DOI: 10.34015/2523-4552.2025.4.14
УДК 35

Кудрявський І. В.,
докторант, Міжрегіональна Академія управління персоналом
ORCID: 0009-0009-5167-7648

МЕТОДИКА ВИКОРИСТАННЯ АЛГОРИТМУ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У ХОДІ ЗАСТОСУВАННЯ МЕХАНІЗМІВ ДЕРЖАВНОГО УПРАВЛІННЯ У СФЕРІ ЗАХИСТУ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ ТА ОЦІНКИ ПРИЙНЯТИХ РІШЕНЬ

У ході попередніх досліджень розроблено, описано та апробовано на реальних прикладах, що мали місце останніми роками, алгоритм підтримки прийняття рішень під час реалізації механізмів державного управління у сфері захисту безпеки інформаційного простору. Результати досліджень демонструють, що рекомендації алгоритму за відповідних вихідних даних цілком корелюють із рішеннями, які в реальній обстановці приймалися досвідченими професійними спеціалістами з питань мінімізації (нейтралізації) наслідків деструктивного інформаційно-психологічного впливу.

У висновках зазначається, що за результатами дослідження сформульовано методику застосування (інструкцію) до алгоритму підтримки прийняття рішень в ході реалізації державного управління у сфері захисту безпеки інформаційного простору та оцінки ефективності прийнятих рішень. Дана методика (інструкція) у випадку її впровадження дозволить спеціалістам у сфері захисту безпеки інформаційного простору за наявності відповідної теоретичної підготовки у максимально короткі терміни (від трьох до шести місяців) набути практичного досвіду, навчитися застосовувати його максимально ефективно та набути практичної спроможності виконувати свої службові обов'язки і завдання за посадою. За відсутності фахової підготовки методика її не замінить, але дозволить сформувати загальне розуміння процесів, які відбуваються в інформаційному просторі, свідомо виконувати завдання за призначенням, узагальнити власний практичний досвід, значно полегшить майбутню теоретичну підготовку на базі спеціалізованих навчальних закладів та скоротить ресурси, включно з фінансовими, і час на проведення такої підготовки.

Крім того, застосування алгоритму підтримки прийняття управлінських рішень у комплексі з методикою їх оцінки дозволить оптимально розподілити наявні ресурси (фінансові, технічні, програмні, кадрові, час та інші), зокрема у питаннях визначення доцільності вжиття заходів, що включають активні інформаційні дії, змісту та характеру власних інформаційних повідомлень, а також визначення максимально ефективних каналів поширення інформації, визначення доцільності адаптації формату та змісту влас-

них інформаційних повідомлень для каналів поширення інформації, де такі повідомлення виявилися менш ефективними.

Загалом методика, у випадку її впровадження, покликана без суттєвих додаткових ресурсних витрат підвищити ефективність роботи механізмів державного управління у сфері захисту безпеки інформаційного простору в умовах дефіциту ресурсів, характерного для обставин ведення оборонної війни, зокрема і її інформаційної складової, проти значно чисельнішого та краще забезпеченого за всіма напрямками противника.

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

Постановка проблеми. За результатами попередніх досліджень розроблено алгоритм підтримки прийняття рішень посадовими особами, які беруть участь у практичній реалізації механізмів державного управління захистом безпеки інформаційного простору. Алгоритм перевірено на реальних ситуаціях, коли в інформаційному просторі з'являлися повідомлення (серії повідомлень), які мали суттєвий деструктивний інформаційно-психологічний вплив на аудиторії та могли створювати несприятливі умови для здійснення професійної (службової) діяльності відповідними посадовими особами, для виконання завдань державних та інших інституцій. З метою нейтралізації вказаних негативних наслідків у досліджуваних ситуаціях приймали рішення та діяли підготовлені досвідчені спеціалісти, які розуміють особливості послаблення (нівелювання) наслідків та ефектів деструктивного інформаційно-психологічного впливу. Як показали результати дослідження, рекомендації алгоритму при відповідних вхідних даних цілком корелюють із рішеннями, які приймалися у відповідних ситуаціях реальними людьми – професіоналами у своїй справі. На даний момент, враховуючи важливість реалізації практичної складової досліджень, постає питання у формуванні методики застосування (прикладної інструкції) до алгоритму прийняття рішень у ході здійснення державного управління 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 останніх досліджень і публікацій. Інформаційний матеріал, необхідний для аналізу, міститься: в іноземних та українських нормативно-правових актах [9; 10; 11; 12; 13; 14; 15; 16]; в офіційних оголошеннях та рекламаціях [1; 2; 3; 4; 5; 6]; відкритих загальнодоступних пошукових системах [7; 8].

