УДК 351.746:007
DOI https://doi.org/10.32782/1813-3401.2024.3.9

І. В. Кудрявський
докторант
Міжрегіональної Академії управління персоналом
https://orcid.org/0009-0009-5167-7648

ОРГАНІЗАЦІЙНІ ПРОБЛЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ У СФЕРІ ЗАХИСТУ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ

Завдання раціонального формування організаційної структури інституцій державного управління у сфері захисту безпеки інформаційного простору є складним та актуальним для будь-якої країни в сучасному світі. Відбиття силами оборони України широкомасштабного російського вторгнення, для забезпечення якого противник активно застосовує увесь арсенал форм і засобів деструктивного інформаційно-психологічного впливу, робить це завдання ще складнішим, але, при цьому, критично важливим для нашої держави.

Державне управління у сфері захисту безпеки інформаційного простору за своєю природою не передбачає ідеальних рішень чи простих шляхів. Особливо, якщо захист безпеки інформаційного простору держави й інформаційної безпеки особистості будується з урахуванням становлення системи стратегічних комунікацій, активної участі у процесах обміну інформацією та наповнення інформаційного простору інституцій громадянського суспільства.

Недостатня координація між суб'єктами наповнення інформаційного простору в умовах постійного деструктивного інформаційно-психологічного впливу противника призводить до низької ефективності механізмів захисту безпеки інформаційного простору. Надмірна централізація – до порушення демократичних принципів, невдоволення аудиторій та, як наслідок, створення сприятливої атмосфери для реалізації противником своїх інформаційно-психологічних акцій і пропаганди. Ще гірше, коли необгрунтовані обмеження і спроби надмірного контролю інформаційного простору з боку носіїв владних повноважень поєднуються з недостатньою координацією зусиль як між державними установами та інституціями громадянського суспільства, так і всередині системи державного управління у сфері захисту безпеки інформаційного простору.

Мета *запропонованого дослідження – пошук способів підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору через аналіз проблем організаційного характеру і шляхів їх вирішення.*

Завдання дослідження *полягає в аналізі наукових праць, офіційних повідомлень та публіцистичних матеріалів, нормативно-правових актів й інших джерел, що надають можливість вивчити проблематику організаційного характеру в питаннях становлення та функціонування механізмів державного управління у сфері захисту безпеки інформаційного простору в умовах відбиття Силами оборони України російського широкомасштабного вторгнення.*

Наукова новизна *дослідження і його результатів полягає у комплексному розгляді проблемних питань організаційного характеру сучасного державного управління у сфері захисту безпеки інформаційного простору України з акцентуацією уваги на реалії розгортання системи стратегічних комунікацій, зокрема інформаційних дій, спрямованих на зниження ефективності деструктивного інформаційно-психологічного впливу противника, що здійснюються в умовах відбиття Силами оборони України російського широкомасштабного вторгнення.*

Методологія. *В ході роботи застосовано такі методи наукового дослідження: історичний, порівняльного аналізу, ретроспективного аналізу, аналізу та синтезу, дедукції, індукції, системно-структурний, лінгвістичний, формально-логічний.*

У **висновках** *зазначено, що однією з ключових причин інформаційної переваги противника та, відповідно, неналежного стану захисту безпеки інформаційного простору України вбачається відсутність необхідної кількості й якості інформаційного контенту, який виробляється в ході реалізації стратегічних комунікацій України. Такий стан речей є наслідком відсутності належної організації виробництва інформаційного контенту, правил та умов*

для його створення, а також відсутності критеріїв кадрового відбору на посади, пов'язані з реалізацією стратегічних комунікацій. На загальнодержавному рівні організаційною причиною проблем захищеності інформаційного простору вбачається прийняття за основу розвитку державної інформаційної політики ідеї розбудови системи стратегічних комунікацій при ігноруванні її важливого елемента – медіаопераций у значенні цільової оперативної своєчасної пропозиції аудиторіям достовірної інформації високої художньої якості у достатній кількості.

З метою відновлення паритету та, у перспективі, здобуття інформаційної переваги над противником, підвищення рівня медіакультури та медіаграмотності громадян України, що сприятиме захищеності безпеки інформаційного простору, інформаційної складової національної безпеки України та особистої інформаційної безпеки її громадян, запропоновані конкретні заходи щодо збільшення кількості якісного достовірного інформаційного контенту та його оперативного поширення.

Ключові слова: *державне управління, інформаційний простір, інформаційна війна, стратегічні комунікації, російська агресія, інформаційно-психологічний вплив.*

Постановка проблеми. Розвиток механізмів державного управління у сфері захисту безпеки інформаційного простору та системи реагування на кризи, викликані діями в інформаційному просторі в Україні, відбувається шляхом реалізації концепції стратегічних комунікацій та розбудови системи стратегічних комунікацій.

