Функціонування і розвиток механізмів державного управління

УДК 351.751:004.056

Кудрявський Іван Володимирович
докторант
Міжрегіональної Академії управління персоналом
Kydriavskyi Ivan
Doctoral Student of the
Interregional Academy of Personnel Management
ORCID: 0009-0009-5167-7648

РЕЗУЛЬТАТИ ЗАСТОСУВАННЯ МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ У СФЕРІ ЗАХИСТУ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ У ДОВГОСТРОКОВІЙ (СТРАТЕГІЧНІЙ) ПЕРСПЕКТИВІ

RESULTS OF THE APPLICATION OF PUBLIC ADMINISTRATION MECHANISMS IN THE FIELD OF INFORMATION SPACE SECURITY PROTECTION IN THE LONG-TERM (STRATEGIC) PERSPECTIVE

Анотація. *Механізми державного управління у сфері захисту безпеки інформаційного простору за самою своєю природою повинні застосовуватися за результатами моніторингу інформаційного простору і прогнозування ситуації швидко, а краще – на випередження. Це пов'язано із високою динамічністю процесів у сучасному інформаційному просторі. Поряд з тим, значною мірою до ситуації, яка виникла в Україні сьогодні, включаючи відбиття широкомасштабної російської агресії, призвели якраз відсутність механізмів державного управління у сфері захисту безпеки інформаційного простору і те, що їх роками не застосовували та навіть не формували належним чином з урахуванням довготривалих*

наслідків – стратегічної перспективи. Зараз, в умовах війни, коли багато факторів неможливо передбачити і спрогнозувати, таке планування реалізувати ще складніше, але, при цьому, воно є ще необхіднішим. Адже сформувати стійку систему якісних механізмів державного управління у сфері захисту безпеки інформаційного простору, яка витримає воєнні стреси і сприятиме просуванню внутрішньополітичних цілей держави у період післявоєнної відбудови неможливо без довгоперспективного планування.

Мета запропонованого дослідження – пошук способів підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору через аналіз історичних та сучасних довгострокових 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 у контексті оцінки довгострокових ефектів від таких заходів.

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

У висновках зазначається: одним із завдань української держави в питані розбудови механізмів державного управління у сфері захисту безпеки інформаційного простору з розрахунком на довгострокову (стратегічну) перспективу постає формування відповідної нормативно-правової бази.

Таку нормативно-правову базу необхідно формувати із урахуванням розвідувальної інформації та відповідного стратегічного прогнозування.

В ході розвідки і стратегічного прогнозування українські державні інституції неминуче стикаються з проблемами забезпечення високопрофесійними кадрами, а також браку фінансових, аналітичних та обчислювальних ресурсів, при чому, навіть у більшій мірі, ніж інші держави, які не змушені відволікати свої ресурси на відбиття широкомасштабної агресії чисельного ворога протягом багатьох років поспіль.

Найбільш раціональним, із урахуванням викладеного, на етапі стратегічного прогнозування видається його ведення паралельними методами:

1. *Формування стратегічних прогнозів на основі прогнозів середньострокової перспективи.*
2. *Формування стратегічних прогнозів на основі співставлення та аналізу стратегій ключових гравців на зовнішньополітичній арені.*
3. *Співставлення та аналіз результатів першого та другого способів стратегічного прогнозування для формування кінцевого*

прогнозу в цілях застосування у відповідних сферах державного управління.

Окрім комплексу заходів, спрямованих на формування документів стратегічного планування та керівних документів, які регламентують державне управління у сфері захисту безпеки інформаційного простору, необхідно постійно приділяти увагу питанням:

кадрового забезпечення та якісної підготовки і військових, і цивільних спеціалістів усіх рівнів державного управління;

залучення необхідних фінансових ресурсів;

залучення необхідних матеріальних (технічних) ресурсів;

створення (залучення) необхідного програмного забезпечення, сучасних технологій, зокрема й на базі штучного інтелекту.

Закладати основи державного управління у сфері захисту безпеки інформаційного простору необхідно уже зараз шляхом також поточного захисту населення від деструктивного інформаційно-психологічного впливу різних учасників наповнення інформаційного простору, розбудови та налагодження коректного ефективного функціонування системи стратегічних комунікацій, а також сприяння розвитку критичного мислення населення.

Напрямок подальших досліджень вбачаються у формуванні алгоритму підтримки прийняття рішень в ході реалізації державного управління у сфері захисту безпеки інформаційного простору.

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

Summary. *The mechanisms of public administration in the field of information space security protection, by their very nature, should be applied based on the results of information space monitoring and situation forecasting*

quickly, and preferably - proactively. This is due to the high dynamism of processes in the modern information space. At the same time, the situation that has arisen in Ukraine today, including the repulsion of large-scale Russian aggression, has largely been caused by the lack of public administration mechanisms in the field of information space security and the fact that they have not been used or even properly formed for years, taking into account the long-term consequences - the strategic perspective. Now, in times of war, when many factors cannot be predicted and forecasted, such planning is even more difficult to implement, but it is even more necessary. After all, it is impossible to form a stable system of high-quality public administration mechanisms in the field of information space security protection that will withstand military stress and contribute to the promotion of the State's domestic political goals in the period of post-war reconstruction without long-term planning.

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 historical and current long-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 long-term effects 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 protecting 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 long term in the

context of repulsing the Russian large-scale invasion by the Ukrainian Defense Forces.

