УДК 351.746:007]:004
DOI https://doi.org/10.51547/ppp.dp.ua/2024.4.5

Кудрявський Іван Володимирович,
докторант
Міжрегіональної Академії управління персоналом
ORCID ID: 0009-0009-5167-7648

ПРОБЛЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ У СФЕРІ ЗАХИСТУ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ, ПОВ'ЯЗАНІ З ДИНАМІКОЮ ТЕХНОЛОГІЧНОГО РОЗВИТКУ

STATE MANAGEMENT PROBLEMS IN THE FIELD OF INFORMATION SPACE SECURITY RELATED TO TECHNOLOGICAL DEVELOPMENT DYNAMICS

Обмін інформацією та комунікативні процеси на всіх етапах розвитку людства виконували не лише побутові утилітарні функції, але й відігравали роль засобів впливу. Навіть коли поширення інформації реалізовувалося шляхом усних переказів, його уже намагалися контролювати. Досвід мандрівних артистів, яких в різних народів могли називати по-різному, коли їм конфіденційно платили за створення і включення у програму виступів тематичних творів мистецтва, або ж навпаки – переслідували через озвучення інформації, що суперечила політиці влади на певній території, відомий в історії та зовсім не рідкісний. З розвитком технологій інформація стала потужним засобом впливу, а в останні десятиліття, без перебільшення, – зброєю.

Технологічний розвиток і технічна можливість для тотального контролю, здавалося б, повинні значно спростити управління інформаційним простором державними структурами. Але, як показує практика, навіть повністю закриті атомізовані суспільства, керовані антидемократичними тоталітарними режимами, все одно залишають можливості для передачі інформації як усередину, так і назовні. Якщо ж мова йде про демократичні держави, які забезпечують своїм громадянам право на обмін інформацією, – питання захисту інформаційного простору, інформаційної безпеки держави та громадянина стає дуже непростим завданням, виконання якого вимагає складної роботи досконалих механізмів державного управління.

Завдання нападу, особливо у сфері, де мало не кожного дня з'являються нові потужні технології, традиційно значно простіше, аніж завдання захисту. Крім того, антидемократичні державні режими, терористичні та злочинні організації, які живуть за рахунок грабунків та вбивств у різних формах, зазвичай можуть дозволити собі серйозні фінансові витрати на засоби інформаційно-психологічного впливу, внаслідок чого стають більш озброєними технологічно, аніж державні структури, які їм протистоять.

Мета *запропонованого дослідження – пошук способів підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору через аналіз проблем, пов'язаних із динамікою технологічного розвитку.*

Завдання дослідження *полягає в аналізі наукових праць, офіційних повідомлень та публіцистичних матеріалів, інших джерел, що надають можливість вивчити проблематику функціонування механізмів державного управління у сфері захисту безпеки інформаційного простору, пов'язану з динамікою технологічного розвитку в умовах відбиття Силами оборони України російського широкомасштабного вторгнення.*

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 динамікою технологічного розвитку 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** *пропонується:*

при формуванні планів розвитку та роботи державних інституцій у стратегічній (довгостроковій) та середньостроковій перспективі враховувати потенційні можливості технологій, які зараз зароджуються або активно розвиваються, але, вірогідно, відіграватимуть значно вагомішу роль у майбутньому;

при довго- та середньостроковому плануванні розвитку державних інституцій, пов'язаних з оборонною та інформаційною сферою, спрямувати зусилля на підготовку умов та заходів, які забезпечать отримання когнітивної переваги у когнітивній війні, з максимальним дотриманням при цьому демократичних принципів державного управління;

у короткостроковій перспективі будувати роботу підрозділів, які здійснюють управління інформаційним простором, інформаційний вплив та протидію інформаційному впливу не лише на підставі результатів автоматизованого чи

іншого моніторингу віртуального інформаційного простору, але й шляхом, як мінімум, вибіркової оцінки когнітивного простору через живе спілкування з доступними аудиторіями, наприклад, шляхом журналістської роботи з ними;

стимулювати теоретичні наукові дослідження та створення спеціального програмного забезпечення на національному рівні, яке дозволить оперативно робити висновки за інформативними індикаторами в ході оцінки віртуального інформаційного простору про зміни у когнітивному вимірі інформаційного простору, оцінювати впливи, їх небезпечність для різних аудиторій, перспективи та оптимальні сценарії нівелювання (зниження ефективності) деструктивних інформаційних впливів;

при формуванні законодавчих вимог та безпосередніх посадових інструкцій для спеціалістів, що працюють з інформаційним впливом та протидією інформаційного впливу, ретельно аналізувати практичний досвід російсько-української війни. Причому, об'єктом аналізу повинні бути як успішні кейси, де дії українських спікерів, медійників та інших суб'єктів наповнення інформаційного простору дозволяли здобути когнітивну перевагу за певною тематикою, так і провальні, в ході яких перевагу отримував ворог. Також необхідно враховувати не лише власні напрацювання, які, безумовно, мають бути пріоритетними з огляду на доступність інформації і наявність спеціалістів, які були безпосередньо залучені до відповідних процесів, але й зовнішню оцінку представників країн-партнерів, які ретельно аналізують події російсько-української війни та у відносно спокійній обстановці роблять кваліфіковані тверезі висновки;

вжити заходів щодо стимулювання критичного мислення та розвитку цифрової грамотності з максимальною, наскільки це дозволяють ресурси і можливості, диференціацією за різними цільовими аудиторіями, враховуючи особливості вразливості цих цільових аудиторій. Для початку пропонується взяти за основу класифікацію цільових аудиторій, стійкість яких необхідно підвищити таким чином, за віком, але в процесі розвитку програм цифрової грамотності цим критерієм не обмежуватися.