Оскільки на рівні кодексів та законів України немає визначення терміну "стратегічні комунікації", правовим значенням цього поняття можемо вважати визначення, що містяться у керівних документах Збройних Сил України.

Стратегічні комунікації – скоординоване і належне використання комунікативних можливостей держави: публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави [1, 2].

У Доктрині зі стратегічних комунікацій Збройних Сил України наведено також визначення поняття "система стратегічних комунікацій":

Система стратегічних комунікацій – сукупність суб'єктів стратегічних комунікацій зі встановленими між ними взаємозв'язками, діяльність яких спрямована на реалізацію стратегічних комунікацій [2].

Отже, як випливає з визначення, ефективність стратегічних комунікацій прямо залежить від ефективності організаційних заходів щонайменше на двох рівнях:

1) штатної структури, повноважень та завдань підрозділів, які є суб'єктами стратегічних комунікацій;

2) взаємозв'язків між такими суб'єктами.

В умовах сучасних глобальних інформаційних процесів, а тим більше в ході відбиття російського широкомасштабного вторгнення, яке характеризується потужною інформаційно-психологічною та пропагандистською складовими, від ефективного функціонування стратегічних комунікацій прямо залежать питання національної безпеки та безпеки кожного громадянина. Стратегічні комунікації є процесом, який покладено в основу забезпечення національної безпеки України, та до його реалізації залучаються як суб'єкти стратегічних комунікацій, так і суб'єкти з інших сфер діяльності [3, с. 102]. Це, у свою чергу, створює певні складності у синхронізації дій та координації між різними суб'єктами.

За сучасних умов стратегічні комунікації та національну стійкість слід розглядати у широкому контексті з урахуванням особливостей розвитку країни. Необхідно враховувати недостатній, як для умов війни, рівень консолідації суспільства, недостатню ефективність державного управління, незавершеність реформування сектору безпеки та оборони і процесів децентралізації, системні вади національної економіки. У цьому широкому контексті основними компонентами національної стійкості держави є кризовий менеджмент, стійкість територіальних громад, економічна стійкість та стійкість суспільства [4, с. 7]. Кризовий менеджмент за умов відбиття широкомасштабного вторгнення й реалізації противником множинної системи психологічних акцій та операцій, розрахованих як на досягнення оперативних цілей, так і на довгострокову перспективу, має ключове значення. Розуміння цього факту і нерозуміння основ та традицій кадрової роботи призводить до того, що на посади, де необхідні досвід і компетентність у сфері стратегічних комунікацій, а також знання щодо сучасного функціонування інформаційного простору, який динамічно змінюється, нерідко призначають осіб, які вміло позиціонують себе як кризові менеджери, хоча за фактом не володіють компетенцією ані у сфері стратегічних комунікацій, ані, тим більше, у сфері кризового менедж-

менту. Такі факти та прізвища є загальновідомими і не потребують окремого згадування, а от наслідки реалізації ними повноважень за високими посадами, окрім сумнівного піару таких осіб, на жаль, призводять в умовах війни не лише до втрат комунікаційних позицій держави на різних рівнях, але, нерідко, і до цілком конкретних людських жертв. У цьому контексті організаційні проблеми та недотримання, а в окремих випадках навіть відсутність правил кадрового комплектування відповідних позицій у структурах державного управління, включно з Силами оборони України, тісно пов'язані з правовими та психологічними аспектами. Системність комплектування кадрами й підготовки кадрів, як і вирішення інших організаційних проблем у цьому аспекті, звісно, здатні значно покращити ситуацію. Більше того, зміни, а в окремих випадках – створення відповідних правил організації підрозділів, що є суб'єктами стратегічних комунікацій, необхідні, як кажуть "на вчора", оскільки вони дозволяють вирішити проблему значною мірою найбільш оперативно. Але необхідно розуміти, що такі дії будуть неповними, а їх результати недостатніми або короткочасними без відповідного закріплення у нормативно-правових (нормативних) актах і, власне, прогресу в етичних та суспільних аспектах: розуміння громадянським суспільством необхідності дотримуватися "правил гри" у питаннях, від яких залежить національна безпека держави (а питання інформаційної безпеки безумовно є одним з таких), відходячи від принципів впливу на рішення через соціальні мережі, керуючись особистими уподобаннями, симпатіями чи антипатіями спільнот, часто віртуальних, які володіють недостатньою інформацією і на які досить просто впливати, знаючи елементарні ази психології натовпу у проекції на цифровізацію сучасного комунікативного середовища.

