УДК 355.343.4
DOI: https://doi.org/10.32782/2786-8141/2026-14-7

Євлампієв А. С.
аспірант,
Національна академія Служби безпеки України
ORCID: https://orcid.org/0009-0001-6082-2220
Artem Yevlampiiev
National Academy of the Security Service of Ukraine

ПОРІВНЯЛЬНИЙ АНАЛІЗ МОДЕЛЕЙ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЯХ США, КНР, РФ ТА УКРАЇНИ

COMPARATIVE ANALYSIS OF MODELS FOR THE USE OF DIGITAL TECHNOLOGIES IN SPECIAL INFORMATION OPERATIONS: THE UNITED STATES, THE PEOPLE'S REPUBLIC OF CHINA, THE RUSSIAN FEDERATION, AND UKRAINE

Анотація. *У статті обґрунтовано, що цифровізація гібридних загроз переводить спеціальні інформаційні операції (СІО) з формату разових кампаній інформаційно-психологічного впливу у режим безперервного соціотехнічного управління, де ключовим об'єктом ураження стає когнітивний домен (воля, розуміння, мотивація та поведінка цільових аудиторій). Метою дослідження є порівняльний аналіз чотирьох національних моделей застосування цифрових технологій у СІО – інституціоналізовано-нормативної (США), централізовано-партійної (КНР), гібридно-деструктивної (РФ) та адаптивно-мережевої (Україна) та визначення напрямів інституційного розвитку української моделі з урахуванням потреби у вимірюванні когнітивних ефектів. Методологічну основу становить критеріально-матричний підхід у поєднанні зі структурно-функціональним і системним аналізом, що охоплює: інституційну архітектуру та тип управління; міжвідомчу координацію і процедури узгодження паралельних впливів (deconfliction); нормативні межі внутрішнього/зовнішнього впливу; технологічне ядро та доступ до даних; реалізацію циклу «дані → аналіз → план → вплив → оцінка → корекція»; підходи до оцінювання результативності й типові уразливості. Показано, що США формують технологічно зрілу, але нормативно обмежену модель із високою підзвітністю; КНР – модель централізованого когнітивного домінування на основі партійного контролю та військово-цивільного злиття; РФ – проксі-екосистему, орієнтовану на інструменталізацію хаосу, поляризації та ерозії довіри; Україна – модель резилієнтності, що поєднує державні контури з мережевими спільнотами та комерційними цифровими рішеннями. На основі порівняння обґрунтовано трисегментну архітектуру розвитку українських цифрових СІО (координаційний, аналітичний та мережевий виконавчий контури) і запропоновано стандарт оцінювання за схемою «ціль → показник → джерела даних → критерій успіху» з мінімальним пакетом метрик (довіра, поляризація/фрагментація, стійкість інтерпретацій, готовність до дії). Практична цінність результатів полягає у можливості використання запропонованої рамки для вдосконалення міжвідомчої координації, формування політик інформаційної безпеки та розробки етичних і правових запобіжників у цифровій сфері.*

Ключові слова: *спеціальні інформаційні операції (СІО), інформаційно-психологічний вплив (ІПВ), психологічні операції (PSYOP/MISO), генеративний штучний інтелект (GenAI), цифрові технології, когнітивний домен, гібридна війна.*

