УДК 005.53:[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

DOI: 10.25313/2520-2294-2025-11-11574

РОЗРОБКА АЛГОРИТМУ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У ХОДІ ЗАСТОСУВАННЯ МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ У СФЕРІ ЗАХИСТУ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ

DEVELOPMENT OF A DECISION SUPPORT ALGORITHM FOR THE APPLICATION OF PUBLIC ADMINISTRATION MECHANISMS IN THE FIELD OF INFORMATION SPACE SECURITY PROTECTION

Анотація. *Механізми державного управління у сфері захисту безпеки інформаційного простору можуть застосовуватися ефективно лише за умов оперативності, проактивності та обґрунтованості у прийнятті управлінських рішень. Особливо це стосується функціонування таких механізмів в умовах відбиття Силами оборони України російського широкомасштабного вторгнення, яке супроводжується та підтримується усіма потужностями ворожих засобів пропаганди та інформаційно-психологічних операцій. Прийняття обґрунтованих рішень вимагає належного пропрацювання питання в кожному окремому випадку, що буває складно, коли діяти необхідно швидко. Крім того, для прийняття швидкого, але обґрунтованого рішення, необхідний навчений персонал, який володіє належною підготовкою і досвідом, що теж нерідко стає проблемою в умовах кадрової кризи, яка в тій чи іншій мірі завжди має місце поряд з іншими ресурсними проблемами у функціонуванні механізмів державного управління. Можливість підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору за таких умов вбачається у розробці алгоритму підтримки прийняття управлінських рішень та системи оцінки інформаційних дій. Поєднання таких інструментів дозволить прискорити навчання персоналу, задіяного у захисті безпеки інформаційного простору. З одного боку, шляхом прискорення прийняття рішення завдяки заздалегідь визначеним критеріям та послідовності дій, з іншого боку – завдяки оцінці результатів прийнятого рішення, що дозволить систематизувати типові кейси і, з високою вірогідністю, застосовувати їх у майбутньому з урахуванням пріоритетності більш ефективних перед менш ефективними. Звісно, кінцеве рішення повинно прийматися з урахуванням людського фактору, і жоден алгоритм, з урахуванням обстановки в інформаційному просторі, що швидко змінюється, не може замінити людину, яка повинна прийняти рішення. Як прийняття рішення у сфері захисту безпеки інформаційного простору, так і оцінка прийнятого рішення є складними процесами. Але за результатами попередньо проведених досліджень, на основі систематизації українського та іноземного досвіду останнього десятиріччя, із урахуванням тенденцій розвитку процесів в інформаційному просторі, видається можливим описати основні закономірності з метою формування механізмів підтримки прийняття рішень та оцінки прийнятих рішень. Такі механізми планується розробляти шляхом декомпозиції складної проблематики на окремі більш прості складові із застосуванням інструментарію багатокритерійного аналізу.*

Мета запропонованого дослідження – підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору шляхом розробки алгоритму підтримки прийняття управлінських рішень та алгоритму оцінки результатів прийнятих управлінських рішень.

Завдання дослідження полягає у розробці механізмів підтримки прийняття управлінських рішень та оцінки результатів управлінських рішень у сфері захисту безпеки інформаційного простору.

Наукова новизна дослідження і його результатів полягає у прикладному застосуванні інструментарію багатофакторного аналізу та розробці інструментів систематизації прийняття управлінських рішень з метою вирішення проблемних питань сучасного державного управління у сфері захисту безпеки інформаційного простору України.

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:

В ході дослідження на основі поточного та попередніх напрацювань розроблено методику підтримки прийняття рішень під час реалізації державного управління у сфері захисту безпеки інформаційного простору. Методика складається з двох основних частин: алгоритму підтримки прийняття управлінських рішень та методики оцінки прийнятих рішень.

Оскільки методика розроблялася як прикладний інструмент, в ході розробки пріоритетними були принципи простоти, практичності та економічності у застосуванні.

Принцип дії методики заснований на декомпозиції складного завдання, яким є, по суті, кожна окрема ситуація у сфері державного управління захистом безпеки інформаційного простору, на окремі прості питання, послідовна відповідь на які дає можливість відповідному спеціалісту, по-перше, самостійно краще зрозуміти ситуацію, і, по-друге, отримати рекомендацію щодо оптимальних дій, яка з високою вірогідністю буде доречною.

Також методика оцінки прийнятих управлінських рішень дозволяє в процесі діяльності коригувати саму методику підтримки прийняття рішень під індивідуальні потреби спеціаліста у сфері захисту безпеки інформаційного простору, а головне – більш ефективно систематизувати досвід, який він отримує в процесі своєї діяльності.

Напрямки подальшого дослідження вбачаються у:

- *описі та обґрунтуванні методики;*
- *верифікації методики;*
- *формуванні методичних рекомендацій щодо застосування методики.*

Ефективне продовження дослідження за умов практичного впровадження його результатів дозволить без додаткових матеріальних чи інших ресурсів, громіздких правових чи складних організаційних змін підвищити ефективність державного управління у сфері захисту безпеки інформаційного простору в умовах відбиття Силами оборони України російського широкомасштабного вторгнення, однією з ключових складових якого виступають заходи деструктивного інформаційно-психологічного впливу.