Постановка завдання. Мета запропонованого дослідження – підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору шляхом розробки методики використання (інструкції) алгоритму підтримки прийняття управлінських рішень і методики оцінки результатів прийнятих управлінських

рішень у сфері захисту безпеки інформаційного простору. Завдання дослідження полягає у створенні простої інструкції з використання алгоритму підтримки прийняття управлінських рішень та методики оцінки результатів управлінських рішень у сфері захисту безпеки інформаційного простору для прикладного застосування відповідними спеціалістами.

Виклад основного матеріалу.

Методика застосування алгоритму підтримки прийняття рішень в ході реалізації механізмів державного управління у сфері захисту безпеки інформаційного простору

1. Визначити ключові слова, які будуть застосовуватися для пошуку. В окремих випадках можуть застосовуватися додаткові ключові слова, зображення, якщо це обумовлено обстановкою в інформаційному просторі.

2. Здійснити пошук за ключовими словами із застосуванням однієї із автоматичних систем моніторингу інформаційного простору, наприклад LOOQME, Semantic Force, Semantrum, Attack index, Ecosap, SoMo bot, [1; 2; 3; 4; 5; 6]. За відсутності доступу до таких систем застосувати пошук у доступній пошуковій системі, наприклад Google, визначивши параметри за вкладками «Інструменти» – «Будь-коли» – «за 24 години» [7]. За необхідності – додати пошук за зображенням (відео), застосувавши сервіс Google Lens [8] або аналогічний.

3. За результатами пошуку обрати результати (інформаційні повідомлення), які можуть мати деструктивний інформаційно-психологічний вплив на важливі для спеціаліста (державної інституції) цільові аудиторії, створювати негативні умови для виконання завдань посадової особи, структурного підрозділу, організації, відомства або створювати негативний вплив на імідж держави за напрямком відповідальності структурного підрозділу.

a. За відсутності таких результатів повторити пошук за періоди: «тиждень», «місяць» та «будь-коли» (без обмежень у часі). У разі відсутності відповідних повідомлень не витрачати час на нейтралізацію наслідків деструктивного інформаційно-психологічного впливу, а зосередитися на інших завданнях, наприклад, висвітленні діяльності та просуванні іміджу організації.

b. У разі виявлення відповідних повідомлень – перейти до дій за наступними етапами методики.

4. Визначити, чи дійсно інформаційне повідомлення за своїм змістом створює негативні умови для виконання завдань організації (структурного підрозділу) або чи погіршує імідж держави перед цільовими аудиторіями за напрямком відповідальності структурного підрозділу, а також чи може бути частиною серії повідомлень, які в результаті багатоетапної комбінації можуть мати такий ефект.

a. У випадку негативних відповідей – діяти за методом «Тиша» за термінологією доктрини НАТО з психологічних операцій [9] – не здійснювати ніяких активних інформаційних дій.

b. У випадку негативної відповіді в реальному часі, але позитивної відповіді чи сумніву щодо

можливості матеріалу здійснити негативний вплив на умови в інформаційному просторі для виконання завдань організації у поєднанні з іншими матеріалами – не здійснювати ніяких активних дій але відстежувати ситуацію протягом наступних трьох – семи днів.

c. У випадку позитивної відповіді – перейти до дій за рекомендаціями наступних етапів алгоритму.

5. Визначити, чи здатне повідомлення за характером каналів донесення інформації та загального охоплення аудиторії чинити суттєвий вплив на ситуацію в інформаційному просторі, чи може мати за технічними показниками поширення суттєвий інформаційний і будь-який фізичний ефект.

a. У випадку негативної відповіді – не здійснювати ніяких дій, але стежити за поширенням (новими публікаціями) повідомлення протягом наступних трьох – семи днів.

b. У випадку позитивної відповіді – перейти до дій, рекомендованих наступними етапами алгоритму.

6. Оцінити анонімність/ відкритість джерела інформації за параметрами:

a. Біле джерело інформації – канал поширення інформації не приховує джерела інформації, і ці відомості відповідають дійсності. У такому випадку діяти відповідно до табл. 1.

b. Сіре джерело інформації – канал поширення інформації приховує конкретне джерело інформації, але дає достатньо його характеристик, і ці відомості з високою вірогідністю відповідають дійсності. У такому випадку діяти відповідно до табл. 2.

c. Чорне джерело інформації – канал поширення інформації приховує джерело інформації або подає у якості джерела інформації завідомо хибну особу (організацію), що не має відношення до публікації. У такому випадку діяти відповідно до табл. 3.

7. Визначити, чи достовірна опублікована інформація (навіть за умов маніпулятивного трактування фактів), чи факти, викладені в інформаційному повідомленні, є дезінформацією.

8. Визначити, чи відомі і чи співпадають автор інформаційного повідомлення та актор (особа або організація, від імені якої озвучується повідомлення).

