднаннями протидіє таким реалізованим проти неї технологіям інформаційно-гібридної війни: «кібервійни», «терористичні війни», «міграційні війни», «екологічні війни» та інші. Водночас визнано, що протидія інформаційно-гібридним війнам, особливо з використанням глобальної мережі Інтернет, соціальних мереж тощо вимагає постійного вдосконалення вітчизняної системи безпеки у зв'язку з розвитком інформаційно-комунікаційних технологій, який практично неможливо зупинити.

Зважаючи на те, що управлінські заходи у сфері інформаційної безпеки Україні носять запізнілий характер, наполягається на необхідності їхнього вдосконалення в напрямку розробки комплексу заходів. Вони повинні реалізовуватися «на випередження», тобто передбачати стратегічне планування та реагування, виходячи зі тенденції щодо зростання кількості зовнішніх і внутрішніх загроз інформаційного характеру. Щодо шляхів вирішення проблем протидії інформаційно-гібридним війнам і вдосконалення інституційної системи публічного управління України в цьому контексті, надано рекомендації:

1. З урахуванням актуальності протидії інформаційно-гібридним війнам у перспективі слід створити єдиний координаційно-аналітичний центр/раду, на зразок Бюро протидії гібридній війні. Таке Бюро функціонує в США та напрацювало дієві управлінські практики реагування на інформаційні загрози. Уважаємо, що до складу вітчизняної інформаційної контргібридної структури варто включити окрему наукову установу, яка має займатися розробкою механізмів дослідження даної проблематики (наукове вивчення, підготовку аналітичних документів щодо виявлення вразливих місць та можливого складу інформаційно-гібридних загроз, надання пропозицій). Ці рекомендації важливі для вироблення політичних рішень і вжиття дієвих заходів протидії з протидії інформаційно-гібридній війні.

2. Для того, щоб уникнути в перспективі дублювання функцій між безпековим і силовим блоком України з питань протидії окремим технологіям інформаційно-гібридних війн таких, як «терористичні війни» та «кібервійни», уважаємо, що доцільно здійснити аналіз і корегування обсягу обов'язків і компетенцій.

3. Обґрунтовано розробити та впровадити Концепцію інформаційної безпеки України з урахуванням нових викликів та загроз, у т.ч. пов'язаних із розвитком інформаційних технологій, що становлять базис для виникнення та масштабування інформаційно-гібридних війн. Дана позиція висловлена з урахуванням основоположних засад науки «Публічне управління та

адміністрування» щодо особливостей планування та стратегування.

4. Підкреслено на важливості дослідження досвіду економічно розвинених країн світу щодо дієвих механізмів протидії інформаційно-гібридним війнам й активізації співробітництва з цими країнами. Зважаючи на виявлений позитивний закордонний досвід застосування ризик-орієнтованих підходів щодо функціонування таких механізмів (у Франції, Казахстані, США та ін.), у дисертації обґрунтовано виважене впровадження цих підходів і на вітчизняних теренах. Ризик-орієнтовані підходи до забезпечення розвитку інституційної системи публічного управління України в умовах інформаційно-гібридної війни дозволили обґрунтувати сценарії реагування на ці війни: 1) проактивний сценарій, який рекомендовано реалізовувати під час стратегічного планування та поступального забезпечення сталого розвитку; 2) реактивний сценарій, що передбачає оперативне реагування на інформаційні загрози, зокрема, у межах уточненої концепції протидії ним.

Резюмовано, що проти України як самостійного суб'єкта міжнародних відносин реалізуються окремі технології інформаційно-гібридних війн, які чинять негативний вплив на безпеку нашої держави. На сучасному етапі її функціонування, інформаційно-гібридну війну необхідно визнавати основним вектором реалізації геополітичних/геоекономічних інтересів інших держав, що продовжують удосконалювати механізми свого впливу. Акцентовано, що інформаційно-гібридні війни, незважаючи на своє багатозначне визначення, сьогодні стали реальністю. Між державами велися та будуть вестися інформаційно-гібридні війни, і не сприяє унеможливленню їхнього виникнення ні утворення ООН, ні проголошення деякими країнами переходу до мирного вирішення всіх проблем, що виникають у взаємовідносинах між державами. Свідченням цього є те, що інформаційно-гібридні війни набули значного поширення в Афганістані, Венесуелі, Сирії, Україні та ін. Ці країни є вдалим прикладом протистояння основних геополітичних гравців із використанням різних технологій ведення інформаційно-гібридних війн. Констатовано, що політичні, економічні, військові, інформаційні та інші ресурси виступають складовими технологій інформаційно-гібридних війн. При цьому процеси глобалізації стимулюють появу нових аспектів інформаційно-гібридних війн.