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

At all stages of human development, information exchange and communication processes have not only fulfilled everyday utilitarian functions, but also played the role of means of influence. Even when the dissemination of information was realized through oral traditions, there were already attempts to control it. Cases when traveling artists, who could be called differently in different nations, were confidentially paid to create and include thematic works of art in their performance programs, or vice versa, when they were persecuted for voicing information that contradicted the information policy of the authorities in a particular territory, are well-known stories and not at all rare. With the development of technology, information has become a powerful tool of influence, and in recent decades, without exaggeration, a weapon.

Technological development and the technical capability for total control should seem to greatly simplify the management of the information space by government agencies. But, as practice shows, even completely closed atomized societies ruled by anti-democratic totalitarian regimes still leave room for information to flow both in and out. When it comes to democratic states that provide their citizens with the right to exchange information, the issue of protecting the information space, information security of the state and the citizen becomes a very difficult task, which requires the complex work of perfect mechanisms of state governance.

The task of attacking, especially in a sphere where new powerful technologies appear almost every day, is traditionally much easier than the task of defense. In addition, anti-democratic state regimes, terrorist and criminal organizations that live off robbery and murder in various forms can usually afford serious financial costs for information and psychological influence, and as a result, they become more technologically advanced than the state structures that oppose them.

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 by analyzing the problems associated with the dynamics of technological development.*

The task of the study *is to analyze scientific papers, official reports and journalistic materials, and other sources that provide an opportunity to study the problems of functioning of public administration mechanisms in the field of information space security protection related to the dynamics of technological development in the context of repulsion of a large-scale Russian 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 modern public administration in the field of information space security protection in Ukraine related to the dynamics of technological development in the context of repulsion of a large-scale Russian 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 *suggest that:*

when formulating plans for the development and operation of state institutions in the strategic (long-term) and medium-term perspective, take into account the potential capabilities of advanced technologies that are currently emerging or actively developing but are likely to play a much more significant role in the future;

in the long- and medium-term planning of the development of state institutions related to the defense and information spheres, to direct efforts to prepare conditions and measures that will ensure a cognitive advantage in cognitive warfare with maximum compliance with democratic principles of public administration;

in the short term, to build the work of units that manage the information space, information influence and countering information influence not only on the basis of the results of automated or other monitoring of the virtual information space, but also by at least selectively assessing the cognitive space through live communication with accessible audiences, for example, through journalistic work with them;

to stimulate theoretical research and creation of special software at the national level that will allow to quickly draw conclusions based on informative indicators during the assessment of the virtual information space about changes in the cognitive dimension of the information space, to assess the impacts, their danger for different audiences, prospects and optimal scenarios for leveling (reducing the effectiveness of) destructive information influences;

when formulating legislative requirements and direct job descriptions for specialists working with information influence and countering information influence, carefully analyze the practical experience of the Russian-Ukrainian war. The object of analysis should be both successful cases where the actions of Ukrainian speakers, media and other subjects of the information space allowed them to gain a cognitive advantage on a particular topic, and failed cases where the enemy gained an advantage. It is also necessary to take into account not only own developments, which should certainly be a priority given the availability of information and the availability of specialists who were directly involved in the relevant processes, but also the external assessment of representatives of partner countries who carefully analyze the events of the Russian-Ukrainian war and draw qualified, sober conclusions in a relatively calm atmosphere;

take measures to stimulate critical thinking and the development of digital literacy with maximum differentiation by different target audiences, taking into account the specific vulnerabilities of these target audiences, as far as resources and capabilities allow. To begin with, it is suggested that the classification of target audiences whose resilience needs to be strengthened in this way be based on age, but this criterion should not be limited to the development of digital literacy programs.

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

Постановка проблеми. 14 квітня 2022 року Верховна Рада України схвалила заяву, якою визнала геноцидом дії збройних сил росії та її політичного і військового керівництва під час повномасштабного вторгнення в Україну. Це більше, ніж політична декларація, адже вона, у поєднанні з пояснювальною запискою, містить правове обґрунтування, чому діяння росії мають розглядатися як геноцид українського народу [1, С. 14]. На офіційному міжнародному рівні залишалася необхідність доказування геноцидальних намірів у діях російського керівництва та військово-терористичних формувань.

Зрозумівши контекст і значення лексики офіційної російської риторики, якою супроводжуються вбивства, тортури, нелюдське поводження та переслідування українців, русифікація українських дітей та широкомасштабне знищення критичної інфраструктури України, неможливо не побачити геноцидальної сутності російської війни проти України та її народу [1. С. 32].

Свої наміри проводити геноцид українського народу російські державні військово-терористичні формування доводять кожного дня. У якості ресурсів для деструктивного інформаційно-психологічного впливу використовують не лише сучасні інформаційні технології, але й ракетне озброєння високої потужності, яке саме для досягнення психологічного ефекту застосовують з винятковою жорстокістю та особливим цинізмом. Однією з промовистих публічних декларацій чинити проти українського народу саме геноцид, а не якісь інші дії, лише під час масованої ракетної атаки 8 липня 2024 року стали удари російських військових злочинців по дитячій лікарні “Охматдит” [2], пологових будинках “Адоніс” [3] та “Ісіда” [4].

