УДК 35 **DOI: 10.32751/2617-5967-2025-03-23**

Кудрявський І. В.
докторант, Міжрегіональна Академія управління персоналом, Київ,
https://orcid.org/0009-0009-5167-7648

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

У ході попередніх досліджень розроблено та описано алгоритм підтримки прийняття рішень під час реалізації механізмів державного управління у сфері захисту безпеки інформаційного простору. Кожна ситуація, яку спричинив деструктивний інформаційно-психологічний вплив ворога та інші дії різних учасників наповнення інформаційного простору, має свій особливий характер, вимагає ґрунтовного підходу та реагування, розробленого спеціально для цієї ситуації з урахуванням усіх умов, обставин та факторів. Поряд з тим, подібні ситуації можливо класифікувати за певними ознаками, і доцільні варіанти реагування на них, з високою вірогідністю, будуть корелювати з характером і типом відповідних ситуацій. Дане припущення є основою алгоритму, створеного за результатами аналізу і спрощення низки аналітичних методик, призначених полегшити роботу цивільних колективів (військових штабів), до чиїх завдань входить нівелювання (мінімізація) наслідків деструктивного інформаційно-психологічного впливу противника та інших дій різних учасників наповнення інформаційного простору, що можуть розцінюватися у якості інформаційної загрози.

***Мета** запропонованого дослідження – підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору шляхом перевірки (верифікації) та, за необхідності, удосконалення, алгоритму підтримки прийняття управлінських рішень і методики оцінки результатів прийнятих управлінських рішень у сфері захисту безпеки інформаційного простору.*

***Завдання дослідження** полягає у перевірці механізмів підтримки прийняття управлінських рішень та методики оцінки результатів управлінських рішень у сфері захисту безпеки інформаційного простору шляхом їх застосування на реальних прикладах.*

***Наукова новизна** дослідження і його результатів полягає у прикладному характері розробленого інструментарію підтримки прийняття управлінських рішень з метою вирішення проблемних питань сучасного державного управління у сфері захисту безпеки інформаційного простору України без суттєвих ресурсних витрат.*

***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: За результатами вибіркового дослідження трьох різних інформаційних повідомлень, які мали негативний вплив на виконання завдань відповідної посадової особи чи організації, при цьому поширені білим, сірим та чорним джерелом інформації відповідно, а також заходів реагування на такі інформаційні повідомлення, які вживалися професіоналами у сфері стратегічних комунікацій, зокрема, в питаннях нівелювання (зниження ефективності) деструктивного інформаційно-психологічного*

впливу, можемо зробити висновок, що запропонований алгоритм підтримки прийняття рішень в цілому відповідає сучасній практиці досвідчених спеціалістів. Дії таких спеціалістів, завдяки ретроспективному аналізу (оскільки події відбулися хоч і не в дуже далекому, але все ж у минулому), на даний момент можна оцінити як успішні. Про це свідчить той факт, що порушена повідомленнями деструктивного інформаційного впливу тематика не стала поширюватися і не набула критичного значення для виконання своїх завдань відповідними посадовими особами та організаціями.

Алгоритм підтримки прийняття рішень не є обов'язковим до виконання протоколом, і при його розробці не ставилося завдання заздалегідь дати єдину вірну відповідь на будь-яку можливу ситуацію, тим більше, що в умовах інформаційної війни це неможливо, а ефективних варіантів дій може бути щонайменше декілька. Поряд з тим, на думку автора, відповідність розробленого алгоритму успішній практиці інформаційних дій компетентних спеціалістів у питаннях зниження ефективності (нівелювання) деструктивного інформаційно-психологічного впливу свідчить про доцільність подальших досліджень та практичного впровадження алгоритму підтримки прийняття управлінських рішень у сфері захисту безпеки інформаційного простору в діяльність представників профільних інституцій.

На відміну від методик, взятих за основу при розробці алгоритму, зокрема викладених у доктринальних документах Північноатлантичного Альянсу [18, 19, 20], його можуть застосовувати не лише чисельні, чітко структуровані ієрархічні колективи (великі центри, військові штаби тощо), але й невеликі робочі групи та, навіть, окремі спеціалісти. Це робить алгоритм підтримки прийняття управлінських рішень у сфері захисту безпеки інформаційного простору гнучким і практичним інструментом в умовах сучасної інформаційної війни та ресурсних обмежень, характерних для країни, яка змушена протистояти значно чисельнішому противнику.

Крім того, у поєднанні з методикою аналізу ефективності прийнятих управлінських рішень у сфері захисту безпеки інформаційного простору алгоритм підтримки прийняття рішень дозволяє забезпечити ефективне навчання (усвідомлене набуття практичного досвіду) профільними спеціалістами без додаткових ресурсних витрат під час реалізації своїх посадових обов'язків за призначенням.

Перспективи подальших досліджень вбачаються у створенні методики застосування алгоритму підтримки прийняття управлінських рішень у сфері захисту безпеки інформаційного простору.

