РЕЗУЛЬТАТИ ЗАСТОСУВАННЯ МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ У СФЕРІ ЗАХИСТУ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ У КОРОТКОСТРОКОВІЙ ПЕРСПЕКТИВІ

RESULTS OF APPLYING STATE GOVERNANCE MECHANISMS FOR PROTECTING INFORMATION SPACE SECURITY IN THE SHORT-TERM PERSPECTIVE

УДК 351.746:007]:316.77
DOI https://doi.org/10.32782/pma2663-5240-2024.43.11

Кудрявський І.В.
докторант
Міжрегіональна Академія управління персоналом

Сучасний розвиток технологій підвищує швидкість взаємодії між людьми та їх об'єднаннями. Це загальна світова тенденція у найрізноманітніших сферах. Але в питаннях наповнення інформаційного простору та масових комунікацій вона виражена особливо яскраво. Ефект від добре спланованої інформаційно-психологічної акції може проявлятися за лічені хвилини, практично миттєво, а чисельність аудиторій, які піддаються деструктивному інформаційно-психологічному впливу нерідко вимірюється мільйонами людей. При цьому набувають розвитку канали донесення інформації, які вимагають мінімальної безпосередньої підготовки для їх застосування і можуть використовуватися без будь-якого ліцензування, державного чи громадського контролю. Соціальні мережі, месенджери відеохостинги, звісно, мають певні механізми безпеки при реєстрації нових користувачів, але все ще дозволяють суб'єктам реалізації інформаційних дій достатньо легко приховувати свою особистість. Механізм набуття новими учасниками популярності, а відповідно – і можливості впливати на чисельні цільові аудиторії, є дещо ефективнішим стримуючим фактором, однак за наявності достатніх фінансових, кадрових ресурсів, необхідного програмного і технічного забезпечення час попередньої підготовки каналу поширення інформації майбутнього деструктивного інформаційно-психологічного впливу зводиться до мінімуму при тому, що розвиток такого каналу може реалізовуватися із застосуванням нейтральної інформації, яка не становить шкоди, але й не дозволяє завчасно виявити його небезпечність.

Враховуючи зазначені особливості сучасного інформаційного середовища, в умовах відбиття Силами оборони України російського широкомасштабного вторгнення від механізмів державного управління у сфері захисту безпеки інформаційного простору вимагається щонайменше безперервне відстеження тенденцій, змін та процесів, які відбуваються в інформаційному середовищі, і блискавична реакція на появу та розвиток інформаційних загроз. На даному етапі російсько-української війни це загалом зрозуміло для осіб, які приймають рішення щодо розбудови механізмів державного управління, описано у наукових працях та частково втілено на практиці, створено низку підрозділів, призначених для моніторингу інформаційного простору, зокрема із застосуванням спеціальних автоматизованих систем та програмного забезпечення. Але традиційно непростим питанням залишається забезпечення швидкості реагування традиційно громіздкою системою державного управління, адже швидкість процесів у медіасередовищі часто вимагає негайних дій і просто не залишає часу на узгодження та дотримання традиційних процедур і протоколів.

Навіть при гіпотетичному забезпеченні високої швидкості реакції на появу інформаційних загроз – це все одно буде лише реактивний запізнілий підхід. Для досягнення когнітивної переваги, інформаційної переваги та завоювання оперативної ініціативи в інформаційному протистоянні з чисельним добре оснащеним ворогом необхідне ефективне прогнозування процесів в інформаційному просторі, дії на випередження, заходи управління інформаційним простором та, зрештою, нав'язування противнику власного "порядку денного". Реалізація таких завдань в умовах ресурсної переваги противника вимагає ґрунтовних наукових досліджень, аналізу досвіду, як власного, так і міжнародного, максимально ефективної реалізації потенціалу всіх наявних ресурсів та можливостей.

Мета запропонованого дослідження – пошук способів підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору через аналіз результатів їх оперативного застосування у короткостроковій перспективі.

Завдання дослідження полягає в аналізі історичних джерел, наукових праць, офіційних повідомлень та публіцистичних матеріалів, що надають можливість вивчити результати застосування механізмів державного управління у сфері захисту безпеки інформаційного простору в умовах відбиття Силами оборони України російського широкомасштабного вторгнення у короткостроковій перспективі.

Наукова новизна дослідження і його результатів полягає у комплексному розгляді проблемних питань оперативного застосування механізмів державного управління у сфері захисту безпеки інформаційного простору України та результатів такого застосування у короткостроковій перспективі в умовах відбиття Силами оборони України російського широкомасштабного вторгнення.

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:

1. Виділити організаційно, окрім підрозділів моніторингу інформаційного простору (які вже створені у багатьох державних відомствах), підрозділи реагування на інформаційні загрози за окремими напрямками відповідальності (тематичними, регіональними).

Організувати роботу єдиного координаційного центру з метою недопущення неузгодженості дій підрозділів реагування на інформаційні загрози (покласти відповідні функції на Центр протидії дезінформації РНБО) при забезпеченні центрів реагування на інформаційні загрози на місцях можливістю діяти максимально оперативно та автономно.