Abstract. *The article argues that the digitalization of hybrid threats transforms special information operations (SIO) from episodic psychological influence campaigns into continuous sociotechnical governance, where the primary target is the cognitive domain (will, understanding, motivation, and behaviour of target audiences). The study aims to compare four national models of digital technology use in SIO – an institutionalized-normative model (United States), a centralized-party model (People's Republic of China), a hybrid-destructive model (Russian Federation), and an adaptive-network model (Ukraine) - and to outline institutional development priorities for the Ukrainian model with a focus on measurable cognitive effects. The methodology combines a criteria-matrix framework with structural-functional and systems analysis. The comparison covers the institutional architecture and command logic; interagency coordination and deconfliction of parallel influences; normative constraints on domestic vs. foreign audiences; the technological core and data access; the management cycle "data → analysis → planning → influence → assessment → adjustment"; approaches to effectiveness evaluation; and key vulnerabilities. The findings show that the U.S. model provides a technologically mature but legally constrained system built around accountability and precision targeting; China's model emphasizes centralized cognitive dominance enabled by party oversight and military-civil fusion; Russia's model relies on a proxy ecosystem designed to weaponize uncertainty, polarization, and erosion of trust; and Ukraine's model is defined by resilience through rapid learning, integration of state capabilities with networked communities, and extensive use of commercial digital solutions. Based on the comparative results, the paper proposes a three-segment architecture for Ukraine's digital SIO (coordination, analytic, and networked execution layers) and introduces an assessment standard structured as "objective → indicator → data sources → success criterion", supported by a minimum metric set (trust, polarization/fragmentation, robustness of interpretations, and readiness to act). The results are practically relevant for refining interagency coordination, designing national information security policies, and embedding ethical and legal safeguards for digital influence activities.*

Keywords: *special information operations (SIO), information-psychological influence (IPI), Military Information Support Operations (PSYOP/MISO), generative artificial intelligence (GenAI), digital technologies, cognitive domain, hybrid war.*

Постановка проблеми. Цифрова трансформація систем національної безпеки зумовила якісну зміну характеру спеціальних інформаційних операцій (СІО): від епізодичних кампаній інформаційно-психологічного впливу вони еволюціонують у комплексні соціотехнічні практики, які поєднують організаційно-управлінські рішення спецслужб і військових структур із масштабним використанням big data, мережевого аналізу, штучного інтелекту та синтетичних медіа. У конфліктах нового типу інформаційно-комунікаційний простір перетворюється на середовище безперервного протиборства, де ключовим об'єктом ураження стає когнітивний домен – воля, розуміння, мотивація та поведінка цільових аудиторій [1]. Ця трансформація не є випадковою: вона відображає глобальний зсув до «когнітивної війни», де перемога досягається не стільки фізичним ураженням, скільки маніпуляцією сприйняттям реальності, що дозволяє досягати стратегічних цілей з мінімальними витратами ресурсів. Наприклад, використання генеративного ШІ для створення персоналізованих наративів може змінити громадську думку швидше, ніж традиційна пропаганда, як це спостерігалося в гібридних кампаніях останніх років.

У межах концепцій 4GW та гібридного протиборства інформаційні дії розглядаються як інструмент стратегічного переформатування культурних кодів, історичної свідомості й системи цінностей; у практичному вимірі це означає перехід від «повідомлення» до «середовища» та від медійного домінування – до алгоритмізованого управління довірою й інтерпретаціями. Водночас однакові цифрові інструменти (аналіз соцмереж, генеративний ШІ, deepfake, платформи планування) демонструють різну ефективність залежно від інституційної архітектури, правового режиму, міжвідомчої координації та стратегічної культури. Наприклад, в демократичних суспільствах, як США, правові бар'єри обмежують внутрішній вплив, тоді як в авторитарних режимах, як КНР, технології використовуються для тотального контролю. Саме тому порівняльний аналіз моделей використання цифрових технологій у СІО є не лише описовим завданням, а способом пояснити механізми результативності впливу на інформаційно-комунікаційний і когнітивний домени. Такий аналіз дозволяє виявити інваріанти (загальні закономірності) та детермінанти (визначальні фактори) ефективності, що має практичне значення для формування національних стратегій безпеки.