Багато вчених порівнюють путінізм із фашизмом та нацизмом зразка ХХ ст. Вони мають спільні ознаки, такі як культ вождя, культ війни, ксенофобію та расистські ідеї, потужну пропаганду, яка насаджує цю ідеологію населенню. Путінський режим, починаючи з 2014 р. стрімко “дрейфує” від авторитаризму до тоталітаризму, що супроводжується повною деградацією суспільства, культури, науки, освіти, оскільки всі сфери життя країни та соціуму підкоряються режиму та особисто диктатору Путіну [5. С. 34]. Попри те, що російські економічна, соціальна та інші сфери традиційно та обґрунтовано мають репутацію відсталих, орієнтований на зовнішню агресивну експансію тоталітарний режим виділяє значні кошти на технології, пов’язані з веденням війни, внутрішньою пропагандою та зовнішньою політикою геноциду.

У 2022 році Урядова команда реагування на комп’ютерні надзвичайні події CERT-UA зареєструвала та дослідила 2194 кібератаки, з 24 лютого – 1655. Хакери, які співпрацюють з рф, не приховують свою приналежність і не надто використовують проксі сервери та відповідне обладнання, водночас вони фінансуються коштом російської держави [6, С 93]. Цей факт яскраво свідчить про те, що ворог має можливість застосовувати високотехнологічні засоби

нападу, які вимагають роботи вузькоспеціалізованих фахівців. Покриття та стимулювання на рівні держави-терориста дій, які у всьому цивілізованому світі вважаються військовими злочинами (включно з вогневими атаками та кібератаками, спрямованими на об'єкти цивільної інфраструктури), та кількість російських військових злочинців успішно компенсують за необхідності їхню низьку якість і недостатню кваліфікацію.

Але наявністю ворога, який має намір знищити українську державу та український народ, достатньо оснащеного технологічно, щоб стати нашою головною фізичною та інформаційною загрозою, перелік проблемних питань захисту безпеки інформаційного простору не обмежується. Самі по собі інформаційно-комунікаційні технології, поява нових популярних способів та форматів спілкування, зміни у масовій психології, викликані соціальними мережами й тотальною цифровізацією життя, формують нові "правила гри", відкривають нові можливості, але і стають причиною нових серйозних викликів. Кількість інформації уже не дозволяє достатньо ефективно орієнтуватися в інформаційному просторі без застосування засобів цільового пошуку, щонайменше умілого використання загальнодоступних пошукових систем. Вирішення більш складних завдань, відповідно, вимагає належних кадрових, технічних і технологічних ресурсів. Вони не можуть бути підготовлені і залучені миттєво, навіть при наявності значного фінансового ресурсу. Ефективність підготовки й застосування таких ресурсів прямо залежить від кількості і, передусім, якості досліджень за тематикою роботи механізмів державного управління у сфері захисту безпеки інформаційного простору та врахування результатів цих досліджень особами, які прийматимуть і втілюватимуть в життя рішення, від яких залежить підготовка технологічних і програмних інструментів, підготовка фахівців, розгортання та організація роботи відповідних державних інституцій.

Завдання дослідження полягає в аналізі наукових праць, офіційних повідомлень та публіцистичних матеріалів, інших джерел, що надають можливість вивчити проблематику функціонування механізмів державного управління у сфері захисту безпеки інформаційного простору, пов'язану з динамікою технологічного розвитку, 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 та іноземних дослідників, таких як: Азаров Д., Венгер В., Коваль Д., Нуріджанян Ґ., Легкодух В., Парфило О., Као К., Глейстер Ш., Пен Е., Денбі Р., Ронг В., Роваліно А., Бішоп С., Роган Х., Сінгх Сайні Дж., Кокрон А., Еронхайм Л., Паулоскас К., Парахонський Б., Яворська Г., Стрельбицький М., Гринько Л. [1, 5, 6, 7, 8, 9, 10, 11, 12].

Мета запропонованого дослідження – пошук способів підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору через аналіз проблем, пов'язаних із динамікою технологічного розвитку.

Виклад основного матеріалу дослідження з обґрунтуванням отриманих результатів. Динаміка технологічного розвитку створює ситуацію, коли традиційно неповороткі бюрократичні машини державного управління не встигають реформуватися, змінюватися і пристосовуватися до умов та обставин технічного світу, які змінюються і розвиваються значно швидше. Безпекові організації в усьому світі, як державні інституції, так і міжнародні спільноти та військові союзи намагаються тримати руку на пульсі цих процесів, формувати стратегії свого розвитку з урахуванням світових тенденцій, зокрема і тих, які стосуються інформаційного простору. Природно, у контексті відбиття Силами оборони України російської агресії цікава позиція Північноатлантичного Альянсу, який протягом багатьох десятиліть має досвід протистояння тоталітарним режимам і терористичним організаціям у частині їхніх зусиль щодо дестабілізації обстановки із застосуванням інструментів інформаційного та психологічного впливу, а також інших дій в інформаційному просторі.

Можемо констатувати, що уже в 2021 році аналітики НАТО достатньо точно передбачили розвиток форм ведення деструктивної діяльності в інформаційному просторі і трансформації методів ведення інформаційних операцій та операцій впливу. Про це, зокрема, свідчить датована відповідним періодом стаття журналу NATO Reviev "Протидія когнітивній війні: інформованість і стійкість": "Перед Альянсом постає цілий ряд викликів у нових сферах конфліктів. Ці сфери можуть виникати внаслідок запровадження нових проривних технологій. Сфера космосу і кіберсфера, наприклад, виникли внаслідок розвитку ракетних, супутникових, комп'ютерних, теле-

комунікаційних і мережевих технологій. Дедалі більш поширене використання соціальних засобів інформації, соціальних мереж, соціальних меседжів і мобільних технологій створює нині нову сферу: когнітивну війну"[7].