2. Забезпечити підрозділи реагування на інформаційні загрози необхідними кадро-

вими, технічними та матеріальними ресурсами для виконання їхніх завдань.
3. Організувати розробку та доведення до відповідного персоналу стратегії участі у боротьбі за когнітивну (інформаційну) перевагу підрозділів реагування на інформаційні загрози у взаємодії з іншими складовими стратегічних комунікацій та інституаціями, що релізовують державну інформаційну політику.
4. Забезпечити взаємодію підрозділів реагування на інформаційні загрози з відповідними інституціями громадянського суспільства з метою консолідації українського громадянського суспільства та належної реалізації його потенціалу спротиву ворожим зусиллям в інформаційному середовищі.
5. З метою належної координації зусиль на міжнародному рівні організувати взаємодію українських підрозділів реагування на інформаційні загрози з колегами з міжнародних організацій та представниками країн-партнерів.
Ключові слова: *державне управління, інформаційний простір, інформаційна війна, стратегічні комунікації, російська агресія, інформаційно-психологічний вплив.*

Modern technological development increases the speed of interaction between people and their associations. This is a global trend in a variety of areas. However, it is particularly pronounced in the areas of information space and mass communications. The effect of a well-planned information and psychological campaign can be manifested in a matter of minutes, almost instantly, and the number of audiences exposed to destructive information and psychological influence is often measured in millions of people. At the same time, channels of information delivery are being developed that require minimal direct training for their use and can be used without any licensing, state or public control. Social networks, messengers, and video hosting sites, of course, have certain security mechanisms when registering new users, but they still allow the subjects of information actions to conceal their identity quite easily. The mechanism of gaining popularity by new participants, and, accordingly, the ability to influence numerous target audiences, is a somewhat more effective deterrent, but if there are sufficient financial, human resources, necessary software and hardware, the time for preliminary preparation of the channel for disseminating information of future destructive information and psychological influence is minimized, while the development of such a channel can be implemented using neutral information that does not cause harm, but also does not allow for.
Given these features of the modern information environment, in the context of repulsion of the Russian large-scale invasion by the Ukrainian Defense Forces, the mechanisms of state administration in the field of information space security require at least continuous monitoring of trends, changes and processes taking place in the information environment and a lightning-fast response to the emergence and development of information threats. At this stage of the Russian-Ukrainian war, this is generally understood by decision-makers who are building public administration mechanisms, described in scientific papers and partially implemented in practice, and a number of units have been created to monitor the information space, including using special automated systems and software. However, ensuring the responsiveness of the traditionally cumbersome public administration system remains a difficult issue, as the speed of the media environment often requires immediate action and simply does not leave time to coordinate and comply with traditional procedures and protocols.
Even if we hypothetically ensure a high speed of response to information threats, it will still be a reactive, delayed approach. To achieve cognitive superiority, information superiority and gain operational initiative in an information confrontation with a large, well-equipped enemy, it is necessary to effectively predict processes in the information space, act proactively, take measures to manage the information space and, ultimately, impose one's own "agenda" on the enemy. Implementation of such tasks in the context of the enemy's resource advantage requires thorough scientific research, analysis of experience, both domestic and international, and the most effective realization of the potential of all available resources and capabilities.
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 results of their application in the short term.
The objectives of the study is to analyze historical sources, scientific works, official reports and journalistic materials that provide an opportunity to study the results of the application of public administration mechanisms in the field of information space security protection in the context of repulsion of a large-scale Russian invasion by the Ukrainian Defense Forces in the short term.
The scientific novelty of the study and its results lies in a comprehensive consideration of the problematic issues of operational application of public administration mechanisms in the field of information space security protection in Ukraine and the results of such application in the short term, 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:
1.In addition to the information space monitoring units (which have already been established in many government agencies), to organize information threat response units in separate areas of responsibility (thematic, regional);
2. Organize the work of a single coordination center to prevent inconsistency in the actions of information threat response units (entrust the NSDC Disinformation Counteraction Center with the relevant functions), while ensuring that local information threat response centers are able to act as quickly and autonomously as possible;
3. Provide information threat response units with the necessary human, technical and material resources to fulfill their tasks;
4. Organize the development and communication to the relevant personnel of a strategy for participation in the struggle for the cognitive (information) advantage of information threat response units in cooperation with other components of strategic communications and institutions that implement the state information policy.
Key words: *public administration, information space, information warfare, strategic communications Russian aggression, information and psychological influence.*

Постановка проблеми. Вже у 2020 році чисельність країн, проти яких застосовувалися інформаційні засоби зі шкідливим контентом, зросла до 81-ї у порівнянні з 70-ма у попередньому періоді, за переважаючої ролі рф, Китаю, Ірану. Важливості загрозам, зокрема напередодні виборчої кампанії-2024 в США, додають висновки експертів Міністерства національної безпеки, позиціонуючи цілеспрямованість акторів походженням із цих трьох країн як джерела інформаційно-психологічного впливу, створення порівняно дешевого синтетичного текстового, візуального й аудіоконтенту достатньо високої якості [1, с. 95]. Якщо соціальні мережі та інші відносно нові форми комунікації в мережі Інтернет відкрили можливість масштабного поширення інформаційного контенту, зокрема і в рамках інформаційно-психологічних акцій, з можливістю приховати авторство й джерело інформації, то технології із застосуванням штучного інтелекту відкрили нову сторінку в можливостях швидко та за витрати мінімального творчого кадрового ресурсу продукувати величезну кількість такого контенту при його достатній різноманітності.