З урахуванням цього обґрунтовано концептуальні засади щодо прогнозування інформаційно-гібридних війн у контексті розвитку інституційних механізмів публічного управління на пострадянському і вітчизняному просторі. Акцентовано, що на ці механізми впливають зовнішні та внутрішні фактори: політичні, соціальні, економічні тощо. Серед них найбільш загрозливими на сучасному етапі визнано соціальні, адже вони пов'язані з рівнем міграції громадян, їхнього добробуту, безробіття, демографічного розвитку та ін., що суттєво знижується в Україні та є перевагою для держав-акторів та агресорів.

Отже, пострадянський простір, до якого входить й Україна, у перспективі продовжуватиме залишатися об'єктом реалізації інформаційно-гібридних війн. На цій підставі акцентовано на необхідності й надалі вдосконалювати вітчизняну правову базу щодо протидії реалізованим проти України окремих

технологій інформаційно-гібридної війни. Цього можна досягти шляхом прийняття відповідних стратегій, концепцій та інших документів, в яких мають бути враховані питання виявлення, прогнозування, планування, координації й управління, розкриття вразливих для інформаційно-гібридних загроз із метою своєчасного на них реагування. Уважаємо, що серед цих питань першочерговими можуть бути: 1) нарощування оборонного потенціалу країни, зокрема інформаційного, що вимагає вдосконалення вітчизняних механізмів швидкого та стратегічного реагування на дезінформаційні матеріали та раптові інформаційні атаки; 2) забезпечення підготовки якісного кадрового потенціалу, здатного розробити та реалізувати намічені заходи щодо протидії інформаційно-гібридним війнам; 3) розвиток вітчизняної інституційної системи та її кооперація з міжнародними організаціями щодо розробки й упровадження технологій протидії таким війнам.

ВИСНОВКИ

Одержані під час дослідження результати передбачають вирішення актуального конкретного наукового завдання, яке полягає у визначенні науково-теоретичних засад формування інституційних механізмів публічного управління в умовах інформаційно-гібридних війн і розробленні практичних рекомендацій щодо вдосконалення таких механізмів в Україні.

На підставі результатів, отриманих під час дисертаційного дослідження, визначено такі висновки та пропозиції:

1. Узагальнено положення про те, що феномен інформаційно-гібридної війни є вищою формою міждержавного інформаційного протистояння, що передбачає конфлікт інтересів суб’єктів геополітичної/геоекономічної конкуренції (протиборства) в інформаційному просторі. З’ясовано, що метою цих протиріч є встановлення зовнішнього політичного керівництва над державою-об’єктом, а також перерозподіл ролі, місця та функцій у політико-управлінській системі сучасного суспільства, в якому зіткнення конфліктуючих сторін відбувається у формі інформаційних та інформаційно-психологічних операцій із застосуванням нетрадиційної зброї, зокрема, інформаційного характеру.

2. Визначено положення про те, що головною небезпекою інформаційно-гібридної війни є відсутність чітко ідентифікованих (видимих) ознак руйнівного впливу, характерного для традиційних війн. Виявлено, що за цих умов ускладненим є приведення захисних механізмів соціального та публічного управління, наявних у розпорядженні, але можливим. На відміну від традиційної війни, що передбачає застосування фізичної, кінетичної та іншої зброї з метою руйнації всього в межах радіусу її дії, інформаційна зброя діє вибірково, охоплюючи по-різному різні верстви населення та публічні інститути. Традиційна ж зброя впливає на будь-яку частину населення однаково. Відтак, наполягається на такій головній небезпеці інформаційно-гібридної війни як потенційна можливість цільового інформаційного, у т.ч. негативного, впливу.

