МЕХАНІЗМИ ПУБЛІЧНОГО УПРАВЛІННЯ

УДК 351.746:007
DOI https://doi.org/10.32782/pdu.2024.3.11

І. В. Кудрявський
докторант
Міжрегіональної Академії управління персоналом
ORCID ID: 0009-0009-5167-7648

СТРАТЕГІЇ НАПАДУ З АКТИВНИМ ЗАСТОСУВАННЯМ ДІЙ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Формування механізмів державного управління у сфері захисту безпеки інформаційного простору вимагає досконалих знань та належного розуміння дій реального і потенційних противників, принципів та механізмів, при застосуванні яких реалізовуються сучасні операції впливу і ведеться когнітивна війна.

Історичний досвід нападу й захисту на основі інформаційної діяльності часто не відповідає сучасним умовам але є важливим підґрунтям для розуміння окремих аспектів функціонування інформаційного простору.

Мета запропонованого дослідження – пошук способів підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору через аналіз історичних та сучасних стратегій нападу із застосуванням інформаційних дій.

Завдання дослідження полягає в аналізі історичних джерел, наукових праць, офіційних повідомлень та публіцистичних матеріалів, що надають можливість вивчити проблематику функціонування механізмів державного управління у сфері захисту безпеки інформаційного простору в умовах відбиття Силами оборони України російського широкомасштабного вторгнення при інтенсивному застосуванні учасниками наповнення інформаційного простору стратегій нападу.

Наукова новизна дослідження і його результатів полягає у комплексному розгляді проблемних питань сучасного державного управління у сфері захисту безпеки інформаційного простору України, пов'язаних з активним веденням учасниками наповнення інформаційного простору інформаційних дій в рамках стратегій нападу.

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 сформульовані пропозиції щодо конкретних організаційних заходів, які можуть підвищити ефективність протидії деструктивному інформаційно-психологічному впливу із застосуванням стратегій нападу в інформаційному просторі в умовах російсько-української війни.

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

Постановка проблеми. Радянська пропаганда з її тоталітарною системою та боротьбою проти «загниваючого Заходу», «військовими загрозами НАТО» еволюціонувала в російський авторитаризм. Як результат, сформувався новий різновид тоталітарної ідеології – рашизм, який увібрав традиції радянського комуністичного режиму, фашистського націоналсоціалізму та російського шовінізму з просуванням імперського «руского міра», комплексним застосуванням військових сил, політичних, економічних, інформаційних та інших засобів, які реалізуються шляхом активного застосування протестного потенціалу населення та можливостей сил спеціаль-

них операцій. При цьому радянсько-російська пропаганда в національному просторі сукупно з глибокою інтеграцією медіа в політичний капітал легітимізовувала таємні політичні рішення еліт, сприяла зведенню інтересів медіа, фінансово-економічних та політичних еліт і проросійської влади на місцях у цілих регіонах. Це створило належні умови для цілеспрямованих атак із використанням сучасних інформаційних технологій, систематичних інформаційних маніпуляцій та дезінформації Кремля. Як наслідок, було підготовлене позитивно-схвальне ставлення до путінсько-російської авторитарної системи [1, с. 41]. Причому, це стосується не тільки внутрішньої російської аудиторії, на яку працювала російська пропаганда, передусім щоб забезпечити підтримку своєї агресивної політики, але й цільових аудиторій на територіях інших держав, де необхідно було послабити потенціал майбутнього спротиву та оборонні можливості в рамках підготовки майбутньої експансії.

При формуванні російської школи агентурно-підривної роботи на території інших країн та тісно пов'язаної з нею традиції проводити дестабілізуючі дії шляхом активності в інформаційному просторі відіграли свою роль не лише столітні традиції ведення агресивної політики, але й поєднання напрацювань найбільш кривавих історичних систем та утворень, від яких відмовилися суспільства й уряди демократичних країн цивілізованого світу. У цьому контексті як власний, так і запозичений історичний досвід, у поєднанні з можливостями сучасних інформаційно-комунікативних технологій, дозволили сформувати й реалізувати небезпечну стратегію нападу, що обумовлює серйозний виклик у сфері захисту безпеки інформаційного простору для Сил оборони України зокрема та української держави загалом.