9. Визначити, який метод використовується автором інформаційного повідомлення – переконання чи навіювання. Переконання спрямоване зазвичай на аудиторію з певним рівнем критичного мислення і характерне наведенням чіткої логічної або псевдологічної аргументації. Навіювання – намагання викликати сильні емоції. Відповідно, необхідно охарактеризувати повідомлення як переважно раціональне чи емоційне. Застосування обох цих методів може поєднуватися, але один із них буде пріоритетним і його не складно визначити в ході аналізу інформаційного повідомлення.

10. Вжити заходів, за необхідності активних інформаційних дій, відповідно до четвертого рядка таблиць 1, 2, 3. У випадку, якщо необхідна додаткова інформація або роз’яснення термінології, – скористатися доктринами НАТО зі стратегічних комунікацій, з інформаційних операцій та з психологічних операцій [10, 11, 9], відповідно до яких

наведені в Алгоритмі терміни та поняття.

Методика оцінки ефективності прийнятих управлінських рішень у сфері захисту безпеки інформаційного простору

1. Якщо було прийнято рішення діяти за методом «тиша» (активні дії в інформаційному просторі не здійснювалися), рішення можна вважати вірним у випадку, коли інформаційне повідомлення не мало фізичного ефекту а інформаційний ефект не відстежується в ході моніторингу у пошуку «за добу», через три – чотири доби та у пошуку «без обмежень у часі» – через три – сім діб. Якщо це твердження не вірне – значить, необхідно повторно провести оцінку інформаційного повідомлення відповідно до алгоритму, визначити, на якому етапі допущена помилка та вжити заходів відповідно до повторного аналізу з урахуванням змін в обстановці.

2. Якщо вживалися активні дії в інформаційному просторі, потрібно провести оцінку ефективності інформаційних дій:

a. Здійснити моніторинг поширення власних інформаційних повідомлень.

b. Визначити середнє арифметичне показників охоплення та залученості аудиторій через канали поширення інформації, які дають такі дані щодо цільового (свого) інформаційного повідомлення, двох повідомлень, опублікованих перед ним, та двох, опублікованих після нього.

c. Порівняти показники охоплення цільових аудиторій та їх залученості з відповідними середніми показниками у різних каналах поширення інформації.

d. Якщо показник охоплення та залученості цільових аудиторій до цільового власного інформаційного повідомлення вищий, аніж середній за каналом поширення інформації у всіх або більшості каналах, через які поширювалося цільове повідомлення, – це свідчить про високу ефективність та розуміння особливостей цільової аудиторії авторським колективом, який формував власне цільове інформаційне повідомлення.

e. Якщо показники охоплення та залученості аудиторій власного цільового інформаційного повідомлення нижчі, аніж середні за відповідними каналами поширення інформації, – це свідчить про недостатню пропрацьованість цільових матеріалів відповідними авторськими колективами або невірно прийняті управлінські рішення у сфері захисту безпеки інформаційного простору.

f. Якщо на одних каналах поширення інформації показники охоплення аудиторій та залученості аудиторій до власних цільових інформаційних матеріалів істотно вищі, аніж середні за каналом поширення інформації, а на інших каналах поширення інформації – навпаки, – це свідчить про необхідність коригувати комплект каналів поширення інформації і пріоритетно спрямувати зусилля на більш ефективні з них, а також вжити заходів щодо адаптації власних інформаційних повідомлень для їх сприйняття аудиторіями менш ефективних каналів поширення інформації.

3. У випадку реалізації інформаційних дій за методами «непрямого спростування», «інформаційної диверсії», «ініціативного

обману», «випередження» та «мінімізації», якщо через три – сім днів після публікації власних інформаційних повідомлень пошук за ключовими словами без обмежень у часі, а також за відповідний період, що пройшов з моменту публікації повідомлення, яке має деструктивний інформаційно-психологічний вплив (доба, тиждень, місяць), не видає посилань на матеріали деструктивного інформаційно-психологічного впливу, і при цьому не спостерігається фізичних ефектів у вигляді наслідків такого впливу, – прийняті управлінські рішення та реалізовані інформаційні дії можна вважати успішними, без огляду на результати аналізу за п. 2 даної методики. При цьому результати аналізу за п. 2 варто врахувати з метою підвищення ефективності майбутніх власних інформаційних дій.

Загальне застереження. За відсутності невідкладних завдань, пов'язаних з інформаційними повідомленнями, які реально здатні істотно негативно впливати на виконання завдань структурного підрозділу (підприємства, установи, організації, відомства, держави в цілому чи посадової особи), спеціалістам, задіяним у реалізації механізмів державного управління у сфері захисту безпеки інформаційного простору, рекомендується застосовувати свої зусилля та ресурси своїх підрозділів максимально ефективно – тобто з метою іміджевої підтримки організації і підтримки постійної активної позиції в інформаційному просторі, не відволікаючись на малозначні (слабо поширені, які не матимуть резонансу протягом тривалого часу) інформаційні повідомлення, навіть якщо вони номінально містять елементи деструктивного інформаційно-психологічного впливу.

