УДК 351.746:007
https://doi.org/10.32689/2617-2224-2025-1(42)-3

Кудрявський Іван Володимирович,
докторант, ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», 03039, м. Київ, вул. Фроменівська, 2, https://orcid.org/0009-0009-5167-7648

Kydriavskyi Ivan Volodymyrovych,
Doctoral Student, Interregional Academy of Personnel Management, 03039, Kyiv, 2, Frometivska Str., https://orcid.org/0009-0009-5167-7648

Крива Людмила Миколаївна,
кандидат історичних наук, директор Центру координації наукових видань та міжнародних проєктів ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», 03039, м. Київ, вул. Фрометівська, 2, https://orcid.org/0000-0002-8766-1543

Kryva Liudmyla Mykolayivna,
Candidate of Historical Sciences, Director of the Center of Scientific Publications Coordination and International Projects, Interregional Academy of Personnel Management, 03039, Kyiv, 2, Frometivska str., https://orcid.org/0000-0002-8766-1543

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

Анотація. Застосування механізмів державного управління у сфері захисту безпеки інформаційного простору, як і будь-яке втручання в інформаційний простір, залежно від його характеру та спрямованості, матиме низку серйозних наслідків у короткостроковій, середньостроковій і довгостроковій перспективі. Уряди держав зазвичай намагаються визначати стратегії розвитку в різних сферах. Переважно їх закріплюють у документах, і Україна не є в цьому винятком. Реагування або дії, зокрема й у сфері захисту безпеки інформаційного простору, які розраховані на коротко-

тривалі наслідки і відповідають на щоденні проблеми та виклики, теж не можуть залишитися поза увагою, оскільки це основна частина роботи як безпосередніх виконавців, так і осіб, що приймають рішення у сфері державного управління. При цьому наслідки дій та ефекти у середньостроковій перспективі, які знаходяться між рівнем стратегічного планування й повсякденними завданнями, іноді бувають обділені увагою спеціалістів і потребують додаткового дослідження через особливості їх пропрацювання.

Мета запропонованого дослідження – пошук способів підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору через аналіз історичних та сучасних середньострокових ефектів від заходів контролю інформаційного простору державними інституціями.

Завдання дослідження полягає в аналізі історичних джерел, наукових праць, офіційних повідомлень та публіцистичних матеріалів, що надають можливість вивчити проблематику функціонування механізмів державного управління у сфері захисту безпеки інформаційного простору в умовах відбиття Силами оборони України російського широкомасштабного вторгнення при інтенсивному застосуванні різними суб'єктами заходів контролю інформаційного простору в контексті оцінки середньострокових ефектів (незапланованих наслідків) від таких заходів.

Наукова новизна дослідження і його результатів полягає в комплексному розгляді проблемних питань сучасного державного управління у сфері захисту безпеки інформаційного простору України, пов'язаних з активним веденням учасниками наповнення інформаційного простору інформаційних дій з акцентом на наслідки таких дій у середньостроковій перспективі 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.

Висновки. Робота державних механізмів у сфері захисту безпеки інформаційного простору передбачає ефекти у середньостроковій перспективі у вигляді результатів сукупності синхронізованих інформаційних дій, а саме: стабільних змін оцінок, переконань, ставлень різноманітних, поєднаних між собою цільових аудиторій, на основі яких можна продовжувати подальшу реалізацію інформаційно-комунікаційної політики держави з метою поетапного наближення до досягнення стратегічного ефекту комунікаційної діяльності.

Для успішного планування й організації інформаційних дій та роботи механізмів державного управління у сфері захисту безпеки інформаційного простору недостатньо застосування доступних механізмів і систем автоматичного моніторингу інформаційного простору, належного кадрового відбору та якісної індивідуальної підготовки спеціалістів, що у своїй сукупності можуть забезпечити інформаційні дії тактичного рівня. Середньострокова перспектива (оперативний рівень інформаційно-комунікаційної діяльності) уже вимагає налагодженої роботи складних організаційних структур і їх колективів, детального аналізу та прогнозування дій учасників наповнення інформаційного простору й чіткої постійної координації як із державним керівництвом, що визначає стратегічні завдання, так і з безпосередніми виконавцями, що діють на тактичному рівні, за умов дотримання принципів якісного лідерства і наявності достатнього авторитету посадових осіб та інституцій інформаційно-комунікаційної діяльності оперативного рівня.

Враховуючи інтенсивність та масштаб бойових дій, які ведуться в рамках відбиття Україною російського широкомасштабного вторгнення, що підтримується повним арсеналом засобів деструктивного інформаційно-психологічного впливу російської федерації, найбільш придатними для застосування можуть бути методики аналізу і сценарії інформаційних дій, які розроблялися й випробовувалися не у цивільних сферах (політичної, економічної чи іншої конкуренції), а саме для протидії (нівелювання, мінімізації ефектів) деструктивному інформаційно-психологічному впливу воєнного противника, який ставить за мету глобальний вплив на чисельні цільові аудиторії з різним характером та особливостями сприйняття з метою досягнення воєнних і воєнно-політичних цілей при мінімальних або відсутніх механізмах стримування такої агресивної діяльності.

Перспективи подальших досліджень вбачаються у вивченні стратегічних ефектів роботи механізмів державного управління у сфері захисту безпеки інформаційного простору (у довгостроковій перспективі).