Аналіз досліджень і публікацій. Інформаційний матеріал, необхідний для аналізу, міститься в наукових працях, зокрема українських дослідників, таких як: Соломін Є., Живоглядов Ю., Калінічева Г., Бебик В., Гапеєва О. [1, 2, 3, 4, 11]; міжнародних нормативно-правових актах [9, 10]; публікаціях у медіа [5, 6, 7, 8]; офіційних звітах державних організацій [12].

Мета запропонованого дослідження – пошук способів підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору через аналіз історичних та сучасних стратегій нападу із застосуванням інформаційних дій.

Виклад основного матеріалу дослідження з обґрунтуванням отриманих результатів. Інформаційно-психологічна війна, яку в засобах масової інформації росія веде проти України, охоплює широкі верстви населення російського суспільства. Державні або тісно пов'язані з державою російські суб'єкти наповнення інформаційного простору активно застосовують технології, які впливають на психологічний стан та свідомість власного населення. З метою просування кремлівських закликів та пропаганди «руского міра» широко використовуються наративи, що базуються на вигаданих чи маніпулятивних актах і подіях. Проведений спеціалістами з нейролінгвістики та психосугестивних впливів психологічний аналіз жертв російської пропаганди – російських військовослужбовців – дав досить однозначні результати. Значення, якими російський окупант наповнює свою поведінку, цілком належать міфологемам відсутність суб'єктності та усвідомленості може свідчити про його конфліктну самосвідомість, ідентичність блокована цілковитою залежністю від міфологічних концептів. Психологічна навігація (сприйняття та розуміння) того, що відбувається, жорстко обмежено мисленнєвими механізмами, тобто образи сприйняття викривлені навіюваннями, більш нафантазовані, ніж реальні, психологічними джерелами ідентичності є міфи та меми. Втрата вибору власної ідентичності, котра є наслідком цих особистісних деформацій, позбавляє російських військовослужбовців (а вірогідно і значну частину інших громадян) можливості відновлення та розвитку особистості [2. с, 234]. Безумовно, російський військовослужбовець-окупант (а саме така категорія була проаналізована у згаданому дослідженні) є представником цільової аудиторії, до якої система пропаганди має якнайкращий доступ і над якою російська

державна тоталітарна машина володіє якнайкращим контролем. Тому наслідки у вигляді фактично повної втрати суб'єктності (стирання особистості) та перетворення людського організму в інструмент із добре керованою мотивацією не здається чимось неймовірним.

Варто враховувати, що внутрішня російська пропаганда спрямована на утримання влади в тоталітарній державі та підготовку контингенту для зовнішньої експансії. Попри жорстку заідеологізованість не варто недооцінювати розумових можливостей та потенційної небезпечності такого контингенту. Тим більше, що ключові негативні мотиваційні напрямки в умовах будь-якого воєнного конфлікту – страх смерті і жадоба наживи – активно підтримуються російською пропагандою серед власного особового складу та мобілізаційного контингенту. У тому, що стосується небезпечності для мирного населення здійснення військових злочинів, швидкості прийняття рішень без огляду на обставини, – в усі часи та історичні епохи фанатики без чітко вираженої власної особистості проявляли неймовірну активність, виключну жорстокість та особливий цинізм за принципом доцільності та впевненості у власній ідеальності (безгрішності) в рамках нав'язаної «системи цінностей». Найбільш ефективним та оперативним засобом захисту від такого контингенту традиційно була і залишається його фізична нейтралізація (збройне стримування силами оборони держави). Але це зовсім не знімає питання пошуку слабких сторін особового складу противника, який піддається інтенсивному деструктивному інформаційно-психологічному впливу пропаганди власної держави, боротьби за перевагу в інформаційному просторі, передусім – когнітивну перевагу на тактичному, оперативному і стратегічному рівні.

Забезпечення тилів (підтримка агресивної експансивної політики власним населенням та готовності особового складу власних військових і терористичних формувань виконувати завдання без огляду на обставини, включно з грубим порушенням Міжнародного Гуманітарного Права та неприхованими військовими злочинами) – безумовно важливий етап інформаційного забезпечення у стратегії нападу, але це лише підготовка. Не менш важливе місце в інформаційній діяльності, яка забезпечує реалізацію стратегій нападу, займає деструктивний інформаційно-психологічний вплив на аудиторії в інших країнах. Перш за все – деморалізація населення та особового складу сил оборони противника. При цьому широко використовуються будь-які внутрішні розбіжності, протестний та конфліктний потенціал. В другу чергу – дезінформування урядів та суспільств третіх країн, легітимізація власних дій, вплив на ключових лідерів у міжнародній політиці.