Така діяльність у цілому відповідає вимогам керівних документів, які регламентують питання захисту безпеки інформаційного простору в Україні, зокрема стратегіям національної безпеки, інформаційної безпеки, кібербезпеки України, доктринам зі стратегічних комунікацій Збройних Сил і Національної гвардії України та іншим [12; 13; 14; 15; 16], і дозволяє вести ініціативну діяльність, формуючи ситуацію в інформаційному просторі, що завжди більш ефективно, аніж реагування на обстановку за фактом.

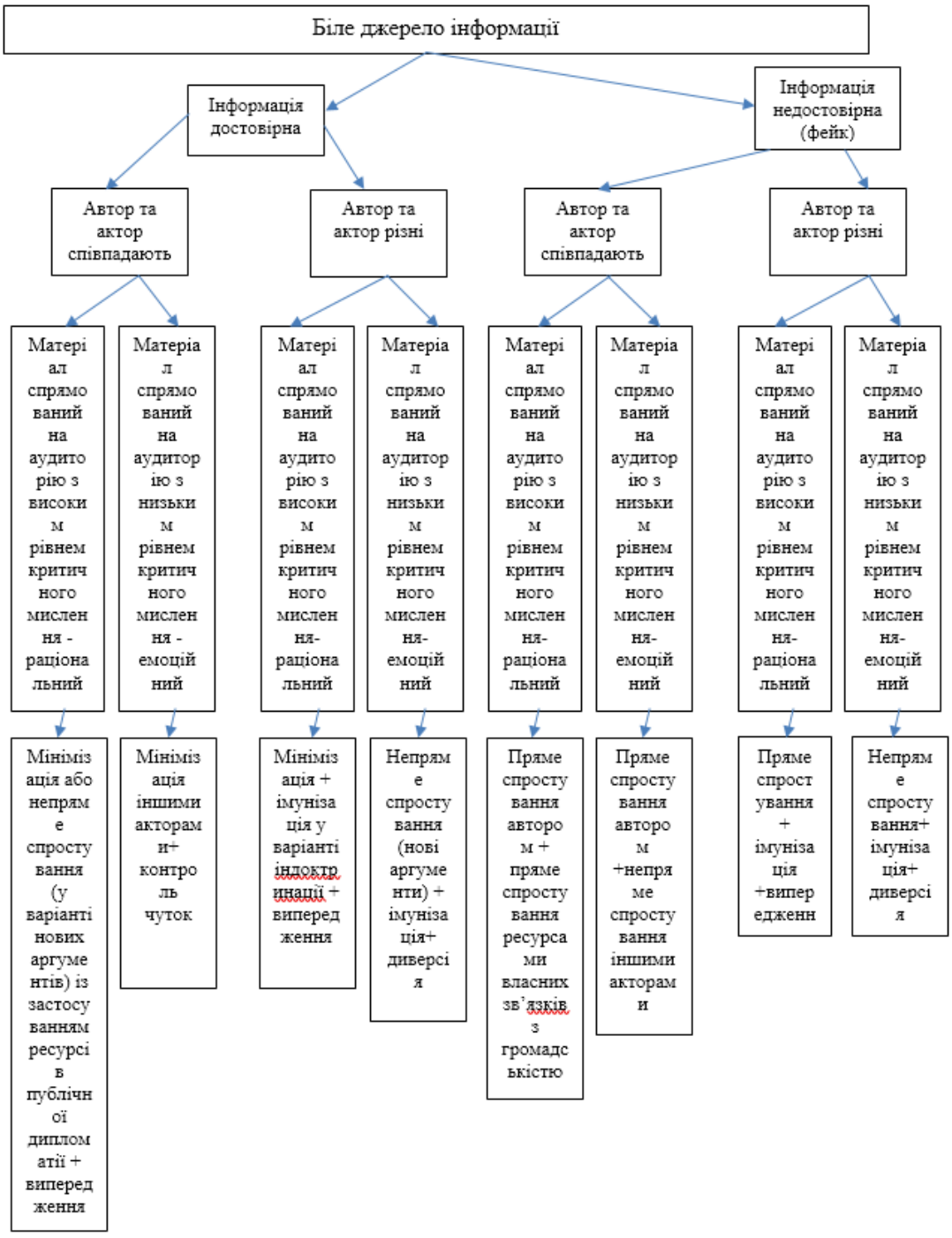
Висновки. За результатами дослідження сформульовано методику застосування (інструкцію) до алгоритму підтримки прийняття рішень в ході реалізації державного управління у сфері захисту безпеки інформаційного простору та оцінки ефективності прийнятих рішень. Дана методика (інструкція) у випадку її впровадження дозволить спеціалістам у сфері захисту безпеки інформаційного простору за наявності відповідної теоретичної підготовки у максимально короткі терміни (від трьох до шести місяців) набути практичного досвіду, навчитися застосовувати його максимально ефективно та набути практичної спроможності виконувати свої службові обов'язки і завдання за посадою. За відсутності фахової підготовки методика її не замінить, але дозволить сформувати загальне розуміння процесів, які відбуваються в інформаційному просторі, свідомо виконувати завдання за

призначенням і узагальнити власний практичний досвід, що значно полегшить майбутню теоретичну підготовку на базі спеціалізованих навчальних закладів та скоротить ресурси, включно з фінансовими, і час на проведення такої підготовки.