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

The conclusions state: One of the tasks of the Ukrainian State in the development of public administration mechanisms in the field of information space security protection with a view to a long-term (strategic) perspective is to form an appropriate legal framework.

Such a legal framework should be formed on the basis of intelligence information and relevant strategic forecasting.

In the course of intelligence and strategic forecasting, Ukrainian state institutions inevitably face the problems of providing highly professional personnel, as well as lack of financial, analytical and computing resources, even more so than other states that do not have to divert their resources to repel large-scale aggression of a numerous enemy for many years in a row.

The most rational, in view of the above, at the stage of strategic forecasting seems to be its conduct by parallel methods:

1. Formation of strategic forecasts based on medium-term forecasts;

2. Formation of strategic forecasts based on comparison and analysis of strategies of key players in the foreign policy arena;

3. Comparison and analysis of the results of the first and second methods of strategic forecasting with the formation of the final forecast for use in the relevant areas of public administration.

In addition to a set of measures aimed at forming strategic planning documents and guiding documents regulating public administration in the field of information space security, it is necessary to pay constant attention to the following issues

staffing and quality training of both military and civilian specialists at all levels of government

attraction of necessary financial resources;

attraction of necessary material (technical) resources;

creation (attraction) of the necessary software, modern technologies, including those based on artificial intelligence.

It is necessary to lay the foundations of public administration in the field of information space security protection now by also protecting the population from the destructive information and psychological influence of various actors, building and establishing the correct and effective functioning of the strategic communications system, and promoting the development of critical thinking of the population.

The direction of further research is to formulate an algorithm for decision support in the course of implementation of public administration in the field of information space security protection.

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

Постановка проблеми. Планування та реалізація захисту безпеки інформаційного простору на рівні держави у стратегічній перспективі завжди було фактором, який впливав на історію. Нерідко такий вплив був визначальним. Тому, документи й алгоритми такого планування нерідко намагалися засекречувати, а їх створення та реалізація являє собою складний механізм. Його налагодження та приведення до ефективного функціонування особливий вид управлінського мистецтва, адже конкуруючі суб'єкти теж вживають заходів щодо реалізації своїх стратегій і, зазвичай, цілі таких суб'єктів бувають взаємовиключними.

На стратегічному рівні інформаційну політику держави не можна відокремлювати від інших сфер державного управління. Вона тісно пов'язана із внутрішньополітичними процесами, ще більше – із зовнішньополітичними. Прорахунки в інформаційній політиці та недостатня ефективність захисту безпеки інформаційного простору, як внутрішнього так і зовнішнього, який прямо стосується держави, може мати трагічні наслідки, і навіть фатальні для існування самої держави. Одним з яскравих прикладів неадекватної оцінки ситуації під впливом процесів в інформаційному просторі, та відповідно, згубного у стратегічній перспективі прийняття рішення з боку українського державного керівництва є Будапештський меморандум. Науковці та практики у сфері міжнародного права досі сперечаються, що це було: політична домовленість, політична угода, дипломатичний документ чи міжнародний договір [1, с. 251]. На практиці ж ми бачимо, що невизначеність понять навіть на доктринальному рівні та безвідповідальність державного керівництва при підписанні меморандуму призвели у довгостроковій перспективі до воєнної агресії сусідньої держави, відсутності стримуючих факторів, одним з яких безумовно була наявність ядерної зброї та, фактично геноциду українського народу внаслідок російської агресії. Варто відзначити, що сам по собі Будапештський меморандум і його сприйняття суспільством, зокрема відсутність активних акцій протесту з боку населення України стали можливими внаслідок низки прорахунків в інформаційній політиці держави, характерних практично для всього періоду української незалежності.

В умовах, коли Сили оборони України реалізовують відсіч російській широкомасштабній агресії а держави, які, зокрема, були гарантами безпеки України, за тим же Будапештським меморандумом, за фактом становлять загрозу для української державності, ретроспективний історичний аналіз важливий, однак, аж ніяк не може задовольнити потреб розбудови

механізмів державного управління у сфері захисту безпеки інформаційного простору.

Радянсько-російська концепція "дружби народів" та "братніх народів", яка фактично протягом століття застосовується у якості когнітивної зброї для послаблення національного опору імперському домінуванню, залишається активною (на окупованих територіях, особливо у навчальних закладах, її і зараз намагаються реанімувати російські окупанти), не кажучи уже про різноманітні пропагандистські заходи та інформаційно-психологічні акції російських спецслужб, спрямовані не лише на внутрішні, але й на зовнішні цільові аудиторії. Власне концепцію "дружби народів" було введено 1936 року на заміну імперської ідеологеми культурної та політичної ієрархії. Ця "дружба народів" веде за собою поняття великого російського народу. Концепція "братніх народів" – це хворий витвір радянської пропаганди на заміну російської імперської концепції "триєдиного народу". Це спроба насильно прив'язати українську історію до російської та заперечити право українців і білорусів на власний історичний вибір [2, с. 19]. Такі концепції, а також ресурси, вкладені в їх реалізацію московськими правителями незалежно від задекларованої форми державного правління й державного устрою росії говорять про те, що стратегічний противник та основна стратегічна загроза українській державності й фізичному виживанню кожного українця застосовує планування у стратегічній перспективі і реалізовує виконання своїх задумів, трансформуючи їх залежно від обставин, протягом багатьох століть. І якщо активний опір Сил оборони України та українського громадянського суспільства на даний момент робить концепцію "братніх народів" абсурдною, це зовсім не означає, що при нагоді російські окупанти не намагатимуться її реставрувати у тому чи іншому вигляді на захоплених територіях і при цьому не матимуть певного успіху.