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 can be used effectively only under conditions of efficiency, proactivity and validity in making managerial decisions. This is especially true for the functioning of such mechanisms in the context of repulsion by the Ukrainian Defense Forces of the Russian large-scale invasion, which is accompanied and supported by all the capabilities of enemy propaganda and information and psychological operations. Making informed decisions requires a proper study of the issue in each individual case, which can be difficult when it is necessary to act quickly. In addition, to make a quick but informed decision, trained personnel with proper training and experience are needed, which also often becomes a problem in the context of the personnel crisis, which to some extent always takes place along with other resource problems in the functioning of public administration mechanisms. The possibility of increasing the efficiency of public administration mechanisms in the field of information space security under such conditions is seen in the development of an algorithm for supporting management decision-making and a system for evaluating information actions. The combination of such tools will accelerate the training of personnel involved in the protection of information space security. On the one hand, by accelerating decision-making through predefined criteria and sequence of actions, and on the other hand, by evaluating the results of the decision, which will allow systematizing typical cases and, with a high probability, applying them in the future, taking into account the priority of more effective over less effective ones. Of course, the final decision must be made taking into account the human factor, and no algorithm can replace a human decision maker in a rapidly changing information space. Both decision-making in the field of information space security protection and evaluation of the decision are complex processes. However, based on the results of preliminary research, systematization of Ukrainian and foreign experience of the last decade, and taking into account the trends in the development of processes in the information space, it seems possible to describe the main patterns in order to form mechanisms for supporting decision-making and evaluating decisions. Such mechanisms are planned to be developed by decomposing a complex problem into separate simpler components using the tools of multicriteria analysis.*

The purpose of the proposed study is to increase the efficiency of public administration mechanisms in the field of information space security by developing an algorithm for supporting management decision-making and an algorithm for evaluating the results of management decisions.

Thetask of thestudy is to develop mechanisms for supporting management decision-making and evaluating the results of management decisions in the field of information space security.

The scientific novelty of the study and its results is the applied use of multifactor analysis tools and the development of tools for systematizing management decision-making in order to solve the problematic issues of modern public administration in the field of information space security protection in Ukraine.

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

The conclusions

In the course of the study, on the basis of current and previous developments, a methodology for supporting decision-making in the implementation of public administration in the field of information space security protection has been developed. The methodology consists of two main parts: an algorithm for supporting managerial decision-making and a methodology for evaluating decisions.

Since the methodology was developed as an applied tool, the principles of simplicity, practicality and cost-effectiveness in application were prioritized during the development.

The principle of the methodology is based on the decomposition of a complex task, which is essentially every single situation in the field of public administration of information space security, into separate simple questions, the consistent answer to which allows the relevant specialist to firstly, better understand the situation on his/her own, and secondly, receive a recommendation on optimal actions that is likely to be appropriate.

Also, the methodology for assessing the management decisions made allows, in the course of activity, to adjust the decision support methodology itself to the individual needs of a specialist in the field of information space security, and most importantly, to more effectively systematize the experience gained in the course of his or her activities.

The directions for further research are as follows:

– description and justification of the methodology;

– verification of the methodology;

– development of methodological recommendations for the application of the methodology.

Effective continuation of the study, subject to practical implementation of its results, will allow, without additional material or other resources, cumbersome legal or complex organizational changes, to increase the efficiency of public administration in the field of information space security protection in the context of repulsion by the Ukrainian Defense Forces of a large-scale Russian invasion, one of the key components of which is the measures of destructive information and psychological influence.

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

Постановка проблеми. Будь-яка управлінська система, як у державному, так і в приватному секторі, на практиці зустрічається з типовою проблематикою: значна кількість завдань при браку ресурсів для їхнього розв'язання. Це стосується кадрового ресурсу, фінансового ресурсу, людських і програмно-технічних аналітичних спроможностей та одного з найбільш ключових, невідновлюваного ресурсу — часу. Спроби оптимізації управлінських систем та підвищення їх ефективності за одним чи декількома критеріями ми часто можемо бачити у вигляді різноманітних реорганізацій. Лише незначна частина таких заходів на практиці доводить свою ефективність, в той час як після більшості з них ефективність роботи управлінських систем падає і призводить до зворотної реорганізації. Скорочення штатів з метою зекономити фінанси при нераціональному здійсненні таких заходів зазвичай призводять до нездатності управлінського підрозділу виконувати свої завдання і зворотного розширення штатів через деяких час. Розширення штатів з надмірною диференціалізацією управлінських процесів при невдалому варіанті також може призводити до погіршення комунікації і зниження оперативності виконання завдань підрозділу, що, з часом, змушує вищі органи управління приймати рішення про спрощення системи. Це найбільш поширені приклади, які ми можемо спостерігати у повсякденному житті. Поряд з організаційними та правовими заходами підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору найбільш економічним та прогресивним видається розробка необхідного інструментарію — протоколу дій, який дозволить при наявності підготовки, характерної для середньостатистичного державного службовця з невеликим досвідом приймати складні рішення у прийнятний для цього час і з прийнятною обґрунтованістю. Однак у питаннях протистояння в інформаційному просторі та власне в умовах сучасної когнітивної війни будь-який жорсткий протокол:

– по-перше, неможливий, оскільки інформаційну боротьбу часто вважають сферою, де єдиним правилом є відсутність правил, і така думка цілком має право на існування, як показує практика;
– по-друге, навіть при наявності можливості розробки ідеального жорсткого протоколу прийняття рішення, за сучасних розвідувальних можливостей усіх сторін інформаційного протистояння такий протокол одразу стане надбанням протиборчих сторін і буде більш ефективно використовуватися не суб'єктом, який його застосує, а якраз в ході роботи проти такого суб'єкта, оскільки його дії будуть апріорі передбачуваними.

За таких умов більш оптимальним видається не протокол з жорстко визначеною послідовністю дій, а орієнтовний алгоритм підтримки прийняття рішень, який підрозділу із середніми інформаційно-обчислювальними можливостями, укомплектованому середньостатистичними кадрами з посередньою підготовкою, надасть механізм декомпозиції склад-

ного рішення шляхом його розподілу на більш прості питання і вибір із декількох можливих сценаріїв, щонайменше один з яких вірогідно буде ефективним. Такий алгоритм дозволить прискорити процес прийняття управлінських рішень при збереженні їх обґрунтованості за рахунок врахування основних критичних факторів і при цьому залишить особі, яка приймає рішення, достатньо простору для маневру щоби не бути передбачуваною для противника чи інших суб'єктів наповнення інформаційного простору.