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

Previous studies have developed and described an algorithm for supporting decision-making in the implementation of state management mechanisms in the field of information space security. Each situation caused by the destructive information and psychological influence of the enemy and other actions of various participants in the information space has its own specific character and requires a thorough approach and response developed specifically for that situation, taking into account all conditions, circumstances, and factors. At the same time, such situations can be classified according to certain criteria, and appropriate responses to them are likely to correlate with the nature and type of the situations in question. This assumption is the basis of an algorithm created as a result of the analysis and simplification of a number of

analytical techniques designed to simplify the work of civilian teams (military headquarters) whose tasks include levelling (minimising) the consequences of destructive information and psychological influence by the enemy and other actions by various participants in the information space that can be regarded as an information threat.

The purpose *of the proposed study is to improve the effectiveness of state management mechanisms in the field of information space security by verifying and, if necessary, improving the algorithm for supporting management decisions and the methodology for evaluating the results of management decisions in the field of information space security.*

The research tasks *are to verify the mechanisms for supporting management decision-making and the methodology for evaluating the results of management decisions in the field of information space security by applying them to real-life examples.*

The scientific novelty *of the research and its results lies in the applied toolkit developed to support management decision-making in order to solve the problems of modern state management in the field of information space security in Ukraine without significant resource costs.*

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

The conclusions *state that****:*** *Based on the results of a selective study of three different information messages that likely had a negative impact on the performance of the relevant official or organization, disseminated by white, gray, and black sources of information, respectively, as well as the response measures to such information messages taken by professionals in the field of strategic communications, in particular in terms of neutralizing (reducing the effectiveness) of destructive information and psychological influence, we can conclude that the proposed decision-making support algorithm is generally consistent with the current practice of experienced specialists. Thanks to retrospective analysis (since the events took place in the not too distant past), the actions of these specialists can currently be assessed as successful. This is evidenced by the fact that the topics raised by the messages of destructive information influence did not spread and did not become critical for the performance of their tasks by the relevant officials and organizations.*

The decision-making support algorithm is not mandatory for implementation by the protocol, and when it was developed, the task was not to provide a single correct answer to any possible situation in advance, especially since this is impossible in the context of information warfare, and there may be at least several effective options for action. At the same time, in the author's opinion, the fact that the developed algorithm is consistent with the successful practice of information activities by competent specialists in reducing the effectiveness (leveling) of destructive information and psychological influence indicates the advisability of further research and practical implementation of the algorithm for supporting management decision-making in the field of information space security in the activities of representatives of specialized institutions.

Unlike the methodologies used as a basis for developing the algorithm, in particular those set out in the doctrinal documents of the North Atlantic Alliance [18, 19, 20], it can be used not only by large, clearly structured hierarchical teams (large centers, military headquarters, etc.), but also small working groups and even individual specialists. This makes the algorithm for supporting management decisions in the field of information space security a flexible and practical

tool in the context of modern information warfare and resource constraints characteristic of a country that is forced to confront a significantly larger enemy.

In addition, in combination with the methodology for analyzing the effectiveness of management decisions in the field of information space security, the decision support algorithm allows for effective training (conscious acquisition of practical experience) of relevant specialists without additional resource costs during the performance of their assigned duties.

Prospects for further research lie in the creation of a methodology for applying the algorithm for supporting management decisions in the field of information space security.

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

За результатами попередніх досліджень розроблено алгоритм підтримки прийняття рішень посадовими особами, які беруть участь у практичній реалізації механізмів державного управління захистом безпеки інформаційного простору. На даний момент постає питання у визначенні адекватності даного алгоритму, відповідності запропонованих ним варіантів дій реальним практичним ситуаціям, що виникають в інформаційному просторі, та придатності до навчання молодих спеціалістів.

Алгоритм передбачає декілька етапів: моніторинг інформаційного простору та визначення потенційних або реальних інформаційних загроз, оцінка інформаційних загроз, прийняття рішення щодо найбільш ефективних інформаційних дій (утримання від дій) та оцінка ефективності вжитих заходів (утримання від інформаційних дій за методом “тиші”).

Запропонований автором механізм моніторингу інформаційного простору є не авторським винаходом, а результатом вивчення попередніх досліджень та практики у сфері зниження ефективності (нівелювання) наслідків деструктивного інформаційно-психологічного впливу. Різноманітні системи та механізми моніторингу інформаційного простору достатньо добре напрацьовані і представлені як методиками роботи спеціалістів із застосуванням загальнодоступних інструментів, так і інформаційно-телекомунікаційними системами, які засновані на взаємодії фахівців, спеціального обладнання та програмного забезпечення, зокрема і з використанням технологій на базі штучного інтелекту. Автоматичні системи моніторингу інформаційного простору сьогодні не є чимось унікальним і їх застосування з достатньо якісною інформацією на виході постає швидше питанням залучення певного бюджету, часто досить помірного [1, 2, 3, 4, 5, 6, 7]. Ці ж системи дозволяють достатньо ефективно визначити успішність поширення інформації (ефективність інформаційних дій) в автоматичному чи напівавтоматичному режимі, хоча в цьому випадку і доведеться корелювати результат з поставленими цілями, які можуть не обмежуватися виключно інформаційним ефектом, а часто зосереджені на ефектах у фізичному вимірі інформаційного простору.