Динаміка змін характеру бойових дій та посилення ролі і значення в кінцевому результаті збройних конфліктів інформаційної складової тим більше ставить питання необхідності стратегічного планування інформаційних ефектів та ефектів від реалізації інформаційної політики держави в цілому. Розвиток інформаційно-комунікаційних технологій, починаючи від обчислювальних спроможностей та закінчуючи наповненням і "навчанням" штучного інтелекту, зокрема його самонавчанням для виконання заздалегідь визначених завдань, ставить під питання не просто можливість збереження громадянського суспільства як такого в умовах активного застосування технологій диверсифікації та управління натовпом, відомих і в далекому минулому, але й індивідуальну безпеку психічного здоров'я кожної особистості.

У сучасній когнітивній війні людський розум формує поле бою. Когнітивна війна насамперед націлена на пізнання, яке є ментальним процесом набуття та осмислення знань, а також інтерпретації та сприйняття інформації. Спираючись на психологічну війну минулого, яка використовувала пропаганду для впливу на емоції, когнітивна війна використовує сучасні технології, щоб "вибудовувати упередження або розумові автоматизми, провокуючи викривлення уявлень, їх спотворення, зміни рішень або навіть гальмування дій, а також для того, щоб спричинити катастрофічні наслідки як на індивідуальному, так і на колективному рівні [3]. Можна констатувати, що на зміну пропаганді та інформаційно-психологічним операціям, які відігравали значу роль в ході протистояння в інформаційному просторі протягом минулого століття уже сьогодні прийшли когнітивна війна та операції впливу. Не можна сказати, що вони не були відомими людству раніше, але сучасні технології перетворили ці засоби ведення бойових дій та досягнення цілей зі складної елітної зброї, доступної незначній кількості вузьких спеціалістів, фактично у засіб масового ураження, який застосовується повсякчас без огляду на простір

ведення бойових дій та не обмежується жодними конвенціями, не кажучи уже про практичну неможливість його обмеження через організаційну, технічну та іншу проблематику.

Складність вивчення стратегічних (довгострокових) наслідків рішень, які приймаються в ході розбудови та реалізації механізмів державного управління у сфері захисту безпеки інформаційного простору, полягає ще й у тому, що необхідно враховувати можливості інструментів і методик, які станом на зараз можуть бути навіть не винайденими, або, щонайменше, достатньо добре засекреченими, а вже через декілька років матимуть можливість у випадку їх застосування стати ключовим вирішальним фактором збройного протистояння, досягнення дипломатичних, політичних чи інших цілей різними учасниками наповнення інформаційного простору, включаючи ворога. Для хоча б умовного уявлення про такі інструменти, не кажучи уже про адекватне врахування їхнього впливу та хід подій у майбутньому в ході розбудови механізмів державного управління та коригування їх функціонування необхідна професійна фахова розвідка та якісне прогнозування. В іншому випадку оцінка майбутніх змін конкурентного інформаційного середовища буде просто неадекватною. Як розвідка, так і адекватне прогнозування, засноване на коректних даних (знову ж таки пов'язаних з роботою розвідки), завжди вимагали колосальних фінансових і рідкісних кадрових ресурсів, з якими природно має проблеми держава, яка змушена захищатися від противника, що багатократно переважає її за усіма чисельними показниками.

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 довгострокових 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: [1; 2; 3; 4; 5; 6; 7; 12]; українських та іноземних нормативно-правових актах [8; 13; 14; 15]; публікаціях у медіа [9; 10; 11].

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

Виклад основного матеріалу дослідження з обґрунтуванням отриманих результатів. Заходи деструктивного інформаційно-психологічного впливу, методика їх проведення, технологічні та інформаційні інструменти переважно у будь-якій державі чи недержавній організації є таємницею, яку намагаються охороняти. Особливо це стосується конкретних заходів та операцій, часу місць, імен людей, які їх проводять, тактичних методик, які дозволяють ідентифікувати суб'єкта деструктивного інформаційно-психологічного впливу і, меншою мірою, доктринальних документів загального характеру. Попри це, на стратегічному рівні в ході масового застосування тих чи інших технологій уже неможливо приховати щонайменше факт деструктивного інформаційно-психологічного впливу, а часто і його характер.

Сьогодні у деяких випадках навіть кращим розвідувальним службам світу може бути складно встановити деталі та елементи окремих проведених операцій впливу, але загальну тенденцію та наміри інших суб'єктів зовнішньо-політичної діяльності та інформаційної активності на глобальному рівні повинні знати керівники держав та представники профільних державних інституцій щонайменше для забезпечення національної безпеки.