Однак сам по собі алгоритм підтримки прийняття управлінського рішення на основі систематичного багатокритерійного аналізу може бути ефективно застосований в одиничних випадках, але недостатньо ефективно сприятиме набуттю спроможностей та акумулюванню досвіду — як індивідуального, так і колективного — в рамках певного підрозділу. Гнучкість методики в управлінському процесі є однією з характеристик, яка може бути реалізована максимально ефективно у тому випадку, коли враховуються результати застосування тих чи інших варіантів за схожих або аналогічних вихідних умов. Крім того, управлінська діяльність у сфері захисту безпеки інформаційного простору характерна тим, що систематизація і типологізація кейсів завжди залишатиметься досить умовною. Кожна конкретна ситуація вимагає конкретної реакції та способу дій. Незначна зміна тактики суб'єктів, які реалізовують деструктивний інформаційно-психологічний вплив, може вимагати значних змін навіть в успішних методиках нейтралізації (мінімізації) такого впливу для того, щоби відповідні заходи залишалися ефективними.

Враховуючи викладене, для комплексного підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору, поряд із алгоритмом підтримки прийняття управлінських рішень, необхідна максимально проста у застосуванні але при цьому достатньо ефективна та інформативна система оцінки ефективності прийнятих управлінських рішень та вжитих заходів (інформаційних дій).

Завдання дослідження полягає у розробці механізмів підтримки прийняття управлінських рішень та оцінки результатів управлінських рішень у сфері захисту безпеки інформаційного простору.

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

Мета запропонованого дослідження — підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору шляхом розробки алгоритму підтримки прийняття управлінських рішень та алгоритму оцінки результатів прийнятих управлінських рішень.

Виклад основного матеріалу дослідження з обґрунтуванням отриманих результатів.

Застосування багатофакторного аналізу для оптимізації систем, діяльність яких стосується безпеки, розглядалося дослідниками і раніше, зокрема у контексті кібербезпеки як складової інформаційної безпеки. Висока складність та масштабованість архітектури сучасних розподілених систем, різнорідність обладнання та інфраструктури, а також постійні зміни конфігурації та масштабування середовища породжують ряд проблем, пов'язаних зі збором та аналізом інформації для оцінки ризиків, необхідністю оперативної обробки великих масивів складних за структурою та гетерогенних за природою даних, що надходять із диференційованих систем безпеки та моніторингу, журналів подій, аудиторських звітів та інших джерел, а також відсутністю єдиного формату їх представлення [1]. Ця проблематика характерна і при формуванні підходів до реагування на інформаційні загрози, зокрема спрямований деструктивний інформаційно-психологічний вплив противника, не кажучи вже про становлення системи проактивної комунікації з урахування щонайменше короткострокового прогнозування сценаріїв розвитку ситуації.

Проблематика аналізу та оцінки інформації, поширеної у відкритому інформаційному просторі, характерна не лише для України, але навіть для провідних держав та армій, які стикаються з інтенсивним деструктивним інформаційно-психологічним впливом у сучасних умовах. Так, американські дослідники говорять про відсутність в армії США інституціоналізованої програми розвитку освіти, призначеної для військовослужбовців, які навчаються виявляти, ретельно перевіряти та аналізувати шкідливу інформацію (тобто — дезінформацію, пропаганду тощо) у відкритому інформаційному середовищі [2]. Очевидна необхідність у формуванні такої програми та її ефективному застосуванні в умовах сучасної інформаційної та когнітивної війни, зокрема для забезпечення когнітивної переваги.

Тільки громадська організація «Детектор медіа», яка у режимі реального часу збирає та документує хроніки Кремлівської пропаганди навколо військового наступу на Україну, станом на 05 квітня 2025 року, 1136-й день широкомасштабного вторгнення, зафіксувала 2733 фейки, 817 маніпуляцій, 774 меседжі російської пропаганди та здійснила 559 викриттів [3]. Центр протидії дезінформації при Раді Національної безпеки і оборони України лише за один тиждень з 24.03.2025 р. по 30.03.2025 р., проаналізувавши 14 060 000 меседжів, виявив 20 472 інформаційні загрози [4]. База даних Оперативної групи Європейського союзу зі стратегічних комунікацій, яка

є частиною дипломатичної служби ЄС, очолюваної Верховним представником ЄС, станом на 05 квітня 2025 року налічує 18 759 випадків поширення спрямованої дезінформації [5]. Наведені цифри характеризують здебільшого виявлені факти поширення дезінформації з метою реалізації деструктивного інформаційно-психологічного впливу, пов'язані з російською інформаційною агресією, яка ведеться не лише проти України, але й проти європейських країн та інших країн світу. Для хоча б приблизного розуміння масштабів інформаційної війни та власне когнітивної війни, яку розв'язав і веде наш ворог, необхідно враховувати, що до цих цифр входять лише опрацьовані, перевірені, доказані та описані випадки, причому, за кожним з них стоять різні версії інформаційного контенту, різні форми його подачі, не кажучи вже про десятки, сотні, а часто і тисячі каналів поширення такої інформації. Тобто, лише наведені цифри, якщо спробувати перевести їх в кількість інформаційних повідомлень, які бачить суб'єкт моніторингу інформаційного простору, необхідно збільшувати в рази. І це без урахування інформаційних дій деструктивного характеру, які не були зафіксовані відповідними профільними організаціями і, відповідно, не увійшли в наведену статистику.

Якщо ж врахувати, що російська інформаційна агресія як супровід російської збройної широкомасштабної агресії є безумовно основною, але точно не єдиною проблемою захисту безпеки інформаційного простору України і в сучасних умовах, і щонайменше — у найближчому майбутньому, стає абсолютно зрозумілою неможливість навіть відстеження, не кажучи вже про адекватну оцінку і професійне реагування на повідомлення, які можуть становити реальну або потенційну інформаційну загрозу, без належної систематизації цієї роботи. За таких масштабів аналітичної діяльності, що вимагає величезної кількості достатньо складних та обґрунтованих рішень, жоден кадровий ресурс, фінансовий ресурс, і навіть ресурс спеціального програмно-технічного забезпечення, не дозволить ефективно виконувати завдання щодо управління у сфері захисту безпеки інформаційного простору без ефективного і водночас простого алгоритму, що дозволить прискорити прийняття рішень без збільшення різноманітних ресурсів та оцінити ефективність рішень у ретроспективі для формування порядку пріоритетності у виборі сценаріїв майбутніх дій.