Аналіз останніх досліджень і публікацій. Існуючі праці з тематики цифрових технологій у СІО є значними за обсягом, але фрагментарними. Дослідники часто зосереджуються на окремих інструментах або описують національні практики без уніфікованих критеріїв порівняння. У доктринальному сегменті важливе місце займають матеріали НАТО, де Info Ops визначено як штабну функцію, що «аналізує, планує, інтегрує та оцінює інформаційні діяльності» для досягнення когнітивних ефектів, а принципи credibility & trust і unity of effort розглядаються як базові запобіжники від інформаційного «дружнього вогню» (information fratricide) [2].

Окремий пласт складають матеріали про дослідницько-інноваційні програми DARPA/IARPA, які інституціоналізують data-driven підхід до планування і оцінювання ефектів (ICEWS, Plan X, Math for Social Networks, Automatic Dossier, програми виявлення аномалій у соцмережах) [3; 4]. Свіжі стратегії, як IC OSINT Strategy 2024–2026, підкреслюють професійну трансформацію OSINT для протидії гібридним загрозам, зокрема інтеграцію ШІ для аналізу дезінформації в реальному часі [5].

Водночас у вітчизняному науковому дискурсі вже сформовано низку прикладних підходів до аналізу цифровізації СІО. Так, А. В. Слюсаренко розглядає еволюцію концептуальних та організаційно-технологічних поглядів на інформаційне протиборство у ЗС США (від кінця «холодної війни» до початку XXI ст.), що важливо для пояснення витоків data-driven підходів у сучасних доктринах [6]. Д. В. Вєдєнєєв узагальнює розвиток концептуальних настанов блоку НАТО в інформаційному протиборстві як елементі реагування на гібридні виклики та інституційну трансформацію механізмів впливу [7]. Практичний вимір координації та "єдності зусиль" у стратегічних комунікаціях безпекового сектору систематизовано у посібнику «Стратегічні комунікації для безпекових і державних інституцій», де запропоновано рамкові підходи до організації взаємодії, планування, реалізації та оцінювання комунікаційних заходів [8].

Таким чином, наявні дослідження створюють достатню базу для узагальнення, однак зберігається прогалина у вигляді відсутності цілісної порівняльної рамки моделей використання цифрових технологій у СІО, що одночасно враховує інституційну архітектуру, нормативні режими, технологічні ядра та механізми оцінювання ефектів. Заповнення цієї прогалини визначає дослідницьку логіку та структуру подальшого аналізу з інтеграцією свіжих даних для підвищення актуальності та практичної цінності.

Мета дослідження. На основі порівняльної інституційно-технологічної типології моделей США, КНР і РФ розробити та обґрунтувати напрями інституційного розвитку української моделі використання цифрових технологій під час проведення СІО, а також запропонувати структурований механізм координації та оцінювання ефектів цифрових СІО в когнітивному домені із збереженням мережевої гнучкості.

Методи дослідження. Для зіставлення чотирьох національних моделей застосування цифрових технологій у СІО використано критеріально-матричний підхід із уніфікованим набором критеріїв: тип управління та інституційна архітектура; механізми міжвідомчої координації; нормативний режим і межі впливу на внутрішню/зовнішню аудиторію; цільовий когнітивний ефект; технологічне ядро й доступ до даних; реалізація управлінського циклу «дані → аналіз → план → вплив → оцінка»; наявність процедур узгодження паралельних впливів (deconfliction); підходи до оцінювання результативності; уразливості та обмеження. Узагальнення виконано шляхом порівняння моделей США, КНР, РФ і України за зазначеними критеріями.

Виклад основного матеріалу. Американська модель СІО сформувалася як інституціоналізована система, інтегрована в планування операцій у логіці Multi-Domain Operations і підпорядкована принципам правової визначеності та цивільного контролю. Польові статути та керівні документи США (зокрема FM 3-0 *Operations*) закріпили уявлення про інформаційне середовище як багатовимірну систему, що вклю-

чає фізичний, віртуальний і когнітивний домени; при цьому когнітивний домен визначається як ключовий, оскільки саме він задає траєкторію прийняття рішень, підтримки або опору та готовності до дії [1]. Це розуміння підкреслює перехід від традиційного ураження до когнітивного впливу, де технології слугують для точного моделювання поведінки.