У середині 2000-х років колишній комендант Військового коледжу армії США генерал-майор Роберт Г. Скейлз висловив думку про майбутнє війни: "Перемога буде визначатися більше з точки зору захоплення психокультурної, а не географічної висоти". 18 липня 2024 року начальник Генерального штабу Збройних сил Канади Ейр, наголосив: "Наші інститути ліберальної демократії перебувають під постійним бомбардуванням теорій змови і брехні, які формують наратив недовіри і занепаду. І це створюється як всередині країни, так і за її межами. У стратегічному підході комуністичного Китаю, що базується на трьох війнах, це називається когнітивною війною. Наша власна інституція стає мішенню щодня, коли ми бачимо, як прокремлівські тролі пристосовують свою підступну пропаганду, щоб завдати максимальної шкоди – у багатьох випадках, за допомогою сфабрикованих особистих нападів" [4, С. 12]. Як бачимо, стратегічний аналіз та стратегічне прогнозування в інтересах захисту безпеки інформаційного простору абсолютно реально здійснювати на рівні держав, чиї воєнно-політичні інституції мають хорошу кадрову школу, доступ до сучасних технологій, необхідних фінансових ресурсів і чий державотворчий досвід та традиції налічують багато десятків або й сотні років.

Адекватність прогнозів на довгострокову (стратегічну) перспективу можна оцінити тверезо коли проходить відповідний період часу (п'ять і більше років). тим більш цікавим є ретроспективний аналіз документів,

створених майже два десятиліття тому. У науковому дослідженні, опублікованому у 2025 році та створеному 1996 року з метою забезпечення майбутнього (у довгостроковій перспективі) домінування в повітрі військово-повітряних сил збройних сил США йдеться про те, що зміна характеру війни і збройних сил підвищить цінність військової освіти і технічних знань. Розумна зброя потребуватиме розумних солдатів, моряків, морських піхотинців і льотчиків. Збройні сили майбутнього потребуватимуть воїнів, які вміють використовувати свій мозок, мати справу з різноманітністю людей і культур, толерантно ставитися до неоднозначності, проявляти ініціативу, задавати питання і навіть ставити під сумнів авторитети [5, С. 59]. З одного боку таке висловлювання можна оцінити як досить загальне. З іншого, зараз, коли пройшло майже два десятиліття з моменту формулювання прогнозу, у зовсім іншій частині планети в ході відбиття російської широкомасштабної агресії Силами Оборони України, ми бачимо що сформульований прогноз на довгострокову перспективу цілком підтверджується. Це стосується і згаданої ролі толерантності, і необхідності участі в бойових діях якісно ґрунтовно підготовлених спеціалістів, при чому не лише для користування розумною зброєю, але і для спілкування з різними людьми і, що найважливіше, спокійного ставлення до обставин невизначеності. Попри зростання технологічної складової та посилення інформаційних спроможностей протиборчих сторін ми на даному етапі розвитку військової науки та змін характеру бойових дій спостерігаємо проблеми з фільтрацією інформації й отриманням достовірної конкретної інформації, що в кінцевому рахунку створює необхідність уміти діяти для усіх учасників збройного протистояння, починаючи від бійців та командирів тактичного рівня і закінчуючи командувачами операцій, включно з персоналом, що відповідає за інформаційну складову забезпечення ведення бойових дій в умовах невизначеності різного ступеню. Таким чином, наведений прогноз

попри його загальність цілком можна вважати прикладом вдалого прогнозування зміни характеру бойових дій загалом та інформаційних операцій зокрема у довгостроковій (стратегічній) перспективі.

У цьому цікавий самоаналіз стратегічного прогнозування наведений у дослідженні представника Відділу військових і стратегічних досліджень, Академії ВПС США Майка Фаулера "Розвідка та оперативне попередження: уроки з України": У дослідженні йдеться про те, що незважаючи на величезний успіх стратегічного попередження, аналітики значно переоцінили звичайні російські військові можливості і недооцінили спроможність і волю українців. Навіть після спостереження за оперативними можливостями і тактикою Росії, аналітики знову переоцінили здатність Росії убезпечити свою присутність у Східній Україні.

Це дослідження показує, що погане розуміння військових кампаній є результатом низки факторів. Зокрема управління ризиками вимагає компромісів, заснованих на конкуруючих пріоритетах і обмежених ресурсах, що неминуче створює "сліпі зони". Через зосередженість на стратегічних вимогах або тактичній розвідці може бути недостатньо інформації для збору оперативних даних. Недостатня кількість аналітиків, необхідних для охоплення широкого спектру тем, робить їх вразливими до таких проблем, як дзеркальне відображення або упередженість одного джерела, що призводить до неякісного аналізу. Російські та західні зовнішні і внутрішні стратегічні наративи були сповнені обману, що впринципі характерно для сучасних ключових гравців у зовнішньо-політичній сфері, суб'єктів наповнення інформаційного простору та характеру сучасного інформаційного простору загалом. Незважаючи на політику необхідності ділитися, західні розвідувальні служби продовжують страждати від кількості інформаційних потоків. І, нарешті, брак професійної військової гри може призвести до аналітичного підходу, який ігнорує цінний досвід операторів і логістів. Автори визнають: кожен із цих факторів призвів до

того, що аналітики погано розуміють оперативний рівень війни в російсько-українському конфлікті [6]. Власне неврахування досвіду, волі, характеру та інших особистісних якостей достатньо чисельних груп людей, а в окремих випадках навіть окремої людини, можуть істотно вплинути на якість прогнозу, зокрема і стратегічного. У документі мова йде про те, що стратегічне прогнозування, а саме передбачення початку російської широкомасштабної агресії проти України, виконало свої завдання. Поряд з тим виникли проблеми на рівні формування адекватних оперативних прогнозів.