Автори також пояснюють та фактично формулюють визначення поняття "Когнітивна війна: "Минулого сторіччя інноваційна інтеграція мобільної піхоти, броні і повітряних сил призвела до нового виду маневрених бойових дій, якому спочатку було важко протистояти. Сьогодні когнітивна війна, заради досягнення своїх цілей, поєднує в собі кібернетичні, інформаційні, психологічні засоби, а також засоби соціальної інженерії. Вона використовує переваги Інтернету і соціальних мереж задля спрямування на впливових осіб, конкретні групи і велику кількість громадян у суспільстві, вибірково та серійно"[7].

Якщо фактично новою формою ведення бойових дій визнається когнітивна війна, то було б логічним визначити, за аналогією зі сферами вогневого ураження, логістики, та іншими важливими військовим напрямками поняття "когнітивної переваги". Північноатлантичний Альянс хоча і не дуже швидкий, але достатньо послідовний у своїх публікаціях, зокрема й відкритих. Тому на початку 2024 року в загальному доступі з'являється визначення цього поняття: "Когнітивна перевага стосується дій: перетворення обізнаності і розуміння обстановки на фактичну перевагу над супротивником при прийнятті рішень. Це означає, що НАТО має розбиратися в ситуації швидше, глибше і ширше, а рішення приймати більш ефективно, ніж супротивник, що завжди забезпечуватиме володіння ініціативою і можливість бути на крок попереду супротивника на стратегічному, оперативному і тактичному рівнях. Це передбачає зменшення відомих загроз, ризиків і слабких сторін при одночасному використанні сильних сторін і можливостей, прискоренні просування вперед у певних сферах технологій і спроможностей, і застосуванні інших, невійськових, інструментів. Зусилля, зв'язані з досягненням когнітивної переваги, можуть бути приблизно поділені на три блоки: обізнаність, розуміння і перевага. [8]. Наголошується на тому, що недостатньо обізнаності про свої та противника сильні і слабкі сторони, але саме така обізнаність, досягнута із використанням сучасних технологій, які дозволяють здобувати та обробляти в автоматичному режимі величезні масиви інформації, і, що не менш важливо, правильно їх інтерпретувати, є ключем до майбутніх кроків, що здатні у комплексі забезпечити когнітивну перевагу. Значення когнітивної переваги не обмежується лише обставинами ведення активних бойових дій, оскільки над нею необхідно постійно працювати, зокрема нижче порогового рівня, який умовно відповідає межі початку вогневої війни.

Безумовно, при веденні когнітивної війни нехтують супутньою шкодою, яка завдається некомбатантам, цивільним об'єктам, інституціям громадянського суспільства та громадянам. Більше того, якщо мова йде про росію чи інші тоталітарні держави, така форма ведення бойових дій не просто нехтує шкодою для громадян, що не є учасниками воєнного конфлікту, але й цинічно використовує її як інструмент для досягнення геополітичних цілей. Саме тому когнітивну війну обґрунтовано вважають формою неконвенційної війни. Конкретні цілі впливу підпорядковані стратегії. Здійснення контрольованого впливу на людські спільноти та окремих індивідів для зміни їхніх когнітивних фреймів і поведінки, зокрема впливу на процедури ухвалення політичних рішень або на поведінку виборців і втручання в електоральні процеси тощо, породжує широкий спектр дослідницьких питань: від використання для цього досягнень нейронауки і до проблемами етики. Основну проблему когнітивної війни вбачають у тому, що вона непомітна, ми бачимо лише наслідки, а тоді часто буває вже пізно [9].

За таких умов має надзвичайно важливе значення технічна допомога, яку партнери надають Україні, зокрема в рамках ІТ-коаліції. Зараз до неї входять: Бельгія, Великобританія, Данія, Естонія, Ісландія, Італія, Латвія, Литва, Люксембург, Японія та Нідерланди. Ці країни уже передали обладнання й технологій на десятки мільйонів євро. Передусім ідеться про сферу інформаційних технологій, захищений зв'язок та кібербезпеку. Але в широкому значенні ІТ-коаліція покликана забезпечити необхідну цифрову основу для розгортання будь-яких нових технологічних рішень [10]. Безумовно, її діяльність буде корисною і для захисту інформаційної безпеки, включно із кібербезпекою та методиками й технологіями виявлення ознак деструктивного інформаційно-психологічного впливу, включно із впливом у когнітивній сфері.

Не менш важливим аспектом, аніж сучасні цифрові технології, у питаннях досягнення когнітивної переваги в сучасній війні є організаційна дисципліна, адекватна стратегія та здатність аналізувати події і процеси в усіх аспектах протистояння, прогнозуючим їх розвиток. Варто відзначити, що Північноатлантичний Альянс та країни-партнери досить ретельно відстежують події росій-