Уточнюючи генезу цієї моделі, доцільно враховувати висновок А. В. Слюсаренка про те, що становлення американських підходів до інформаційного протиборства відбувалося через поступове ускладнення організаційних контурів і методів, а також через технологізацію інструментів аналізу та впливу (що надалі стало підґрунтям для сучасних платформ моніторингу, прогнозування та таргетованого впливу) [6].

Інституційна архітектура характеризується розмежуванням ролей і високим рівнем міжвідомчої координації: інформаційні операції здійснюються у взаємодії між Збройними силами, розвідувальним співтовариством, дипломатичними структурами та органами стратегічних комунікацій [9–11]. Принцип *unity of effort* у документах НАТО та США визначається критичним для запобігання фрагментації інформаційного впливу та взаємному нівелюванню ефектів (*information fratricide*) [9–11]. Наприклад, координація між DARPA та Державним департаментом забезпечує синхронізацію технологій з дипломатією.

Нормативним обмежувачем виступає заборона операцій впливу на внутрішню аудиторію, яка формує зовнішню орієнтацію CIO й задає режим підзвітності. Саме в цій логіці цифрові технології розвиваються як інструменти точного таргетингу, вимірювання та прогнозування, а не як механізм тотального внутрішнього контролю. Технологічне ядро моделі становлять програми, що формують повний цикл управління CIO – від моніторингу до оцінювання ефектів [3; 4]. Система ICEWS (*Integrated Crisis Early Warning System*), запущена у 2010 році, орієнтована на моніторинг і виокремлення індикаторів наростання соціальної напруженості з використанням даних соцмереж і медіа. Програма *Anomaly Detection at Multiple Scales* (з 2010 р.) спрямована на виявлення аномальних соціальних процесів і нетипових поведінкових патернів у цифрових середовищах, що розширює можливості раннього попередження та контрвпливу [3].

У 2011 році DARPA запустила *Math for Social Networks*, метою якої є розробка нових математичних методів аналізу соціальних мереж із побудовою в реальному часі зв'язків, що відображають зміни у «реальному світі». Важливим є акцент на просторово-часовому аналізі, моделюванні поведінки та виявленні груп ризику, що на практиці підтримує як прогнозування криз, так і ідентифікацію ворожих мереж [4]. Програма *Plan X* (2012) концептуалізується як платформа, що дозволяє «розуміти, планувати і управляти інформаційною війною у режимі реального часу» в масштабних і динамічних мережевих інфраструктурах; суттєво, що в первинному описі проекту інформаційна війна включає як кібервплив (нанесення шкоди програмам і техніці), так і вплив на людей (маніпулювання), тобто розглядається як інтегрована операційна функція [4]. Нарешті, приклад *Automatic Dossier* (2012), створеної підрядником *Raytheon BBN Technologies*, демонструє автоматизацію побудови досьє на осіб і організації на основі відкритих джерел (соцмережі, форуми, чати, блоги), що узгоджується з переходом до профайлінгу й поведінкового таргетингу [4].

Свіжі стратегії, як *IC OSINT Strategy 2024–2026*, інтегрують AI для професійної трансформації OSINT, фокусуючись на протидії гібридним загрозам, включаючи дезінформацію в Україні [5]. У сукупності ці програми формують технологічний контур «дані – аналітика – моделювання – планування – оцінка ефектів», який робить американську модель взірцем технологічно досконалої, але нормативно обмеженої системи. Її ефективність у когнітивному домені полягає у здатності задавати керовані, вимірювані ефекти й зменшувати невизначеність через прогнозування, однак ця ж модель потенційно поступається у швидкості реалізації впливу тим системам, де відсутні обмеження щодо внутрішніх аудиторій. Слабкість – бюрократичні бар'єри, що уповільнюють адаптацію до швидких криз, як у випадку з війною в Україні [12].