Здатність штучного інтелекту формувати зв'язні тексти уже давно застосовується для написання цілих літературних серій у жанрах повістей та романів, зазвичай фантастичної тематики, де автор переважно переховується за псевдонімом, а в тексті приховаються окремі закладки, які, з урахуванням контекстів, повинні досягнути ефектів у когнітивному вимірі. Пропагандистська література використовувалася суб'єктами деструктивного інформаційно-психологічного впливу і раніше, але можливість продукувати сотні сторінок за лічені тижні, а то і дні, відсутність необхідності тратити кошти на друк (за умов публікації в Інтернеті) та зручність маскування невеликих цільових епізодів серед значного загального обсягу матеріалу створили новий дешевий та ефективний механізм впливу на освічену аудиторію, якій читати подобається більше, ніж, наприклад, дивитися відео. Звісно, начитана людина здатна вирахувати "підробку", але на це йде певний час та декілька десятків прочитаних сторінок, а далі аудиторію нерідко "затягує" сюжет.

Штучний інтелект кардинально змінив можливості застосування ботів. Раніше вони зазвичай використовувались для просування реклами, забороненого контенту. Прості програми, які, будучи швидшими за людину, могли одразу після публікації контенту створювати коментарі з заданим вмістом. Далі цей метод почали використовувати і в психологічних операціях, та особливого успіху він не мав через те, що бот не міг відповідати на коментарі реальних людей, а його відповіді часто не збігались з контентом, тому користувачі швидко визначали таких "співрозмовників". Але розвиток технологій штучного інтелекту змінив і логіку використання подібних програм, надавши їм можливість спілкуватися з користувачами. Наразі це, зазвичай, ще не повноцінна переписка на довільні теми, проте вже і не прості запрограмовані речення [2. с. 32]. Репліки ботів відповідають контексту матеріалу і за певних обставин їх не одразу вдається відрізнити від живих співрозмовників.

Окремою сторінкою сучасних інформаційно-психологічних акцій стало масове поширення графічних зображень та відео, згенерованих штучним інтелектом. Не настільки швидко, з об'єктивних причин, але ґрунтовно, противник працює над реалізацією психологічного впливу через відеоігри, при- чому, враховуючи психологію геймерів та інтерактивність процесу гри, має непогані шанси досягнути суттєвих ефектів саме у когнітивній сфері. Попереду у перспективі нас очікує застосування в рамках психологічних акцій технологій віртуальної реальності, які поки що недостатньо поширені виключно через відносно високу вартість споживацького обладнання.

Згадані сучасні можливості форм психологічного впливу зовсім не виключають, а лише посилюють ефект нейролінгвістичного програмування, так званого "25-го кадру" та інших давно відомих і добре перевірених технологій.

За таких обставин має принципово важливе значення здатність персоналу, який реалізовує роботу механізмів державного управління у сфері захисту інформаційного простору, діяти активно, виборюючи, у взаємодії з іншими складовими Сил оборони, когнітивну перевагу у противника та формуючи власний порядок денний, який сприятиме гармонійному розвитку національного інформаційного середовища, консолідації громадянського суспільства, захисту інформаційної безпеки держави та особистої інформаційної безпеки її громадян. Але зробити це в умовах, коли фінансові та кадрові ресурси противника дозволяють кількісно заповнити інформаційний простір хай навіть не завжди досконалим, але завжди новим, контентом деструктивного інформаційно-психологічного впливу, зовсім не просто. Оскільки передбачити всі без винятку дії противника у когнітивній війні неможливо, а ефекти його інформаційно-психологічних акцій можуть бути масштабними і миттєвими, – це вимагає належного рівня моніторингу інформаційного простору і бли-

скавичної фахової реакції хоча б уже за актом інформаційно-психологічної атаки. Тоді хоч залишаються можливості порушити запланований порядок реалізації ворожої багатоетапної акції і, відповідно, змінити її кінцевий результат, частково знизивши деструктивний ефект ворожого інформаційно-психологічного впливу на власне населення та особовий склад. Але й для таких заходів, як показує практика, недостатня кількість спеціалізованих підрозділів, неналежна підготовка персоналу таких підрозділів, а головне – традиційна система прийняття рішень, переважно забирає надто багато часу на затвердження варіантів дій, не встигаючи за швидкоплинними змінами обстановки.

Завдання дослідження полягає в аналізі історичних джерел, наукових праць, офіційних повідомлень та публіцистичних матеріалів, що надають можливість вивчити результати застосування механізмів державного управління у сфері захисту безпеки інформаційного простору в умовах відбиття Силами оборони України російського широкомасштабного вторгнення у короткостроковій перспективі.

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 українських дослідників: Бондар В., Недодай М., Дячук О., Примаченко Д., Святська Н., Уманець А., Гаргаун Я., Тулупніков Д., Максименко С., Деркач Л., Висоцька О.; іноземних вчених: [1, 2, 3, 4, 11, 12]; іноземних вчених: Ana Mathas, luhs Cardoso, Andrzej Jarynowski Łukasz Krzowski Stanisław Maksymowicz., Кеті Као, Шон Глейстер, Едріена Пена, Денбі Р, Вільям Ронг, Александер Роваліно Сем Бішоп, Роган Ханна, Джейтін Сінгх Сайні, Лоуренс Еронхайм, Александер Кокрон, Кестутіс Паулаускас [7, 8, 9, 10]; стандартах НАТО [6], публікаціях у медіа [5].