3. Структуризовано інституційні механізми публічного управління

України в умовах інформаційно-гібридної війни, у складі яких виокремлено насамперед організаційні та правові механізми державного впливу. Базис для висловлення такої позиції становили враховані загальні положення фундаментальної науки щодо визначення понять «інститут», «інституція», «організація» та ін. Обґрунтовано, що інституційні механізми публічного управління України в умовах інформаційно-гібридної війни покликані забезпечувати виникнення та розвиток суб'єктно-об'єктних відносин в означеній сфері, що вимагають результативного застосування методів, інструменти та ресурсів публічного управління з метою налагодження зворотного зв'язку й унеможливлення трансформації ризиків інформаційного характеру в загрози, кризи та війни. Зважаючи на таку мету формування та функціонування інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни, уточнено визначення поняття «інформаційна безпека».

4. Визначено особливості функціонування інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни крізь призму виокремлених ризиків їхнього функціонування, а саме: 1) ризику не протидії поширенню неправдивої та видозміненої інформації з боку країни-агресора, що впливає на розвиток суспільства й держави; 2) ризику не формування цілісної інформаційної концепції і стратегії поширення об'єктивної інформації та протидії загрозам інформаційного характеру; 3) ризику не забезпечення підвищення рівня медіа-культури суспільства та його цифровізованого розвитку тощо. З огляду на збільшення виявів цих ризиків охарактеризовано стан упровадження інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни як незадовільний. Цьому сприяли зовнішні та внутрішні фактори, до яких віднесено насамперед зовнішню агресію проти України, посилення з боку рф інформаційного негативного впливу, що наразі вже набув вигляду інформаційно-гібридної війни, недосконаліть вітчизняної правової бази в досліджуваній сфері на предмет визначення функцій органів державної влади в інформаційній сфері. На цій підставі конкретизовано склад суб'єктної підсистеми у сфері інституційного забезпечення публічного управління в умовах інформаційно-гібридної війни. При цьому здійснено групування складових суб'єктної підсистеми залежно від того, чи є гарантування інформаційної безпеки основною або другорядною функцією, чи їх реалізують державні органи або інші публічні інституції тощо. Усе це дозволило обґрунтувати шляхи підвищення результативності функціонування цих підсистем з наведенням конкретних нормотворчих пропозицій щодо усунення дублювання функцій органів державної влади у сфері інформаційної безпеки.

5. Проаналізовано інструменти дисфукнціоналізації інституційних механізмів публічного управління в умовах інформаційно-гібридної війни, які передбачають застосування, зокрема, технологій «м'якої сили». Під ними розуміється сукупність інституційних, проектно-ідеологічних, міжнародно-правових, організаційних, фінансових, інформаційно-пропагандистських, розвідувальних та інших механізмів проектування, алгоритмізації, реалізації,

забезпечення та контролю процесів дисфункціоналізації, дискредитації або тотальної руйнації іншої суверенної держави (держави-об'єкта) з метою трансформації цієї держави в неспроможну, що веде до повного її знищення у межах колишньої території або примусової її трансформації у субмісивні форми з редукованим або повністю втраченим суверенітетом, а також для досягнення інших цілей на користь держави-актора. З'ясовано, що застосування «м'якої сили» завжди передбачає агресивні дії противника, зокрема, інформаційного характеру. На цій підставі застосування інструментів «м'якої сили» обґрунтовано інтерпретувати як здійснення щодо держави-об'єкта (держави-мішені) неоголошеної гібридної війни, як-то відбувається по відношенню до України. Аргументовано визначення заходів з випередження негативного впливу держави-актора на державу-об'єкт шляхом застосування ризик-орієнтованих підходів. Виявлено, що вони активно впроваджується як в економічно розвинених державах (наприклад, у Франції), так і в тих країнах, що тільки стали на шлях забезпечення сталого розвитку (Казахстан). Для обох цих країн характерним є впровадження ризико-орієнтованих підходів в інституційну систему публічного управління, що відображається в ключових правових документах стратегічного планування. Зважаючи на це й інтеграційні прагнення України, рекомендовано здійснити на її теренах проектування інструментів ризик-орієнтованого публічного управління в умовах інформаційно-гібридної війни з урахуванням позитивно верифікованої багаторічної закордонної практики реагування на інструменти «м'якої сили».