Наприкінці XX ст. національний Інститут Оборони США опублікував роботу Мартіна Ч. Лібікі «Що таке інформаційна війна?». Автор виокремив сім форм інформаційної війни. Командно-управлінська, яка спрямована на канали зв'язку між командуванням та виконавцями і має на меті позбавлення управління. Розвідувальна війна – збір стратегічно важливої військової інформації та захист власної. Електронна війна, що спрямована проти засобів електронних комунікацій, – радіозв'язку, радіолокаційних станцій, комп'ютерних мереж. Психологічна війна, яка використовує пропаганду та інформаційно-психологічний вплив на свідомість населення. В її структурі виокремлено чотири основних напрями: підрив громадянського духу, деморалізація збройних сил, дезорієнтація командування та війна культур. Хакерська війна має на меті здійснення диверсійних дій проти цивільних об'єктів противника та захист від таких дій (дії проти військових розцінюються як електронна війна). Зброя хакерів, на думку Мартіна Лібікі, – це комп'ютерні віруси. Економічна інформаційна війна, яка існує у двох формах – інформаційної блокади та інформаційного імперіалізму. Кібервійна, на відміну від хакерської війни, передбачає захоплення комп'ютерних даних, що дозволяють вистежити ціль (особу) або шантажувати її. В окремий специфічний напрямок виділено семантичні атаки [3, с. 56]. Зараз, через чверть століття, ми можемо оцінити прогноз як доволі точний. Більше того, практично усі складові стра-

тегії нападу інформаційної війни сучасності у праці М. Лібікі промальовуються достатньо точно. Єдине, що не прописується у прогнозі американського військового дослідника, але активно застосовується на практиці російськими військово-терористичними та псевдодипломатичними формуваннями, – це диверсійно-підривна діяльність, убивства, залякування, підкуп та вербування, які за фактом не лише дають розвідувальну інформацію для планування заходів психологічного впливу, але й самі по собі застосовуються у якості вагомого елемента деструктивного інформаційно-психологічного впливу. Це пояснюється зокрема «національними особливостями» і «традиціями» нашого ворога, для якого необґрунтована жорстокість та порушення правил ведення війни традиційно було окремим способом психологічного впливу.

Російські стратегії нападу в інформаційному просторі тісно пов'язані з традиціями ведення гібридної війни тоталітарних режимів минулого. У так званій громадянській війні в Іспанії на боці республіканців (головна сепаратистська база – Каталонія) воювали переодягнені в іспанську форму радянські (читай – російські) офіцери і солдати, а на боці армії Франко – переодягнені у відповідну форму німецькі військові. Перемогли, як відомо, німці та іспанські фашисти. В цей же час Радянський Союз і Німеччина активно (і стратегічно) дружили диктаторами (Іосіф Сталін, Адольф Гітлер), арміями (РСЧА, Вермахт) і спецслужбами (НКВС, Гестапо). Аналогічно діяв СРСР і в Китаї, де підтримував Компартію Китаю (голова – Мао Цзедун) в боротьбі проти легітимного президента Китайської республіки (Чан Кайші). Російські «добровольці» теж були перевдягнені в китайську форму, так само мали фальшиві документи, воювали на російських літаках і танках, вдаючи із себе учасників китайської «громадянської війни» [4]. До слова, в ході російсько-української війни росіяни також використовують українську форму під час штурмів, що неодноразово фіксувалося учасниками бойових дій [5], Генеральним штабом Збройних Сил України [6], Уповноваженим Верховної Ради України з прав людини [7] на різних ділянках фронту та в різний час [5, 7, 8]. Представники російських військово-терористичних формувань традиційно ігнорують пункт f статті 23 IV Женевської конвенції (Положення про закони і звичаї війни на суходолі) [9] та п. 2 ст. 39 Додаткового протоколу до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів [10], які прямо забороняють такі дії.