Указ Президента України «Про стратегію інформаційної безпеки» покладає моніторинг інформаційного простору, прогнозування та виявлення інформаційних загроз національній безпеці держави у воєнній сфері на Міністерство оборони України, а також сили оборони в межах їх компетенції [6]. Стаття 45 Стратегії національної безпеки України першим серед пріоритетних завдань правоохоронних, спеціальних, розвідувальних та інших державних органів, відповідно до їх компетенції, визначає активну та ефективну протидію розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам, російській та іншій підривній пропаганді [7]. Однак, зі зрозумілих причин, жоден зі згаданих документів не описує та не визначає конкретних механізмів моніторингу й аналізу інформаційного простору, і тим більше — як повинна здійснюватися протидія російській та іншій «підривній пропаганді».

Доктрини зі стратегічних комунікацій Збройних Сил України та Національної гвардії України можуть розглядатися як цікавий, хоча і не зовсім вдалий приклад впровадження стандартів НАТО на рівні національних підзаконних актів у сфері стратегічних комунікацій та власне державного управління процесами захисту безпеки інформаційного простору. Попри те, що ці документи більш наближені до визначення порядку дій безпосередніх виконавців, аніж загальнодержавні стратегії, — вони теж не дають відповідей на запитання, яким чином має здійснюватися моніторинг інформаційного простору і реагування на інформаційні загрози чи недопущення виникнення інформаційних загроз [8; 9]. Чи не єдине суттєве досягнення документів — декларація необхідності проективної ініціативної позиції персоналу, який бере участь у процесах державного управління захистом безпеки інформаційного простору, та відхід від концепцій реагування за фактом, що в принципі виключає здобуття когнітивної переваги.

Дещо цікавіші у контексті конкретних механізмів відстеження реальних та потенційних інформаційних загроз першоджерела, під суттєвим впливом яких, очевидно, формувалися наведені доктрини. Мова йде про документи Північноатлантичного альянсу, а саме доктрини НАТО зі стратегічних комунікацій, з інформаційних операцій та з психологічних операцій [10; 11; 12]. Вони містять цілу низку інструментів, які військовим штабам оперативного рівня, відповідно до різних процедур прийняття військового рішення у процесі кризового планування, рекомендується використовувати для досягнення максимального ефекту, зокрема й інформаційних дій. Ці методики достатньо детальні, а самі протоколи виписані досить чітко. Зокрема цікавими для нас є принципи побудови аналізу PMESII (політичних, військових, економічних, суспільних, інформаційних та інфраструктурних факторів), а особливо — SCAME — Analysis of an adversary's psychological activity involves the detailed examination of the Source, Content, Audience, Media and Effects, тобто Аналіз психологічної активності противника з детальним вивченням джерела, контенту, аудиторії, носіїв та ефектів [12]. Згадані методики розроблені для планування та реалізації інформаційного супроводу воєнних операцій із різним ступенем застосування сили, але використовуються у найрізноманітніших сферах, починаючи від

реклами й закінчуючи контрпропагандою та іншою діяльністю, пов'язаною з протидією деструктивному інформаційно-психологічному впливу.

Зміст згаданих та інших методик містить ключові характеристики й запитання, на які повинен дати відповідь спеціаліст, який аналізує інформацію і приймає рішення щодо подальших дій.

Попри те, що деструктивний інформаційно-психологічний вплив може здійснюватися різноманітними методами, включаючи застосування неелектронних ресурсів, чуток, друкованої продукції тощо, доцільно побудувати алгоритм підтримки прийняття рішення шляхом аналізу контенту, розміщеного в Інтернет-просторі. Достатньо потужні інформаційні дії, здатні вплинути на умови виконання завдань державної організації та функціонування держави, усе одно будуть там відображені тим чи іншим чином, навіть якщо вони у своїй основі ведуться засобами, не пов'язаними із діями саме в Інтернет-просторі.

Враховуючи значний обсяг завдань та брак ресурсів будь-якої управлінської системи, в алгоритм підтримки прийняття рішень посадових осіб необхідно одразу закласти максимальну точність та економічність витрати кадрового ресурсу і часу, наскільки це можливо, тобто реалізувати максимально раціональний розподіл зусиль.

Як показує практика і чисельні дослідження, зокрема [13; 14] та інші, одним з найбільш ефективних є метод моніторингу інформаційного простору за ключовими словами. Він може здійснюватися як із застосуванням автоматичних систем моніторингу інформаційного простору, так і персоналом із використанням загальнодоступних пошукових систем без спеціального програмного забезпечення. З метою раціонального розподілу зусиль персоналу доцільно виділити до трьох ключових слів та словосполучень, за якими реалізовується періодичний моніторинг. Зазвичай, якщо поширений контент є частиною активності, яка вимагає залучення механізмів державного управління захистом безпеки інформаційного простору, — він так чи інакше потрапить у пошукову вибірку. В ідеальному варіанті обирається один комплект ключових слів (словосполучення), який може перевірятися у періодичному моніторингу різними мовами. Оптимальний період пошуку та, відповідно, періодичність, для більшості загальнодоступних пошукових систем і новинних агрегаторів станом на зараз — 24 години. При застосуванні автоматичних систем моніторингу інформаційного простору ця цифра теж має значення, але не настільки суттєве.

Визначення ключового для пошуку словосполучення доцільно здійснювати найпростішим способом. Це має бути поняття, сфера діяльності, державний орган або посадова особа, діяльність якої забезпечує відповідний підрозділ, що входить до системи державного управління захистом безпеки інформаційного простору та реалізовує протидію деструктивному інформаційно-психологічному впливу противника. До прикладу, якщо завдання підрозділу (прес-служби, підрозділу інформаційної протидії тощо) включає забезпечення сприятливих умов в інформаційному просторі для діяльності Бориспільської районної державної адміністрації, — ключовими словами доцільно буде вибрати, відповідно, «Бориспільська районна адміністрація», опціонально, додатково, як варіант, слово «Бориспіль», а з урахуванням наявності у місті міжнародного аеропорту, після закінчення дії воєнного стану та відновлення авіасполучення проводити моніторинг не лише за пошуком українською мовою, але й англійською та, бажано, іншими іноземними, якими найчастіше публікуються новини, пов'язані з містом чи районом.