Мета запропонованого дослідження – пошук способів підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору через аналіз результатів їх оперативного застосування у короткостроковій перспективі.

Виклад основного матеріалу дослідження з обґрунтуванням отриманих результатів. Навіть протягом нетривалого часу добре спланована та забезпечена належними ресурсами інформаційна (інформаційно-психологічна) акція може призвести до серйозних наслідків. Такими наслідками можуть бути: внесення в суспільну свідомість і свідомість окремих людей визначених ідей і поглядів, дезорієнтація та дезінформація населення, ослаблення на короткий період усталених переконань людей, що складають основу суспільства, прийняття управлінських рішень, на які розраховує агресор, отримання компрометуючих матеріалів, дестабілізація економічної та політичної ситуації, залякування жертви могутністю країни-агресора [3. с. 108], залякування власного суспільства образом ворога для підтримки війни всередині своєї країни і, звісно, деморалізація особового складу противника та зниження його мотивації до ведення бойових дій, а мотивації населення противника – до реалізації акцій спротиву та підтримки сил оборони.

Без підтримки таких акцій подальшою інформаційною діяльністю їх ефект також може бути короткотривалим через динамічність сучасного інформаційного простору та постійну появу нових, більш актуальних інформаційних приводів. Але навіть короткочасний дезорієнтуючий та дезорганізуючий ефект може бути вирішальним, особливо в умовах динамічних бойових дій, виборчих процесів чи в інших конкурентних сферах, що передбачають змагальність сторін і важливість результату в конкретний час та в конкретному місці. Крім того, інформаційно-психологічні акції, зазвичай, хоч і мають один або декілька кульмінаційних моментів, передбачають етапи інформаційної підготовки та етапи активності після кульмінаційного періоду, якими закріплюється досягнутий ефект. В реальному житті суб'єкт деструктивного інформаційно-психологічного впливу зазвичай поєднує постійну деструктивну інформаційну активність з окремими цільовими потужними, максимально якісно пропрацьованими акціями, на які покладає ключові завдання впливу.

Так, російський уряд ухвалив численні закони про "фейкові новини", щоб перешкоджати свободі преси та вираження думок. Це дозволило контролювати та регулювати поширення пропаганди й дезінформації на своїх телеканалах. RT, також відомий як Russia Today, є основним прикладом цього. Цей канал вважається пропагандистською зброєю російської держави, а його метою є поширення історій, які підривають віру російського суспільства у західні інститути. Досить активно дезінформація шириться цим каналом і за кордоном. На сьогодні у низці країн є Russia Today, який дивиться достатня кількість іноземців як серед європейських країн,

так і країн Латинської Америки, і не лише. Головним наративом нинішньої інформації RT у країнах ЄС є небезпека війни в Україні для нормального життя європейців. Так, наприклад, у грудні 2023 р. на платформі YouTube з'явилося відео, нібито створене німцями, про можливість втрати пишного святкування Різдва європейцями через необхідність виділяти величезну фінансову допомогу Україні для боротьби з Росією. Пізніше було з'ясовано, що всі ролі виконували російські актори. Тобто російський уряд, застосовуючи пропаганду та дезінформацію, намагався дискредитувати Україну в очах європейців і змусити останніх через призму фінансових складнощів мінімізувати допомогу Україні [4, с. 57]. Враховуючи, що лише у 2023 році RT витратив 27,5 млрд рублів [5] (317,3 млн доларів США), а переважна більшість величезної кількості матеріалів, які публікуються цим ресурсом, є дезінформацією, пропагандою та містить матеріали деструктивного інформаційно-психологічного впливу, реагувати на всі 100% контенту таких каналів немає ані можливості, ані сенсу. Поряд з тим, найбільш яскраві та небезпечні у контексті потенційного впливу у когнітивній сфері цільові акції вимагають оперативного та професійного реагування. Таке реагування у випадку його успішної реалізації повинно виконувати завдання одразу за двома напрямками, відповідно до методики протидії психологічним атакам Об'єднаної доктрини НАТО з психологічних операцій AJP 3.10.1. Зазвичай це "пряме спростування" або "непряме спростування" за вибором суб'єкта реагування та "Імунізація" [6. d.110], тобто кондиціонування суспільної думки щодо певних учасників наповнення інформаційного простору. Дізнавшись, що емоційний яскравий контент пропагандистського каналу виявився брехнею або маніпуляцією, аудиторія наступного разу більш критично відноситиметься до схожого контенту з цього джерела.

Хоча короткострокові наслідки деструктивного інформаційно-психологічного впливу здаються не такими небезпечними як ті, що наступають у середньостроковій та запланові у стратегічній перспективі, – враховуючи контекст умов та обстановки, це далеко не завжди так. Крім того, процеси в інформаційному просторі, як сама інформаційно-психологічна акція, так і заходи реагування на неї, залишають після себе певний "післясмак" в аудиторій, який, безумовно, впливатиме на сприйняття ними інформації від учасників наповнення інформаційного простору в майбутньому. Отже, оперативне реагування на заходи деструктивного інформаційно-психологічного впливу противника є одними з найважливіших, а від професійності та швидкості його реалізації безпосередньо залежить успіх таких заходів. Це обумовлює необхідність постановки питання про максимальну самостійність суб'єктів державного управління у сфері захисту інформаційного простору, які безпосередньо займаються протидією ворожим інформаційно-психологічним впливам, та максимальну децентралізацію процесу прийняття рішень у питаннях інформаційної протидії.