Тому ключовим питанням у ході верифікації алгоритму підтримки прийняття рішень постає власне сам алгоритм, оскільки модулі прогнозування автоматичних систем моніторингу інформаційного простору, як і модулі підтримки прийняття рішень, залишаються недостатньо досконалими для їх практичного застосування в реальному часі, і не передбачають достатньо добре перепрацьованого механізму навчання персоналу самостійному прийняттю відповідних рішень.

Таким чином, критично важливим елементом верифікації методики постає перевірка передусім самого розробленого алгоритму прийняття рішень на адекватність сучасним

реаліям. Зробити це можливо шляхом аналізу випадків останніх років, коли на інформаційні загрози (деструктивний інформаційно-психологічний вплив) вживали заходів реагування служби та спеціалісти, компетентні у такій роботі.

Завдання дослідження полягає у перевірці механізмів підтримки прийняття управлінських рішень та методики оцінки результатів управлінських рішень у сфері захисту безпеки інформаційного простору шляхом їх застосування на реальних прикладах.

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 іноземних нормативно-правових актах [18, 19, 20]; в офіційних оголошеннях та рекламаціях [1, 2, 3, 4, 5, 6, 7]; в повідомленнях медіа [8, 9, 10, 11, 12, 13, 14, 15, 16, 17].

Мета запропонованого дослідження – підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору шляхом перевірки (верифікації) та, за необхідності, удосконалення, алгоритму підтримки прийняття управлінських рішень і методики оцінки результатів прийнятих управлінських рішень у сфері захисту безпеки інформаційного простору.

Інформаційне агентство “Наше місто” висвітлює ситуацію, коли активіст Денис Селін звинуватив мера Дніпра Дмитра Філатова у покупці дорогого автомобіля, імовірно, за кошти, отримані корупційним шляхом [8]. У даному випадку, оскільки застосовувався ресурс (сторінка у Фейсбук, з якої активіст постійно публікував свої дописи протягом тривалого часу), джерело інформації ідентифіковане як надійне, тобто біле, а не анонімний ресурс. Поряд з тим, сама інформація ідентифікована як загроза. Припускаємо, що мер обласного центру мав можливість залучити достатньо компетентних спеціалістів у питаннях протидії деструктивному інформаційному впливу. Також очевидним є намір Дениса Селіна деструктивно вплинути щонайменше на репутацію мера Дніпра (але не виключає й інших намірів).

Відповідно до розробленого алгоритму, джерело інформації є білим. Отже, відпрацювання відбувається за першою таблицею. Поряд з тим, оприлюднена інформація ідентифікована як неправдива.

Як свідчать публікації [9, 10, 11], позиція осіб, які приймали рішення у виборі заходів реагування на інформаційну загрозу, полягає у тому, що діяльність Дениса Селіна пов’язана з активністю “кримінального авторитета Олександра Петровського”. Таким чином відповідь на наступне питання алгоритму полягатиме у тому, що автор повідомлення та актор, який його озвучив, вірогідно є різними особами.

Стилістика стартового допису в Фейсбук Дениса Селіна, наведеного на скриншоті в публікації [8], у зв’язку з певною іронічністю повідомлення і тим, що аудиторія з низьким рівнем критичного мислення, в принципі, не надто часто цікавиться порушеною тематикою і питаннями, дає підстави зробити висновки, що матеріал скоріше спрямований на аудиторію з високим критичним мисленням і є більше раціональним, ніж емоційним.

У такому випадку алгоритмом пропонується застосування методу прямого спростування у поєднанні з інструментарієм методик імунізації та випередження. Публікації у медіа [12, 13, 14] є нічим іншим, як застосуванням методу прямого спростування. Поряд з тим, публікації [8, 9, 10, 11] дають можливість чітко простежити застосування методів імунізації та випередження можливих або вірогідних дій опонента.

Таким чином, можемо констатувати, що достатньо компетентний спеціаліст (колектив спеціалістів) вжив заходів, які корелюють із рекомендаціями, передбаченими розробленим алгоритмом прийняття рішень у випадках, коли джерелом контенту, яке становить потенційну інформаційну загрозу, є біле джерело інформації.

Видання Militarnyi повідомляє про пожежу, яка сталася на водолазному судні "Нетішин", посилаючись на інформацію з власних джерел [15]. Безсумнівно, така інформація є достатньо чутливою та не сприяє іміджу ВМС, а отже може бути розцінена як інформаційна загроза. Хоча видання не конкретизує джерела, інформаційним агентством не приховується авторство цього медіа при створенні новини. Таким чином, джерело інформації ідентифікується як "сіре", коли, зокрема, автором вказується категорія джерел, але не називається конкретне джерело.

Як свідчать наступні публікації, зокрема офіційна заява Командування ВМС України [16], вказана інформація є достовірною. Безсумнівно, фахівці прес-служби Командування ВМС знали про це, приймаючи рішення щодо реагування на відповідну публікацію.

Характер повідомлення свідчить про те, що автор та актор (видання "Militarnyi") у даному повідомленні вірогідно співпадають, оскільки не відмічається масового поширення новин іншими інформаційними агентствами, а стилістика, характер та зміст у цілому відповідають стандартній стилістиці видання.

Фактова подача новини, відсутність маніпулятивного стилю та спеціальних елементів, покликаних спровокувати сильні емоції, свідчить про те, що матеріал спрямований на аудиторію з високим критичним мисленням і за характером є раціональним, а не емоційним.