Централізовано-партійна модель КНР відображає логіку політичного управління інформаційним середовищем як безперервним процесом, де межа між «внутрішнім» і «зовнішнім» впливом є рухомою, а пріоритетом виступає досягнення когнітивного домінування [13]. Витоки цієї моделі пов'язані з доктриною «трьох війн» (психологічної, війни громадської думки, правової), яка еволюціонувала в концепцію когнітивної війни та «інтелектуалізованої війни», де цифрові технології та ШІ виступають базовими інструментами формування бажаних інтерпретацій і поведінкових патернів [13]. На відміну від західних підходів, де акцент на обороні, китайська модель орієнтована на проактивний контроль, що дозволяє запобігати кризам на ранніх стадіях.

Організаційно модель характеризується централізацією управління під партійним контролем і посиленням спеціалізованих військових контурів, що інтегрують кібернетичні, електронні, космічні та психологічні компоненти. У матеріалах зазначається інституціоналізація відповідних структур, включно з розвитком Сил інформаційної підтримки як окремого виду спроможностей, а також роль структур на кшталт Третього управління Генштабу у контурах технічної розвідки та кібервпливу [13].

Ключовим механізмом масштабування виступає військово-цивільне злиття, що забезпечує перетік технологій і даних із цивільного сектору до безпекового. Це дозволяє державі використовувати ресурс приватних корпорацій для доступу до великих масивів даних, побудови алгоритмів та впровадження систем управління інформаційним середовищем. У порівняльному вимірі це створює інституційну перевагу в здатності до довготривалого когнітивного впливу, оскільки операції можуть спиратися на інтегровані державні інфраструктури спостереження, аналізу та контентної генерації. Звіти 2024 р. фіксують домінування КНР у emerging technologies, як-от AI, що посилює конкуренцію з США [14].

Технологічне ядро китайської моделі описується як поєднання генеративного ШІ, big data та синтетичних медіа, що забезпечує автоматизацію персоналізованого впливу та управління довірою через конвеєрний випуск контенту і таргетовану доставку наративів. Окремі дослідження відзначають також розвиток нейротех-

нологічних напрямів і експериментальних контурів, які розширюють рамки когнітивного впливу від комунікаційних практик до технологічно опосередкованих інтерфейсів взаємодії. У підсумку ефективність цієї моделі оцінюється передусім через керованість інформаційного середовища як стратегічну метрику: контроль інформаційного поля і стабільність бажаних інтерпретацій розглядаються як індикатори досягнення когнітивного домінування [11; 13].

Водночас централізовано-партійна модель має структурну вразливість: висока залежність від централізованих механізмів управління й контролю створює ризики зниження адаптивності в ситуаціях, де інформаційне середовище стає надто динамічним або де потрібні децентралізовані інноваційні рішення. Наприклад, у гібридних конфліктах, як в Україні, така модель може стикатися з опором від децентралізованих мереж [12]. Проте в умовах довгострокових стратегічних протистоянь саме ця модель демонструє високу спроможність до масштабування впливу на інформаційно-комунікаційний і когнітивний домени.

Гібридно-деструктивна модель РФ походить від радянських «активних заходів» і адаптована до умов цифрової гібридної війни. Її концептуальною основою виступає рефлексивне управління, що передбачає маніпулювання інформаційним середовищем для схилення супротивника до прийняття рішень, вигідних агресору, через підміну інтерпретацій, створення викривлених «картин реальності» та розмивання межі між фактом і симулякром [15]. Цей підхід відрізняється від інших моделей фокусом на деструкції, а не на будівництві, що робить його ефективним для короткострокових тактичних перемог, але ризикованим для довгострокової стабільності.