Така парадоксальна ситуація, коли прогнозування довгострокової (стратегічної) перспективи буває більш вдалим, аніж прогнозування в оперативній (середньостроковій) перспективі, насправді має цілком логічне пояснення. Хоча на перший погляд складність прогнозування прямо пропорційна періоду часу, на який формується прогноз, на практиці у питаннях захисту безпеки інформаційного простору та національної безпеки загалом, як і в питанні ведення активних бойових дій це часто не відповідає дійсності.

Стратегічні довгострокові проекти держав чи інших потужних суб'єктів наповнення інформаційного простору і зовнішньополітичної, воєнної міжнародної злочинної чи терористичної активності вимагають тривалого багатоетапного комплексу дій, які дозволяють зрозуміти загальну стратегію і передбачити наступні кроки. В ході реалізації стратегічного задуму при сучасних технічних можливостях інших учасників будь-якого процесу, особливо якщо мова іде про наповнення інформаційного простору та деструктивний інформаційно-психологічний вплив зокрема, просто неможливо обійтися виключно прихованою інформацією та обійтися без оприлюднення інформації, яка дає можливість в результаті якісного аналізу зрозуміти загальну стратегію суб'єкта. А це вже у свою чергу дає можливість для передбачення його наступних кроків

на шляху до реалізації стратегічних планів і досягнення стратегічних ефектів та цілей. У свою чергу оперативна середньострокова перспектива, хоча вона і здається більш простою для аналізу часто може залежати (хоча і в меншій мірі, аніж, наприклад, короткострокова тактична) від того, що у популярній літературі називають роллю особистості в історії.

Власне прорахунки психологічного та соціологічного аналізу, на перший погляд, можна назвати причинами неточностей, наведених у дослідженні. Якби це було дійсно так, проблему можна було б вирішити інструментами класичної традиційної психології, соціології та, можливо, історії. Однак, для адекватного формування оперативного прогнозу, на основі якого було б логічним скласти стратегічний прогноз, необхідно не просто правильно спрогнозувати дії спільнот людей чи конкретних людей, а ще і знати, чиї рішення і дії матимуть вплив на ситуацію в оперативній перспективі і в якій мірі та, відповідно, чиї психологічні характеристики або соціологічні характеристики яких груп потребують більш ґрунтовного аналізу. Розуміння цієї особливості розкриває власне, сутність проблем ресурсів навіть в умовах профільних наукових підрозділів США, які не є найбіднішими за ресурсним потенціалом і дає розуміння, чому власне для адекватного прогнозу оперативного рівня може не вистачати обчислювальних (аналітичних) можливостей, про що теж ідеться в документі.

Власне, будь-який стратегічний прогноз ускладняється динамікою технічного розвитку. З одного боку обчислювальні потужності сучасної техніки та сучасні інформаційні технології дозволяють розвантажити персонал і підсилити можливості аналітиків, беручи на себе значну частину типових операцій. З іншої ж сторони поєднання кіберспроможностей та відомих раніше методів обману (пропаганди, інформаційно-психологічних операцій), що багатьма дослідниками розцінюється, власне, як основа когнітивного впливу та когнітивної війни, формує абсолютно

безпрецедентні масштаби впливу і, як наслідок, нові правила гри, коли багато закономірностей, правил і тактичних прийомів минулого можуть бути неефективними і не такими непорушними, якими вважалися традиційно.

Когнітивну війну представляють як нову сферу військово-політичних операцій, що виникла на основі поєднання психологічних операцій і кібервійни. Як повідомляється в документах першого засідання НАТО у 2021 році, головною метою когнітивного впливу є встановлення контролю і домінування шляхом маніпулювання когнітивними механізмами населення, які підтримують його спонтанне уявлення про реальність. З цією метою в ході когнітивного впливу синтезується десятиліттями досягнутий прогрес в науках про мозок і поведінку, в комп'ютерних і мережевих технологіях, а також в складних і адаптивних системах. В ході реалізації когнітивного впливу застосовуються елементи цієї сукупності знань для підтримки втручання у зміст і сам механізм, процес мислення цивільного населення й військовослужбовців, незалежно від того, мирний це час чи воєнний [7, С.9]. Як бачимо, європейські, зокрема іспанські, дослідники стратегічного застосування деструктивного інформаційного впливу з метою досягнення зовнішньополітичних цілей, аж до інформаційно-психологічного супроводження актів широкомасштабної воєнної агресії, цікавляться природою та характером когнітивної війни, яка, вірогідно, визначатиме формат зовнішньої політики і формат інформаційних дій стратегічного рівня, причому, не лише найближчим часом.

Це виглядає логічним на фоні російської агресії проти України, яка становить безпосередню загрозу для країн Європейського союзу у вигляді вторинних наслідків широкомасштабних бойових дій (зміни масштабів вимушеної міграції, екологічні проблеми, фінансові витрати, зміна характеру необхідності підтримання власного оборонного потенціалу

тощо) та у довгостроковій (стратегічній) перспективі вірогідно становитиме цілком реальну воєнну загрозу.