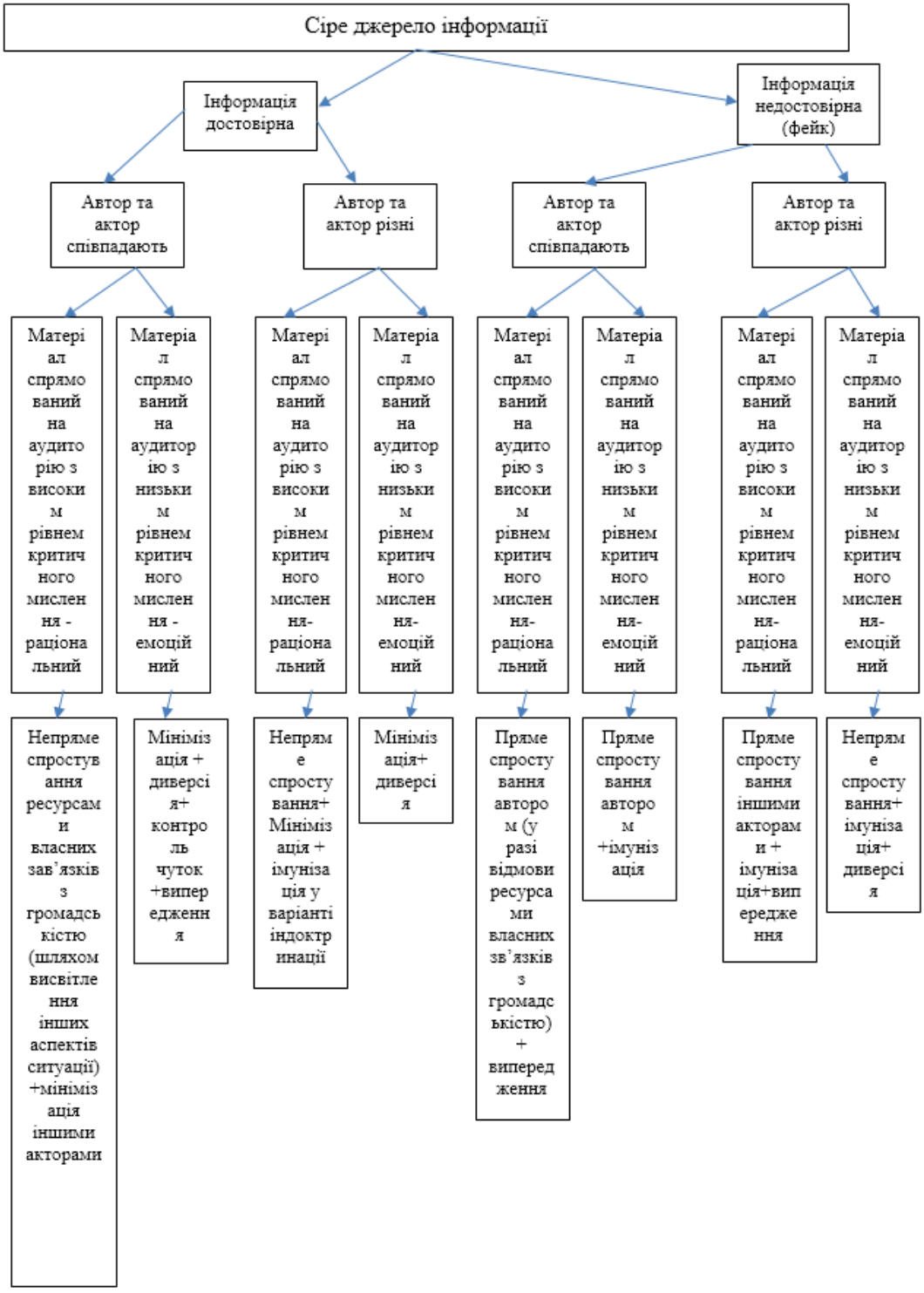
Крім того, застосування алгоритму підтримки прийняття управлінських рішень у комплексі з методикою їх оцінки дозволить оптимально розподілити наявні ресурси (фінансові, технічні, програмні, кадрові, час та інші), зокрема у питаннях визначення доцільності вжиття заходів, що включають активні інформаційні дії, змісту та характеру власних інформаційних повідомлень, а також визначення максимально ефективних каналів поширення інформації, визначення доцільності адаптації формату та змісту власних інформаційних повідомлень для каналів поширення інформації, де такі повідомлення виявилися менш ефективними.