Реагування на інформаційну загрозу вимагає її чіткої ідентифікації, адже витрачати і так дефіцитні ресурси, включаючи час та роботу кваліфікованого персоналу, на кожен елемент масштабних інформаційних хвиль контенту деструктивного інформаційно-психологічного впливу противника просто недоцільно. Крім того, зазвичай необхідний певний час на дорозвідку, встановлення дійсних фактичних даних, якщо інформаційна атака не базується на повністю вигаданих фактах, вивчення реакцій, які вже проявили аудиторії. Уже під час цих дій підрозділ планування і творчий персонал повинен займатися виробництвом контенту інформаційної протидії та узгоджувати питання його розміщення (виділення часу в ефірі телеканалів, отримання згоди від редакторів медіа на потенційне розміщення матеріалу тощо). Усе це достатньо тривалий процес, тим більше що в окремих випадках він може вимагати, наприклад, виїзду і роботи на місцевості журналістської групи з оперативною передачею матеріалу редакційній, що оброблятиме його на місці постійного базування.

З кожною наступною хвилиною ефект деструктивного інформаційно-психологічного впливу противника посилюється, а його характер погіршується через обговорення у суспільстві однієї чи декількох, вигідних противнику, точок зору на ситуацію. У гру вступають інші учасники наповнення інформаційного простору, які можуть не брати участі в інформаційному протиборстві, але при наявності достатнього авторитету у суспільстві суттєво змінювати обстановку своїми заявами, поглядами, припущеннями чи іншими висловлюваннями. За таких обставин надто тривале очікування команди чи дозволу від вищих органів управління, осіб, які приймають рішення, але відповідають за значно ширший спектр завдань, аніж дії в інформаційному просторі, і, відповідно, не є вузькими спеціалістами в питаннях протидії інформаційно-психологічним атакам, зазвичай призводить до того, що на момент, коли рішення нарешті прийняті і дії узгоджені, – вони вже просто стають не акту-

альними, оскільки обстановка в інформаційному середовищі встигає змінитися настільки, що планування реакції та створення інформаційного контенту необхідно починати спочатку.

Поряд з тим, децентралізація у прийнятті рішень щодо реагування на кризові ситуації, викликані деструктивним інформаційно-психологічним впливом противника, теж не є ідеальним варіантом і має свої недоліки. По-перше, чим вищий орган управління приймає рішення про реагування – тим серйозніші ресурси він може залучити до відповідної інформаційної діяльності. Власних можливостей конкретного підрозділу реагування на інформаційні загрози може і не вистачити в ситуаціях, які вимагають консолідації зусиль значної частини державного апарату та інституцій громадянського суспільства. З іншого боку, при творчих авторських підходах окремих керівників на місцях їхні не узгоджені між собою, навіть вдалі за окремими задумами, дії можуть призвести до того, що в кінцевому рахунку декілька суб'єктів інформаційної діяльності просто заважатимуть одні одним. Частково може розв'язати зазначену проблематику миттєве інформування вищого керівництва про виявлену загрозу, прийняті рішення та заходи, які будуть вживатися з боку підрозділів, що безпосередньо займаються виявленням інформаційних загроз та мінімізацією результатів деструктивного інформаційно-психологічного впливу без очікування відповіді чи дозволу діяти, але з урахуванням можливості вищого керівництва заборонити інформаційні дії по ходу реалізації, якщо це обґрунтовано надходженням інформації, невідомої виконавцям на місцях. Крім того, чим краще підрозділи інформаційних дій знатимуть загальні наративи й особливості державної інформаційної політики і чим якісніше для них будуть прописані "правила гри" у вигляді нормативно-правових, нормативних актів, інструкцій та покрокових протоколів, тим менша вірогідність "дружнього вогню" внаслідок неузгодженості реагування на інформаційну загрозу різними суб'єктами.

Звісно, кризова ситуація, зокрема і викликана інформаційно-психологічним впливом противника, не виникає нізвідки, а реакції суб'єктів наповнення інформаційного простору й аудиторій залежатимуть від репутації та попередніх дій ініціатора атаки і тих, хто здійснює реагування, намагаючись нівелювати або послабити деструктивні наслідки інформаційно-психологічної акції. Дослідники питань кризової комунікації справедливо зазначають, що будь-яка організація повинна не лише в умовах кризи, а постійно, підтримувати гармонійну комунікацію зі своєю внутрішньою та зовнішньою аудиторією, і що ця комунікація стає абсолютно необхідною в надзвичайних ситуаціях, які можуть поставити під загрозу довіру та життєздатність інституції. Насправді, організації, зокрема і державу, сьогодні не можна розглядати з суто механістичної точки зору, з точки зору внутрішнього функціонування або зовнішніх зв'язків. Діалог має важливе значення, і гарантія репутації установи базується на спланованій і безперервній комунікації під час кризи; тільки активний діалог з громадськістю та участь у формуванні громадської думки дозволить зберегти або відновити довіру до організації і досягти її цілей. Усі організації, незалежно від їхньої природи, вразливі до криз. Різниця полягає в тому, що деякі, більш підготовлені, головним чином з точки зору комунікації, краще справляються з проблемами [7, с. 10]. Таким чином, персонал, який реагуватиме на деструктивний інформаційно-психологічний вплив противника, повинен однозначно узгоджувати свої дії з персоналом, який на постійній основі займається розробкою та реалізацією інформаційної стратегії просування цілей держави (державної організації, міністерства, відомства, структурного підрозділу тощо). Поряд з тим, саме персонал, який займається нейтралізацією деструктивного інформаційно-психологічного впливу противника, повинен мати перевагу в отриманні інформації та впливі на прийняття рішення, оскільки від його активності залежить результат інформаційного протистояння у найбільш відповідальні моменти – в моменти кризи. При цьому фахові дії осіб, які забезпечують просування іміджу організації на постійній основі (спеціалістів PR, прес-служб, прес-секретарів, прес-офіцерів), значно полегшують роботу персоналу, який займається протидією деструктивному інформаційно-психологічному впливу, в той час як систематичні побутові помилки PR-спеціалістів у спокійні періоди роблять ефективне відбиття інформаційних атак у період кризи практично неможливим.