Багато традиційних засобів політичної експансії та гібридної агресії, випробуваних та перевірених протягом минулих століть, застосовуються і сьогодні. Це зокрема незаконна видача паспортів громадянам інших держав з наступним проголошенням «захисту громадян нашої нації, мови, релігії» та інші засоби інфільтрації. Застосування російськими пропагандистами тез про захист російського світу та російськомовних громадян інших країн є одним з типових прикладів застосування такої методики. Далі розвиток подій може бути найрізноманітніший: відкрита інтервенція, проголошення маріонеткової квазідержави, яка фактично стає озброєним анклавом під контролем агресора, дестабілізація ситуації на території противника шляхом розгортання під виглядом сепаратистського «визвольного» руху своїх напіврегулярних військово-терористичних формувань та парамілітарних утворень, що, крім усього іншого, створює надзвичайно сприятливі умови для роботи кадрових співробітників спецслужб. Послідовність та порядок таких дій у кінцевому рахунку не має особливого значення для країни – жертви нападу, хоча і може певним чином впливати на результативність перелічених заходів. Але всі вони стають можливими за достатньо активного інформаційного прикриття та при ефективній реалізації інформаційної складової загалом. Пори те, що у російсько-українській війні українці не поспішали без крайньої необхідності отримувати паспорти країни-агресора, активна, як внутрішня так і зовнішньо спрямована, пропаганда дозволяла російському воєнно-політичному керівництву тривалий час реалізовувати стратегію нападу, не зустрічаючи особливих перешкод з боку міжнародної спільноти та міжнародних організацій.

У XXI столітті, коли роль інформаційних технологій зростає достатньо, щоби без них уже було неможливо уявити собі звичайних повсякденних побутових процесів, набувають зовсім нових значень електронна війна та кібератаки. Аналіз причин, умов, перебігу та результатів російсько-грузинської війни 2008 р. свідчить, що, окрім традиційних суто воєнних методів впливу, у серпневій кампанії було застосовано потужні засоби інформаційного протиборства, зокрема цілеспрямовані дії в кіберпросторі. Деякі джерела містять інформацію, що перші DDoS-атаки на офіційний сайт Президента Грузії відбулися задовго до початку воєнних дій – 20 липня 2008 р. А в період із 7 по 16 серпня 2008 р. внаслідок потужних хакерських атак на інформресурси країни заблоковано сайти Президента Грузії, Національного банку та агенцій новин. Атака на сайт Президента Грузії здійснювалась одночасно з 500 IP-адрес. На сайті Міністерства закордонних справ Грузії тривалий час розміщувався колаж із чорно-білих фотокарток М. Саакашвілі й А. Гітлера. Яскравим прикладом однієї з результативних кібероперацій стала зміна хакерами курсу національної грузинської валюти – ларі, унаслідок чого впала її цінність. Західні фахівці стверджують, що внаслідок кібератак перервано обмін інформацією між підрозділами ЗС Грузії. Методи й алгоритми шифрування, які при цьому застосовувалися, свідчать про заздалегідь сплановану та добре скоординовану операцію, яку потрібно розглядати як самостійну складову російсько-грузинської інформаційної війни. [11, с. 116]. Поряд з цим, задум кібероперацій був, очевидно, підпорядкований загальній стратегії нападу, а дії в кіберпросторі мали на меті досягнути психологічних ефектів, зокрема й у когнітивній сфері.

Відмінною рисою інформаційних операцій під час російсько-грузинської війни 2008 р. стали цілеспрямовані атаки не лише на сайти органів державної влади й об'єкти критичної інфраструктури Грузії, але й на портали інформаційних агенцій, новинні сайти, що позбавило світову спільноту можливості оперативно отримувати достовірну інформацію про події, які відбуваються. Внаслідок блокування інформаційних ресурсів Грузії виникла ситуація штучно створеної міжнародної ізоляції країни з одночасним веденням проти неї бойових дій [11, с. 117]. Застосування технічних спроможностей для отримання переваги в інформаційному просторі шляхом забезпечення власних можливостей деструктивного інформаційно-психологічного впливу та зниження можливостей інших суб'єктів щодо реагування на такий вплив інтенсивно застосовується російськими окупантами і в ході широкомасштабного вторгнення в Україну.