За таких обставин розробленим алгоритмом рекомендується застосування методу "непрямого спростування" у контексті висвітлення особливостей ситуації та введення нових рядків аргументації в дискусію у поєднанні з методом мінімізації іншими акторами.

В реальній ситуації у повідомленні прес-служби командування ВМС [16] чітко прослідковується застосування даних методів, при чому метод мінімізації також частково використовується власними ресурсами, оскільки головними меседжами є те, що особовий склад не постраждав і за фактом події призначено службове розслідування.

Отже, можна констатувати, що дії реальних спеціалістів у питаннях нівелювання (мінімізації) наслідків запланованого чи супутнього деструктивного інформаційно-психологічного впливу загалом корелюють із рекомендаціями розробленого алгоритму для дій у випадках інформаційних загроз, що походять від активності сірих джерел інформації. Також можна зробити висновок, що додатковий елемент методу "мінімізації" зусиллями не власних зв'язків з громадськістю, а інших авторитетних акторів, як пропонується в алгоритмі, точно не погіршив би ситуації, що склалася.

Ворожі ресурси (російські пропагандисти) поширили інформацію про повідомлення нібито українського англомовного медіа United24, у якому представлені перехоплені "українською стороною" радіоперемовини. Російський командир просить своїх солдатів вживати лише привезену з собою їжу. У сюжеті розповідається про випадки смертельних отруєнь з-поміж українських військових, які воюють на курському напрямку, після буцімто вживання вкрадених з місцевих супермаркетів продуктів [17].

Дана інформація поширена чорним джерелом і є недостовірною.

Актор, тобто ворожі телеграм-канали та інші канали поширення інформації, відомий, як і псевдо-актор, – United24. Контрольоване синхронне поширення інформації

різними ворожими каналами робить очевидним факт, що вони діяли за вказівкою. Це відповідає розділу розробленого алгоритму “автор та актор різні” у таблиці “Чорні джерела поширення інформації”, тобто такі, при яких автор інформації, а в окремих випадках і актор, – приховуються, маскуються.

Характер інформаційного повідомлення, де окреме фейкове перехоплення супроводжується багатоетапними висновками, явно спрямований на переконання, а не виключно на блискавичну емоційну реакцію. Таким чином, повідомлення розраховане на аудиторію з наявним критичним мисленням і є раціональним, а не емоційним.

За таких обставин алгоритмом пропонується пряме спростування іншими акторами у поєднанні з методами імунізації та випередження. Публікація спростування інформації не самим United24, а Центром протидії дезінформації, причому з ремаркою: “Центр уже не вперше фіксує фейкові сюжети, нібито створені United24 media. Тому закликаємо довіряти лише офіційним ресурсам та джерелам верифікованої інформації”, – промовисто свідчить про поєднання названих методик, включаючи імунізацію щодо ворожих неперевірених джерел інформації та випередження майбутніх інформаційних дій ворога, які, вірогідно, включатимуть дезінформацію [17].

Отже, можемо констатувати факт, що спеціалісти Центру протидії дезінформації в реальній обстановці прийняли рішення за результатами аналізу інформації, поширеної чорним джерелом, яке повністю корелює рекомендаціям розробленого алгоритму.

Висновки та перспективи подальших розвідок у даному напрямку

За результатами вибіркового дослідження трьох різних інформаційних повідомлень, які, імовірно, мали негативний вплив на виконання завдань відповідної посадової особи чи організації, при цьому поширені білим, сірим та чорним джерелом інформації відповідно, а також заходів реагування на такі інформаційні повідомлення, які вживалися професіоналами у сфері стратегічних комунікацій, зокрема в питаннях нівелювання (зниження ефективності) деструктивного інформаційно-психологічного впливу, можемо зробити висновок, що запропонований алгоритм підтримки прийняття рішень в цілому відповідає сучасній практиці досвідчених спеціалістів. Дії таких спеціалістів, завдяки ретроспективному аналізу (оскільки події відбулися хоч і не в дуже далекому, але все ж у минулому) на даний момент можна оцінити як успішні. Про це свідчить той факт, що порушена повідомленнями деструктивного інформаційного впливу тематика не стала поширюватися і не набула критичного значення для виконання своїх завдань відповідними посадовими особами та організаціями.