Інформаційні дії стратегічного рівня реалізовуються нечасто і ще рідше бувають ефективними. Набагато частіше кінцеві оперативні і стратегічні наслідки деструктивного інформаційно-психологічного впливу досягаються шляхом послідовного поступового проведення узгоджених за своєю метою чисельних психологічних акцій тактичного рівня. На цьому принципі побудована значна частина системної роботи російської пропаганди та психологічних операцій з метою досягнення когнітивної переваги не лише в українському

інформаційному середовищі, але і в процесі впливу на уряди та населення інших країн. Польські дослідники визначили шість фаз адаптації стратегії деструктивного інформаційно-психологічного впливу російських розвідувальних служб на польське населення та констатували, що в кінцевому рахунку стратегічні цілі російських INFOOPS (інформаційних операцій) не були досягнуті. Дезінформаційна кампанія "Біолаб" (з приводу загроз для Європи від українських біологічних лабораторій) є виключно продуктом пропагандистських офісів і не приділяла жодної уваги реальній бактеріологічній безпеці. Однак підживлення поляризації в суспільстві, страху в питаннях продовольчої безпеки, поєднання тематики біологічних лабораторій з начебто небезпечністю української сільськогосподарської продукції, провокації протестів тваринників і спекуляції на тематиці здоров'я біженців можна інтерпретувати у вимірі PSYOPS (психологічних операцій), як такі, що дозволили досягнути оперативних цілей російської розвідки. Наслідки деструктивного інформаційно-психологічного впливу на польське суспільство у контексті застосування інформації згаданої тематики зросли у 2022 році та продовжили відігравати свою роль у 2023 році [8, с. 3, 4]. У ґрунтовному дослідженні цікава фіксація польськими вченими факту та наслідків російського деструктивного інформаційно-психологічного впливу на польське населення і розробка заходів протидії такому впливу. Але в контексті нашого дослідження значно більше значення мають висновки про те, що шляхом чисельних інформаційно-психологічних акцій, кожна з яких сама по собі могла оцінюватися як така, що матиме лише короткостроковий вплив, противник зумів досягти оперативних результатів (при тому, що планував узагалі стратегічні). Відповідно, за своєчасного вжиття оперативних заходів у ході тривалої інформаційної діяльності противника, окремими повідомленнями, спрямованими на зниження ефективності (нівелювання) російського деструктивного інформаційно-психологічного впливу, можна було запобігти досягненню ворогом його цілей, навіть частковому.

Наведене дослідження черговий раз доводить надзвичайну важливість тактичних заходів реагування відповідних механізмів державного управління у сфері захисту безпеки інформаційного простору буквально в перші години після поширення ключового інформаційного матеріалу деструктивного інформаційно-психологічного впливу противника. Оскільки в інформаційному просторі новина часто живе не довше однієї-двох діб, а поширюється до піку своєї популярності зазвичай протягом однієї – шести годин, цілком доречно, за аналогією з термінологією, популярною для позначення відповідного поняття при евакуації поранених, говорити про три – п'ять "золотих" годин. За цей час із загального потоку ворожої дезінформації та інформаційного середовища загалом (оскільки контент інформаційного впливу може бути добре замаскований) необхідно виділити дійсно небезпечні теми та меседжі, які мають перспективу сприяти досягненню ворогом когнітивного ефекту, розгадати наступні дії ворога (інформаційні повідомлення, терористичні атаки тощо), створити, підготувати й донести до широкої аудиторії матеріал реагування, який не просто змінить ефект від інформаційно-психологічної акції противника чи нівелює його, але й унеможливить або зробить невигідним для противника продовження інформаційно-психологічної акції (операції) за попереднім задумом. У випадку, якщо відповідний час був пропущений, задіювати механізми державного управління у сфері захисту безпеки інформаційного простору зазвичай уже занадто пізно та недоцільно. Навіть якщо вдасться переконати частину аудиторії у тому, що попередньо оприлюднена дезінформація противника не відповідає дійсності, у підсвідомості аудиторій залишиться зв'язок негативних емоцій з дискусійною тематикою, тобто факт когнітивного впливу уже відбудеться та обов'язково буде використаний ініціатором інформаційної (психологічної) атаки у майбутньому.