сько-української війни, намагаючись винести з неї уроки для себе. Як зазначив командувач ОЗС НАТО з питань трансформації генерал Філіп Лавінь, "Україна показала, як майбутні бойові дії можуть бути швидкоплинними і надзвичайно конкурентними". Партнери відзначають, що в Україні вперше застосовуються нові види озброєння, такі як гіперзвукові ракети (які запускає росія), і використовуються такі інноваційні способи, як українське програмне забезпечення ГІС Арта, змодельована за зразком застосунку "Юбер". Комерційні дійові особи і представники громадянського суспільства залучені безпосередньо: Майкрософт посилила українську кібероборону, а "Анонімос" посіяли хаос в російському кіберпросторі. Такий розвиток подій вказує на те, що НАТО необхідно покращувати розуміння своїх можливостей через виявлення слабких і сильних сторін Альянсу. Це так само важливо, як розуміння слабких і сильних сторін наших супротивників для того, щоб випереджати криву загроз – усвідомлювати падіння і піднесення інтенсивності конкретних загроз протягом тривалого періоду – і формувати безпекове середовище на користь НАТО. Цей непідвладний часу імператив когнітивної переваги був сформульований Сунь Цзи тисячу років тому: "Якщо ви знаєте ворога і знаєте себе, вам не потрібно боятися результату сотні битв" [8]. З одного боку, такі висновки свідчать, що досвід країн-партнерів і здатність їхніх спеціалістів аналізувати питання, пов'язані з протистоянням в інформаційному просторі та когнітивною війною, мають беззаперечну цінність для представників українського політичного та військового керівництва, а також для осіб, які прийматимуть рішення щодо розвитку механізмів державного управління у сфері захисту безпеки інформаційного простору. З іншого боку, склалося так, що саме Україна опинилася на передовій захисту сучасної світової безпеки, зокрема і в інформаційному просторі. І ніхто, крім представників української держави, не має кращих можливостей своєчасно оцінювати, аналізувати та прогнозувати розвиток загроз, зокрема і в когнітивній сфері.

Когнітивна війна не обмежується виключно воєнними аспектами, а результатом вдалих операцій та інформаційних дій у цій війні є не лише перевага або поразка військових підрозділів чи державних утворень. Незалежно від стратегічного результату в майбутньому когнітивна війна уже зараз несе смертельну небезпеку для цільових аудиторій, на які спрямований ворожий деструктивний інформаційно-психологічний вплив та діяльність інших акторів (суб'єктів наповнення інформаційного простору), які нехтують інтересами психологічного та фізичного здоров'я представників аудиторій при реалізації своєї інформаційної діяльності. У зв'язку з цим від механізмів державного управління у сфері захисту безпеки інформаційного простору вже сьогодні вимагається ефективний результативний захист найбільш уразливих цільових аудиторій. Вплив у когнітивній сфері не є універсальним, відповідно, способи впливу на різні цільові аудиторії будуть різними. Зазвичай різними, диференційованими, мають бути і засоби нівелювання деструктивного інформаційно-психологічного впливу (або зниження його ефективності) залежно від того, на які цільові аудиторії спрямований цей вплив. Розглянемо одну з найбільш універсальних класифікацій цільових аудиторій, запропонованих вітчизняними дослідниками – за віком:

Діти не є активними учасниками соціуму, тому когнітивний вплив здійснюється за рахунок нав'язування певних моделей поведінки та мислення, які сприймаються дітьми без критичного аналізу. Прикладом є мультфільми "Маша і ведмідь", серії мультфільмів "Три богатирі", "Іван Царевич та Сірий вовк", низки YouTube-програм, тощо.

Підлітки мислять більш критично ніж діти, але вони знаходяться у стадії соціальної адаптації, тому для них надзвичайно важливою є соціальна оцінка. Когнітивний вплив впроваджується через деструктивні тренди у соціальних мережах, популяризацію субкультурних течій, які дають можливість підлітку стати частиною якоїсь спільноти, часто із вираженими ознаками, яка відрізняє цю спільноту від інших.

Молодь здатна критично осмислювати інформацію, проте вона знаходиться у стадії активного розвитку і пошуку можливостей реалізації. Когнітивний вплив реалізовується через соціальні мережі, відеохостинги, месенджери, де поширюються та заохочуються способи легкого заробітку матеріальних ресурсів, на противагу поступовому збільшенню свого професіоналізму у певних галузях.

Люди середнього віку, зазвичай, є більш поміркованими, ніж попередні вікові групи, і тому потребують стабільності. Когнітивний вплив реалізується через соціальні медіа та відеоконтент (телеефір, YouTube). Середня вікова група критично осмислює інформацію, але обтяжена життєвим досвідом, а тому основні зусилля робляться на актуалізацію когнітивних упереджень, які заважають об'єктивно ставитися до інформації. Як наслідок, ворог просуває свої стратегічні наративи.

Люди похилого віку найбільш схильні до рефлексії, тому ворогом застосовується ностальгія як основне джерело впливу у когнітивній сфері. Апеляція до минулого є ефективним засобом, особливо якщо використовується поруч із матеріальними привілеями. Джерела поширення можуть бути різні, але здебільшого це теле- і радіоефіри, а також інтернет-ЗМІ [11, С. 49]. Варто додати, що інтеграція, зокрема і людей похилого віку, до спільнот соціальних мереж при тому, що вони далеко не завжди можуть достатньо швидко та якісно оволодіти основами цифрової грамотності, нерідко призводить або до розчарування процесами в інформаційному просторі загалом і повернення до традиційних медіа, або ж до того, що ця цільова аудиторія стає легкою ціллю для спеціалістів ворога, які планують та реалізовують деструктивний інформаційно-психологічний вплив з яскраво вираженими ефектами у когнітивній сфері.