Ключовим питанням для існування держави в умовах широкомасштабної війни було і залишається ефективне функціонування стратегічних комунікацій Сил оборони України. В Силах оборони нині відбувається два протинаправлених процеси. З одного боку, стоїть задача по уніфікації та стандартизації усіх процесів, включно з комунікаційними, – прагнучи більшої професійності та ефективності. З іншого – ми спостерігаємо постійне множення комунікаційних сутностей, усі підрозділи намагаються виробляти контент, усі займаються інформаційно-психологічними операціями, кожен взаємодіє з пресою та створює сторінки в соцмережах, збираючи пожертви. Виходячи зі спроможностей, треба визнати, що більшість суб'єктів комунікації Сил оборони не здатні в нинішньому стані забезпечити справді ефективну комунікацію. Прагнучи стандартизації та унормування процесів виробництва контенту, важливо одночасно не знищити творчу ініціативу окремих командирів та фахівців з комунікації. От якраз тут і потрібні процеси ефективних стратегічних комунікацій та медіапланування. Так само – як і навчання та підвищення кваліфікації [5, с. 60]. Такі особливості організаційних процесів, за своїм призначенням покликані підвищити ефективність механізмів державного управління у сфері захисту безпеки інформаційного простору, на практиці, на жаль, мають зовсім інший результат. Ефективно вести будь-які інформаційні дії, спрямовані на отримання інформаційної переваги, неможливо без створення інформаційного контенту. Поряд з тим, стандартизація та реорганізація у Силах оборони України, як і в будь-яких інших державних структурах, неминуче призводить до супутніх кадрових змін. Як результат, від процесу створення інформаційного контенту відсторонюється величезна кількість творчих спеціалістів, досвід і можливості яких становлять цінність у контексті умов та обставин інформаційного протистояння. Особливо це стосується посадових осіб, які добросовісно виконували свої обов'язки, створювали контент, спрямований на досягнення ефектів в інформаційному просторі в інтересах військових частин та підрозділів, не витрачаючи час на особистий самопіар. Таким чином найбільш цінні спеціалісти, не передавши свого досвіду та напрацьованих методик роботи, зазвичай переводяться на посади, не пов'язані з творчою роботою, щоби на їхньому фоні не створювався негативний контраст для "нових молодих команд". Нові команди за наявності творчих даних, чи без таких, і точно за відсутності необхідного досвіду, починають "винаходити велосипед". Відсутність або неефективність комплексної підготовки за принципом викладання "практичних правил бою" у контексті інформаційних дій не додає ефективності механізмам державного управління у сфері захисту безпеки інформаційного простору в цілому. Адже спеціаліст, який може розповісти, як планувати інформаційну операцію за стандартами НАТО (більшість з яких є відкритими та загальнодоступними, принаймні англійською мовою), може елементарно не володіти досвідом та знаннями щодо правил роботи

зі знімальною апаратурою, монтажем, основами публіцистичного та інших жанрів літератури. При сумнівній фактичній можливості такого спеціаліста спланувати інформаційну кампанію чи інші інформаційні дії в реальному житті, він може виявитися абсолютно нездатним зробити цю роботу особисто або об'єктивно та компетентно перевірити якість виконання завдань підлеглим творчим персоналом.

Як наслідок, виникла ситуація, коли російська інформаційно-психологічна операція щодо зриву мобілізації в Україні досягла настільки значних успіхів, що її негативні наслідки неможливо ігнорувати. І такий приклад далеко не єдиний. Зрозуміло, що державні механізми захисту безпеки інформаційного простору в Україні не виконують своїх завдань належним чином та, відповідно, потребують змін і реформування. Поряд з тим, стиль та характер розпочатих змін і реформування станом на зараз дає найрізноманітніші ефекти: починаючи від законних засобів фактичного ухилення від військової служби друзів та родичів нових керівників низки державних структур шляхом розміщення їх без відповідної освіти й компетенції на посадах, пов'язаних з інформаційними діями, і закінчуючи втратою чисельного, хай і не ідеального, але професійного кадрового ресурсу. Єдиний ефект, якого поки не вдається виявити, – це збільшення кількості та підвищення якості необхідного під час війни інформаційного контенту. Як і загалом підвищення ефективності механізмів державного управління у сфері захисту інформаційного простору.

Таким чином, головна проблема полягає в тому, що, з одного боку, на певному етапі (починаючи з літа 2022 року) система державного управління у сфері захисту безпеки інформаційного простору почала демонструвати свою недостатню, і навіть незадовільну ефективність, що вимагало реформування та змін. З іншого боку, на фоні інформаційної активності противника, (який зрозумів прорахунки у своїх інформаційно-психологічних операціях та пропаганді і зробив належні висновки, посиливши фінансову складову, відмовившись від непродуктивних сценаріїв та акцентувавши увагу на більш реалістичних і небезпечних для нас) характер та способи реформування суб'єктів стратегічних комунікацій в Україні поки тільки посилюють хаос у їхній роботі та не дають відчутного позитивного ефекту. У ситуації, коли "залишатися на місці" не можна, а вжиті заходи (зміни) мають "від'ємну" ефективність, існує гостра необхідність для дослідження ситуації й коригування характеру розбудови механізмів державного управління у сфері захисту безпеки інформаційного простору.