Якщо співпраця росії, Північної Кореї, Ірану та Білорусі за напівприхованої підтримки Китаю сприймалися як логічне об'єднання спільних інтересів країн з антидемократичними режимами й експансивною зовнішньою політикою, то надійне приєднання до цього блоку через механізми контролю над ключовими лідерами Угорщини і США, колишнього стратегічного противника більшості з названих вище, не просто ставить планету на поріг третьої світової війни, але і змушує європейських лідерів терміново вживати заходів, які дозволять захистити власну національну безпеку у стратегічній перспективі, зокрема й заходів інформаційного характеру.

Найпростішими для розуміння та найбільш широковідомими прикладами таких заходів є повідомлення про підтримку України європейських лідерів, які відповідно до Доктрини зі стратегічних комунікацій Північно-атлантичного альянсу відносяться до заходів публічної дипломатії [8]. Оперативність та потужність таких заходів безумовно є перевагою а вони самі мають суттєвий вплив на ситуацію, зокрема, в даному випадку, стабілізуючий, який дозволяє усунути або послабити наслідки деструктивного інформаційно-психологічного впливу противника та потенційні воєнно-політичні наслідки ситуації, яка склалася.

Поряд з тим, подібні заяви не можна характеризувати й розглядати виключно у контексті інформаційної політики, адже за ними стоять цілком конкретні дії і наслідки, які істотно впливають на оборонну, економічну, внутрішньополітичну, соціальну та інші сфери державного управління цілої низки країн. Заяви європейських та інших світових лідерів, не самі по собі, а в поєднанні з їх майбутніми наслідками (адже у стратегічній перспективі різні сфери державного управління в принципі інтегровані значно сильніше, аніж на оперативному чи тактичному рівні) по-суті декларують

розстановку сил у світі напередодні вірогідної третьої світової війни та, природно, відображаються в інформаційному просторі, зокрема і на шпальтах провідних світових медіа [9; 10; 11]. Поряд з тим, розуміння розвідками провідних країн і, відповідно, їхніми лідерами небезпечності ситуації, яка складається у стратегічній перспективі та заходи, які вони вживають з метою стабілізації ситуації черговий раз підтверджують, що формування стратегічного прогнозу з одного боку може бути значно складнішим, аніж прогнозів на більш короткі періоди, але з іншого є абсолютно реальним. Навіть в обставинах, коли відносно чітко й доказово прораховуються вірогідності і розстановка сил на геополітичній карті світу на найближчих декілька років, про що можна зробити висновок за результатами реагування на цей прогноз, які уже цілком чітко видно навіть у відкритому інформаційному просторі, динамічний розвиток ситуації не дозволяє впевнено відповісти на запитання, що відбудеться в інформаційному просторі завтра або через місяць.

Дослідники і практики у сфері державного управління безпекою інформаційного простору стикаються із парадоксальною ситуацією коли далеке майбутнє, принаймні на рівні загальних тенденцій, спрогнозувати виявляється можливо та цілком реально, а найближчий розвиток ситуації – значно важче, і вірогідність похибки при цьому значно вища. Зараз на фоні активних декларацій позицій демократичних країн очільниками їхніх урядів чи відповідними уповноваженими дипломатичними представниками, джерелом сюрпризів та факторів, які буде важко прорахувати у найближчому майбутньому, цілком можуть стати представники блоку авторитарних держав, які намагаються вести зовнішню політику експансивного характеру максимально приховано. Зокрема, враховуючи економічні, політичні, військові можливості, а також напрацьованість методик когнітивної війни, особливої уваги у цьому контексті заслуговує Китай.

Аналіз методів, застосованих Китаєм проти Тайваню, наочно демонструє, як стратегії когнітивної війни можуть бути адаптовані для застосування в Південно-Східній Азії. Однак ефективність когнітивної війни проти Тайваню обмежена певними характеристиками, які не настільки помітні в Південно-Східній Азії. Тайвань має сильну національну ідентичність і чітке відчуття власної окремішності від материкового Китаю. Історичні події, такі як попередні конфлікти та перехід острова до демократії, посилили стійкість тайванців до зовнішнього впливу. Тайванське населення загалом скептично ставиться до китайських наративів, що знижує ефективність зусиль Китаю у когнітивній війні, спрямованих на зміну громадської думки [12, с. 79]. Безумовно, між Китаєм та росією є певні відмінності, які стосуються економічного потенціалу, зваженості у зовнішній політиці та застосуванні військової сили. Поряд з тим, історичні передумови і здатність опиратися пропаганді, інформаційно-психологічним операціям, деструктивному інформаційному впливу загалом та, зрештою, інструментам когнітивної війни у населення Тайваню та України певним чином схожі і будуються на особливостях ментальності та історичних передумовах. Зараз не викликає сумніву, що Китай, який має агресивні плани стосовно Тайваню і росія, яка протягом багатьох років веде неспровоковану агресивну війну проти України, обмінялися технологіями та інструментами ведення когнітивної війни. Такі інструменти й технології, особливо у контексті стрімкого розвитку штучного інтелекту, поєднаного з історичним тисячолітнім досвідом кривавих війн та цілеспрямованої розробки засобів обману не можна недооцінювати.

Розбудова механізмів державного управління у сфері захисту безпеки інформаційного простору в Україні безумовно піддається впливу відповідних законодавчих актів та керівних документів. Стратегія національної безпеки України прийнята у 2020 році [13], Стратегія інформаційної безпеки України – у 2021 [14] році, Стратегія кібербезпеки

України – теж у 2021 році [15]. При тому, що Сили оборони України понад 10 років здійснюють відсіч російської агресії і понад 3 роки – відсіч російської широкомасштабної агресії, названі документи швидше могли б виконати завдання нормативного врегулювання певних процесів мирного, ніж воєнного часу. Безумовно будуть розроблені нові стратегічні документи, і вони повинні розроблятися з урахуванням зміни реальності зовнішньої політики у світі та завдань, які постають перед українською державою й українським народом починаючи з основного: захистити своє фізичне виживання й державність.