Безумовно, когнітивна війна як неконвенційна форма ведення бойових дій та сукупність заходів, які вживаються для цілеспрямованої руйнації процесу прийняття рішень чи світогляду багатомільйонних аудиторій, є першочерговою інформаційною загрозою життю та здоров'ю населення. Але, розглядаючи ситуацію з позиції роботи механізмів державного управління у сфері захисту безпеки інформаційного простору, не можна забувати і про інші загрози, пов'язані із сучасними технологіями, передусім у сфері комунікації. Традиційно на другому місці списку загроз після зовнішньої військової агресії стоїть як міжнародна, так і внутрішня злочинність. У період з 2018 по 2022 рік кількість інформаційних злочинів в Україні збільшилася у 2,5 разу. При цьому статистика демонструє зростання кіберзлочинності лише на 25% [12. С. 18]. Отже, переважна більшість приросту кількості таких злочинів, якщо говорити про суто кримінальний аспект, а не масовані кібератаки ворога, який переслідує воєнні чи терористичні цілі, пов'язана зі злочинним контингентом, який не володіє спеціальними знаннями у сфері інформаційних технологій. У зв'язку зі зручністю маскування, складністю розслідування, високою латентністю і розширеними можливостями для психологічного впливу значна частка злочинів проти власності, що стосується шахрайства та найрізноманітніших афер, стали реалізовуватися пріоритетно шляхом використання інформаційно-комунікаційних технологій. Разом з новими можливостями для злочинців та аферистів сучасні технології та програмне забезпечення дають і принципово нові інструменти для правоохоронних органів, включаючи можливості для розслідування злочинів, вчинених як за допомогою мережі Інтернет, так і без її використання. Але цей процес набуває властивостей перегонів правоохоронця з правопорушником, де перемагає той, хто швидше адаптується і вивчає тонкощі нових технологій, пов'язані зі своєю основною професією.

Часто окремим блоком виділяють проблематику, пов'язану з недобросовісним використанням технологій штучного інтелекту. При організації деструктивного інформаційно-психологічного впливу на даний момент такі технології просто незамінні і дозволяють вивільнити величезну кількість кадрового ресурсу на роботу, пов'язану, наприклад, із плануванням інформаційних атак, або ж більш інтелектуальною творчою діяльністю. За допомогою технологій штучного інтелекту генерують у значних кількостях зображення, які вимагали б десятків годин роботи спеціалістів, створюють діпфейки та іншу відеопродукцію дезінформуючого характеру, ботоферми в автоматичному режимі можуть десятками годин сперечатися у коментарях під дописами соцмереж зі справжніми довірливими користувачами, якщо не переконуючи їх у чомусь, то принаймні піднімаючи популярність відповідних цільових дописів.

Але дійсно революційний за своїми масштабами вплив на сучасне життя, який необхідно враховувати в процесі розвитку механізмів державного управління, передусім у сфері захисту безпеки інформаційного простору, чинять сучасні технології побутового характеру. Їх створення та впровадження зазвичай не має на меті досягнення ані воєнних, ані кримінальних цілей. Такі технології входять в наше життя непомітно, змінюють нашу мотивацію, спосіб мислення, прийняття рішень. Цифровізація побутових процесів стає невід'ємною частиною нашого життя, формує звички, порядок дій, нові механізми прийняття рішень, які швидко стають типовими, загальноприйнятими і можуть легко застосовуватися для провокації когнітивних спотворень. Не знаючи, що робити на побутовому рівні, ми зазвичай шукаємо інструкцію на відеохостингах (в ютубі), або ж просто у пошукових системах. Те, що популярні (перші результати за релевантністю (кількістю звернень користувачів) у пошукових системах) відповіді не завжди є точними, достовірними, і навіть зовсім не обов'язково правдою, – переважно залишається поза процесом прийняття рішень. Лише незначна частина користувачів, які володіють достатньою цифровою грамотністю, намагаються перевірити джерела та переконатися, чи дійсно отримані результати пошуку

можуть зарадити у тій чи іншій ситуації. Це непогано допомагає проти випадкових помилок, але у ситуації, коли спотворення ввідних даних провокується навмисне, з метою досягнення ефектів деструктивного інформаційного психологічного впливу, – інформація зазвичай маскується під достовірну, дублюється у різних варіантах виконання за формою та поширюється з різних джерел. На фоні загальної кількості недостовірної інформації і просто інформаційного сміття подібні маніпуляції здебільшого проводяться практично безслідно а їх виявлення та профілактика, не кажучи вже про усунення наслідків, вимагають спеціальної системної роботи в ході реалізації механізмів державного управління у сфері захисту безпеки інформаційного простору.