Завдання дослідження полягає в аналізі наукових праць, офіційних повідомлень та публіцистичних матеріалів, нормативно-правових актів та інших джерел, що надають можливість вивчити проблематику організаційного характеру в питаннях становлення й функціонування механізмів державного управління у сфері захисту безпеки інформаційного простору в умовах відбиття Силами оборони України російського широкомасштабного вторгнення.

Методологія. В ході роботи застосовано такі методи наукового дослідження: історичний, порівняльного аналізу, ретроспективного аналізу, аналізу та синтезу, дедукції, індукції, системно-структурний, лінгвістичний, формально-логічний.

Аналіз досліджень і публікацій. Інформаційний матеріал, необхідний для аналізу, міститься в наукових працях, зокрема українських дослідників, таких як: Юськів Б., Карпчук Н., Пелех О., Благодарний А., Кононець О., Войтко О., Єргідзей К., Сіманський Д., Зінорук М., Косогоров О., Руснак Ю., Стужук Ю., Прокопенко О., Недохлєбов І. [3, 4, 5, 6, 7, 8, 9, 12]; українських та іноземних нормативних актах [1, 2, 10, 11].

Мета запропонованого дослідження – пошук способів підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору через аналіз проблем організаційного характеру і шляхів їх вирішення.

Виклад основного матеріалу дослідження з обґрунтуванням отриманих результатів. Як би це дивно не звучало, але навіть контент-аналіз наукових досліджень дає змогу стверджувати значний ухил у бік досліджень прав людини, людиноцентризму, гуманізму, соціального виміру державної політики і гуманістичної ролі права, розвитку інститутів громадянського суспільства, націєтворення на противагу державотворенню. У цьому науковому і творчому процесі певним чином було занедбано державознавство, втрачено розуміння первісного призначення держави і взагалі змісту вектора державності, державотворчих процесів. Широкомасштабне російське вторгнення в Україну 24 лютого 2022 року з-поміж багатьох причин стало можливим через слабкість саме державницьких позицій, недостатню ефективність державного апарату, відсутність функці-

онуючої не на папері, а в реальності, системи забезпечення національної безпеки [6, с. 9]. Так само дослідження наукових праць і практичних кроків реформування державного управління у сфері захисту безпеки інформаційного простору дає можливість зробити висновок, що основний акцент у дослідженні і практиці цих питань робиться на моніторинг інформаційного простору [7, 8, 9] на противагу системі створення якісного інформаційного контенту, що здатен вплинути не лише на стан захищеності інформаційного простору, але і сприяти здобуттю такої необхідної під час війни інформаційної переваги над ворогом.

В жодному разі не применшуючи важливості належним чином налагодженого моніторингу та аналізу інформаційного простору, який забезпечує своєчасне попередження про інформаційні загрози, а у випадку ефективного функціонування такої системи, – навіть можливість прогнозування ситуації та належну підтримку для прийняття рішень відповідним посадовим особам, необхідно розуміти, що питання моніторингу – це лише питання обізнаності. Порівнюючи інформаційне протистояння з бойовими діями, моніторинг інформаційного простору можна назвати розвідкою, без якої активні дії відбуватимуться "всліпу" та, з високою вірогідністю, не даватимуть необхідних ефектів. Поряд з тим, маючи на озброєнні лише одну розвідку (в нашому випадку – моніторинг) будь-яка армія перетворюється на пасивного спостерігача за ситуацією. Так само, як армії на полі бою потрібні боєприпаси та засоби ураження, в інформаційному протиборстві необхідна величезна кількість інформаційних матеріалів та канали донесення їх до аудиторій. Причому це стосується як об'єктивного достовірного якісного інформування своїх аудиторій, так і не менш якісної реалізації заходів інформаційних і психологічних операцій, спрямованих на ворожі цільові аудиторії. Це величезна кількість роботи, яка щоденно вимагає тисяч людино-годин. При чому виконавці такої роботи мають бути не просто досвідченими висококласними спеціалістами, а ще й достатньо комунікабельними творчими особистостями, здатними виготовляти контент, цікавий для аудиторій, конкурентний і кращий за якістю виконання (не кажучи вже про достовірність) у порівнянні з матеріалами деструктивного інформаційно-психологічного впливу противника. Це питання станом на зараз практично залишене поза увагою як науковців, так і відповідних посадових осіб, які приймають рішення щодо реформування та розбудови системи стратегічних комунікацій загалом і механізмів державного управління у сфері захисту безпеки інформаційного простору зокрема.