6. Обґрунтовано ризик-орієнтовані підходи до забезпечення розвитку інституційної системи публічного управління України в умовах інформаційно-гібридної війни, у межах яких (підходів) визначено сценарії реагування на зазначений види війни. Серед цих сценаріїв виокремлені такі: 1) проактивний, який рекомендовано реалізовувати під час стратегічного планування та поступального забезпечення сталого розвитку, що вимагає, у свою чергу, удосконалення стратегії сталого розвитку України; 2) реактивний сценарій, що на відміну від попереднього, передбачає оперативне реагування на інформаційні загрози. У цьому контексті доведена необхідність у розробці та прийнятті концепції протидії інформаційним загрозам та інформаційно-гібридній війні, у якій (концепції) рекомендовано закріпити на рівні правової норми визначення такому виду війни, що наразі відсутнє.

7. Запропоновано шляхи розвитку інституційної системи публічного управління України в умовах інформаційно-гібридних війн, що передбачають, по-перше, створення вітчизняної інформаційної контргібридної пропагандистської структури, на зразок, Бюро протидії гібридній війні, яке функціонує в США та напрацювало дієві управлінські практики реагування на інформаційні загрози. По-друге, налагодження результативної взаємодії України з іншими міжнародними організаціями в напрямку вчасного визначення та протистояння цим загрозам. Серед таких організацій визначено Європейський центр із протидії гібридним загрозам, Парламентську Асамблею Ради Європи, Центр передового досвіду стратегічних комунікацій (StratCom) та ін. По-третє, доведена необхідність щодо реалізації заходів щодо належного

забезпечення інформаційної безпеки України й іншими публічними інституціями – НУО та НКО, що мають залучатися до реального формування та контролю за державною інформаційною політикою. Крім того, що розвиток вітчизняної інституційної системи публічного управління в умовах інформаційно-гібридних війнах має бути забезпечений шляхом створення Державного унітарного підприємства «Центр технічного захисту інформації, сертифікації та експертизи».

8. Визначено концептуальні засади щодо прогнозування інформаційно-гібридних війн у контексті розвитку інституційних механізмів публічного управління на пострадянському і вітчизняному просторі. Доведено, що на сучасному етапі його розвитку на ці інституційні механізми публічного управління впливають зовнішні та внутрішні фактори, які можуть, у свою чергу, становити підґрунтя для виникнення та посилення інформаційно-гібридної війни. Серед цих факторів загрозливими визнано такі: 1) політичні, що зумовлені багатовекторною й ізольованою політикою країни; 2) економічні, що виникають через «митні», «санкційні» та інші аналогічні війни, що ведеться проти конкретно взятої держави; 3) соціальні, що пов'язані з посиленням міграційних процесів (вимушеного виїзду громадян до інших країн), а, відтак, зростанням рівня безробіття, зниженням добробуту та демографічних показників тощо. На цій підставі уточнено комплекс заходів, що слід реалізовувати в межах досліджених інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни, що ведеться проти неї.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у фахових наукових виданнях з державного управління:

1. Новіков В.О. Ризик-орієнтований підхід до формування інституційних механізмів публічного управління в умовах інформаційно-гібридних війн: досвід Франції, Казахстану й України // *Вісник Національного університету цивільного захисту України. Серія: Державне управління.* 2020. Вип. 1 (12). С. 300–308. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/18672/1/journal12.20.pdf.

2. Новіков В.О. Дисфукнціоналізація інституційної системи та механізмів публічного управління в умовах інформаційно-гібридних війн // *Вісник Національного університету цивільного захисту України. Серія: Державне управління.* 2020. Вип. 2 (13). С. 345–354. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/18688/1/vdu13.pdf.