Цікаво, що, за даними Оперативного центру реагування на кіберінциденти державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України, у першому кварталі 2023 року помітно (з різницею у 1.5–2.9 разу для різних секторів) знизилась кількість атак, організованих проросійськими угрупованнями хактивістів, націлених на комерційний, фінансовий сектор, уряд та місцеві органи влади, сектор безпеки та оборони (порівняно з IV кварталом 2022 року). У цей же період інтенсивність атак на сектор енергетики та Засоби масової інформації залишається на тому ж рівні [12, с. 3]. Очевидно, що енергетична інфраструктура визначена противником як центр гравітації, при виведенні з ладу якого можна отримати дуже суттєву перевагу, а може навіть перемогу, стратегічного чи, щонайменше, оперативного рівня. Поряд з цим, важливішими цілями для російських хакерів, навіть у порівнянні з ресурсами органів державної влади та Сил оборони України, за сталою кількістю атак залишаються медіа (засоби масової інформації). Наведений досвід російської інтервенції до Грузії у 2008 році свідчить про те, що подібна ситуація зовсім не є випадковою. Така пріоритетність у постановці цілей російським кіберпідрозділам, коли чиниться всебічний вплив і тиск на медіасферу, повністю відповідає концепції підпорядкування технічних можливостей потребам деструктивного інформаційно-психологічного впливу і стратегії, спрямованій на отримання в кінцевому результаті інформаційної, психологічної та когнітивної

переваги у когнітивній війні, яку свідомо ведуть російські окупанти. Наявність і втілення в життя такої наступальної стратегії в інформаційній сфері змушує більш ніж серйозно ставитися до ворога, його небезпечності, латентності (прихованості) його дій, і тих завдань, які постають в ході формування та розвитку українських механізмів державного управління у сфері захисту безпеки інформаційного простору.

Враховуючи, що медіасфера, журналісти, представники культури та мистецтва були, є і залишаються пріоритетними цілями російських окупантів не лише при застосуванні дій у кіберпросторі, але й при реалізації інших спроможностей силового блоку терористичної держави, що нерідко виливається у відверті військові або просто кримінальні злочини, для збереження українського мовного, культурного, та зрештою – інформаційного, середовища, необхідна суттєва державна підтримка і створення відповідних умов для митців та спеціалістів інформаційної сфери, аж до їх фізичного захисту від замахів в окремих випадках.

При цьому необхідно враховувати, що росіяни активно реалізовують у всіх своїх операціях, передусім якщо це стосується здобуття інформаційної та когнітивної переваги, ресурс спецслужб, вербування контингенту в силах оборони та цивільних державних інституціях держави противника, потенціал агентурно- і диверсійно-підривної роботи. Виявити, а тим більше – притягнути до юридичної відповідальності, агентів впливу, в яких противник роками вкладав фінансові засоби, розвиваючи їхні репутаційні спроможності повноваження і зв'язки, буває досить не просто. Агенти впливу зазвичай ефективно користуються в аспектах, у яких їм це вигідно, демократичними правами, свободами та гарантіями для забезпечення власної недоторканності, достатньо вільно при цьому трактуючи і легко порушуючи законодавство в ході виконання своїх основних функцій. Як наслідок, на жаль, доводиться констатувати, що державна політика і державні механізми, які повинні забезпечувати належні умови для розвитку та повноцінного функціонування національного інформаційного середовища (включно з професійними засобами масової інформації, конкурентними творами мистецтва, зокрема й сучасними, популяризацією традиційних культурних надбань і створенням середовища для зародження нових) залишають бажати кращого. Лобіювання російськомовних та російських музики, фільмів та серіалів, літератури найрізноманітніших жанрів і створення атмосфери повної неможливості реалізувати свій потенціал для українських митців інакше, як за власний кошт і з подоланням бюрократичних перешкод, створених представникам держави й політикою так званих «авторитетів» у сфері шоу-бізнесу, безумовно, було частиною добре профінансованої та жорстко організованої експансивної інформаційної політики.

Орієнтація ворога на здобуття когнітивної переваги з подальшою ліквідацією самоідентифікації та національної ідентичності населення, як це було зроблено в ході знищення особистостей представників особового складу російських окупаційних військово-терористичних формувань, виводить питання захисту безпеки інформаційного простору України за межі моніторингу інформаційного простору, протидії окремим заходам деструктивного інформаційно-психологічного впливу, і навіть системи стратегічних комунікацій в цілому. Адже яким би досконалим не було вивчення питання та наукове обґрунтування майбутніх змін механізмів державного управління захистом безпеки інформаційного простору у середньо– й довгостроковій перспективі, російські агенти впливу, які діють свідомо, а в окремих випадках і ті, які самі залишаються жертвами ворожої пропаганди чи перебувають під постійним психологічним впливом кураторів (коучів, священників російської православної церкви, начальників на місцях роботи тощо), чинитимуть запеклий опір будь-яким конструктивним змінам, застосовуючи для цього весь традиційний потенціал системно-бюрократичного саботажу, добре відомий і неодноразово перекладений різними мовами в ході різних воєнних конфліктів.