На фоні відмовок про те, що "країні необхідні сильні кризові менеджери", відсутні нормативно-правові (нормативні) акти, які вимагали б певного набору компетенцій і здатності виконувати конкретні завдання творчого характеру від осіб, що займають посади, пов'язані із реалізацією стратегічних комунікацій. Елементарний контент-аналіз доктрин зі стратегічних комунікацій Збройних Сил та Національної гвардії України, не кажучи вже про інші нормативно-правові акти, дозволяє зробити висновок, що, беручи на озброєння ідею розбудови стратегічних комунікацій від Північно-Атлантичного Альянсу та країн-партнерів, українські законотворці забули про такий важливий напрямок, як медіаоперації. Під приводом, що вони начебто є частиною інформаційних операцій, у наведених документах немає жодної згадки щодо зазначеної форми інформаційних дій [2, 10]. Відповідно до Об'єднаної доктрини НАТО з інформаційних операцій AJP 10.1, медіа-операції – це військова інформаційна діяльність, яка пропонує точну і своєчасну інформацію визначеній аудиторії через засоби масової інформації з метою створення бажаного комунікаційного ефекту і досягнення згоди щодо національних цілей, підтримуючи при цьому безпеку операцій та особисту безпеку [11]. На жаль, доводиться констатувати, що напрямок забезпечення аудиторій власного громадянського суспільства, урядів і суспільств країн-партнерів точною і своєчасною інформацією на даний момент занедбаний не лише на законодавчому рівні, але й у ході практичної реалізації стратегічних комунікацій. Це, у свою чергу, призвело до того, що спеціалісти, здатні результативно проводити медіа-операції, яких жодна країна в принципі не може мати багато, стали в Україні не просто не потрібними, але навіть "шкідливими", оскільки своєю діяльністю створюють негативний фон для різноманітних колег з виключно формально-адміністративним стилем роботи, "селфі-зірок" соціальних мереж, "лідерів громадської думки" та некомпетентних у питаннях створення інформаційного контенту "кризових менеджерів".

Більш глобальним негативним наслідком, ніж фактична втрата унікального кадрового ресурсу, стала практична відмова України, яка

веде справедливу оборонну війну, від реалізації свого найсильнішого аргументу у питаннях захисту безпеки інформаційного простору та ведення стратегічних комунікацій загалом – оперативного і професійного поширення правди, яка без елемента обману аудиторій дозволяє ефективно впливати на їхні переконання та забезпечувати прийняття на основі об'єктивної інформації рішень, які сприяють майбутній перемозі. Якщо негативні наслідки середньострокової перспективи у вигляді зриву мобілізаційної кампанії та знекровлення Сил оборони України помітні уже зараз, то не можна оминути увагою й очевидні проблеми у довгостроковій перспективі. Постраждав процес фіксації історичних подій та збереження історичної пам'яті. Попри технічний прогрес і можливість фіксувати на камери дронів практично кожен рух на полі бою, ми практично втратили саму сутність мотивації, емоцій, оцінок та суб'єктивного сприйняття ситуації учасниками бойових дій, що завжди вважалися найбільшою цінністю та історичним надбанням, досвідом, який необхідно передати, для будь-якого суспільства. Цього процесу не здатні забезпечити фахівці-історики, чий механізм інтерв'ювання надмірно формалізований і не сприяє відвертості з боку респондентів, а способи публікації через стилістику не сприяють поширенню інформації, тим більше оперативному. Так само зазвичай не здатні ефективно та професійно виконати функції реалізації медіаоперацій представники служб зв'язків з громадськістю спільно з цивільними журналістами, оскільки їхня спільна діяльність передбачає складний бюрократичний механізм, з одного боку, обмеженість можливостей, з іншого, та нерідко різну мотивацію – з третього.

І. Недохлєбов пропонує такі критерії визначення стану інформаційної безпеки держави:

1) рівень медіакультури, медіаграмотності та інформаційної гігієни суспільства й особистості;

2) стан імплементації позитивного зарубіжного досвіду забезпечення інформаційної безпеки;

3) рівень забезпечення однакових стандартів державного управління у сфері інформаційної безпеки;

4) стан координації і взаємодії влади та громадськості у сфері забезпечення інформаційної безпеки;

5) відповідність здобутків влади очікуваним результатам, зафіксованим у стратегії інформаційної безпеки;

6) якість задоволення інформаційних потреб суб'єктами відповідних правовідносин;

7) стан гарантованості інформаційного суверенітету України [12, с. 14].

З описаного вище випливає, що через некоректне виконання пунктів 2 (ігнорування напрямку медіаоперацій та деструктивний організаційний вплив на роботу військових і цивільних журналістів, знищення та реорганізація редакцій) та 3 (відсутність таких стандартів в принципі або їх виключно формальний декларативний характер) виникли проблеми із пунктом 6 (споживачі інформації не задоволені кількістю та якістю інформаційного контенту), що сприяє погіршенню ситуації за напрямком, описаним у пункті 1 (медіаграмотність, медіакультура та інформаційна гігієна можливі, коли споживач щонайменше має вибір між більшменш рівнозначними потоками дезінформації і достовірних повідомлень з перевірених джерел, а не змушений вираховувати окремі елементи правдивих даних з суцільного масиву дезінформації різних авторства та якості, у якому переважає контент, створений відкрито або під прикриттям суб'єктами противника). У підсумку стан інформаційної безпеки важко назвати задовільним чи навіть достатнім (що під час війни не викликає особливого здивування, хоча повинно викликати щонайменше стурбованість), а стан інформаційного суверенітету України оцінювати в принципі некоректно, враховуючи, що контент деструктивного інформаційно-психологічного впливу противника легко доходить до українських аудиторій, викликаючи потужний когнітивний ефект.