3. Новіков В.О. Theoretical and institutional features of the modern definition of the concept of hybrid war // *Вісник Національного університету цивільного захисту України. Серія: Державне управління.* 2023. Вип. 2 (19). С. 207–212.

4. Новіков В.О. Аналіз сучасної концепції інформаційно-гібридної війни // *Державне управління: удосконалення та розвиток:* елек. журнал. 2023. № 9. URL: https://www.nayka.com.ua/index.php/dy/article/view/2133.

5. Новіков В.О. Information and hybrid wars in the current environment: public-administrative aspect // *Public administration and state security aspects.* 2023. Vol. 2. P. 43–51.

6. Помаза-Пономаренко А.Л., Новіков В.О. Шляхи трансформації інституційних механізмів публічного управління в Україні: від інформаційних загроз до гібридних війн // Державне будівництво: елек. журнал. 2023. № 1 (33). URL: https://periodicals.karazin.ua/db/article/view/22921.

Статті в закордонних виданнях за напрямком:

7. Novikov V. Approaches to improvement of the institutional system and mechanisms of public administration in the conditions of information-hybrid wars // *Eurasian Academic Research Journal*. 2020. Vol. 37. Pp. 75–80.

Тези конференцій:

8. Новіков В.О. Особливості сучасного концепту інформаційно-гібридної війни по відношенню до України // Публічне управління в системі координат: демократія, децентралізація, місцеве самоврядування: матеріали Всеукраїнської науково-практичної конференції (18.10.2019 р., м. Мелітополь) / відп. ред. Ортіна Г.В. Мелітополь: ФОП Однорог Т.В., 2019. С. 410–411.

9. Новіков В.О. Аналіз інституційних особливостей формування сучасної концепції інформаційно-гібридної війни // Modern research in science and education: матеріали I Міжнародної науково-практичної конференції (14-16.09.2023 р., м. Київ). Київ: Науково-видавничий центр «Sci-conf.com.ua». 2023. С. 286–289. URL: https://sci-conf.com.ua/wp-content/uploads/2023/09/MODERN-RESEARCH-IN-SCIENCE-AND-EDUCATION-14-16.09.23.pdf.

10. Новіков В.О. Напрями вдосконалення інституційних механізмів публічного управління в умовах інформаційно-гібридних війн // Наука і вища освіта : матеріали XXXII Міжнародної наукової конференції здобувачів вищої освіти і молодих учених (08.11.2023 р., м. Запоріжжя). 2023. С. 263–264.

11. Новіков В.О. Особливості розвитку механізмів публічного управління в умовах інформаційно-гібридних війн // Національна безпека в умовах війни, післявоєнної відбудови та глобальних викликів XXI століття : матеріали Всеукраїнської науково-практичної конференції (07-08.12.2023 р., м. Житомир). С. 276–278.

АНОТАЦІЯ

Новіков В.О. Інституційні механізми публічного управління в умовах інформаційно-гібридних війн – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку. – Національний університет цивільного захисту України. – Харків, 2024.

У дисертації запропоновано розв’язання актуального конкретного наукового завдання, яке полягає у визначенні науково-теоретичних засад формування інституційних механізмів публічного управління в умовах

інформаційно-гібридних війн і розробленні практичних рекомендацій щодо вдосконалення таких механізмів в Україні. Для цього узагальнено теоретичні засади інформаційно-гібридних війн як інструменту соціогуманітарного протиборства в системі публічного управління. Досліджено особливості функціонування структурно-функціонального механізму виникнення інформаційних війн та механізми формування інформаційних технологій в умовах інформаційно-гібридних війн. Структуризовано інституційні механізми публічного управління України в умовах інформаційно-гібридної війни. Охарактеризовано особливості та ризики функціонування інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни. Проаналізовано інструменти дисфукнціоналізації інституційних механізмів публічного управління в умовах інформаційно-гібридної війни. Обґрунтовано ризик-орієнтовані підходи до вдосконалення інституційної системи публічного управління України в умовах інформаційно-гібридної війни. Уперше запропоновано шляхи розвитку інституційної системи публічного управління України в умовах інформаційно-гібридних війн. Визначено концептуальні засади прогнозування інформаційно-гібридних війн у контексті розвитку інституційних механізмів публічного управління.