Інституційно модель демонструє комбінацію формальної централізації та фактичної мережевої реалізації через проксі-акторів. У матеріалах зазначається, що паралельно з офіційними контурами інформаційних військ та спецслужб суттєву роль відіграють напівдержавні й напівкримінальні кіберугруповання, які забезпечують масштабування атак, підвищують заперечуваність участі та дозволяють застосовувати інструменти, що не проходять через формальні правові обмеження. Така архітектура підвищує тактичну гнучкість, але знижує керованість результатів і довгострокову стабільність операційних ефектів [11; 15].

Технологічно російська модель спирається на масове використання бот-мереж і «тролівських фабрик» для імітації громадської думки, мобілізації штучної підтримки та підсилення поляризації; синтетичні медіа (у т. ч. *deepfake*) використовуються як інструмент дискредитації і делегітимації; кібератаки на критичну інфраструктуру комбінуються з інформаційними кампаніями для посилення соціальної тривожності, недовіри і відчуття керованого хаосу. Наприклад, інструмент *Meliorator* на базі AI створює тисячі фейкових акаунтів для поширення дезінформації про Україну та США [16]. Важливо, що ефективність у цій моделі досягається не шляхом стабільного «керування думкою», а через руйнування когнітивної здатності суспільства до раціонального осмислення подій і довгострокового планування; саме тому показниками результативності виступають поляризація, фрагментація довіри та зниження легітимності інститутів [11].

Нормативна база РФ у сфері інформаційної безпеки фіксує пріоритет протидії зовнішнім інформаційним впливам, однак практична реалізація гібридно-деструктивної моделі часто передбачає агресивний наступальний контур, у тому числі з використанням проксі-інструментів і транснаціональних платформ.

Адаптивно-мережева модель України сформувалася як відповідь на реальну гібридну агресію РФ і розвивається у межах концепції всеохоплюючої оборони, що інституційно закріплюється стратегіями інформаційної безпеки, воєнної безпеки, кібербезпеки та пов'язаними програмними документами [17–20]. Її відмінність полягає в поєднанні державного управління та мережевої взаємодії, де значна частина цифрових спроможностей реалізується на стику офіційних структур і громадянського суспільства. Ця модель є унікальною, оскільки виникла не як результат довгострокового планування, а як органічна відповідь на кризу, що поєднує державну вертикаль з горизонтальними мережами волонтерів.

Організаційно модель можна описати як двоконтурну: з одного боку діють спеціалізовані державні та військові інституції, що відповідають за інформаційно-психологічні операції, контррозвідувальні СІО, контрдезінформацію та кібероперації; з іншого – існує мережа волонтерських кібер- та OSINT-спільнот, які взаємодіють із державними структурами, зберігаючи автономію, і тим самим формують емерджентну екосистему, де ініціатива часто йде «знизу», а держава виступає координатором і легітиматором [17–20].

Технологічно українська модель спирається на масову OSINT-розвідку (соцмережі, супутникові знімки, відкриті бази даних), автоматизовані інструменти аналізу фото/відео та каналізоване збирання інформації через цифрові інструменти на кшталт «eVorog» та інших ботів. Важливим елементом є цифрові системи управління боєм, що інтегрують розвідані, цілевказівку та вогневе ураження (зокрема «Кропива», GIS Arta, «Дельта» та інші платформи), а також масове використання комерційних технологій зв'язку на кшталт Starlink для забезпечення стійкості комунікацій [17–20].

Аналітика даних та ШІ використовуються для виявлення аномалій, класифікації цілей, аналізу інформаційних кампаній противника й підвищення точності реагування; при цьому можливе поєднання західних рішень (типу Palantir) і власних розробок [17–20]. Роль big tech компаній, як описано в звітах 2025 р., забезпечує незамінну підтримку для цифрової фронтової лінії, дозволяючи інтегрувати дані в реальному часі [12]. У результаті Україна реалізує функціональний аналог багатодоменного підходу: інформаційно-психологічні дії синхронізуються з кіберопераціями, маневром військ і точковими ударами, що підсилює операційний ефект і формує стійкий контур резилієнтності.