Висновки та перспективи подальших розвідок у даному напрямку. Проблеми розбудови та функціонування механізмів державного управління у сфері захисту безпеки інформаційного простору, пов'язані з динамікою технологічного розвитку, можна, в свою чергу, умовно поділити на декілька категорій. Серед них ми передусім виділяємо загрози воєнного характеру, а саме – можливість ведення ворогом неконвенційної когнітивної війни, яку фактично відкриває і значною мірою посилює характер сучасних інформаційно-комунікативних технологій. У другу чергу, слід приділити увагу загрозам кримінального характеру, оскільки злочини, при реалізації яких використовується Інтернет-мережа, можливості штучного інтелекту та інші сучасні технології і програмне забезпечення, передбачають досягнення незаконних цілей при свідомому ігноруванні супутньої шкоди, завданої психічному і фізичному здоров'ю громадян, а в окремих випадках, як і у випадках з інформаційними загрозами воєнного характеру, ця шкода і є головною метою злочину. Цифровізація у спілкуванні та побутових питаннях спричиняє не лише виклики і загрози, але й можливості, зокрема – і для подолання викликів та загроз. Це третій основний фактор, який повинен враховуватися при розбудові механізмів державного управління у сфері захисту безпеки інформаційного простору, оскільки в різних сферах (починаючи від реклами й маркетингу і закінчуючи пошуком інструкції до побутового приладу чи поради з приводу ремонту недорогого обладнання) даний фактор змінює алгоритми прийняття рішень та пошуку інформації, створює безліч можливостей як для конструктивного розвитку механізмів в інформаційному просторі, так і для деструктивного інформаційно-психологічного впливу, а в широкому значенні формує нову сучасну реальність у всіх трьох вимірах інформаційного простору – фізичному, віртуальному та когнітивному. Не рахуватися з цим уже немає можливості. Звичка людей довіряти допоміжним інформаційним системам на кшталт GPS-навігатора, доступного зараз у будь-якому смартфоні чи планшеті, неодноразово приводила водіїв у районі бойових дій до позицій противника, не кажучи вже про спричинення несвідомих порушень правил дорожнього руху у разі несвоєчасного оновлення карт та встановлення нових дорожніх знаків. Технології та програмне забезпечення стають досконалішими, рідше допускають помилки і частіше підвищують ефективність у будь-якій сфері. Поряд з тим, збільшується їх вплив на всі сфери суспільних відносин та процесів і небезпечність будь-якого несанкціонованого втручання у функціонування таких технологій та програм. Враховуючи традиційно повільний процес реформування будь-яких механізмів державного управління, динаміку технологічного розвитку необхідно закладати як фактор при формуванні стратегій розвитку відповідних державних інституцій.

Враховуючи викладене, з метою забезпечення підвищення ефективності розбудови та функціонування механізмів державного управління у сфері захисту безпеки інформаційного простору пропонується:

при формуванні планів розвитку та роботи державних інституцій у стратегічній (довгостроковій) та середньостроковій перспективі враховувати потенційні можливості перспективних технологій, які зараз зароджуються або активно розвиваються, але вірогідно відіграватимуть значно вагомішу роль у майбутньому;

при довго- та середньостроковому плануванні розвитку державних інституцій, пов'язаних з оборонною та інформаційною сферою, спрямувати зусилля на підготовку умов та заходів, які забезпечать отримання когнітивної переваги у когнітивній війні з максимальним дотриманням при цьому демократичних принципів державного управління;

у короткостроковій перспективі будувати роботу підрозділів, які здійснюють управління інформаційним простором, інформаційний вплив та протидію інформаційному впливу не лише на підставі результатів автоматизованого чи іншого моніторингу віртуального інформаційного простору, але й шляхом як мінімум вибіркової оцінки когнітивного простору через живе спілкування з доступними аудиторіями, наприклад, шляхом журналістської роботи з ними;

стимулювати теоретичні наукові дослідження та створення спеціального програмного забезпечення на національному рівні, яке дозволить оперативно робити висновки за інформативними індикаторами в ході оцінки віртуального інформаційного простору про зміни у когнітивному вимірі інформаційного простору, оцінювати впливи, їхню небезпечність для різних аудиторій, перспективи та оптимальні сценарії нівелювання (зниження ефективності) деструктивних інформаційних впливів;

при формуванні законодавчих вимог та безпосередніх посадових інструкцій для спеціалістів, які працюють з інформаційним впливом та протидією інформаційному впливу, ретельно аналізувати практичний досвід російсько-української війни. Причому, об'єктом аналізу повинні бути як успішні кейси, де дії українських спікерів, медійників та інших суб'єктів наповнення інформаційного простору дозволяли здобути когнітивну перевагу за певною тематикою, так і провальні, в ході яких перевагу отримував ворог. Також необхідно враховувати не лише власні напрацювання, що, безумовно, мають бути пріоритетними з огляду на доступність інформації і наявність спеціалістів, які були безпосередньо залучені до відповідних процесів, але й зовнішню оцінку представників країн-партнерів, які ретельно аналізують події російсько-української війни та у відносно спокійній обстановці роблять кваліфіковані тверезі висновки;

вжити заходів щодо стимулювання критичного мислення та розвитку цифрової грамотності з максимальною, наскільки це дозволяють ресурси і можливості, диференціацією за різними цільовими аудиторіями, враховуючи особливості вразливості цих цільових аудиторій. Для початку пропонується взяти за основу класифікацію цільових аудиторій, стійкість яких необхідно підвищити таким чином, за віком, але в процесі розвитку програм цифрової грамотності цим критерієм не обмежуватися.

Перспективи подальших досліджень вбачаються у деталізованому вивченні стратегій нападу і стратегій захисту цільових аудиторій у сучасній когнітивній війні.

REFERENCES:

1. Azarov D. S. Venher V. M. Koval D. O.Nuridzhanian G. S. Viina rosii proty Ukrainy yak henotsyd ukrainskoho narodu. [Azarov D. S. Wenger V. M. Koval D. O. Nuridzhanyan G. S. Russia's war against Ukraine as genocide of the Ukrainian people.]. Naukovi zapysky NaUKMA. Yurydychni nauky. Scientific Notes of NaUKMA. Legal sciences. 2023, 1. 12–39. DOI: https://doi.org/10.18523/2617-2607.2023.11.12-39. [in Ukrainian].

2. Raketnyi udar po «Okhmatdytu» maie rozsliduvatysia u katehorii voiennykh zlochyniv – Bilyi dim. [The missile attack on Okhmatdyt should be investigated as a war crime - White House.]. Ukrinform. URL: https://www.ukrinform.ua/rubric-ato/3883206-raketnij-udar-po-ohmatditu-mae-rozsliduvatisa-u-kategorii-voennih-zlociniv-bilij-dim.html [in Ukrainian].