Висновки та перспективи подальших розвідок у даному напрямку. Однією з ключових причин інформаційної переваги противника та, відповідно, неналежної захищеності безпеки інформаційного простору України вбачається відсутність необхідної кількості й якості інформаційного контенту, який виробляється в ході реалізації стратегічних комунікацій України. Такий стан речей є наслідком відсутності належної організації виробництва інформаційного контенту, правил та умов для його створення, а також відсутності критеріїв кадрового відбору на посади, пов'язані з реалізацією стратегічних комунікацій. На загальнодержавному рівні організаційною причиною проблем захищеності інформаційного простору вбачається прийняття за основу розвитку державної інформаційної політики ідеї розбудови системи стратегіч-

них комунікацій, при ігноруванні її важливого елемента – медіаопераций, у значенні цільової оперативної своєчасної пропозиції аудиторіям достовірної інформації високої художньої якості у достатній кількості.

З метою відновлення паритету та, у перспективі, здобуття інформаційної переваги над противником, підвищення рівня медіакультури та медіаграмотності громадян України, що сприятиме захищеності безпеки інформаційного простору, інформаційної складової національної безпеки України та особистої інформаційної безпеки її громадян, пропонується вжити заходів щодо збільшення кількості якісного достовірного інформаційного контенту та його оперативного поширення:

Створити не численний, але професійний підрозділ медіаопераций у складі Сил оборони України, який координуватиме свою діяльність з керівництвом інших складових стратегічних комунікацій, зокрема – зв'язків з громадськістю та інформаційних операцій. Такий підрозділ повинен забезпечувати не просто перевірку створеного контенту з урахуванням безпеки операцій та особистої безпеки, а створення цього контенту спеціалістами, які вже знають та враховують зазначені аспекти.

Розподілити посади підрозділів, що відповідають за створення інформаційного контенту і є суб'єктами наповнення інформаційного простору на творчі, яких повинно бути не менше 80–90 % від загальної кількості, і технічні. Встановити вимоги до посадових осіб, які перебувають на творчих посадах, щодо особистого відпрацювання конкретної кількості інформаційних матеріалів з прив'язкою до кількості опублікованих повідомлень, кількості та якості тексту, графічного, аудіовізувального (відео) та іншого творчого контенту.

Створити та застосовувати щонайменше раз у квартал систему оцінювання відпрацьованого творчого контенту з урахуванням критеріїв: кількість інформації, кількість опублікованих матеріалів, достовірність, оперативність, ризик при зборі первинної інформації, відповідність цілям і завданням державної інформаційної політики, чисельність аудиторії, яка ознайомилася з інформаційним контентом, емоційні та інші реакції аудиторії, вирішення конкретних завдань поза межами віртуального виміру інформаційного простору (підвищення кількості та якості комплектування за напрямком роботи органу державного управління, результати соціологічних опитувань, зниження кількості деструктивного інформаційно-психологічного впливу противника за певною тематикою, зміна кількості проявів невдоволення за певною тематикою, об'єктивні свідчення підвищення рівня медіаграмотності чи обізнаності суспільства за певними напрямками тощо). У випадку реалізації колективних проектів враховувати участь кожного із учасників пропорційно внеску роботи у виготовлення інформаційного продукту, а не за штатно-посадовою категорією. В обов'язковому порядку надана для оцінювання інформація повинна бути підтверджена результатами об'єктивного контролю – посилання на публікації, скриншоти тощо.

Запровадити систему виплати гонорарів за створення журналістських і творчих матеріалів за умови дотримання відповідних стандартів та критеріїв, забезпечивши прозору систему контролю їх нарахування (з прив'язкою до конкретного матеріалу та імені чи псевдоніму автора).

Запровадити систему санкцій за плагіат або виконання творчих завдань іншими особами, включно з забороною займати певні посади на термін не менше трьох років.

Оскільки для управління підрозділами, які займаються створенням інформаційного контенту, та для керівництва творчим персоналом необхідні відповідні знання і досвід, – унеможливити призначення та перебування на керівних посадах у таких підрозділах осіб, які особисто не відповідають зазначеним вимогам та не виконують норми щодо відпрацювання і публікації інформаційного контенту належної кількості та якості.

У випадку незадовільного проходження оцінювання (невиконання нормативів щодо створення інформаційного контенту) передбачити перепідготовку осіб, які займають творчі посади. У випадку повторної неможливості підтвердити відпрацювання та належне поширення відповідної кількості інформаційного контенту після перепідготовки забезпечити звільнення або переведення таких посадових осіб на посади за іншими напрямками державної (військової) служби як непридатних до творчої роботи.