За ключовими словами у періодичному пошуку щодо організацій середнього (оперативного) рівня управління зазвичай може бути виявлено від п'яти до 50 інформаційних повідомлень, об'єднаних у тематичні групи в кількості від однієї до трьох, при чому інформація з повідомлень всередині тематичних груп повністю або частково дублюється, хоча і може відрізнятися контекстами.

З метою прийняття обґрунтованого рішення щодо подальших дій, або утримання від них слід послідовно відповісти на низку запитань:

1. Чи є вказаний інформаційний контент достатньо поширеним (або чи може мати тенденції для достатнього поширення) серед цільової аудиторії, аби мати вплив на ситуацію?

У разі негативної відповіді на це запитання подальша робота з таким матеріалом є недоцільною витратою ресурсів. Застосовується метод «Тиша».

У разі позитивної відповіді формулюється наступне запитання:

2. Чи створює вказаний контент несприятливі умови в інформаційному просторі для виконання завдань організації, діяльність якої забезпечує відповідний підрозділ захисту безпеки інформаційного простору, або чи має тенденцію до створення таких несприятливих умов у майбутньому? При відповіді на це запитання також слід враховувати контекст, попередні повідомлення в інформаційному просторі, поширені за пов'язаною тематикою.

У разі чіткої негативної відповіді подальша робота з таким матеріалом є недоцільною витратою ресурсів. Застосовується метод «Тиша».

У разі позитивної відповіді необхідно виявити першоджерело. У подальшому доцільно визначити, сірим, білим чи чорним є першоджерело інформації, та діяти за наступною схемою (в останньому рядку викладені пропозиції щодо оптимальних дій, відповідно до розділу VI AJP 3.10.1 [12] (рис. 1, 2, 3).

Алгоритм має своїм завданням лише прискорити роботу відповідних спеціалістів, а його рекомендації не є догмою. В окремих випадках, з урахуванням конкретних обставин, рішення можуть прийматися

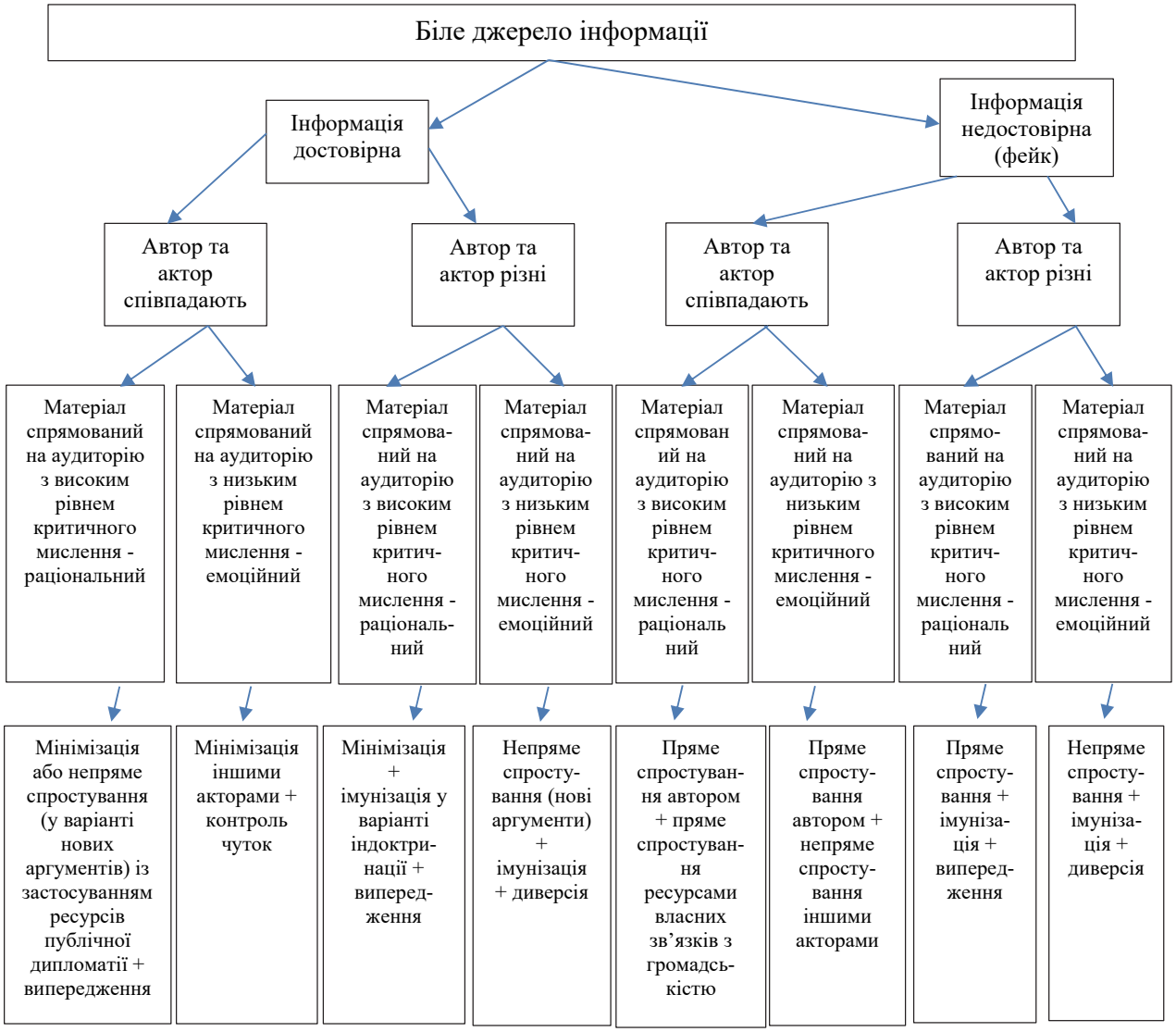

Рис. 1

за ситуацією. Для ефективної роботи методики також необхідна її друга частина — методика оцінки прийнятих рішень.