Безумовно розробку нових нормативних документів доведеться реалізовувати із врахуванням розвідувальної інформації та прогнозів. При цьому, як випливає із цього дослідження, класичний метод, коли прогнози довгострокової (стратегічної) перспективи формуються на основі прогнозів середньострокової перспективи не завжди буває релевантним. Досвід показує, що навіть держави, які володіють більш потужними фінансовими ресурсами, організаційною структурою та більш давніми школами підготовки кадрів стикаються із ситуацією при якій стратегічний прогноз виявляється релевантним і підтверджується після проходження відповідного часу в той час як оперативний прогноз (середньострокової перспективи) має значні, в окремих випадках – критичні, похибки, що легко можуть призвести до прийняття хибних рішень.

Висновки та перспективи подальших розвідок у даному напрямку. Одним із завдань української держави в питані розбудови механізмів державного управління у сфері захисту безпеки інформаційного простору з розрахунком на довгострокову (стратегічну) перспективу постає формування відповідної нормативно-правової бази.

Таку нормативно-правову базу необхідно формувати із урахуванням розвідувальної інформації та відповідного стратегічного прогнозування.

В ході розвідки і стратегічного прогнозування українські державні інституції неминуче стикаються з проблемами забезпечення високопрофесійними кадрами, а також браку фінансових, аналітичних та обчислювальних ресурсів, при чому, навіть у більшій мірі, ніж інші держави, які не змушені відволікати свої ресурси на відбиття широкомасштабної агресії чисельного ворога протягом багатьох років поспіль.

Найбільш раціональним, із урахуванням викладеного, на етапі стратегічного прогнозування видається його ведення паралельними методами:

4. Формування стратегічних прогнозів на основі прогнозів середньострокової перспективи.
5. Формування стратегічних прогнозів на основі співставлення та аналізу стратегій ключових гравців на зовнішньополітичній арені.
6. Співставлення та аналіз результатів першого та другого способів стратегічного прогнозування для формування кінцевого прогнозу в цілях застосування у відповідних сферах державного управління.

Окрім комплексу заходів, спрямованих на формування документів стратегічного планування та керівних документів, які регламентують державне управління у сфері захисту безпеки інформаційного простору, необхідно постійно приділяти увагу питанням:

кадрового забезпечення та якісної підготовки і військових, і цивільних спеціалістів усіх рівнів державного управління;

залучення необхідних фінансових ресурсів;

залучення необхідних матеріальних (технічних) ресурсів;

створення (залучення) необхідного програмного забезпечення, сучасних технологій, зокрема й на базі штучного інтелекту.

Закладати основи державного управління у сфері захисту безпеки інформаційного простору необхідно уже зараз шляхом також поточного

захисту населення від деструктивного інформаційно-психологічного впливу різних учасників наповнення інформаційного простору, розбудови та налагодження коректного ефективного функціонування системи стратегічних комунікацій, а також сприяння розвитку критичного мислення населення.

Напрямок подальших досліджень вбачаються у формуванні алгоритму підтримки прийняття рішень в ході реалізації державного управління у сфері захисту безпеки інформаційного простору.

Література

1. Стешенко В. Міжнародно-правова характеристика Будапештського меморандуму 1994 року. *Юридичний науковий електронний журнал*. 2016. № 6. С. 251-254. URL: https://lsej.org.ua/6_2016/70.pdf (дата звернення: 25.02.2025).

2. Вівсяна І. Радянський концепт «дружба народів» у сучасних підручниках з історії. *Історія та археологія*. 2024. (2). С. 17–27. DOI: https://doi.org/10.32782/cusu-hist-2024-2-2

3. Семенюк Н. Когнітивна війна в сучасній архітектурі гібридної війни. *Міжнародний науковий журнал «Military Science».* 2024. 2(3). С. 99-107. DOI: https://doi.org/10.62524/msj.2024.2.3.08

4. Nikoula D., Mcmahon D. Cognitive Warfare: Securing Hearts and Minds. University of Ottawa. July 2024. URL: https://infolab.uottawa.ca/common/Uploaded%20files/PDI%20files/InfoLab%20-%20Cognitive%20Warfare,%20Securing%20Hearts%20and%20Minds.pdf (дата звернення: 25.02.2025).

5. Мерфі, LCEF, Бендер, MGC, Шефер, MLJ, Шепард, MMM, і Вільямсон III, MCW (2025). Інформаційні операції: Wisdom warfare for 2025. У дослідницькій статті, представленій BBC. URL:

https://libraryofrickandria.com/wp-content/uploads/2024/05/2025_volume1.pdf (дата звернення: 01.03.2025).