3. Udar po Kyievu: u pryvatnii klinitsi zahynuly 7 liudei, zhertvamy staly patsiienty y spivrobitnyky. [Kyiv is hit: 7 people are killed in a private clinic, including patients and staff.]. Unian. URL: https://www.unian.ua/war/udar-po-kiyevu-u-privatniy-klinici-na-livoberezhniy-zaginuli-semero-lyudey-novini-kiyeva-12690579.html [in Ukrainian].

4. U klinitsi "Isida" cherez raketnyi udar ahresora poshkodzheno budivliu, vybyto vikna, postrazhdalykh nemaie. [The building of the Isis clinic was damaged by an aggressor's missile attack, windows were smashed, and no one was injured.]. Interfax-Ukraina – Interfax-Ukraine. URL: https://interfax.com.ua/news/general/998797.html [in Ukrainian].

5. Lehkodukh V. V. Rosiiska propahanda viiny yak zahroza demokratychnym tsinnostiam. [Legkodukh V. V. Russian war propaganda as a threat to democratic values.]. Materialy Mizhnarodnoi naukovoi konferentsii. Uzhhorod. Proceedings of the International Scientific Conference. Uzhhorod. 2024. 34–36. DOI: DOI https://doi.org/10.30525/978-9934-26-451-1-8 [in Ukrainian].

6. Parfylo O. Kiberataky yak odna iz skladovykh rosiiskoi ahresii proty Ukrainy. [Parfylo O. Cyberattacks as one of the components of Russian aggression against Ukraine.]. Zbirnyk materialiv Vseukrainskoi naukovo-praktychnoi konferentsii "Derzhavna bezpeka Ukrainy v umovakh rosiiskoi ahresii: aktualni pytannia ekspertno-kryminalistychnoho ta naukovo-tekhnichnoho zabezpechennia". Proceedings of the All-Ukrainian Scientific and Practical Conference "State Security of Ukraine in the Context of Russian Aggression: Topical Issues of Forensic, Scientific and Technical Support". 2023. 91–94. URL: http://ndekc.lviv.ua/pdf/zbirnik.pdf#page=91 [in Ukrainian].

7. Keti Kao, Shon Hleister, Edriena Pena, Denbi R, Viliam Ronh, Aleksander Rovalino, Sem Bishop, Rohan Khanna, Dzheitin Sinhkh Saini Pid kerivnytstvom: Lourensa Eronkhaima, dotsenta, i Aleksandera Kokrona, lektora Inzhenernoi shkoly Vaitinh universytetu Dzhonsa Hopkinsa. Protydiia kohnityvnii viini: informovanist i stiikist. [Katie Kao, Sean Glaister, Adrienne Pena, Denby R, William Rong, Alexander Rovalino, Sam Bishop, Rogan Hannah, Jatin Singh Saini Under the guidance of: Lawrence Eronheim, Associate Professor, and Alexander Cochran, Lecturer, Whiting School of Engineering, Johns Hopkins University. Countering cognitive warfare: awareness and resilience.]. NATO Reviev. 2021. URL: https://www.nato.int/docu/review/uk/articles/2021/05/20/protidya-kogntivnj-vjn-nformovanst-stjkst/index.html [in Ukrainian].

8. Keti Kao, Shon Hleister, Edriena Pena, Denbi R, Viliam Ronh, Aleksander Rovalino, Sem Bishop, Rohan Khanna, Dzheitin Sinhkh Saini Pid kerivnytstvom: Lourensa Eronkhaima, dotsenta, i Aleksandera Kokrona, lektora Inzhenernoi shkoly Vaitinh universytetu Dzhonsa Hopkinsa. Protydiia kohnityvnii viini: informovanist i stiikist. [Dr. Kestutis Paulauskas. Why cognitive superiority is an imperative.]. NATO Reviev. 2024. URL: https://www.nato.int/docu/review/uk/articles/2024/02/06/index.html [in Ukrainian].

9. Parakhonskyi B., Yavorska H. Porodzhennia viiny z bezsyllia myru: smyslova lohika viiny. [Parakhonsky B., Yavorska G. The Genesis of War from the Powerlessness of Peace: The Semantic Logic of War.]. Natsionalnyi instytut stratehichnykh doslidzhen. National Institute for Strategic Studies. URL: https://niss.gov.ua/news/statti/porodzhennya-viyny-z-bezsyllya-myru-smyslova-lohika-viyny. [in Ukrainian].

10. IT-koalitsiia: Doiednalys Niderlandy, novi vnesky krain-partneriv. [IT Coalition: The Netherlands joined, new contributions from partner countries.]. Ministerstvo oborony Ukrainy – Ministry of Defense of Ukraine. 2024. URL: https://www.mil.gov.ua/news/2024/01/27/it-koalicziya-doednalis-niderlandi-novi-vneski-krain-partneriv/. [in Ukrainian].

11. Strelbytskyi M., Hryn M. Kohnityvna viina rosii proty Ukrainy. [Strelbitsky M., Grin M. Russia's cognitive war against Ukraine.]. Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Scientific works of the Interregional Academy of Personnel Management. 2023, 1 (64). 46–52. DOI: https://doi.org/10.32689/2522-4603.2023.1.7. [in Ukrainian].

12. Hrynko L. “Slidova kartyna” shakhraistv, vchynenykh cherez merezhu Internet. [Hrynko L. "Trace Picture" of Frauds Committed via the Internet.]. Poltavskyi pravovyi chasopys. Poltava Legal Journal. 2022, 3. 16–27. DOI: https://doi.org/10.21564/2786-7811.3.287946. [in Ukrainian].