У випадку негативних відповідей на перші два запитання, коли застосовується метод «Тиша», пропонується вважати рішення ефективним, якщо в результаті його прийняття протягом наступних трьох діб (актуально для сучасного стану інформаційного простору, у майбутньому показник вірогідно змінюватиметься) не відбулося відомих відповідному спеціалісту злочинів, людських жертв, матеріальних втрат, і ситуація не змінилася до стану позитивної відповіді на перших два запитання. У випадку, якщо через п'ять діб пошукові системи не виявляють нових повідомлень за відповідною тематикою, відстеження поширення відповідного контенту тематичного деструктивного інформаційно-психологічного впливу можна призупиняти.

У випадку, якщо приймаються рішення на застосування інших заходів, пов'язаних з інформаційними діями, пропонується оцінювати їх ефективність шляхом аналізу статистичних даних щодо подій, які відбулися фізично, а за відсутності таких даних якість відпрацювання матеріалів та сприйняття їх цільовими аудиторіями оцінювати за формулою:

$$E_1 = r_{(\text{цільового матеріалу1})} - r_{(\text{сер.1})},$$

де

E_1 — ефективність інформаційних дій за першим (1) каналом поширення інформації;

$r_{\text{цільового матеріалу}}$ — реакції аудиторії та інші доступні статистичні дані (коментарі, поширення, тощо) у кількісному відношенні на каналі поширення інформації 1.

$r_{\text{сер.1}}$ — середнє арифметичне, що визначається сумою усіх реакцій (коментарів, поширень, інших доступних даних про реагування аудиторії) двох матеріалів, що передували за часом публікації на каналі поширення інформації 1 цільовому матеріалу та двом матеріалам, опублікованим після цільового матеріалу, поділеною на 4.

Відповідно,

$$E_{\text{інформаційних дій}} = (E_1 + E_2 + E_3):3,$$

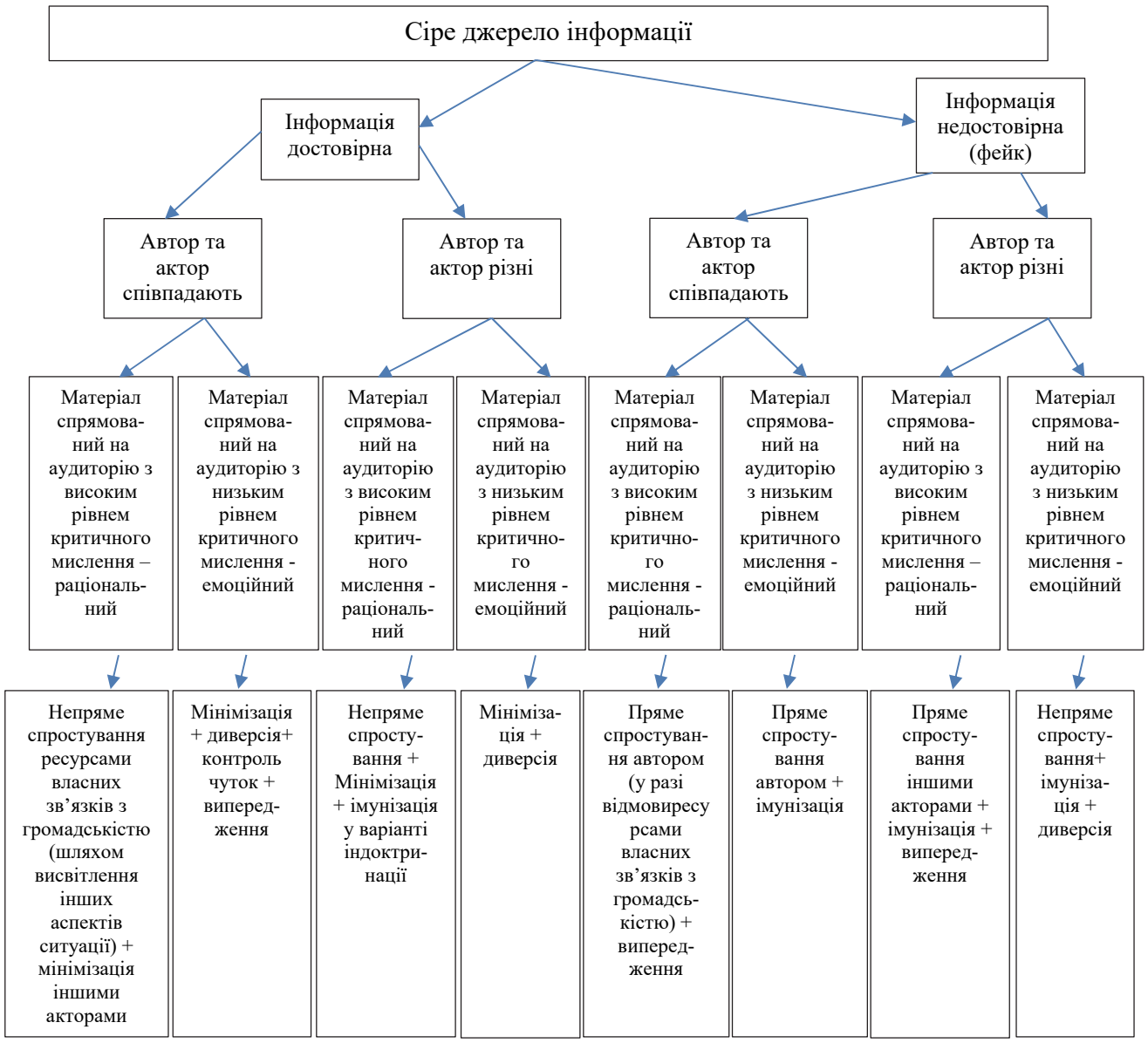

Рис. 2

де E_1, E_2 та E_3 — ефективність поширення цільового матеріалу через 1-й, 2-й і 3-й канал поширення інформації. E_1, E_2 та E_3 обираються з загальної кількості каналів поширення інформації за принципом максимального охоплення аудиторії або, якщо має критичне значення реакція саме цільової аудиторії, — за принципом максимальної відповідності каналів поширення інформації запитам певної цільової аудиторії.