6. Майк Фауллер. Розвідка та оперативне попередження: уроки з України. *Журнал поліції, розвідки та боротьби з тероризмом.* 2024. Том 19, Вип. 4 : Інтелектуальні прогнози щодо загроз завтрашнього дня. DOI: https://doi.org/10.1080/18335330.2024.2319128

7. Pastor A. Cognitive warfare. HAL science ouverte. Barcelona, Spain. 2024. DOI: https://doi.org/10.31234/osf.io/zgsej

8. Allied Joint Publication-10, Allied Joint Doctrine for Strategic Communications. URL: https://www.gov.uk/government/publications/allied-joint-doctrine-for-strategic-communications-ajp-10 (дата звернення: 02.03.2025).

9. Kalika Mehta. Europe loudly states support for Ukraine, quietly eyes Trump. *Deutsche Welle*. URL: https://www.dw.com/en/europe-loudly-states-support-for-ukraine-quietly-eyes-trump/a-71790839 (дата звернення: 02.03.2025).

10. Mercer D. European leaders back Zelensky after Trump clash. *BBC News.* URL: https://www.bbc.com/news/articles/cz9n5jq42pdo (дата звернення: 02.03.2025).

11. Andrew Gray. European leaders show support for Zelenskiy after Trump clash. *Reuters*. URL: https://www.reuters.com/world/europe/european-leaders-show-support-zelenskiy-after-trump-clash-2025-02-28/ (дата звернення: 02.03.2025).

12. Singh Sukhjinder. In what ways does the rise of china's emerging cognitive warfare capabilities pose a threat to South-East Asia? Monterey. Naval Postgraduate School. URL: https://core.ac.uk/download/pdf/618458559.pdf. (дата звернення: 02.03.2025).

13. 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: 02.03.2025).

14. 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: 02.30.2025).

15. 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: 02.03.2025).

References

1. Steshenko, V. (2016). Mizhnarodno-pravova kharakterystyka Budapeshtskoho memorandumu 1994 roku. [Steshenko V. Mizhnarodno-pravova kharakteristika Budapeshtskoho memorandum 1994 roku.]. *Yurydychnyi naukovyi elektronnyi zhurnal – Legal scientific electronic journal*. 6. P. 251-254. https://lsej.org.ua/6_2016/70.pdf [in Ukrainian].

2. Vivsiana, I. (2024). Radianskyi kontsept «druzhba narodiv» u suchasnykh pidruchnykakh z istorii [The Soviet concept of "friendship of peoples" in modern history textbooks.] *Istoriia ta arkheolohiia. – History and archeology,* (2), 17–27. https://doi.org/10.32782/cusu-hist-2024-2-2 [in Ukrainian].

3. Semeniuk, N. (2024). Kohnityvna viina v suchasnii arkhitekturi hibrydnoi viiny. [Cognitive warfare in the modern architecture of hybrid warfare.] *Mizhnarodnyi naukovyi zhurnal «Military Science» – International scientific journal "Military Science",* 2(3), 99-107. https://doi.org/10.62524/msj.2024.2.3.08 [in Ukrainian].

4. Daniel Nikoula, Dave Mcmahon. Cognitive Warfare: Securing Hearts and Minds. University of Ottawa. July 2024. URL:

https://infolab.uottawa.ca/common/Uploaded%20files/PDI%20files/InfoLab%20-%20Cognitive%20Warfare,%20Securing%20Hearts%20and%20Minds.pdf

5. Murphy, LCEF, Bender, MGC, Schaefer, MLJ, Shepherd, MMM, and Williamson III, MCW (2025). Information operations: Wisdom warfare for 2025. In a research paper presented to the BBC. URL: https://libraryofrickandria.com/wp-content/uploads/2024/05/2025_volume1.pdf

6. Mike Fowler. Intelligence and Early Warning: Lessons from Ukraine. Journal of Police, Intelligence and Counterterrorism Vol. 19, 2024 - Issue 4: Intelligent *Forecasts of Tomorrow's Threats.* https://doi.org/10.1080/18335330.2024.2319128

7. Alvaro Pastor. Cognitive warfare. HAL science ouverte. Barcelona, Spain. 2024. https://doi.org/10.31234/osf.io/zgsej

8. Allied Joint Publication-10, Allied Joint Doctrine for Strategic Communications. URL: https://www.gov.uk/government/publications/allied-joint-doctrine-for-strategic-communications-ajp-10

9. Kalika Mehta. Europe loudly states support for Ukraine, quietly eyes Trump. *Deutsche Welle*. URL: https://www.dw.com/en/europe-loudly-states-support-for-ukraine-quietly-eyes-trump/a-71790839

10. David Mercer. European leaders back Zelensky after Trump clash. *BBC News.* URL: https://www.bbc.com/news/articles/cz9n5jq42pdo .

11. Andrew Gray. European leaders show support for Zelenskiy after Trump clash. *Reuters.* URL: https://www.reuters.com/world/europe/european-leaders-show-support-zelenskiy-after-trump-clash-2025-02-28/. .

12. Singh Sukhjinder. In what ways does the rise of china's emerging cognitive warfare capabilities pose a threat to South-East Asia? Monterey. *Naval Postgraduate School.* URL: https://core.ac.uk/download/pdf/618458559.pdf.

13. 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 – Verkhovna Rada of Ukraine.* URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text [in Ukrainian].

14. 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 – Verkhovna Rada of Ukraine.* URL: https://zakon.rada.gov.ua/laws/show/685/2021/print [in Ukrainian].

15. 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 – Verkhovna Rada of Ukraine.* URL: https://zakon.rada.gov.ua/laws/show/447/2021/print [in Ukrainian].