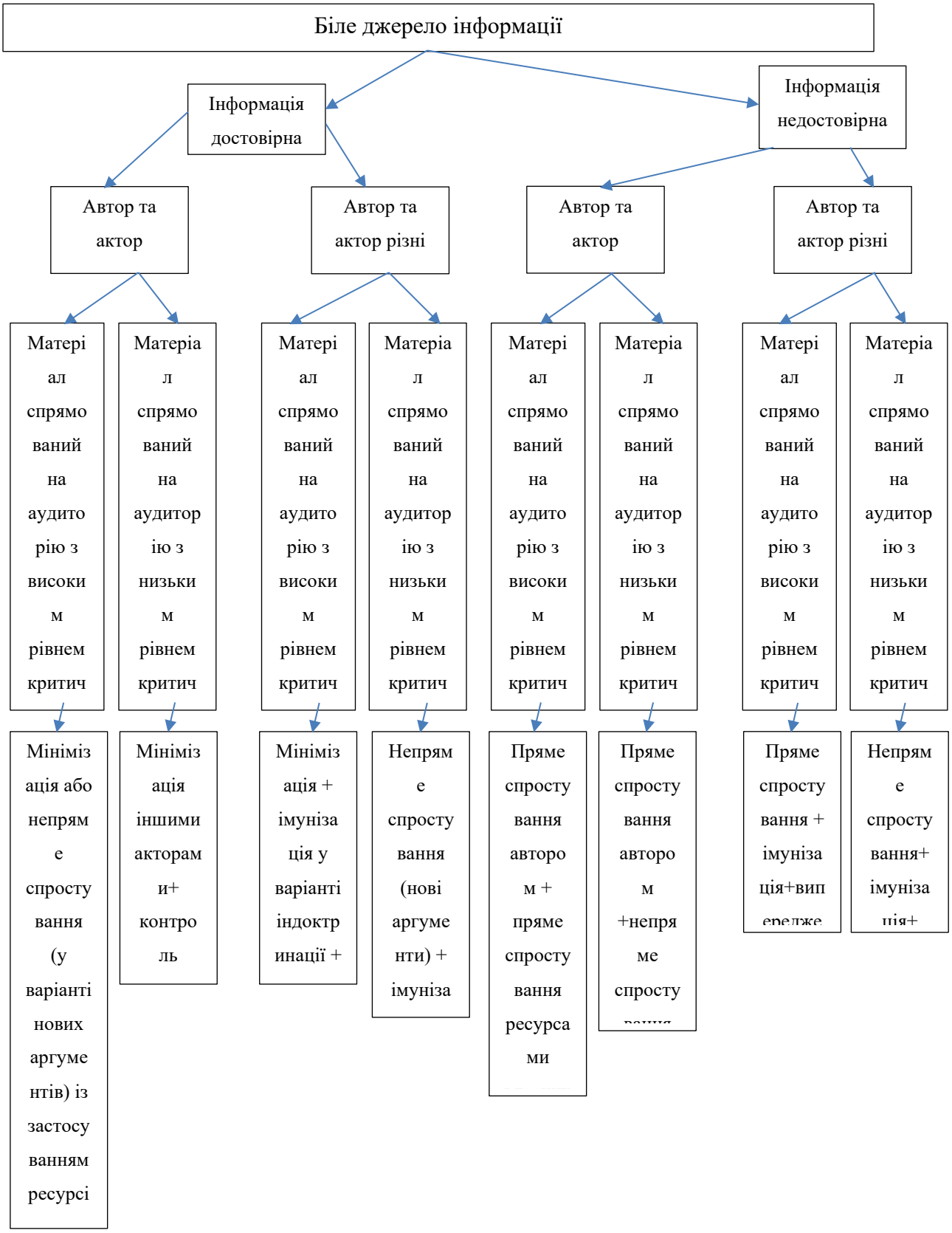
Алгоритм підтримки прийняття рішень не є обов’язковим до виконання протоколом, і при його розробці не ставилося завдання заздалегідь дати єдину правильну відповідь на будь-яку можливу ситуацію, тим більше що в умовах інформаційної війни це неможливо, а ефективних варіантів дій може бути щонайменше декілька. Поряд з тим, на думку автора, відповідність розробленого алгоритму успішній практиці інформаційних дій компетентних спеціалістів у питаннях зниження ефективності (нівелювання) деструктивного інформаційно-психологічного впливу свідчить про доцільність подальших досліджень та практичного впровадження алгоритму підтримки прийняття управлінських рішень у сфері захисту безпеки інформаційного простору у діяльність представників профільних інституцій.