Поряд з цим, брехлива інформація або фейкові новини, які широко застосовуються російськими розвідувальними службами та військово-терористичними формуваннями, навіть не потрібні для досягнення цілей когнітивної війни. Для провокування незгоди достатньо делікатного урядового документа, викраденого з електронної пошти державної посадової особи, анонімно завантаженого на відкритий сайт соціальної мережі, або вибірково злитого опозиційним групам через соціальну мережу. У когнітивній війні перевагу отримує той, хто робить хід першим і обирає час, місце і засоби наступу. Когнітивна війна може вестися за допомогою різноманітних векторів і засобів [9]. Реагування на публікації матеріалів інформаційно-психологічних акцій противника при всій складності і динамічності цього процесу залишається необхідним, але лише допоміжним, засобом у когнітивній війні. Оскільки сама природа цієї війни обумовлює обставини, коли нападати значно легше, аніж захищатися.

Таким чином, основні зусилля в реалізації механізмів державного управління у сфері захисту безпеки інформаційного простору повинні бути зосереджені не на реагуванні за фактом загроз, що виникли, а на виборюванні когнітивної переваги, тобто здатності до виняткового розуміння і прийняття рішень, які дозволяють переграти і обійти супротивника, володіти швидшим, ширшим і глибшим розумінням оперативного середовища, супротивника і своїх сил, приймати більш дієві і кращі рішення, ніж супротивник [10]. Когнітивна перевага є ключем до захоплення та утримання оперативної ініціативи і необхідною умовою завоювання перемоги як на полі бою, так і в інформаційному протистоянні, де події іноді розвиваються з такою ж високою динамічністю і можуть мати наслідки, що не поступаються бойовим діям за своїми масштабами.

Війна росії проти України вплинула на структуру ідентичності не лише пересічних громадян, а й військовослужбовців Збройних Сил України. Їх героїчна, самовіддана боротьба за Україну, єдність, солідарність, патріотизм, довіра, професійна ідентичність та професійна свідомість – цінності, які є проявом трансгенераційного зв'язку з культурою предків, генетичним кодом української нації: соціопсихологічні типи, в яких закодовані генетичні показники української нації. Від початку російського вторгнення в Україну, 24 лютого 2022 року, українська армія розгорнула й реалізувала масштабні контрнаступальні дії, у низці випадків ефективно використовуючи новітні технології когнітивної війни, що суттєво відрізняє даний військовий потенціал в українському контексті від інших видів воєнних дій [11, с. 6]. Враховуючи відсутність системного розуміння та системної роботи в отриманні когнітивної переваги та перемоги у когнітивній війні, окремі, безумовно визначні, успіхи, включаючи військове звільнення частини тимчасово окупованих територій та ґрунтовне розширення співпраці з країнами партнерами, зовсім не є приводом для самозаспокоєння. Але вони, як і сам факт того, що противник, незважаючи на чисельну перевагу і значно краще забезпечення усіма видами ресурсів, не зміг протягом десяти років гібридної агресії та трьох років широкомасштабних бойових дій досягнути поставлених цілей у когнітивній війні – знищити ідентичність українців та зламати їхній потенціал до спротиву, – свідчить, зокрема, про те, що нарощення динаміки інформаційних війн і фактичне формування когнітивної війни, поряд з новими викликами й загрозами, несе і нові можливості.

Зазвичай за цілями рівні комунікативної взаємодії в межах державного управління поділяють на довгострокові, які передбачають стратегічні цілі і відповідний стратегічний комунікативний ефект, середньострокові, спрямовані на отримання накопичувального ефекту при здійсненні комунікативного впливу та короткострокові, які забезпечують одноразовий комунікативний ефект [12 с. 133]. Погоджуючись в цілому із цією тезою, варто відзначити, що, як свідчать результати проведеного дослідження і практика, заходи державного управління у сфері захисту безпеки інформаційного простору, навіть якщо вони сплановані як короткострокові з одноразовим комунікативним ефектом, все одно мають ознаки оперативних (певний накопичувальний ефект) і, в кінцевому рахунку, можуть впливати на досягнення сторонами інформаційного протиборства стратегічного результату. Це, в свою чергу, вимагає від таких заходів ґрунтовної підготовки, ретельного планування та кваліфікованої реалізації у дуже стислі терміни.

Висновки та перспективи подальших розвідок у даному напрямку. Заходи державного управління у сфері захисту безпеки інформаційного простору, орієнтовані на отримання короткострокового результату (досягнення одноразових комунікативних цілей) є найбільш чисельними, але при цьому критично важливими, і до їх проведення висуваються надзвичайно високі вимоги. Такі вимоги стосуються оперативності моніторингу інформаційного простору, якості аналізу інформаційного середовища, точності визначення інформаційних загроз, ретельності планування реакції (прийняття рішення про її недоцільність), пропрацьованості інформаційного контенту для реагування, і передусім – виконання усіх цих та інших необхідних дій в надзвичайно стислі терміни.

Попри загалом правильні зусилля щодо розгортання в Україні та інших країнах підрозділів та структур, які повинні займатися протидією російській дезінформації, пропаганді та деструктивному інформаційно-психологічному впливу в цілому, доводиться констатувати недостатність чисельності таких підрозділів, фаховості їхнього персоналу, в окремих випадках – технічного та програмного забезпечення. Як наслідок, зусилля російських спецслужб, військово-терористичних формувань та пропагандистів у досягненні когнітивних ефектів і досі мають частковий, але досить суттєвий успіх.

З метою підвищення ефективності механізмів державного управління у сфері захисту

безпеки інформаційного простору пропоную вжити заходів:

1. Виділити організаційно, окрім підрозділів моніторингу інформаційного простору (які вже створені у багатьох державних відомствах), підрозділи реагування на інформаційні загрози за окремими напрямками відповідальності (тематичними, регіональними).