Сама стратегія нападу противника, з яким доводиться мати справу Силам оборони України, передбачає власне

напад у вигляді інтенсивної пропаганди та деструктивного інформаційно-психологічного впливу, заходи нейтралізації, нерідко – фізичної, колективів і особистостей, які здатні формувати конкурентний контент та наповнювати національний інформаційний простір, сприяючи розвитку критичного мислення аудиторій, і, в обов'язковому порядку, регулярний контроль за процесами руйнації будь-яких, навіть перспективних, організаційних структур державного управління, здатних протистояти заходам російської інформаційної експансії, або таких, що можуть набути відповідну здатність у майбутньому.

Враховуючи активне застосування противником можливостей розвідки для забезпечення своєї інформаційної діяльності та власне деструктивного інформаційно-психологічного впливу, недбале ставлення осіб, які приймають рішення, що впливають на функціонування механізмів державного управління у сфері захисту безпеки українського інформаційного простору та інформаційної безпеки громадян України до питань наповнення інформаційного простору, ігнорування контррозвідувальних можливостей, які могли б хоча б на своїй території частково урівноважити шанси у боротьбі за інформаційну та когнітивну перевагу, на жаль продовжують мати місце і викликати негативні наслідки.

Безумовно, спроможності деяких складових сил оборони України, особливо тих, які мають повноваження здійснювати оперативно-розшукову діяльність, достатньо сильно завантажені за іншими напрямками діяльності. Крім того, їх застосування вимагає досить суворого дотримання законодавства, навіть в умовах воєнного стану, та демократичних принципів, що забезпечують права і свободи громадян. Як застосовувати розвідувальні та контррозвідувальні органи в питаннях боротьби за інформаційну і, зрештою, когнітивну, перевагу,– це окреме питання, яке потребує ретельного вивчення. Але відмова від застосування таких інституцій на фоні активної реалізації противником у боротьбі за когнітивну перевагу потенціалу аналогічних структур, навіть під приводом дотримання демократичних принципів (як і під будь-яким іншим приводом) є не чим іншим, як злочином у формі бездіяльності проти власної держави, власного народу і, зрештою, банальною дурістю.

Висновки і пропозиції. Стратегії нападу, в основі яких покладена інформаційна діяльність, ґрунтуються на історичних надійних перевірених бойових прийомах, які часто суперечать звичаям ведення війни, а нерідко і правилам, зафіксованим нормами Міжнародного Гуманітарного Права. Поряд із традиційними засобами активно розвиваються нові форми інформаційних дій, пов'язані з можливостями сучасної техніки, передусім – інформаційно-комунікативних технологій. З цим пов'язаний розвиток підходів нападу в інформаційному просторі на тактичному, оперативному і стратегічному рівні. Визначення гібридної війни та інформаційної війни, інформаційних операцій та операцій впливу відрізняються між собою окремими деталями, але їхня послідовна поява у наукових дослідженнях і військовій термінології приховує глибокий сенс переосмислення процесу завдання шкоди противнику та отримання переваги некінетичними засобами.

І представники НАТО та країн-членів НАТО, і російські військові злочинці на сучасному етапі розвитку військової науки приходять до висновків про формування когнітивної війни та ключове значення ефектів інформаційних дій у когнітивному вимірі інформаційного простору. За великим рахунком, після різноманітних зміщень акцентів у напрямку технічних і технологічних сторін процесу ведення бойових дій в інформаційній сфері знову починає приділятися головна увага тому, з чого і починало людство при створенні перших методик обману – смислам, оцінкам, переконанням, ставленню, світогляду та, власне, процесу прийняття рішень. Поки що з двох основних складових інформаційної війни – інформаційно технічного та інформаційно-психологічного впливу – основна увага багатьма державами та збройними формуваннями продовжує приділятися захисту і нападу в інформаційно-технічній сфері. Попри це, практика ведення найбільш масштаб-

ної війни XXI століття показує, що наш ворог – керівництво російських військово-терористичних формувань – застосовує величезний спектр спроможностей, включаючи агентурно-підривні, розвідувально-диверсійні та інформаційно-технічні, у боротьбі за інформаційну перевагу з акцентом на когнітивну перевагу на стратегічному рівні та з метою забезпечення ефективного деструктивного інформаційно-психологічного впливу на оперативному рівні.