Ефективність адаптивно-мережевої моделі визначається не тотальним контролем і не хаотизацією, а швидкістю навчання системи, довірою й здатністю відновлювати когнітивну стійкість під постійним тиском. Водночас саме мережева природа моделі створює виклики для стандартизації процедур та довгострокового інституційного закріплення результатів, що потребує розвитку механізмів координації та оцінювання ефектів без втрати гнучкості, з опорою на напра-

цьовані в Україні практичні підходи до стратегічних комунікацій у секторі безпеки [11]. Слабкість – фрагментація зусиль, яка може призводити до дублювання або пробілів у покритті [12].

На основі порівняльного аналізу інституційно-технологічних моделей США, КНР і РФ для України доцільно зафіксувати власну конфігурацію адаптивно-мережевої моделі як керовану мережеву спроможність із обов'язковою оцінкою когнітивного ефекту та механізмом узгодження дій.

Так, з американської інституціоналізовано-нормативної моделі запозичуються три прикладні принципи: єдність зусиль (unity of effort), узгодження впливів (deconfliction) та повний цикл управління «дані → план → виконання → оцінка → корекція», у якому оцінювання є не додатком, а завершальною фазою. З китайської централізовано-партійної моделі береться лише функціональний елемент масштабування технологій і даних через інституційно оформлені зв'язки з цивільним сектором, але в українській версії – у форматі правових і процедурних партнерств без авторитарного контролю. Із російської гібридно-деструктивної моделі не запозичуються практики впливу; натомість її логіка використовується як основа для контуру раннього попередження й атрибуції, спрямованого на виявлення проксі-активності, бот-мереж, синтетичних вкидів і атак на довіру та поляризацію.

Інституційно запропонована нами модель зводиться до трьох функціональних сегментів: координаційного (пріоритезація та узгодження дій), аналітичного (моніторинг, виявлення аномалій, базові виміри до втручання) і виконавчого мережевого (державні, військові та громадянські актори, які реалізують заходи децентралізовано). Центр не монополізує контент і канали, а забезпечує узгодженість і відтворюваність циклу.

Ключовою умовою результативності стає механізм оцінювання когнітивних ефектів, побудований як стандарт «ціль → показник → джерела даних → критерій успіху». Мінімальний пакет метрик охоплює: довіру (до інституцій і джерел), поляризацію/фрагментацію, стійкість інтерпретацій до маніпуляцій та готовність до дії у логіці оборони; оцінювання здійснюється через тріангуляцію (соціомедійна аналітика, OSINT-сигнали, за можливості – опитувальні/панельні дані). У підсумку Україна отримує не централізований апарат, а керовану мережеву систему, що поєднує швидкість і ініціативність мережі з узгодженістю та вимірюваним когнітивним результатом.

Висновки. У проведеному дослідженні встановлено, що цифрова еволюція спеціальних інформаційних операцій переводить їх у режим безперервного соціотехнічного протиборства, де ключовим об'єктом впливу стає когнітивний домен, а результативність визначається не стільки набором інструментів (big data, мережевий аналіз, ШІ, синтетичні медіа), скільки інституційною архітектурою, нормативним режимом і здатністю системи забезпечувати узгодженість та вимірюваність ефектів. Порівняльний аналіз моделей США, КНР і РФ показав інваріантність управлінського циклу «дані → аналіз → план → вплив → оцінка», але різну його реалізацію. На цій основі обґрунтовано напрям інституційного розвитку України як керованої мережевої спроможності. Її сутність полягає у збереженні децентралізованого виконання завдань державними, військовими та громадянськими акторами. Однак ця система доповнюється спеціальним механізмом узгодження паралельних впливів (deconfliction) для уникнення суперечливих сигналів шляхом розведення дій за аудиторіями, меседжами, каналами та часом. Обов'язковим елементом також є оцінювання когнітивного ефекту.