2. Організувати роботу єдиного координаційного центру з метою недопущення неузгодженості дій підрозділів реагування на інформаційні загрози (покласти відповідні функції на Центр протидії дезінформації РНБО) при забезпеченні центрів реагування на інформаційні загрози на місцях можливістю діяти максимально оперативно та автономно.

3. Забезпечити підрозділи реагування на інформаційні загрози необхідними кадровими, технічними та матеріальними ресурсами для виконання їхніх завдань.

4. Організувати розробку та доведення до відповідного персоналу стратегії участі у боротьбі за когнітивну (інформаційну) перевагу підрозділів реагування на інформаційні загрози у взаємодії з іншими складовими стратегічних комунікацій та інституціями, що реалізовують державну інформаційну політику.

5. Забезпечити взаємодію підрозділів реагування на інформаційні загрози з відповідними інституціями громадянського суспільства з метою консолідації українського громадянського суспільства та належної реалізації його потенціалу спротиву ворожим зусиллям в інформаційному середовищі.

6. З метою належної координації зусиль на міжнародному рівні організувати взаємодію українських підрозділів реагування на інформаційні загрози з колегами з міжнародних організацій та представниками країн-партнерів.

Перспективи подальших досліджень вбачаю у більш детальному вивченні середньострокових (оперативних) та довгострокових (стратегічних) наслідків застосування механізмів державного управління у сфері захисту безпеки інформаційного простору.

ЛІТЕРАТУРА:

1. Бондар В. Фактор перспективи США та протидія дезінформації: удосконалення системи національної безпеки. *Вчені записки ТНУ імені В. І. Вернадського.* 2023. №5. С. 94–98. DOI https://doi.org/10.32782/TNU-2663-6468/2023.5/16. (дата звернення 30.07.2024).

2. Недодай М., Дячук О., Примаченко Д., Святська Н. Використання можливостей штучного інтелекту у створенні інформаційно-психологічних операцій. Телекомунікаційні та інформаційні технології. 2024. № 2(83). С. 30–36. DOI: https://doi.org/10.31673/2412-4338.2024.024047. (дата звернення 30.07.2024).

3. Уманець А. Психологія національної безпеки та безпеки життєдіяльності. *Вчені записки ТНУ імені В.І. Вернадського.* 2022. № 3. DOI https://doi.org/10.32838/2709-3093/2022.3/18. (дата звернення 30.07.2024).

4. Гаргаун Я., Тулупніков Д. Пропаганда і дезінформація в російських та українських медіа: інформаційні технології у конфлікті. *Acta de Historia & Politica: Saeculum XXI*. 2024. №8. С. 53–61. DOI: https://doi.org/10.26693/ahpsxxi2024.08.053. (дата звернення 30.07.2024).

5. Мельник Р. Російський RT витратив у 2023 році рекордний бюджет. *Детектор-медіа* : вебсайт. 2024. URL: https://detector.media/infospace/article/225995/2024-04-26-rosiyskyy-rt-vytratyv-u-2023-rotsi-rekordnyy-byudzhet. (дата звернення 30.07.2024).

6. AJP-3.10.1(A) Allied joint doctrine for psychological operations. 2007. URL: https://info.publicintelligence.net/NATO-PSYOPS.pdf. (дата звернення 28.07.2024).

7. Ana Matías, luís Cardoso. Crisis communication. Theoretical perspectives and dynamics of a complex concept. *Visual Review.* 2023. С. 1–15. https://doi.org/10.37467/revvisual.v10.4597. (дата звернення 28.07.2024).

8. Andrzej Jarynowski Łukasz Krzowski Stanisław Maksymowicz. Biological mis(dis)- information in the Internet as a possible Kremlin warfare. 2023. 48 С. DOI: https://doi.org/10.5281/zenodo.7932530. (дата звернення 28.07.2024).

9. Кеті Као, Шон Глейстер, Едріена Пена, Денбі Р, Вільям Ронг, Александер Роваліно Сем Бішоп, Роган Ханна, Джейтін Сінгх Сайні, Лоуренс Еронхайм, Александер Кокрон. Протидія когнітивній війні: інформованість і стійкість. *NATO Reviev*. 2021. URL: https://www.nato.int/docu/review/uk/articles/2021/05/20/protidya-kogntivnj-vjn-nformovanst-stjkst/index.html. (дата звернення 28.07.2024).

10. Кестутіс Паулаускас. Чому когнітивна перевага є імперативом. *NATO Reviev*. – 2024. URL: https://www.nato.int/docu/review/uk/articles/2024/02/06/index.html. (дата звернення 28.07.2024).

11. Максименко С., Деркач Л. Генеза сучасної інформаційно когнітивної [гібридної] війни в українському контексті та глобальному вимірі. Наукове дослідження. 2024. 128 с. URL: https://lib.iitta.gov.ua/id/eprint/740932/1/LayOut02%20(1).pdf. (дата звернення 28.07.2024).

12. Висоцька О. Технології комунікативної політики держави як інструменти здійснення інформаційних війн. *Війни інформаційної епохи: міждисциплінарний дискурс: монографія.* 2021. 558 с. URL: http://library.dnu.dp.ua/vijni.pdf. (дата звернення 28.07.2024).