Від'ємний показник $E_{\text{інформаційних дій}}$ свідчить про недостатній рівень ефективності прийняття рішень у сфері захисту безпеки інформаційного простору та необхідності коригування тактики дій, інших аспектів управління, аж до кадрових змін.

Нульовий показник $E_{\text{інформаційних дій}}$ свідчить про достатній, але невисокий рівень ефективності прийняття рішень, необхідність удосконалювати в подальшому тактику дій і підготовку персоналу.

Додатний показник $E_{\text{інформаційних дій}}$ свідчить про достатній рівень ефективності прийняття рішень. Стабільне зростання додатного показника $E_{\text{інформаційних дій}}$ свідчить про правильний напрямок набуття досвіду та розвитку тактики дій персоналу, залученого до реалізації механізмів державного управління захисту безпеки інформаційного простору.

Висновки та перспективи подальших розвідок у даному напрямку. В ході дослідження на основі поточного та попередніх напрацювань розроблено методику підтримки прийняття рішень під час реалізації державного управління у сфері захисту безпеки інформаційного простору. Методика складається з двох основних частин: алгоритму підтримки прийняття управлінських рішень та методики оцінки прийнятих рішень.

Оскільки методика розроблялася як прикладний інструмент, в ході розробки пріоритетними були

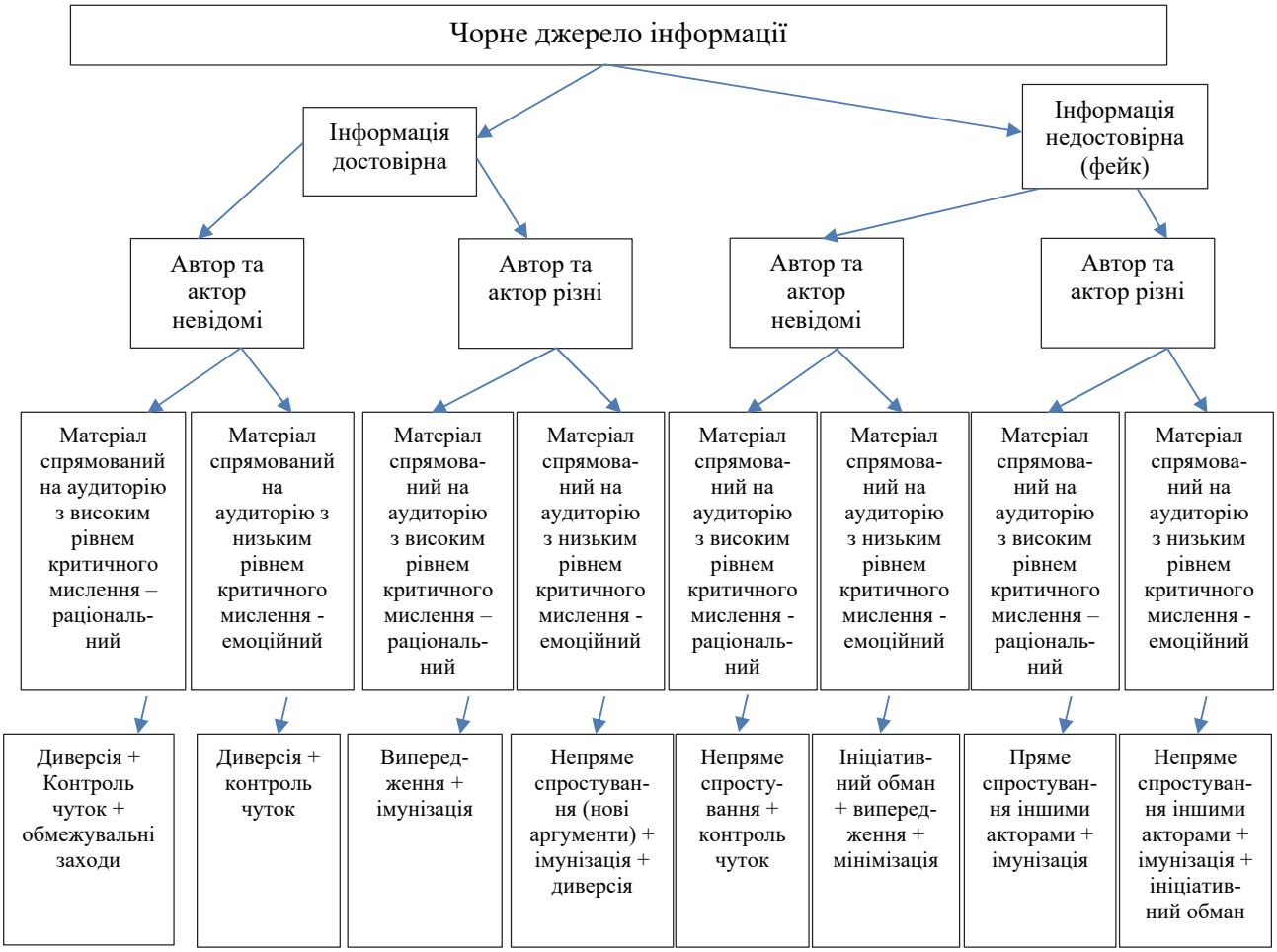

Рис. 3

принципи простоти, практичності та економічності у застосуванні.

Принцип дії методики заснований на декомпозиції складного завдання, яким є, по суті, кожна окрема ситуація у сфері державного управління захистом безпеки інформаційного простору, на окремі прості питання, послідовна відповідь на які дає можливість відповідному спеціалісту, по-перше, самостійно краще зрозуміти ситуацію, і, по-друге, отримати рекомендацію щодо оптимальних дій, яка з високою вірогідністю буде доречною.

Також методика оцінки прийнятих управлінських рішень дозволяє в процесі діяльності коригувати саму методику підтримки прийняття рішень під індивідуальні потреби спеціаліста у сфері захисту безпеки інформаційного простору, а головне — більш ефективно систематизувати досвід, який він отримує в процесі своєї діяльності.