Загалом методика, у випадку її впровадження, покликана без суттєвих додаткових ресурсних витрат підвищити ефективність роботи механізмів державного управління у сфері захисту безпеки інформаційного простору в умовах дефіциту ресурсів, характерного для обставин ведення оборонної війни, зокрема і її інформаційної складової, проти значно чисельнішого та краще забезпеченого за всіма напрямками противника.

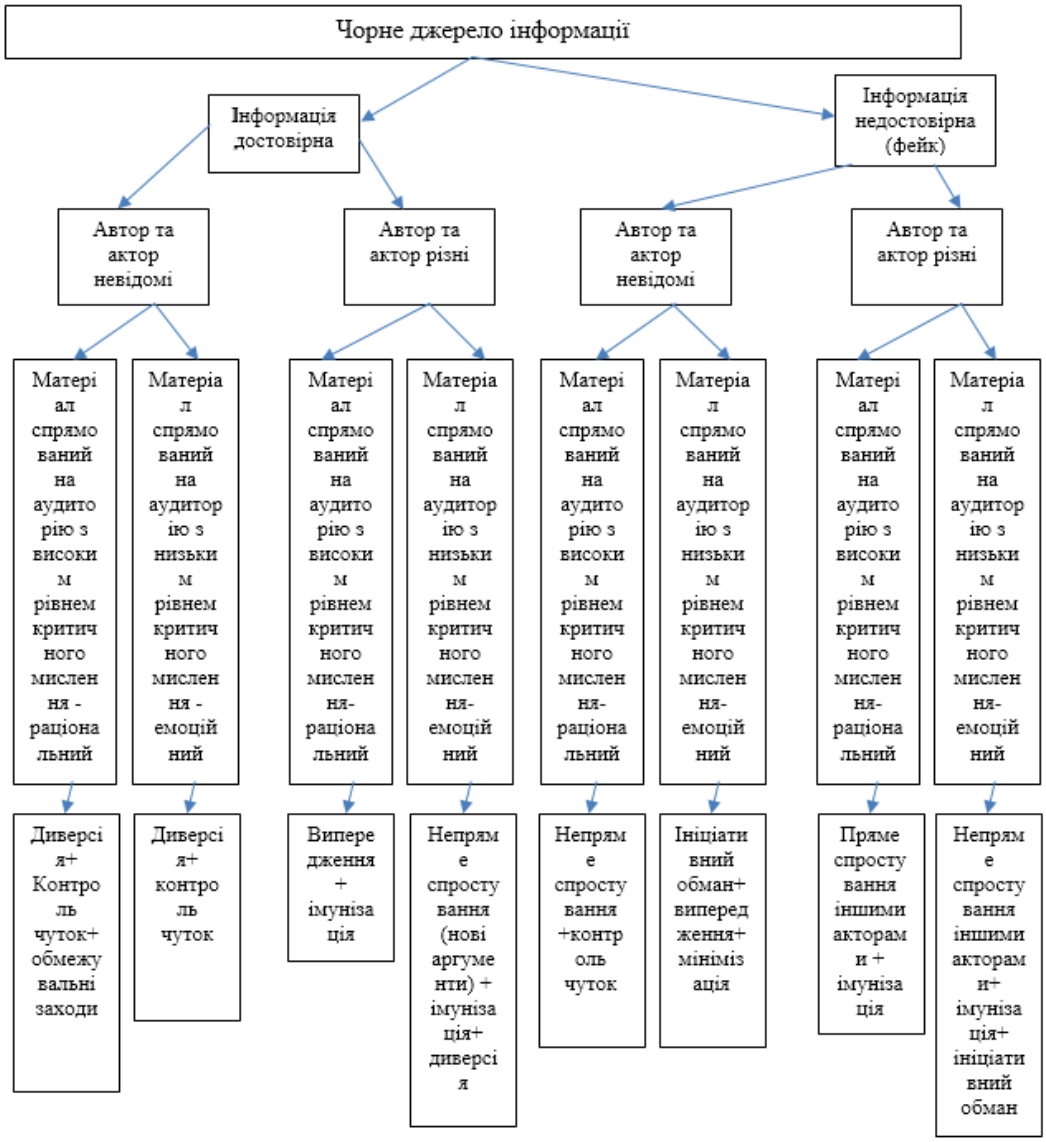
Таблиця 1


Біле джерело інформації
Інформація достовірна
Інформація недостовірна (фейк)
Автор та актор співпадають
Автор та актор різні
Автор та актор співпадають
Автор та актор різні
Матеріал спрямований на аудиторію з високим рівнем критичного мислення - раціональний
Матеріал спрямований на аудиторію з низьким рівнем критичного мислення - емоційний
Матеріал спрямований на аудиторію з високим рівнем критичного мислення- раціональний
Матеріал спрямований на аудиторію з низьким рівнем критичного мислення- емоційний
Матеріал спрямований на аудиторію з високим рівнем критичного мислення- раціональний
Матеріал спрямований на аудиторію з низьким рівнем критичного мислення- емоційний
Матеріал спрямований на аудиторію з високим рівнем критичного мислення- раціональний
Матеріал спрямований на аудиторію з низьким рівнем критичного мислення- емоційний
Мініміз ація або непрям е спросту вання (у варіанті нових аргуме нтів) із застосу ванням ресурсі в публічн ої диплом атії + випере д ження
Мініміз ація іншими акторам и+ контро ль чуток
Мініміз ація + імуніза ція у варіанті індоктр инації + випере д ження
Непрям е спросту вання (нові аргуме нти) + імуніза ція+ диверсі я
Пряме спросту вання автором + пряме спросту вання ресурса ми власних зв'язків з громадс ькістю
Пряме спросту вання автором +непря ме спросту вання іншими акторам и
Пряме спрост ування + імуніза ція +випер едженн
Непрям е спросту вання+ імуніза ція+ диверсі я

Таблиця 2


Сіре джерело інформації
Інформація достовірна
Інформація недостовірна (фейк)
Автор та актор співпадають
Автор та актор різні
Автор та актор співпадають
Автор та актор різні
Матеріал спрямований на аудиторію з високим рівнем критичного мислення - раціональний
Матеріал спрямований на аудиторію з низьким рівнем критичного мислення - емоційний