Ключові слова: публічне управління та адміністрування, інституційні механізми публічного управління в умовах інформаційно-гібридних війн, органи публічної влади, національна безпека, інформаційна безпека.

ANNOTATION

Novikov V.O. Institutional mechanisms of public administration in the conditions of information and hybrid wars. – Qualifying scientific paper, as the manuscript.

Thesis for the scientific degree of a Candidate of Science in Public Administration, speciality 25.00.05 – Public Administration of State Security and Enforcement of Public Order. – National University of Civil Defence of Ukraine. – Kharkiv, 2024.

The thesis introduces solution for an essential scientific and applied task consisting in determination of scientific and theoretical principles of institutional mechanisms of public administration in the conditions of information and hybrid wars, as well as in elaboration of practical recommendations for the development for improving such mechanisms in Ukraine.

It became possible to solve an applied science task with the help of the first proposed definition of the ways of development of an institutional system of public administration in Ukraine under the conditions of hybrid and information warfare. Among these ways, the following were defined as the main ones: 1) establishing the coordination and analytical centre / council in Ukraine similar to the Centre on Combating Hybrid Threats, which functions in the USA and has already created effective administrative practices aimed at the response to information threats; 2) building effective relationships between Ukraine and other countries and

international organizations aimed at countering these threats in time.

The above-mentioned author's proposals were given based on the improved definition of the main threat of hybrid and information warfare as a potential possibility of purposeful informational, particularly negative influence on the objectively established and available contradictions practically at all levels of state and public system in any country or region with the purpose of forced manifestation of this influence at the predetermined level of intensity and in the predetermined direction.

Positive foreign public and administrative practices in the field of countering information threats (in France, Kazakhstan, the USA, etc.) were defined. The analysis of these practices made it possible to state that the applied risk-oriented approaches guarantee their successful implementation. On this ground, the thesis proves the necessity to apply these approaches for the development of institutional system of public administration in Ukraine under the conditions of hybrid and information warfare. These approaches, in turn, made it possible to prove the following scenarios of response in this war: 1) a proactive scenario, which is recommended to implement for strategic planning and progressive achievement of sustainable development; 2) a reactive scenario, which stipulates prompt response to information threats, in particular within the framework of specified conception of counteraction.

In addition, the conceptual framework for forecasting hybrid and information warfare in the context of the development of institutional mechanisms of public administration in the post-Soviet and local area was improved. It was proved that both external and internal factors (political, social, economic, etc.) influence these mechanisms. It was proved that the most threatening among them at the current stage are the social ones, as they are directly connected with the level of migration of citizens, their well-being, unemployment, demographic development, etc.

A special part of the thesis contains the provisions, within which the definition of asymmetry as a fundamental characteristic of hybrid and information warfare obtained its further development. It was emphasized that it is characterized by abeyance and focus on the most vulnerable aspects in the enemy's informational defence, the consequences of imperfection of which may be compared with the use of unconventional weapon aimed at significant reduction of conventional arms expenditures and at gaining information advantage over the enemy.

The thesis structurizes the institutional mechanisms of public administration in Ukraine under the conditions of hybrid and information warfare from the point of view of distinction of organizational and legal mechanisms of public administration out of these mechanisms. They trigger its relevant subjective subsystem. As of today, this subsystem is characterized as the one that functions inadequately. Based on this, the effectiveness improvement ways were substantiated by providing the specific regulatory proposals concerning the elimination of doubling of functions of the state authorities in the field of information security.

Keywords: public management and administration, institutional mechanisms of public management in the conditions of information-hybrid wars, public authorities, national security, informational security.

Відповідальний за друк *Помаза-Пономаренко А.Л.*

Підписано до друку 15.02.2024 р.
Формат 60х84 $^{1}/_{16}$. Обл.-вид. арк. 0,9.
Гарнітура Таймс. Тираж 100 прим.

Віддруковано з оригінал-макета в друкарні ФОП Леонов Д.С.
61023, м. Харків, вул. Весніна, 12, тел. (057) 717-28-80.