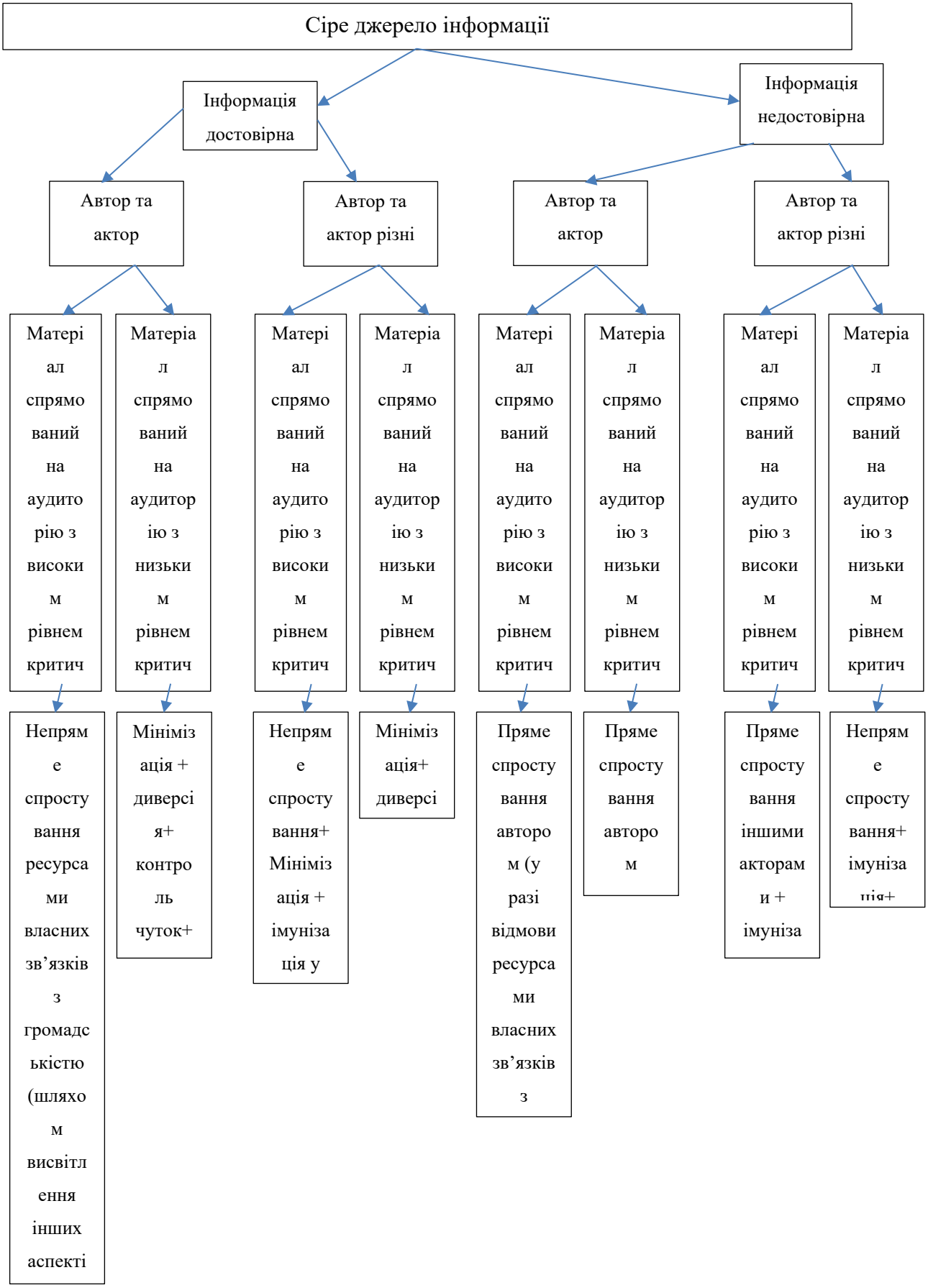
На відміну від методик, взятих за основу при розробці алгоритму, зокрема викладених у доктринальних документах Північноатлантичного Альянсу [18, 19, 20], його

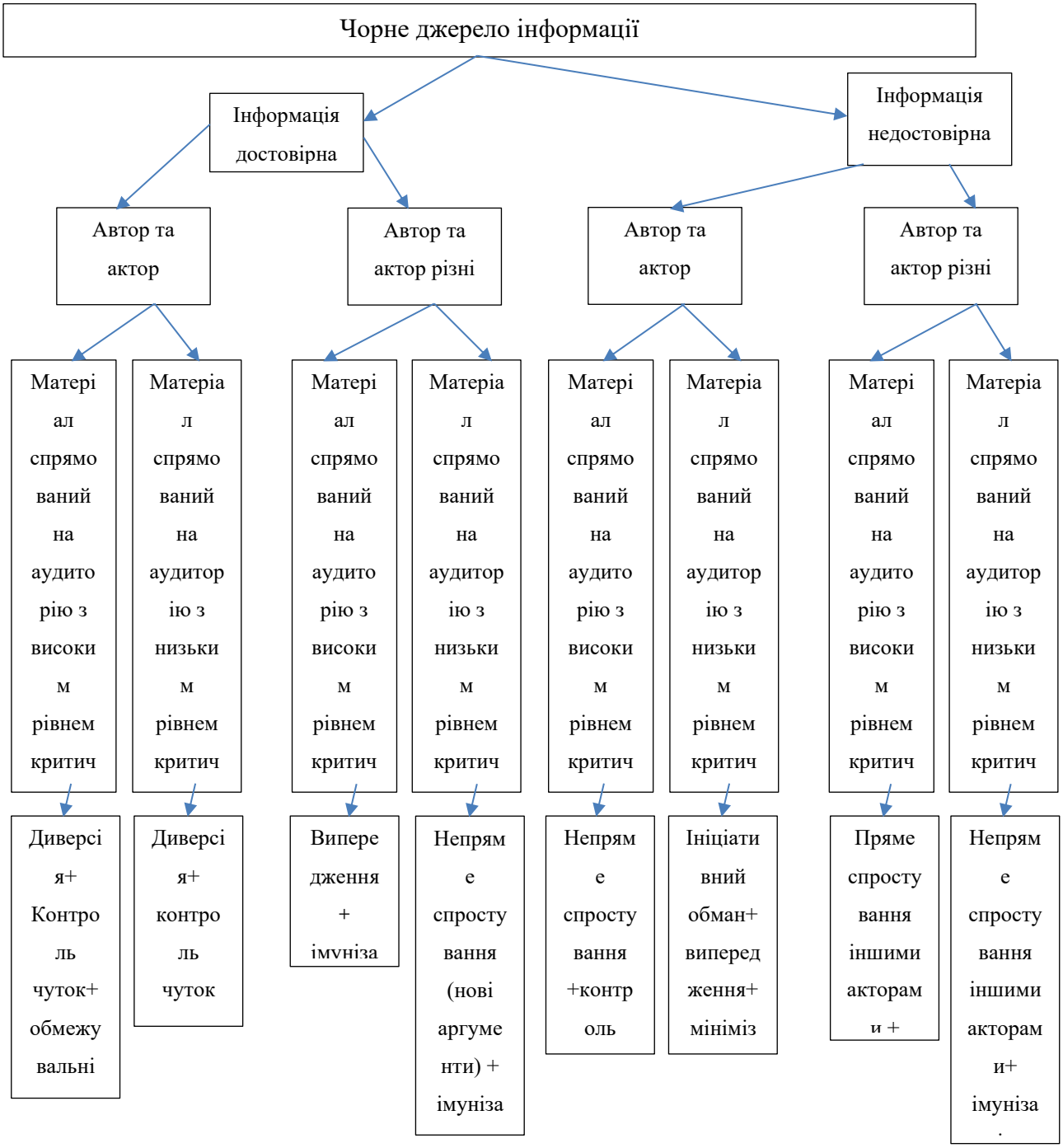
можуть застосовувати не лише чисельні, чітко структуровані ієрархічні колективи (великі центри, військові штаби тощо), але й невеликі робочі групи та, навіть, окремі спеціалісти. Це робить алгоритм підтримки прийняття управлінських рішень у сфері захисту безпеки інформаційного простору гнучким і практичним інструментом в умовах сучасної інформаційної війни та ресурсних обмежень, характерних для країни, яка змушена протистояти значно чисельнішому противнику.