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

RESULTS OF APPLICATION OF PUBLIC ADMINISTRATION MECHANISMS IN THE FIELD OF INFORMATION SPACE SECURITY PROTECTION IN THE MEDIUM TERM

Abstract. The use of public administration mechanisms in the field of information space security, as well as any intervention in the information space, depending on its nature and focus, will have a number of serious consequences in the short, medium and long term. Governments usually try to define development strategies in various areas. Most of them are enshrined in documents, and Ukraine is no exception. Reactions or actions, including in the field of information space security, which are designed for short-term consequences and respond to daily problems and challenges, cannot be ignored, as this is the main part of the work of both direct executors and decision-makers in the field of public administration. At the same time, the consequences of actions and effects in the medium term, which lie between the level of strategic planning and everyday tasks, are sometimes deprived of the attention of specialists and require additional research due to the peculiarities of their elaboration.

The purpose of the proposed study is to find ways to improve the efficiency of public administration mechanisms in the field of information space security protection by analyzing the historical and current medium-term effects of information space control measures by state institutions.

The objective of the study is to analyze historical sources, scientific papers, official reports and journalistic materials that provide an opportunity to study the problems of functioning of public administration mechanisms in the field of information space security protection in the context of repulsion of the Russian large-scale invasion by the Ukrainian Defense Forces with intensive use of information space control measures by various actors in the context of assessing the medium-term effects (unintended consequences) of such measures.

The scientific novelty of the study and its results lies in a comprehensive consideration of the problematic issues of modern public administration in the field of protection of the security of Ukraine's information space related to the active conduct of information actions by participants in filling the information space with an emphasis on the consequences of such actions in the medium 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, formal and logical.

The conclusions. The work of state mechanisms in the field of information space security provides for effects in the medium term in the form of the results of a set of synchronized information actions, namely, stable changes in assessments, beliefs, attitudes of various interconnected target audiences, on the basis of which it is possible to continue further implementation of the state information and communication policy in order to gradually approach the achievement of the strategic effect of communication activities.

For successful planning and organization of information actions and operation of public administration mechanisms in the field of information space security protection, it is not enough to use available mechanisms and systems of automatic monitoring of the information space, proper personnel selection and high-quality individual training of specialists, which together can provide information actions of the tactical level. The medium-term perspective (the operational level of information and communication activities) already requires well-coordinated work of complex organizational structures and their teams, detailed analysis and forecasting of actions of participants in filling the information space and clear ongoing coordination with both the state leadership, which defines strategic tasks, and direct executors operating at the tactical level, provided that the principles of quality leadership are observed and that officials and institutions of information and communication have sufficient authority.

Given the intensity and scale of the hostilities that are being conducted as part of Ukraine's repulsion of Russia's large-scale invasion, supported by a full arsenal of destructive information and psychological influence, the most suitable for use may be the methods of analysis and scenarios of information actions that were developed and tested not in civilian spheres (political, economic or other competition), but specifically to counteract (level, minimize the effects of) the destructive information and psychological influence of the military enemy.

Prospects for further research are seen in the study of the strategic effects of the mechanisms of public administration in the field of information space security (in the long term).

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

Постановка проблеми. Питання стратегічного планування розвитку механізмів державного управління у сфері захисту безпеки інформаційного простору потребує постійної уваги з боку державного керівництва. В Україні прийнято низку нормативно-правових, нормативних актів та інших керівних документів, які регламентують стратегію розвитку механізмів державного управління у сфері захисту безпеки інформаційного простору. Це, зокрема, Стратегія інформаційної безпеки, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021 (Про Стратегію інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021), Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 р. № 392/220 (Про Стратегію національної безпеки України: Указ президента України від 14 вересня 2020 р. № 392/220), Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021 (Про стратегію кібербезпеки України: Указ президента України від 26 серпня 2021 р. № 447/2021), та багато інших. Як бачимо, основоположні документи, що визначають напрямки розвитку механізмів захисту безпеки інформаційного простору в Україні, закладалися ще до початку російського широкомасштабного вторгнення.

Стратегічне планування буде ускладненим за умов гострої кризи, особливо – викликаної активними бойовими діями в усіх відомих просторах ведення бойових дій, включаючи інформаційний простір. При цьому розуміння стратегічної мети та проміжних цілей в ході її поетапного досягнення є необхідною умовою забезпечення можливості планування й державного управління. Зрозуміло, що стратегічні документи і настанови не можуть змінюватися при кожній зміні зовнішніх обставин. Але надмірна консервативність призводить до того, що зміст, підхід, філософія та деякі окремі терміни у таких документах, як, наприклад, "гібридна агресія російської федерації" (Про стратегію кібербезпеки України: Указ президента України від 26 серпня 2021 р. № 447/2021), яка вже давно перейшла у формат широкомасштабної агресії за фактом, здаються дещо дивними. Досить сумнівно, що без відповідних редакцій та інтерпретацій такі документи можна ефективно застосовувати й керуватися ними в ході розробки керівних документів, розрахованих на врегулювання відповідних питань у середньостроковій перспективі.

Накази міністерств і відомств як доктрини зі стратегічних комунікацій Збройних Сил України (Доктрина зі стратегічних комунікацій Збройних Сил України: наказ Головнокомандувача Збройних Сил України від 12.10.2020 року № ВКП 10-00(49).01) та Національної гвардії України (Доктрина стратегічних комунікацій Національної гвардії України ВКП НГУ. Наказ командувача Національної гвардії України від 22.11.2021 № 541), відповідно, більш прив'язані до реальності, але теж не в повній мірі відповідають сучасним вимогам до процесу державного управління у сфері захисту безпеки інформаційного простору. Очевидна спроба взяти за основу при підготовці таких документів керівні положення відповідних доктрин Північно-атлантичного альянсу – зі стратегічних комунікацій, з інформаційних операцій та з психологічних комунікацій (NATO standard AJP-10, 2023; NATO standard AJP-10.1, 2023; NATO standard AJP-3.10.1(A), 2007) – загалом позитивно вплинула на кінцевий результат, але недостатнє пропрацювання першоджерел і їх неналежна адаптація до вимог умов відбиття широкомасштабної російської агресії, коли відбуваються довготривалі бойові дії, що не поступаються масштабами театрам бойових дій світових воєн, призвели до того, що ці документи (на зразок (Доктрина зі стратегічних комунікацій Збройних Сил України: наказ Головнокомандувача Збройних Сил України від 12.10.2020 року № ВКП 10-00(49).01; Доктрина стратегічних комунікацій Національної гвардії України ВКП НГУ. Наказ командувача Національної гвардії України від 22.11.2021 № 541)) фактично стали застарілими і вимагають доопрацювання практично з моменту їх прийняття.