Напрямки подальшого дослідження вбачаються у:

– описі та обґрунтуванні методики;
– верифікації методики;
– формуванні методичних рекомендацій щодо застосування методики.

Ефективне продовження дослідження за умов практичного впровадження його результатів дозволить без додаткових матеріальних чи інших ресурсів, громіздких правових чи складних організаційних змін підвищити ефективність державного управління у сфері захисту безпеки інформаційного простору в умовах відбиття Силами оборони України російського широкомасштабного вторгнення, однією з ключових складових якого виступають заходи деструктивного інформаційно-психологічного впливу.

Література

1. Палко Д., Мирутенко Л. Метод комплексної оцінки ризиків кібербезпеки в розподілених інформаційних системах. *Кібербезпека: освіта, наука, техніка.* 2024. № 2. С. DOI: https://doi.org/10.28925/2663-4023.2024.26.731

2. Вайтсайд Р.Д. Розгляд основ засобів масової інформації, інформації та даних армії США проти шкідливої інформації у відкритому інформаційному середовищі: якісне прикладне дослідження. *Рукопис дисертації, поданий до Національного університету Санфордського педагогічного коледжу на здобуття наукового ступеня доктора педагогічних наук. Національний університет ProQuest.* Дисертації та тези, 2024. URL: https://www.proquest.com/openview/4bad2c7f9236292c9bcb14389acde41f/1?cbl=18750&diss=y&pq-origsite=gscholar (дата звернення: 05.04.2025).

3. Будь на сторожі якісної інформації — ставай частиною спільноти «Детектор медіа». URL: https://disinfo.detector.media (дата звернення: 05.04.2025).

4. Центр протидії дезінформації. URL: https://cpd.gov.ua (дата звернення: 05.04.2025).

5. База даних. URL: https://euvsdisinfo.eu/disinformation-cases/ (дата звернення: 05.04.2025).

6. 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: 05.04.2025).

7. 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: 05.04.2025).

8. 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: 05.04.2025).

9. 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: 05.04.2025).

10. 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: 05.04.2025).

11. 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: 05.04.2025).

12. 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: 05.04.2025).

13. Фабрикатор М., Яганов П. Інтелектуальні технології телекомунікацій для систем моніторингу та оперативного інформування. *Herald of Khmelnytskyi National University. Technical Sciences.* 2024. 339(4). P. 97–101. DOI: https://doi.org/10.31891/2307-5732-2024-339-4-15

14. Глобенко С. Моделювання публічного управління захистом інформаційного простору в контексті застосування ризик-орієнтованого підходу. *Державне управління.* 2024. 1 (15). С. 67–81. DOI: https://doi.org/10.33269/2618-0065-2024-1(15)-67-81

References

1. Palko D., Myrutenko L. Metod kompleksnoi otsinky ryzykiv kiberbezpeky v rozpodilenykh informatsiinykh systemakh [Method of comprehensive assessment of cybersecurity risks in distributed information systems]. *Kiberbezpeka: osvita, nauka, tekhnika — Cybersecurity: Education, Science, Technology.* 2024. № 2. C. DOI: https://doi.org/10.28925/2663-4023.2024.26.731https://lsej.org.ua/6_2016/70.pdf [in Ukrainian].

2. Vaitsaid R.D. Rozghliad osnov zasobiv masovoi informatsii, informatsii ta danykh armii SShA proty shkidlyvoi informatsii u vidkrytomu informatsiinomu seredovyshchi: yakisne prykladne doslidzhennia. Rukopys dysertatsii, podanyi do Natsionalnoho universytetu Sanfordskoho pedahohichnoho koledzhu na zdobuttia naukovoho stupenia doktora pedahohichnykh nauk [Examining the U.S. Army's media, information, and data framework against malicious information in an open information environment: a qualitative case study. Manuscript submitted to the National University of Sanford College of Education for the degree of Doctor of Education]. Natsionalnyi universytet ProQuest. Dysertatsii ta tezy. National University ProQuest. Dissertations and theses. 2024. № 2. C. URL: https://www.proquest.com/openview/4bad2c7f9236292c9bcb14389acde41f/1?cbl=18750&diss=y&pq-origsite=gscholar

3. Bud na storozhi yakisnoi informatsii — stavai chastynoiu spilnoty "Detektor media" [Be on the lookout for quality information — become part of the Detector Media community]. URL: URL: https://disinfo.detector.media [in Ukrainian].

4. Tsentr protydii dezinformatsii [Center for Countering Disinformation]. URL: https://cpd.gov.ua [in Ukrainian].

5. Baza danykh [Database]. URL: https://euvsdisinfo.eu/disinformation-cases/ [in Ukrainian].

6. 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].

7. 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].

8. 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 — Territorial Defense Forces of the Armed Forces of Ukraine.* 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 [in Ukrainian].

9. 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 — The National Guard of Ukraine.* URL: https://ngu.gov.ua/wp-content/uploads/2022/12/vkp-11–0101.01-doktryna-strategichnyh-komunikaczij-ngu.pdf.pdf [in Ukrainian].

10. 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

11. 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

12. NATO standard AJP-3.10.1(A) Allied Joint Doctrine for psychological operations. October 2007. URL: https://info.publicintelligence.net/NATO-PSYOPS.pdf

13. Fabrykator M., Yahanov P. Intelektualni tekhnolohii telekomunikatsii dlia system monitorynhu ta operatyvnoho informuvannia [Intelligent telecommunications technologies for monitoring and operational information systems]. *Herald of Khmelnytskyi National University. Technical Sciences.* 2024. 339(4). P. 97–101 [in Ukrainian].

14. Hlobenko S. Modeliuvannia publichnoho upravlinnia zakhystom informatsiinoho prostoru v konteksti zastosuvannia ryzyk-oriientovanoho pidkhodu [Modeling of public management of information space protection in the context of risk-based approach]. *Derzhavne upravlinnia — Public Administration.* 2024. 1 (15). P. 67–81. DOI: https://doi.org/10.33269/2618-0065-2024-1(15)-67-81 [in Ukrainian].