Матеріал спрямований на аудиторію з високим рівнем критичного мислення-раціональний
Матеріал спрямований на аудиторію з низьким рівнем критичного мислення-емоційний
Матеріал спрямований на аудиторію з високим рівнем критичного мислення-раціональний
Матеріал спрямований на аудиторію з низьким рівнем критичного мислення-емоційний
Матеріал спрямований на аудиторію з високим рівнем критичного мислення-раціональний
Матеріал спрямований на аудиторію з низьким рівнем критичного мислення-емоційний
Непряме спростування ресурсами власних зав'язків з громадськістю (шляхом висвітлення інших аспектів ситуації) +мінімізація іншими акторами
Мінімізація + диверсія+ контроль чуток +випередження
Непряме спростування+ Мінімізація + імуніза ція у варіанті індоктринації
Мінімізація+ диверсія
Пряме спростування автором (у разі відмови ресурсами власних зв'язків з громадськістю) + випередження
Пряме спростування автором +імунізація
Пряме спростування іншими акторами + імуніза ція+випередження
Непряме спростування+ імуніза ція+ диверсія

Таблиця 3


Чорне джерело інформації
Інформація достовірна
Інформація недостовірна (фейк)
Автор та актор невідомі
Автор та актор різні
Автор та актор невідомі
Автор та актор різні
Матеріал спрямований на аудиторію з високим рівнем критичного мислення - раціональний
Матеріал спрямований на аудиторію з низьким рівнем критичного мислення - емоційний
Матеріал спрямований на аудиторію з високим рівнем критичного мислення- раціональний
Матеріал спрямований на аудиторію з низьким рівнем критичного мислення- емоційний
Матеріал спрямований на аудиторію з високим рівнем критичного мислення- раціональний
Матеріал спрямований на аудиторію з низьким рівнем критичного мислення- емоційний
Матеріал спрямований на аудиторію з високим рівнем критичного мислення- раціональний
Матеріал спрямований на аудиторію з низьким рівнем критичного мислення- емоційний
Диверсія+ Контроль чуток+ обмежувальні заходи
Диверсія+ контроль чуток
Випередження + імуніза ція
Непряме спростування (нові аргументи) + імуніза ція+ диверсія
Непряме спростування +контроль чуток
Ініціативний обман+ випередження+ мініміз ація
Пряме спростування іншими акторами + імуніза ція
Непряме спростування іншими акторами+ імуніза ція+ ініціативний обман