Серед українських дослідників існує думка, що, з урахуванням стану розвитку поточної ситуації, рівень загрози збройної агресії росії проти України можливо вважати критичним. У середньостроковій перспективі після завершення бойових дій на території України рівень загрози повторного вторгнення з боку рф залишатиметься високим (Братко, 2023). Поряд з тим, немає факторів, які дозволяли б на даний момент адекватно спрогнозувати сам момент завершення бойових дій, тому точка відліку середньострокової перспективи у даному випадку теоретично може настати у період, що відповідає довгостроковому стратегічному плануванню. Але навіть при цьому в процесі державного управління у сфері захисту безпеки інформаційного простору доведеться враховувати наслідки середньострокової перспективи та загрозу повторного нападу з боку росії (якщо, звісно, вона не буде нейтралізована у процесі

війни як держава, що станом на зараз видається маловірогідним).

В ідеальних умовах планування на довгострокову, середньострокову та короткострокову перспективу в процесі державного управління повинно здійснюватися на основі прогнозування. Саме у процесі прогнозування на державному рівні формується стратегічне бачення розвитку держави на довгострокову, середньострокову та короткострокову перспективи. При цьому середньострокові прогнозні розробки служать базою для формування багатоваріантного довгострокового прогнозу, де в основі більшості варіантів лежать не обмежені коливання вихідних даних, а варіанти кінцевих цільових настанов, що мають явно виражений соціально-економічний зміст (Євмєшкіна, 2017). Але в умовах кризи, та особливо – війни, сам по собі процес прогнозування може бути дуже ускладнений високою вірогідністю настання різноманітних подій, які кардинально змінюють ситуацію.

Залишається нерозкритим питання визначення самих понять довго- середньо- та короткострокової перспективи у питаннях реалізації інформаційних дій та стратегічних комунікацій загалом. Спробуємо розглянути це питання на прикладі дослідження позиції учасників наповнення інформаційного простору, що працюють із соціальними мережами. Глибинні інтерв'ю розкрили дві головні теми:

– використання соціальних медіа повинно керуватися стратегічним плануванням;

– тактика соціальних медіа має обертатися навколо розмов. Результати опитування показали, що фахівці-практики, залучені до розробки та тактичної реалізації стратегії соціальних медіа, бачать свою участь як пов'язану здебільшого зі стратегічною, а не з тактичною діяльністю їхніх організацій у соціальних мережах.

Крім того, практики окреслюють стратегію та тактику соціальних мереж інакше, ніж теоретичні концептуалізації (Плаумен, Вілсон, 2018). Попри те, що проблема відома достатньо давно, не можна сказати, щоби дослідники та практики дуже сильно просунулися у її розв'язанні.

Отже, питання середньострокової перспективи у державному управлінні захистом безпеки інформаційного простору доцільно розділити щонайменше на дві основні складові, поєднані між собою, але все ж різні за своєю природою:

– середньострокова перспектива у плануванні розвитку механізмів державного управління захистом безпеки інформаційного простору;

– середньострокова перспектива реалізації механізмів захисту безпеки інформаційного простору (як етап реалізації стратегічних комунікацій, віддалені за часом наслідки застосування множини синхронізованих інформаційних дій).

Якщо у військовій сфері застосування будь-яких видів озброєння або будь-якого впливу на будь-який простір ведення бойових дій, включаючи й інформаційний простір, вирішено поділом на стратегічний, оперативний і тактичний рівні, то у сфері цивільних аспектів державного управління загальноприйнята система поділу на довго- середньо- та короткострокове планування за періодом часу (до 1 року, від 1 до 5 років і більше 5 років) явно потребує коригування за умов глобального нерівномірного прискорення проходження соціальних процесів та блискавичності сучасних дій і процесів в інформаційному просторі.

Найбільш актуальним та найменш дослідженим за таких умов, залишається питання планування й реалізації інформаційних дій, які мають наслідки у середньостроковій перспективі. При цьому якщо питання стратегічних комунікацій і стратегічної перспективи інформаційно-комунікаційної діяльності є постійним об'єктом уваги дослідників і практиків, як і питання інформаційних дій тактичного рівня, що реалізовуються щоденно, – то питання середньострокової перспективи реалізації синхронізованої множинності інформаційних дій (інформаційної акції, серії матеріалів деструктивного інформаційно-психологічного впливу тощо) і на сьогодні є недостатньо дослідженим. У той же час середньострокові наслідки втручання, зокрема і шляхом застосування механізмів державного управління, в інформаційний простір мають суттєву специфічну проблематику в їх прогнозуванні. Адже діяльність посадових осіб, які реалізовують державне управління та планування в масштабі середньострокової перспективи, повинно поєднувати відповідність стратегічному задуму з адекватною постановкою завдань для реалізації адекватних інформаційних дій у повсякденному житті (на тактичному рівні). Це, своєю чергою, вимагає досягнення успіху в розвитку низки складових:

– у питанні юридичного забезпечення: наявності достатньої кількості керівних документів на рівні наказів центральних органів виконавчої влади, їх своєчасного постійного оновлення у відповідності до вимог часу та обстановки;

– у питані кадрового відбору та реалізації управлінської діяльності: поєднання лідерства (щодо посадових осіб, які діють на тактичному рівні та безпосередньо реалізовують інформаційні дії) з глибоким розумінням проблематики

на стратегічному рівні та дисциплінованістю й адекватністю впровадження стратегічних тенденцій в оперативне планування;

– у питанні ресурсного забезпечення: здатність, виходячи зі стратегічних завдань, спланувати, та щонайменше – замовити, необхідні ресурси, які знадобляться у середньостроковій перспективі не лише для виконання завдань посадових осіб оперативного рівня, але й для тих, хто буде безпосередньо реалізовувати інформаційні дії у відповідний період часу;

– у питанні інформаційно-аналітичної діяльності: за наявності надлишкової кількості інформації сформувати, відповідно до умов часу, обстановки та конкретних стратегічних напрямків розвитку механізмів державного управління захистом безпеки інформаційного простору, систему відбору інформації для аналізу та її коректної обробки з метою постановки належним чином завдань персоналу тактичного рівня.

Цей перелік питань, досягнення успіху у кожному з яких є непростим завданням, особливо в умовах кризи, а тим більше, як у нашому випадку, війни, є далеко не повним. Їх розв'язання доцільно починати з визначення власне того, що таке наслідки інформаційно-комунікаційної діяльності у середньостроковій перспективі, якими вони можуть бути, та, відповідно, якими можуть бути наслідки застосування механізмів державного управління захистом безпеки інформаційного простору у середньостроковій перспективі при застосуванні інструментарію інформаційно-комунікаційної діяльності (переважно) та інших доступних інструментів (меншою мірою).

Завдання дослідження полягає в аналізі історичних джерел, наукових праць, офіційних повідомлень та публіцистичних матеріалів, що надають можливість вивчити проблематику функціонування механізмів державного управління у сфері захисту безпеки інформаційного простору в умовах відбиття Силами оборони України російського широкомасштабного вторгнення при інтенсивному застосуванні різними суб'єктами заходів контролю інформаційного простору у контексті оцінки середньострокових ефектів (незапланованих наслідків) від таких заходів.

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, серед яких: (Братко, 2023; Євмєшкіна, 2017; Vakaliuk, Pilkevych, et al. 2022); українських та іноземних нормативно-правових актах (Про Стратегію інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021; Про Стратегію національної безпеки України: Указ президента України від 14 вересня 2020 р. № 392/220; Про стратегію кібербезпеки України: Указ президента України від 26 серпня 2021 р. № 447/2021; Доктрина зі стратегічних комунікацій Збройних Сил України: наказ Головнокомандувача Збройних Сил України від 12.10.2020 року № ВКП 10-00(49).01; Доктрина стратегічних комунікацій Національної гвардії України ВКП НГУ. Наказ командувача Національної гвардії України від 22.11.2021 № 541; NATO standard AJP-10, 2023; NATO standard AJP-10.1, 2023; NATO standard AJP-3.10.1(A), 2007); публікаціях у медіа (Semantic Force Listen; Attack index; LOOQME).

Мета запропонованого дослідження – пошук способів підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору через аналіз історичних та сучасних середньострокових ефектів від заходів контролю інформаційного простору державними інституціями.

Виклад основного матеріалу дослідження з обґрунтуванням отриманих результатів. Досвід військової агресії російської федерації проти України показав актуальність та необхідність осмислення проблем морально-психологічного забезпечення у Збройних Силах України в сучасних умовах. Проблема постійної дезінформації населення, поширення пропаганди та здійснення деструктивного психологічного впливу в інтересах противника є дуже чутливою. Найпростішим інструментом для поширення дезінформації є Інтернет (легкий доступ і широка популярність). Зараз важливою є розробка методології моніторингу негативних психологічних впливів в онлайн-медіа (Vakaliuk, Pilkevych, et al. 2022). Системи автоматичного моніторингу інформаційного простору, без яких практично неможливо організувати ефективну діяльність посадових осіб органів державного управління у сфері захисту безпеки інформаційного простору на тактичному рівні, які повинні забезпечувати необхідні ефекти інформаційних дій та захист безпеки інформаційного простору в короткостроковій та середньостроковій

перспективі, далеко не завжди виконують свої завдання належним чином.

Протягом останніх років системи моніторингу інформаційного простору були сильно удосконалені. Практично всі вони побудовані із застосуванням нейромереж, здатних до активного навчання, що володіють високою адаптивністю. За основу таких комплексів, що зазвичай поєднують у собі складні технології з роботою кваліфікованих спеціалістів, можуть братися різні види інформації для аналізу або поєднання цих видів (типів) інформації. Чи не найбільш поширений та популярний сьогодні моніторинг інформаційного простору на основі нейролінгвістичного або семантичного аналізу, який застосовується, зокрема, такими автоматичними системами моніторингу інформаційного простору, як Semantic Force (Semantic Force Listen) чи українська Attack index (Attack index). Може також активно застосовуватися або братися за основу аналіз візуальних образів, зокрема глибинний аналіз оперативних результатів візуальної психодіагностики, як у роботі системи автоматичного моніторингу інформаційного простору LOOQME (LOOQME). Такі інструменти, попри те, що вони є достатньо дорогими (вимагають регулярної оплати, встановлення спеціального програмного забезпечення, в окремих випадках – встановлення та налаштування спеціальної апаратури, навчання персоналу організації), здатні значно полегшити роботу посадових осіб, які беруть участь в діяльності механізмів державного управління захистом безпеки інформаційного простору на тактичному рівні. Вони дозволяють достатньо швидко та ефективно знайти інформацію за необхідною тематикою, в окремих випадках – визначити тональність цієї інформації (позитивну, негативну, нейтральну тощо). Це досить сильно допомагає в аналізі поточної обстановки. Компанії, які презентують такі автоматичні системи моніторингу інформаційного простору, зазвичай вказують наявність аналітичного модуля та декларують можливість автоматичного створення прогнозів, прогнозування дій суб'єктів інформаційної атаки, деструктивного інформаційно-психологічного впливу. На практиці ж такий продукт виглядає зазвичай малопридатним для застосування і переважно не може задовольняти потреби персоналу, що реалізовує планування інформаційних дій на рівні середньострокової перспективи.