Крім того, у поєднанні з методикою аналізу ефективності прийнятих управлінських рішень у сфері захисту безпеки інформаційного простору алгоритм підтримки прийняття рішень дозволяє забезпечити ефективне навчання (усвідомлене набуття практичного досвіду) профільними спеціалістами без додаткових ресурсних витрат під час реалізації своїх посадових обов'язків за призначенням.

Перспективи подальших досліджень вбачаються у створенні методики застосування алгоритму підтримки прийняття управлінських рішень у сфері захисту безпеки інформаційного простору.


Біле джерело інформації
Інформація достовірна
Інформація недостовірна
Автор та актор
Автор та актор різні
Автор та актор
Автор та актор різні
Матеріал спрямований на аудиторію з високим рівнем критич
Матеріал спрямований на аудиторію з низьким рівнем критич
Матеріал спрямований на аудиторію з високим рівнем критич
Матеріал спрямований на аудиторію з низьким рівнем критич
Матеріал спрямований на аудиторію з високим рівнем критич
Матеріал спрямований на аудиторію з низьким рівнем критич
Матеріал спрямований на аудиторію з високим рівнем критич
Матеріал спрямований на аудиторію з низьким рівнем критич
Мініміз ація або непрям е спросту вання (у варіанті нових аргуме нтів) із застосу ванням ресурсі
Мініміз ація іншими акторам и+ контро ль
Мініміз ація + імуніза ція у варіанті індоктр инації +
Непрям е спросту вання (нові аргуме нти) + імуніза
Пряме спросту вання авторо м + пряме спросту вання ресурса ми
Пряме спросту вання авторо м +непря ме спросту
Пряме спросту вання + імуніза ція+вип ередже
Непрям е спросту вання+ імуніза ція+


Сіре джерело інформації
Інформація достовірна
Інформація недостовірна
Автор та актор
Автор та актор різні
Автор та актор
Автор та актор різні
Матеріал спрямований на аудиторію з високим рівнем критич
Матеріал спрямований на аудиторію з низьким рівнем критич
Матеріал спрямований на аудиторію з високим рівнем критич
Матеріал спрямований на аудиторію з низьким рівнем критич
Матеріал спрямований на аудиторію з високим рівнем критич
Матеріал спрямований на аудиторію з низьким рівнем критич
Матеріал спрямований на аудиторію з високим рівнем критич
Матеріал спрямований на аудиторію з низьким рівнем критич
Непряме спростування ресурсами власних зв'язків з громадськістю (шляхом висвітлення інших аспекті
Мініміза ція + диверсія+ контроль чуток+
Непряме спростування+ Мініміза ція + імуніза ція у
Мініміза ція+ диверсі
Пряме спростування автором (у разі відмови ресурсами власних зв'язків з
Пряме спростування автором
Пряме спростування іншими акторами + імуніза
Непряме спростування+ імуніза ція+


Чорне джерело інформації
Інформація достовірна
Інформація недостовірна
Автор та актор
Автор та актор різні
Автор та актор
Автор та актор різні
Матеріал спрямований на аудиторію з високим рівнем критич
Матеріал спрямований на аудиторію з низьким рівнем критич
Матеріал спрямований на аудиторію з високим рівнем критич
Матеріал спрямований на аудиторію з низьким рівнем критич
Матеріал спрямований на аудиторію з високим рівнем критич
Матеріал спрямований на аудиторію з низьким рівнем критич
Матеріал спрямований на аудиторію з високим рівнем критич
Матеріал спрямований на аудиторію з низьким рівнем критич
Диверсія+ Контроль чуток+ обмежувальні
Диверсія+ контроль чуток
Випередження + імуніза
Непряме спростування (нові аргументи) + імуніза
Непряме спростування +контроль
Ініціативний обман+ випередження+ мініміз
Пряме спростування іншими акторами +
Непряме спростування іншими акторами+ імуніза .