З метою реалізації потенціалу спеціалістів, які мають достатній досвід і мотивацію для створення якісного цільового інформаційного контенту, створити та забезпечити функціонування каналів поширення інформації (друковані, теле-, радіосторінки у соціальних мережах та інші канали відповідно до часу й обстановки)

з вільним наповненням їх позаштатними авторами на основі виплати справедливого гонорару за умов відповідності інформаційних матеріалів поточним, середньо та довгоперспективним завданням за відповідними напрямками стратегічних комунікацій. З метою унеможливлення зловживань редакційні завдання, умови та розміри виплат розміщувати публічно та реалізовувати за прозорим механізмом, який враховує критерії, зазначені вище у пунктах 2 і 3. Забезпечити, зокрема із застосуванням семантичного аналізу, необхідних автоматизованих засобів перевірки контенту, недопущення публікації у таких виданнях матеріалів деструктивного інформаційно-психологічного впливу на громадян України, матеріалів, що можуть негативно вплинути на просування іміджу України як держави або українських державних інституцій, а також інформаційних матеріалів, які сприяють просуванню наративів противника чи реалізації його завдань в інформаційному просторі.

Шляхом організації відповідних редакцій та реалізації редакційної політики, а також участі представників інших компетентних інституцій, у ході збільшення кількості інформаційного контенту унеможливити витік державної таємниці, конфіденційної інформації, даних, що можуть негативно плинути на стан захищеності життя і здоров'я громадян України, загрожувати безпеці операцій або особистій безпеці.

Перспектива подальшого дослідження вбачається у вивченні проблематики функціонування та розбудови механізмів державного управління у сфері захисту безпеки інформаційного простору психологічного та соціального характеру.

Список використаної літератури:

1. Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України: Наказ Міністерства оборони України № 612 від 22.11.2017. https://zakon.rada.gov.ua ; URL: https://zakon.rada.gov.ua/rada/show/v0612322-17#Text (дата звернення 29.06.2024 р.).
2. Доктрина зі стратегічних комунікацій Збройних Сил України: наказ Головнокомандувача Збройних Сил України від 12.10.2020 року № ВКП 10-00(49).01. [Електронний ресурс]. Сили територіальної оборони ЗСУ. URL: https://sprotyvg7.com.ua/wp-content/uploads/2022/04/%D0%92%D0%9A%D0%9F-10-0049.01-%D0%94%D0%BE%D0%BA%D1%82%D1%80%D0%B8%D0%BD%D0%B0-%D0%B7%D1%96-%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%87%D0%BD%D0%B8%D1%85-%D0%BA%D0%BE%D0%BC%D1%83%D0%BD%D1%96%D0%BA%D0%B0%D1%86%D1%96%D0%B8%CC%86.pdf (дата звернення – 29.06.2024).
3. Юськів Б., Карпчук Н., Пелех О. Структура стратегічних комунікацій як основа ефективного комунікаційного менеджменту України в умовах війни. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2023, № 2 (16). С. 92–118. DOI: https://doi.org/10.29038/2524-2679-2023-02-92-118 (дата звернення – 29.06.2024).
4. Благодарний А., Кононець О. Стратегічні комунікації у секторі безпреки і оборони України. *Національна безпека.* 2023. № 1. С. 5–9. DOI: https://doi.org/10.32839/2304-5809/2023-1-113-2 (дата звернення – 29.06.2024).
5. Войтко О., Єргідзей К., Сіманський Д. Спроможності Сил оборони України щодо виробництва медіаконтенту у процесі стратегічних комунікацій – практичний аспект. *Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи* : тези доповідей IV міжнародної науково-практичної конференції. 2023. С. 58–60. URL: http://repositsc.nuczu.edu.ua/bitst23456789/18942/1/2_530094898863408430O.pdf#page=30 (дата звернення – 29.06.2024).
6. Зінорук М. Чинники впливу на забезпечення державної безпеки україни на сучасному етапі. *Науковий юридичний журнал*. 2023, № 1. С. 7–16. DOI: https://doi.org/10.32782/ln.2023.21.01 (дата звернення – 29.06.2024).
7. Косогоров О. Модель динаміки інтенсивності інформаційного впливу для виявлення цілеспрямованих інформаційних атак. *Наукові орієнтири: терия та практика досліджень* : матеріали III міжнародної наукової конференції. 2024. С. 184 – 189. DOI: https://doi.org/10.62731/mcnd-17.05.2024.007. (дата звернення – 29.06.2024).
8. Руснак Ю., Стужук Ю. Стратегічне інформаційне управління в системі безпеки та оборони: інтеграція та оптимізація. *Збірник наукових праць Національної академії Державної прикордонної служби України*. 2024, № 1 (том 94). DOI: https://doi.org/10.32453/3.v94i1.1584 (дата звернення – 29.06.2024).
9. Прокопенко О. Технологічні аспекти удосконалення інформаційно-аналітичного забезпечення моніторингу інформаційного простору. *Воєнні конфлікти та техногенні катастрофи: історичні та психологічні наслідки* : збірник тез III Міжнародної наукової конференції. 2023. С. 159–162. URL: https://elartu.tntu.edu.ua/bitstream/lib/40929/1/Zbirnyk_tez_konferentsiyi_2023.pdf#page=161 (дата звернення – 29.06.2024).
10. Доктрина стратегічних комунікацій Національної гвардії України: ВКП НГУ. Наказ командувача Національної гвардії України від