Попри здатність до навчання нейромереж, інтеграція зусиль технічних спеціалістів та експертів у сфері масової інформації поки не досягла такого рівня, щоби враховувати усі соціокультурні особливості, традиції та висловлювання, які можуть не бути широковідомими, але активно застосовуватися у середовищі окремих субкультур, та інші елементи контенту, які недостатньо аналізувати за їхнім прямим лексичним значенням чи навіть за результатами візуальної психодіагностики графічної складової контенту, який поширюється. Добра усмішка далеко не завжди означає відсутність деструктивного інформаційно-психологічного впливу або його елементів у контенті, що поширюється, а прямого лінгвістичного аналізу без урахування контекстів, тим більше, може бути недостатньо. Особливо це стосується випадків, коли деструктивний інформаційно-психологічний вплив планується у декілька етапів на середньострокову перспективу та передбачає поступове, поетапне, досягнення результатів. За таких обставин само по собі питання визначення, якого кінцевого ефекту намагається досягнути суб'єкт реалізації деструктивного інформаційно-психологічного впливу, вимагає не просто застосування програмно-технічного забезпечення достатньої якості, але й тривалої роботи вузьких спеціалістів.

Більше того, механізми державного управління захистом безпеки інформаційного простору в Україні мають своїм завданням не просто врегулювання та легке коригування нормального функціонування інформаційного простору, але й протидію деструктивному інформаційно-психологічному впливу противника, який в умовах війни здійснюється безперервно протягом багатьох років на тактичному, оперативному та стратегічному рівні усіма доступними способами та інструментами.

Якщо атакуючій стороні для досягнення тактичного чи оперативного (у середньостроковій перспективі) ефекту деструктивного інформаційно-психологічного впливу достатньо правильно обрати вразливу цільову аудиторію та глибоко вивчити контексти й усю доступну інформацію за якоюсь вузькою тематикою, чутливою саме для обраної аудиторії, то посадовій особі, яка намагатиметься протидіяти такому деструктивному інформаційно-психологічному впливу, навіть просто для його ідентифікації та оцінки, не кажучи вже про розробку шляхів протидії, необхідно знати набагато більший об'єм інформації, аніж тому, хто планує деструктивний інформаційно-психологічний вплив. За приблизно однакового рівня знань, загальної ерудиції, досвіду і професіоналізму в цілому, у конкретній життєвій ситуації протистояння спеціаліст з інформаційно-психологічних опе-

рацій, який реалізовує деструктивний інформаційно-психологічний вплив, завжди матиме суттєву перевагу над посадовою особою органів державного управління, що забезпечує протидію (нівелювання наслідків) деструктивному інформаційно-психологічному впливу.

Тому для адекватної реалізації захисту безпеки інформаційного простору необхідно мати або значно вищий професійний рівень та, одночасно, кількісну перевагу кадрів, які працюють у напрямку протидії (нівелювання результатів) ворожому деструктивному інформаційно-психологічному впливу, що в наших умовах завідомо неможливо, враховуючи багатократну перевагу противника у ресурсах, або ж виходити з ситуації шляхом удосконалення систем та механізмів державного управління, нав'язування ініціативи в ході протистояння в інформаційному просторі, здобуття когнітивної переваги, та власне, шляхом активного застосування нелінійних асиметричних заходів у поєднанні з дотриманням правил комунікації, які дозволяють уникнути дискредитації каналів поширення інформації не лише у короткостроковій, але й у середньостроковій та довгостроковій перспективі.

Якщо цивільні, загальнодоступні, особливо – виключно програмні, механізми аналізу контенту можуть задовольняти потреби короткострокової перспективи (тактичного рівня) у питаннях захисту безпеки інформаційного простору, але бути абсолютно непридатними для планування й активності на оперативному рівні (у середньостроковій перспективі), то видається логічним звернутися до систем та аналітичних методик, які спеціально розроблялися і призначалися для протидії (нівелювання наслідків) деструктивному інформаційно-психологічному впливу противника (у значенні озброєного ворога, мотивація якого спрямована на знищення), а не емоційного ображеного окремого представника цільової аудиторії чи, у крайньому разі, бізнес-конкурента.

Так, доктрина з психологічних операцій НАТО AJP 3.10.1 пропонує застосовувати для оцінки діяльності противника у питаннях деструктивного інформаційно-психологічного впливу SCAME-аналіз. Аналіз психологічної активності противника передбачає детальне вивчення джерела, змісту, аудиторії, носіїв та ефектів (SCAME) його повідомлень з метою отримання розвідувальних даних, які доповнюють традиційні форми розвідки. Аудиторія та ефекти можуть бути як ненавмисними, так і навмисними. Основною метою аналізу психологічної активності противника є збір розвідувальної інформації, пов'язаної з деструктивним інформаційно-психологічним впливом (PSYOPS). Це робиться для того, щоб оцінити її вплив на власні війська, а також на дружню і неприхильну цивільну аудиторію в межах району відповідальності, щоб мати можливість усунути або зменшити негативні наслідки, а також використати будь-яке протиріччя в цій психологічній діяльності противника. Аналіз також передбачає систематичне вивчення іноземних засобів масової комунікації, призначених для внутрішньої та/або міжнародної аудиторії (NATO standard AJP-3.10.1(A), 2023).