Як особливо небезпечних для реалізації своєї стратегії нападу в інформаційній сфері та ведення когнітивної війни об'єктів сам ворог, за півтисячолітньою традицією, визначив освітні і творчі колективи, а також особистостей, які здатні продукувати якісний інформаційний контент, починаючи від оперативно-інформативного й медійно-побутового і закінчуючи творчим у найрізноманітніших сферах, формуючи конкурентний національний інформаційний простір. Це обумовлює витрату противником значних зусиль та ресурсів на реалізацію заходів нейтралізації українських медіа-об'єктів, інтелектуальних еліт, починаючи від дій у кіберпросторі і завершуючи військовими, кримінальними злочинами, терористичними актами індивідуальної спрямованості.

Особливості стратегій нападу з активним застосуванням інформаційної діяльності, безумовно, повинні враховуватися при формуванні та організації функціонування механізмів державного управління у сфері захисту безпеки інформаційного простору. В умовах відбиття Силами оборони України російського широкомасштабного вторгнення найбільш актуальним з позиції побудови механізмів державного управління є дослідження стратегій нападу російських військово-терористичних окупаційних формувань та логіки побудови російських воєнних та воєнно-інформаційних стратегій.

Враховуючи викладене, з метою підвищення ефективності функціонування механізмів державного управління у сфері захисту безпеки інформаційного простору, вважаю за доцільне:

Передбачити механізм підтримки діяльності, спрямованої на отримання когнітивної переваги та інформаційної переваги, шляхом використання спроможностей органів та підрозділів, уповноважених на здійснення оперативно-розшукової діяльності, причому як у розвідувальній, так і в контррозвідувальній сфері.

Не обмежуватися механізмами пасивного захисту безпеки інформаційного простору, а зосередити діяльність частини підрозділів державних структур при залученні неурядових організацій для вивчення протиріч та уразливостей атомізованого суспільства тоталітарної держави противника з метою побудови активної інформаційної діяльності, яка спонукала б поневолені народи російської федерації більш активно проявляти свою національну ідентичність, в оптимальному варіанті – боротися за власні права, майбутній демократичний устрій своїх національних держав, відстоювати свої релігійні переконання, мову, традиції та прагнення до самостійності, за необхідності – шляхом масштабних збройних виступів проти центрального тоталітарного державного керівництва в рамках визнаного ООН права народів на самовизначення.

Вжити заходів щодо підтримки колективів та окремих осіб – суб'єктів наповнення інформаційного простору якісним конкурентним інформаційним контентом з метою забезпечення формування потужного національного інформаційного середовища. Особливу увагу приділити забезпеченню належних умов діяльності журналістів, а також осіб та організацій, що створюють культурне надбання й інформаційний продукт у традиційних та сучасних формах: книговидавництво, кінематограф, комп'ютерні ігри, наповнення соціальних, електронних медіа та інтернет-простору загалом.

Акцентувати увагу на діяльності підрозділів захисту безпеки інформаційного простору та інформаційної безпеки громадян України у когнітивній сфері шляхом побудови роботи повного циклу – від вивчення ситуації до створення та поширення інформаційного контенту компетентними спеціалістами, не просто інтегрованими у свій інформаційний простір та інформаційний простір противника, але й такими, які мають постійний практичний

досвід спілкування з представниками відповідних аудиторій.

Посилити контроль, зокрема правоохоронних органів, кіберполіції за видами діяльності, які передбачають когнітивний вплив на аудиторії та погіршення критичного мислення аудиторій, у тому числі деструктивний вплив у когнітивній сфері – онлайн-ігри, особливо азартні (онлайн-казино), агресивний маркетинг тощо.

Посилити контроль за створенням та функціонуванням фейкових сторінок у соціальних мережах (сайтів) офіційних органів державної влади України та військових підрозділів, створених противником, за допомогою яких реалізується деструктивний інформаційно-психологічний вплив та збирається розвідувальна інформація.

Акцентувати увагу підрозділів кібербезпеки на протидії заходам противника у кіберпросторі включно з хакерськими атаками, спрямованим на порушення роботи (здобуття інформації для наступного фізичного впливу чи вогневого ураження) українських суб'єктів наповнення інформаційного простору.