22.11.2021 № 541. [Електронний ресурс] Національна гвардія України. URL: https://ngu.gov.ua/wp-content/uploads/2022/12/vkp-11-0101.01-doktryna-strategichnyh-komunikaczij-ngu.pdf.pdf (дата звернення – 29.06.2024).
11. NATO standard AJP-10.1. Allied Joint Doctrine for information operations. january 2023. URL: https://assets.publishing.service.gov.uk/media/650c03bf52e73c000d9425bb/AJP_10_1_Info_Ops_UK_web.pdf (дата звернення – 30.06.2024).
12. Недохлєбов І. Інформаційна безпека України в умовах сучасних загроз: організаційно-правові аспекти. // [Електронний ресурс]. Автореферат дисертації. – 2024. URL: http://phd.znu.edu.ua/page/aref/03_2024/Nedokhlebov_avtoreferat.pdf (дата звернення – 30.06.2024).

Kydriavskyi I. V. Formation of the strategic communications system in Ukraine

The task of rationally forming the organizational structure of the components of public administration in the field of information space security is complex and relevant for any country in the modern world. The repulsion by the Ukrainian defense forces of a large-scale Russian invasion, to ensure which the enemy is actively using the entire arsenal of forms and means of destructive information and psychological influence, makes this task even more difficult, but at the same time, critically important for our state.

Public administration in the field of information space security by its nature does not provide for ideal solutions or easy ways. Especially if the protection of the security of the information space of the state and the individual is based on the formation of a system of strategic communications, active participation in the processes of information exchange and filling the information space of civil society institutions.

Insufficient coordination between the subjects of information space content in the conditions of constant destructive information and psychological influence of the enemy leads to low efficiency of mechanisms for protecting the security of the information space. Excessive centralization leads to a violation of democratic principles, dissatisfaction of the audience and, as a result, creation of a favorable atmosphere for the enemy to implement its information and psychological actions and propaganda. It is even worse when unreasonable restrictions and attempts at excessive control of the information space by those in power are combined with insufficient coordination of efforts between government agencies and civil society institutions, as well as within the public administration system in the field of information space security.

The purpose *of the proposed study is to find ways to improve the efficiency of public administration mechanisms in the field of information space security protection by analyzing organizational problems and ways to solve them.*

The objective *of the study is to analyze scientific works, official reports and journalistic materials, regulations and other sources that provide an opportunity to study organizational issues in the formation and functioning of public administration mechanisms in the field of information space security protection in the context of repulsing the Russian large-scale invasion by the Ukrainian Defense Forces.*

The scientific novelty *of the study and its results lies in a comprehensive consideration of the problematic issues of the organizational nature of modern public administration in the field of information space security protection in Ukraine with an emphasis on the realities of deploying a system of strategic communications, in particular, information actions aimed at reducing the effectiveness of the enemy's destructive information and psychological influence, which are implemented in the context of repulsing the Russian large-scale invasion by the Ukrainian Defense Forces.*

Methodology*. The following methods of scientific research were used in the course of the study: historical, comparative analysis, retrospective analysis, analysis and synthesis, deduction, induction, systemic and structural, linguistic, and formal logical.*

The conclusions *note that one of the key reasons for the enemy's information advantage and, accordingly, the inadequate state of protection of the security of Ukraine's information space is the lack of the necessary quantity and quality of information content produced in the course of the implementation of Ukraine's strategic communications. This state of affairs is a consequence of the lack of proper organization of information content production, rules and conditions for its creation, as well as the absence of criteria for personnel selection for positions related to the implementation of strategic communications. At the national level, the organizational reason for the problems of information space security is the adoption of the idea of building a system of strategic communications as the basis for the development of the state information policy, while ignoring its important element – media operations in the sense of targeted, timely and reliable information of high artistic quality in sufficient quantity.*

With a view to restoring parity and, in the long run, gaining an information advantage over the enemy, raising the level of media culture and media literacy of Ukrainian citizens, which will contribute to the security of the information space, the information component of Ukraine's national security and the personal information security of its citizens, it is proposed to take specific measures to increase the amount of high-quality reliable information content and its prompt dissemination.

Key words: *public administration, information space, information warfare, strategic communications Russian aggression, information and psychological influence.*