Доктрина не обмежується методикою аналізу активності противника у питаннях деструктивного інформаційно-психологічного впливу і пропонує десять технік, які виявилися ефективними у минулому та можуть застосовуватися у майбутньому для нівелювання (мінімізації) ефектів деструктивного інформаційно-психологічного впливу противника. Це, зокрема, пряме спростування, непряме спростування, випередження, відволікання уваги, ініціативний обман, мінімізація, імунізація, ізоляція, мовчання, обмежувальні заходи та контроль над чутками (NATO standard AJP-3.10.1(A), 2007). Такі заходи реалізовуються й зараз і залишаються ефективними, оскільки при їх розробці враховувався не лише розвиток науки, техніки та сучасного інформаційно-комунікативного середовища, але передусім – сама людська природа, яка, попри розвиток технологій, у багатьох питаннях залишається практично незмінною, а в період екстремальних ситуацій, катаклізмів, воєн та революцій дуже швидко повертається до традиційної жорсткої форми, дуже швидко втрачаючи будь-які гуманістичні нашарування цивілізації.

З іншого боку, хоча методики на кшталт SCAME-аналізу теоретично може застосовувати один висококваліфікований аналітик із достатнім програмно-технічним забезпеченням самостійно, на практиці вони розроблялися та вдосконалювалися з урахуванням роботи штабу чи аналогічного колективу людей, які є фахівцями у своїй справі, та робота яких підпорядкована чітким правилам управління й ієрархічної взаємодії. Безумовно, утримання таких фахівців та забезпечення їхньої роботи буде значно дорожчим, аніж підписка на автоматичну систему моніторингу інформаційного простору, але й результат прогнозів, і прийняті рішення щодо роботи державних механізмів у сфері захисту безпеки інформаційного простору, розрахованої на ефекти у середньостроковій пер-

спективі, у такому випадку можуть стати більш ефективними.

Залишається відкритим питання, що вважати наслідками інформаційних дій у середньостроковій перспективі та за якими критеріями їх визначати. Якщо мова йде про період від одного до п'яти років, – то в умовах сучасної динаміки інформаційного середовища ми, переважно, не можемо згадати, що було актуальним в інформаційному порядку денному рік тому. Поряд з тим, поняття когнітивної зброї, наприклад, передбачає закладку нешкідливих, на перший погляд, наративів, які в окремих випадках повинні спрацювати навіть не у середньостроковій, а в довгостроковій стратегічній перспективі, коли будуть досягнуті необхідні умови, створення яких може бути покладено на зовсім інші механізми державного управління, не завжди прямо пов'язані з інформаційним простором.

Прикладом типового завдання інформаційних дій, розрахованих на ефект у середньостроковій перспективі, може виступати стабільна, належним чином зафіксована зміна оцінок та переконань цільової аудиторії щодо певного об'єкта, яка, відповідно, дає можливість проводити подальшу інформаційну політику, аж до поетапного досягнення кінцевого стратегічного ефекту відповідної інформаційно-комунікаційної діяльності. Це значно більше, аніж одноразова диверсифікація (відволікання) суспільної думки від важливих чи чутливих питань з метою вирішення повсякденних епізодичних завдань тактичного рівня, але й значно менше, аніж наприклад, налагодження взаємовідносин з урядом іншої країни при сприятливій позитивній думці населення обох країн чи зайняття певного становища держави у визначеній міжнародній спільноті з визначеними переговорними (іншими) позиціями щодо певного спектру питань.

Висновки та перспективи подальших розвідок у даному напрямку. Робота державних механізмів у сфері захисту безпеки інформаційного простору передбачає ефекти у середньостроковій перспективі у вигляді результатів сукупності синхронізованих інформаційних дій, а саме: стабільних змін оцінок, переконань, ставлень різноманітних, поєднаних між собою цільових аудиторій, на основі яких можна продовжувати подальшу реалізацію інформаційно-комунікаційної політики держави з метою поетапного наближення до досягнення стратегічного ефекту комунікаційної діяльності.

Для успішного планування й організації інформаційних дій та роботи механізмів державного управління у сфері захисту безпеки інформаційного простору недостатньо застосування доступних механізмів і систем автоматичного моніторингу інформаційного простору, належного кадрового відбору та якісної індивідуальної підготовки спеціалістів, що у своїй сукупності можуть забезпечити інформаційні дії тактичного рівня. Середньострокова перспектива (оперативний рівень інформаційно-комунікаційної діяльності) уже вимагає налагодженої роботи складних організаційних структур і їх колективів, детального аналізу та прогнозування дій учасників наповнення інформаційного простору й чіткої постійної координації як із державним керівництвом, що визначає стратегічні завдання, так і з безпосередніми виконавцями, що діють на тактичному рівні, за умов дотримання принципів якісного лідерства і наявності достатнього авторитету посадових осіб та інституцій інформаційно-комунікаційної діяльності оперативного рівня.