Список використаної літератури:

1. Соломін Є. Інформаційна безпека в умовах війни та втручань у медіасередовище. Держава та регіони. 2023. №2 (54). С. 40–47. DOI: https://doi.org/10.32840/cpu2219-8741/2023.2(54).5 (дата звернення 19.07.2024).
2. Живоглядов Ю. Психо-сугестивний аналіз переконань в контексті інформаційно-психологічного впливу російської пропаганди на світогляд та поведінку росіян. Вчені записки університету «КРОК». – 2024. № 1(73). С. 234–243. DOI: https://doi.org/10.31732/2663-2209-2024-73-234-243 (дата звернення 19.07.2024).
3. Калінічева Г. Використання інформаційно-психологічної зброї в умовах російсько-української війни. Acta de historia & politica: saeculum XXI. – 2023. № 6. С. 53–65. DOI: https://doi.org/10.26693/ahpsxxi2023.06.053. (дата звернення 19.07.2024).
4. Бебик В. Інформаційний простір як театр військових дій: війська, зброя, розвідка, контррозвідка. Міжнародні відносини. 2018. № 18–19. URL: http://journals.iir.edu.ua/index.php/pol_n/article/view/3391. (дата звернення 19.07.2024).
5. «З боку росіян бачив всі можливі воєнні злочини». Війна у розповідях британських добровольців, що б'ються за Україну. Суспільне : веб-сайт. URL: https://suspilne.media/donbas/740613-z-boku-rosian-baciv-vsi-mozlivi-voenni-zlocini-vijna-u-rozpovidah-britanskih-dobrovolciv-so-butsa-za-ukrainu/. (дата звернення 20.07.2024).
6. Росіяни одягають українську форму перед штурмом позицій армії України. mil.in.ua. : веб-сайт. URL: https://mil.in.ua/uk/news/rosiyany-odyagayut-ukrayinsku-formu-pered-shturm-pozytsij-armiyi-ukrayiny/. (дата звернення 20.07.2024).
7. Російські окупанти шиють форму ЗСУ: можливі провокації – омбудсмен. Кореспондент : веб-сайт. URL: https://ua.korrespondent.net/ukraine/4475344-rosiiski-okupanty-shyuit-formu-zsu-mozhlyvi-provokatsii-ombudsmen. (дата звернення 20.07.2024).
8. РФ на Таврійському напрямку використовує форму української армії. У ЗСУ розповіли деталі. rbc.ua. : веб-сайт. URL: https://www.rbc.ua/rus/news/rf-tavriyskomu-napryamku-vikoristovuyut-formu-1695658006.html. (дата звернення 20.07.2024).
9. IV Конвенція про закони і звичаї війни на суходолі та додаток до неї: Положення про закони і звичаї війни на суходолі. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/995_222#Text. (дата звернення 20.07.2024).
10. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року. База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/995_199#top. (дата звернення 20.07.2024).
11. Гапеєва О. Інформаційні операції в Інтернет-середовищі як складова російсько-грузинської війни 2008 р. Науковий вісник Східноєвропейського національного університету імені Лесі Українки. 2017. С. 113–121. URL: https://evnuir.vnu.edu.ua/bitstream/123456789/13186/1/23.pdf. (дата звернення 20.07.2024).
12. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки Оперативного центру реагування на кіберінциденти державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України за I квартал 2023 року. Державна служба спеціального зв'язку та захисту інформації України : веб-сайт. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=53656. (дата звернення 20.07.2024).

Kydriavskyi I. Attack strategies with active use of actions in the information space

The formation of public administration mechanisms in the field of information space security requires a thorough knowledge and proper understanding of the actions of real and potential adversaries, principles and mechanisms used to implement modern influence operations and cognitive warfare.

The historical experience of attack and defense based on information activities often does not correspond to modern conditions, but it is an important basis for understanding certain aspects of the functioning of the information space.

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 historical and modern strategies of attack using information actions.

The task of the study is to analyze historical sources, scientific works, official reports and journalistic materials that provide an opportunity to study the problems of functioning of public administration mechanisms in the field of information space security protection in the context of repulsion of the Russian large-scale invasion by the Ukrainian Defense Forces with intensive use of attack strategies by the participants in the information space.

The scientific novelty of the study and its results lies in a comprehensive consideration of the problematic issues of modern public administration in the field of protection of the security of Ukraine's information space related to the active conduct of information actions by participants in filling the information space as part of attack strategies.

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

The article concludes with proposals for specific organizational measures that can increase the effectiveness of counteracting destructive information and psychological influence using attack strategies in the information space in the context of the Russian-Ukrainian war.

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