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. LOOQME. // [Електронний ресурс]. Веб-сайт. https://www.looqme.io/about-us (дата звернення 29.06.2025).
2. Google-об'єктив. // [Електронний ресурс]. https://lens.google/intl/uk/ (дата звернення 25.04.2025).
3. Semantic Force. // [Електронний ресурс]. Веб-сайт. https://semanticforce.ai/ua/company/about-us (дата звернення 29.06.2025).
4. Semantrum. // [Електронний ресурс]. Веб-сайт. https://www.promo.semantrum.net/aboutus [in Ukrainian].
5. Attack index. // [Електронний ресурс]. Веб-сайт. https://attackindex.com/uk/golovna-attakindex/ (дата звернення 29.06.2025).
6. Ecosap. // [Електронний ресурс]. Веб-сайт. https://ecosap.media/ (дата звернення 25.04.2025).
7. SoMo bot. // [Електронний ресурс]. Веб-сайт. https://cityhost.ua/uk/blog/somo-bot-bot-dlya-sbora-i-analiza-informacii-iz-media.html (дата звернення 29.06.2025).
8. Фейк про Porsche для мера: як активіст Денис Селін програв суд і втратив репутацію. Наше місто. //[Електронний ресурс]. Веб-сайт. URL: https://nashemisto.dp.ua/2025/06/13/feik-pro-porsche-dlia-mera-iak-aktyvist-denys-selin-prohrav-sud-i-vtratyv-reputatsiiu/ (дата звернення 29.06.2025).
9. Як Денис Селін вигадав Porsche для мера, а зганьбив себе. 49000.com.ua. //[Електронний ресурс]. Веб-сайт. URL: https://49000.com.ua/yak-denis-selin-vigadav-porsche-dlya-mera-a-zga/ (дата звернення 29.06.2025).
10. Активіст Селін поширював брехню щодо міського голови Дніпра - рішення суду. Дніпро оперативний. //[Електронний ресурс]. Веб-сайт. URL: https://dnepr.express/ua/post/aktivist-selin-poshiryuvav-brehnyu-shodo-miskogo-golovi-dnipra-rishennya-sudu. (дата звернення 29.06.2025).
11. Поширював брехню щодо міського голови Дніпра: рішення суду стосовно активіста Селіна. Днепр час. //[Електронний ресурс]. Веб-сайт. URL: https://dpchas.com.ua/dnepr/poshiryuvav-brekhnyu-schodo-miskogo-golovi-dnipra-rishennya-sudu-stosovno-aktivista-selina (дата звернення 29.06.2025).
12. Борис Філатов подав до суду на Дениса Селіна за розповсюдження недостовірної інформації про купівлю Porsche. Наше місто. //[Електронний ресурс]. Веб-сайт. URL: https://nashemisto.dp.ua/2023/06/15/borys-filatov-podav-do-sudu-na-denysa-selina-za-rozpovsiudzhennia-nedostovirnoi-informatsii-pro-kupivliu-porsche/. (дата звернення 30.06.2025).
13. Суд у Дніпрі зареєстрував заяву від адвоката Бориса Філатова щодо розповсюдження недостовірної інформації Денисом Селіним. Дніпро оперативний. //[Електронний ресурс]. Веб-сайт. URL: https://dnepr.express/ua/post/sud-u-dnipri-zareyestruvav-zayavu-vid-advokata-borisa-filatova-shodo-rozpovsyudzhennya-nedostovirnoyi-informaciyi-denisom-selinim. (дата звернення 30.06.2025).
14. Вигадав Porsche для мера: як активіст Денис Селін зганьбився, програвши суд. Днепр. Главное. //[Електронний ресурс]. Веб-сайт. URL: https://glavnoe.dp.ua/articles/vyhadav-porsche-dlia-mera-iak-aktyvist-denys-selin-zhanbyvsia-prohravshy-sud/. (дата звернення 30.06.2025).

15. На водолазному судні ВМС України сталась пожежа. Militarny. //[Електронний ресурс]. Веб-сайт. URL: https://militarnyi.com/uk/news/na-vodolaznomu-sudni-vms-ukrayiny-stalas-pozhezha/. (дата звернення 30.06.2025).

16. Особовий склад Водолазного судна "Нетішин" під час нештатної ситуації не постраждав. Офіційна сторінка командування ВМС ЗСУ у Фейсбук. //[Електронний ресурс]. Веб-сайт. URL: https://www.facebook.com/navy.mil.gov.ua/posts/741552332714706. (дата звернення 30.06.2025).

17. Фейковий сюжет від імені UNITED24 media про буцімто отруєння військових ЗСУ їжею з магазинів у Курську. Центр протидії дезінформації. //[Електронний ресурс]. Веб-сайт. URL: https://cpd.gov.ua/warnin/fejkovyj-syuzhet-vid-imeni-united24-media-pro-buczimto-otruyennya-vijskovyh-zsu-yizheyu-z-magazyniv-u-kursku/ (дата звернення 05.04.2025).

18. 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).

19. 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).

20. 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).