Враховуючи інтенсивність та масштаб бойових дій, які ведуться в рамках відбиття Україною російського широкомасштабного вторгнення, що підтримується повним арсеналом засобів деструктивного інформаційно-психологічного впливу російської федерації, найбільш придатними для застосування можуть бути методики аналізу і сценарії інформаційних дій, які розроблялися й випробовувалися не у цивільних сферах (політичної, економічної чи іншої конкуренції), а саме для протидії (нівелювання, мінімізації ефектів) деструктивному інформаційно-психологічному впливу воєнного противника, який ставить за мету глобальний вплив на чисельні цільові аудиторії з різним характером та особливостями сприйняття з метою досягнення воєнних і воєнно-політичних цілей при мінімальних або відсутніх механізмах стримування такої агресивної діяльності.

Перспективи подальших досліджень вбачаються у вивченні стратегічних ефектів роботи механізмів державного управління у сфері захисту безпеки інформаційного простору (у довгостроковій перспективі).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про Стратегію інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/685/2021/print (дата звернення – 18.01.2025).
2. Про Стратегію національної безпеки України: Указ президента України від 14 вересня

2020 р. № 392/220. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення – 18.01.2025).
3. Про стратегію кібербезпеки України: Указ президента України від 26 серпня 2021 р. № 447/2021. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/447/2021/print (дата звернення – 18.01.2025).
4. Доктрина зі стратегічних комунікацій Збройних Сил України: наказ Головнокомандувача Збройних Сил України від 12.10.2020 року № ВКП 10-00(49).01. Сили територіальної оборони ЗСУ. URL: https://sprotyvg7.com.ua/wp-content/uploads/2022/04/%D0%92%D0%9A%D0%9F-10-0049.01-%D0%94%D0%BE%D0%BA%D1%82%D1%80%D0%B8%D0%BD%D0%B0-%D0%B7%D1%96-%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%87%D0%BD%D0%B8%D1%85-%D0%BA%D0%BE%D0%BC%D1%83%D0%BD%D1%96%D0%BA%D0%B0%D1%86%D1%96%D0%B8%CC%86.pdf (дата звернення – 18.01.2025).
5. Доктрина стратегічних комунікацій Національної гвардії України ВКП НГУ. Наказ командувача Національної гвардії України від 22.11.2021 № 541. Національна гвардія України. URL: https://ngu.gov.ua/wp-content/uploads/2022/12/vkp-11-0101.01-doktryna-strategichnyh-komunikaczij-ngu.pdf.pdf (дата звернення – 18.01.2025).
6. NATO standard AJP-10. Allied Joint Doctrine for strategic communications. March 2023. URL: https://assets.publishing.service.gov.uk/media/6525459d244f8e00138e7343/AJP_10_Strat_Comm_Change_1_web.pdf (дата звернення 18.01.2025).
7. NATO standard AJP-10.1. Allied Joint Doctrine for information operations. january 2023. URL: https://assets.publishing.service.gov.uk/media/650c03bf52e73c000d9425bb/AJP_10_1_Info_Ops_UK_web.pdf (дата звернення 18.01.2025).
8. NATO standard AJP-3.10.1(A) Allied Joint Doctrine for psychological operations. October 2007. URL: https://info.publicintelligence.net/NATO-PSYOPS.pdf (дата звернення 18.01.2025).
9. Братко А. Аналіз загроз безпековому середовищу в прикордонному просторі. Соціальний розвиток і безпека, 2023. 13 (4), С. 14. https://doi.org/10.33445/sds.2023.13.4.2 (дата звернення 18.01.2025).
10. Євмєшкіна О. Реалізація функції прогнозування на різних рівнях державного управління. *Державне управління та місцеве самоврядування*, 2017. Вип. 1(32). URL: https://scholar.googleusercontent.com/scholar?q=cache:vJnIMqsViesJ:scholar.google.com/+Державне+управління:+стратегічне,+середньострокове+і+короткострокове+планування&hl=uk&as_sdt=0,5 (дата звернення 19.01.2025)
11. Плаумен К. Д., Вілсон, К. Стратегія і тактика в стратегічній комунікації: вивчення їх перетину з використанням соціальних медіа. *Міжнародний журнал стратегічних комунікацій*. 2018. 12 (2), 125–144. https://doi.org/10.1080/1553118X.2018.1428979 (дата звернення 19.01.2025).
12. Vakaliuk, T. A., Pilkevych, I. A., Fedorchuk, D. L., Osadchyi, V. V., Tokar, A. M. and Naumchak, O. M., 2022. Methodology of monitoring negative psychological influences in online media. *Educational Technology Quarterly.* 2022(2), pp. 143–151. Available from: https://doi.org/10.55056/etq.1 (дата звернення 19.01.2025).
13. Semantic Force Listen. Understand. Act. URL: https://semanticforce.ai/ua (дата звернення 19.01.2025).
14. Attack index. Контролюй та коригуй інформацію про себе. URL: https://attackindex.com/uk/golovna-attakindex/ (дата звернення 19.01.2025).
15. LOOQME. Комплексні аналітичні звіти про бренд. URL: https://www.looqme.io/reports/content-analysis (дата звернення 19.01.2025).