Список використаних джерел

1. LOOQME. URL: https://www.looqme.io/about-us (дата звернення 02.08.2025).
2. Semantic Force. URL: https://semanticforce.ai/ua/company/about-us (дата звернення 02.08.2025).
3. Semantrum. URL: https://www.promo.semantrum.net/aboutus (дата звернення 02.08.2025).
4. Attack index. URL: https://attackindex.com/uk/golovna-attakindex/ (дата звернення 02.08.2025).
5. Ecosap. URL: https://ecosap.media/ (дата звернення 02.08.2025).
6. SoMo bot. URL: https://cityhost.ua/uk/blog/somo-bot-bot-dlya-sbora-i-analiza-informacii-iz-media.html (дата звернення 02.08.2025).
7. Ключове слово, результати пошуку Google. URL: https://www.google.com/search?q=%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%B2%D0%B5+%D1%81%D0%BB%D0%BE%D0%B2%D0%BE&sca_esv=2e740b31309555e0&sxsrf=AE3TifPRZULKkXMuaKDR2XXICtGCj3vLcQ:1754164336485&source=lnt&tbs=qdr:d&sa=X&ved=2ahUKEwjArJ2x8-yOAxX3BNsEHUojLgUQpwV6BAgDEAs&biw=1440&bih=683&dpr=2 (дата звернення 02.08.2025).
8. Google-об'єктив // URL: https://lens.google/intl/uk/ (дата звернення 02.08.2025).
9. 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 02.08.2025).
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: 02.08.2025).
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: 02.08.2025).
12. Про Стратегію інформаційної безпеки : Указ Президента України від 28.12.2021 року № 685/2021 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/685/2021/print (дата звернення: 02.08.2025).
13. Про Стратегію національної безпеки України : Указ президента України від 14.09.2020 р. № 392/220 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 02.08.2025).
14. Про стратегію кібербезпеки України: Указ президента України від 26.08.2021 р. № 447/2021 / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/447/2021/print (дата звернення: 02.08.2025).
15. 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/ВКП-10-0049.01-Доктрина-зі-стратегічних-комунікацій.pdf (дата звернення: 02.08.2025).
16. *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: 02.08.2025).*

References

1. LOOQME. Website. https://www.looqme.io/about-us [in Ukrainian].
2. Semantic Force. https://semanticforce.ai/ua/company/about-us [in Ukrainian].
3. Semantrum. https://www.promo.semantrum.net/aboutus [in Ukrainian].
4. Attack index. https://attackindex.com/uk/golovna-attakindex/ [in Ukrainian].
5. Ecosap. https://ecosap.media/ [in Ukrainian].
6. SoMo bot. https://cityhost.ua/uk/blog/somo-bot-bot-dlya-sbora-i-analiza-informacii-iz-media.html [in Ukrainian].
7. Kliuchove slovo, rezultaty poshuku Google. [Keyword, Google search results.]. https://www.google.com/search?q=%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%B2%D0%B5+%D1%81%D0%BB%D0%BE%D0%B2%D0%BE&sca_esv=2e740b31309555e0&sxsrf=AE3TifPRZULKkXMuaKDR2XXICtGCj3vLcQ:1754164336485&source=lnt&tbs=qdr:d&sa=X&ved=2ahUKEwjArJ2x8-yOAxX3BNsEHUojLgUQpwV6BAgDEAs&biw=1440&bih=683&dpr=2 [in Ukrainian].
8. Google Lens. https://lens.google/intl/uk/ [in Ukrainian].
9. NATO standard AJP-3.10.1(A) Allied Joint Doctrine for psychological operations. October 2007. URL: https://info.publicintelligence.net/NATO-PSYOPS.pdf [in English].
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 [in English].
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 [in English].
12. 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].
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 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].
15. 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: URL: https://sprotyvg7.com.ua/wp-content/uploads/2022/04/ВКП-10-0049.01-Доктрина-зі-стратегічних-комунікацій.pdf [in Ukrainian].
16. *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].

Kydriavskyi Ivan, *Doctoral student, Interregional Academy of Personnel Management*

ORCID: 0009-0009-5167-7648

Methodology for Using the Decision-Making Support Algorithm in the Application of State Administration Mechanisms in the Field of Information Security and Evaluation of Decisions made

In previous studies, an algorithm for supporting decision-making during the implementation of public administration mechanisms in the field of information space security has been developed, described, and tested on real-life examples from recent years. The results of the research demonstrate that the algorithm's recommendations, based on the relevant initial data, fully correlate with the decisions that were made in real situations by experienced professionals in the field of countering destructive information and psychological influence.

The conclusions state that, based on the results of the study, a methodology (instruction) has been formulated for applying the algorithm to support decision-making in the implementation of public administration in the field of information space security and the assessment of the effectiveness of decisions made. If implemented, this methodology (instructions) will enable specialists in the field of information space security, provided they have the relevant theoretical training, to gain practical experience in the shortest possible time (three to six months), learn how to apply it as effectively as possible, and acquire the practical ability to perform their official duties and tasks. In the absence of professional training, the methodology will not replace it, but it will allow for the formation of a general understanding of the processes taking place in the information space, the conscious performance of assigned tasks, and the generalization of practical experience, which will greatly facilitate future theoretical training at specialized educational institutions and reduce resources, including financial and time resources for such training.

In addition, the use of an algorithm for supporting management decisions in combination with a methodology for evaluating them will allow for the optimal allocation of available resources (financial, technical, software, human, time, and others), particularly in determining the feasibility of measures involving active information activities, the content and nature of their own information messages, as well as determining the most effective channels for disseminating information and the feasibility of adapting the format and content of their own information messages for channels where such messages have proven to be less effective.

In general, if implemented, the methodology is designed to improve the effectiveness of public administration mechanisms in the field of information space security without significant additional resource costs in conditions of resource scarcity characteristic of a defensive war, including its information component, against a significantly more numerous and better equipped enemy in all areas.

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