REFERENCES:

1. Pro Stratehiiu informatsiinoi bezpeky: Ukaz Prezydenta Ukrainy vid 28 hrudnia 2021 roku № 685/2021. [On the Information Security Strategy: Decree of the President of Ukraine of December 28, 2021 No. 685/2021]. Verkhovna Rada Ukrainy. Retrieved from: https://zakon.rada.gov.ua/laws/show/685/2021/print. [in Ukrainian].
2. Pro Stratehiiu natsionalnoi bezpeky Ukrainy: Ukaz prezydenta Ukrainy vid 14 veresnia 2020 r. № 392/220. [On the National Security Strategy of Ukraine: Decree of the President of Ukraine of September 14, 2020, No. 392/220]. Verkhovna Rada Ukrainy. Retrieved from: https://zakon.rada.gov.ua/laws/show/392/2020#Text. [in Ukrainian].
3. Pro stratehiiu kiberbezpeky Ukrainy: Ukaz prezydenta Ukrainy vid 26 serpnia 2021 r. № 447/2021. [On the cybersecurity strategy of Ukraine: Decree of the President of Ukraine of August 26, 2021, No. 447/2021]. Verkhovna Rada Ukrainy. Retrieved from: https://zakon.rada.gov.ua/laws/show/447/2021/print. [in Ukrainian].
4. Doktryna zi stratehichnykh komunikatsii Zbroinykh Syl Ukrainy: nakaz Holovnokomanduvacha Zbroinykh Syl Ukrainy vid 12.10.2020 roku № VKP 10-00(49).01. [Doctrine on Strategic Communications of the Armed Forces of Ukraine: Order of the Commander-in-Chief of the Armed Forces of Ukraine of 12.10.2020 No. VKP 10-00(49).01.]. Syly terytorialnoi oborony ZSU. Retrieved from: https://sprotyvg7.com.ua/wp-content/uploads/2022/04/%D0%92%D0%9A%D0%9F-10-0049.01-%D0%94%D0%BE%D0%BA%D1%82%D1%80%D0%B8%D0%BD%D0%B0-%D0%B7%D1%96-%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%87%D0%BD%D0%B8%D1%85-%D0%BA%D0%BE%D0%BC%D1%83%D0%BD%D1%96%D0%BA%D0%B0%D1%86%D1%96%D0%B8%CC%86.pdf [in Ukrainian].

5. Doktryna stratehichnykh komunikatsii Natsionalnoi hvardii Ukrainy VKP NHU. Nakaz komanduvacha Natsionalnoi hvardii Ukrainy vid 22.11.2021 № 541. [The Doctrine of Strategic Communications of the National Guard of Ukraine of the NGU. Order of the Commander of the National Guard of Ukraine of 22.11.2021 No. 541]. Natsionalna hvardiia Ukrainy. Retrieved from: https://ngu.gov.ua/wp-content/uploads/2022/12/vkp-11-0101.01-doktryna-strategichnyh-komunikaczij-ngu.pdf.pdf. [in Ukrainian].
6. NATO standard AJP-10. Allied Joint Doctrine for strategic communications. March 2023. Retrieved from: https://assets.publishing.service.gov.uk/media/6525459d244f8e00138e7343/AJP_10_Strat_Comm_Change_1_web.pdf. [in English].
7. NATO standard AJP-10.1. Allied Joint Doctrine for information operations. january 2023. Retrieved from: https://assets.publishing.service.gov.uk/media/650c03bf52e73c000d9425bb/AJP_10_1_Info_Ops_UK_web.pdf [in English].
8. NATO standard AJP-3.10.1(A) Allied Joint Doctrine for psychological operations. October 2007. Retrieved from: https://info.publicintelligence.net/NATO-PSYOPS.pdf [in English].
9. Bratko, A. (2023). Analiz zahroz bezpekovomu seredovyshchu v prykordonnomu prostori. [Bratko A. Analiz zahroz bezbekovomu seredovyshchu v prykordonnomu prostori]. Sotsialnyi rozvytok i bezpeka. [Social development and security]. 13 (4). DOI: https://doi.org/10.33445/sds.2023.13.4.2 [in Ukrainian].
10. Ievmieshkina, O. (2017). Realizatsiia funktsii prohnozuvannia na riznykh rivniakh derzhavnoho upravlinnia. [Realization of the forecasting function at different levels of public administration]. *Derzhavne upravlinnia ta mistseve samovriaduvannia*. 1(32). Retrieved from: https://scholar.googleusercontent.com/scholar?q=cache:vJnIMqsViesJ:scholar.google.com/+%D0%94%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%BD%D0%B5+%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F:+%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%87%D0%BD%D0%B5,+%D1%81%D0%B5%D1%80%D0%B5%D0%B4%D0%BD%D1%8C%D0%BE%D1%81%D1%82%D1%80%D0%BE%D0%BA%D0%BE%D0%B2%D0%B5+%D1%96+%D0%BA%D0%BE%D1%80%D0%BE%D1%82%D0%BA%D0%BE%D1%81%D1%82%D1%80%D0%BE%D0%BA%D0%BE%D0%B2%D0%B5+%D0%BF%D0%BB%D0%B0%D0%BD%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F&hl=uk&as_sdt=0,5 [in Ukrainian].
11. Plaumen, K., Vilson, K. (2018). Stratehiia i taktyka v stratehichnii komunikatsii: vyvchennia yikh peretynu z vykorystanniam sotsialnykh media [Ploumen, K., Wilson, K. Strategy and tactics in strategic communication: exploring their intersection with the use of social media]. *Mizhnarodnyi zhurnal stratehichnykh komunikatsii*. 12 (2), 125–144. https://doi.org/10.1080/15531 18X.2018.1428979 [in Ukrainian].
12. Vakaliuk, T. A., Pilkevych, I. A., Fedorchuk, D. L., Osadchyi, V. V., Tokar, A. M. and Naumchak, O. M., (2022). Methodology of monitoring negative psychological influences in online media. *Educational Technology Quarterly.* (2), pp.143–151. Retrieved from: https://doi.org/10.55056/etq.1 [in English].
13. Semantic Force Listen. Understand. Act. Retrieved from: https://semanticforce.ai/ua [in Ukrainian].
14. Attack index. Control and correct information about yourself. Retrieved from: https://attackindex.com/uk/golovna-attakindex/ [in English].
15. LOOQME. Comprehensive analytical reports on the brand. Retrieved from: https://www.looqme.io/reports/content-analysis [in English].