Для реалізації цього підходу запропоновано трисегментну архітектуру, що включає координаційний, аналітичний та мережевий виконавчі контури. Також запроваджується стандарт оцінювання за схемою «ціль → показник → джерела даних → критерій успіху». Його основу становить мінімальний пакет метрик: довіра, поляризація/фрагментація, стійкість інтерпретацій та готовність до дії.

Цей комплекс дає змогу перевести українську модель із режиму ситуативної синхронізації в режим відтворюваної інституційної спроможності. Перспективи подальшої роботи пов'язані з операціоналізацією та валідацією цих метрик на емпіричних кейсах, удосконаленням процедур раннього попередження й атрибуції, а також нормативним оформленням партнерств із цивільним технологічним сектором. Останнє необхідне для масштабування аналітики без втрати легітимності й мережевої гнучкості.

References:

1. U.S. Department of the Army. (2022). *FM 3-0 Operations.* Washington, DC: Department of the Army.

2. NATO. (2015). *Allied Joint Doctrine for Information Operations (AJP-3.10)*. Brussels: NATO Standardization Office.

3. O'Brien, S. P. (2010). Crisis early warning and decision support: Contemporary approaches and thoughts on future research. *International Studies Review*, Vol. 12, no. 1, pp. 87–104.

4. Nakashima, E. (2012, May 30). With Plan X, Pentagon seeks to spread U.S. military might to cyberspace. *The Washington Post.*

5. Office of the Director of National Intelligence. (2024). *The IC OSINT Strategy 2024–2026.* Washington, DC: ODNI.

6. Sliusarenko, A. V. (2024). Informatsiinyi front: vytoky i suchasnist [Information front: origins and modernity]. *Voienno-istorychnyi visnyk*, no. 5 (52), pp. 79–90. DOI: 10.33099/2707-1383-2024-52-5-79-90. Available at: https://viv.nuou.org.ua/article/download/307162/298553/709370 (accessed February 4, 2026).

7. Viedienieiev, D. V. (2024). Rozvytok kontseptualnykh nastanov bloku NATO v informatsiinomu protiborstvi [Development of NATO conceptual guidelines in information confrontation]. In *Svit i Ukraina u hlobalnomu bezpekovomu prostori: materialy naukovo-praktychnoi konferentsii* (Kyiv, 25 kvitnia 2024 r.) (pp. 71–77). Kyiv: NUOU.

8. Kompantseva, L. F., Davlikanova, O. A., Cherevatyi, T. K., & Akulshyn, O. S. (2022). *Stratehichni komunikatsii dlia bezpekovykh i derzhavnykh instytutsii: praktychnyi posibnyk* [Strategic communications for security and government institutions: A practical guide]. Zaporizhzhia: ZNU.

9. NATO. (2017). *Comprehensive Approach to Strategic Communications*. Brussels: NATO.

10. NATO. (2019). *NATO Military Policy for Information Operations (MC 0422/6).* Brussels: NATO.

11. NATO StratCom Centre of Excellence. (2019). *Measuring the Effectiveness of Strategic Communications*. Riga: NATO StratCom COE.

12. Schroeder, E. (2025). *Building the Digital Front Line: Understanding Big Tech Decision-Making in the Ukraine War.* Washington, DC: Atlantic Council.

13. Beauchamp-Mustafaga, N. (2023). *Cognitive Warfare and China's Concept of Intelligentized Warfare.* Santa Monica, CA: RAND Corporation.

14. U.S.-China Economic and Security Review Commission. (2024). *U.S.–China Competition in Emerging Technologies* (Chapter 3). Washington, DC: U.S.-China Economic and Security Review Commission.

15. Paul, C., & Matthews, M. (2016). *The Russian "Firehose of Falsehood" Propaganda Model.* Santa Monica, CA: RAND Corporation.

16. Federal Bureau of Investigation. (2024). *State-Sponsored Russian Media Leverages Meliorator Software for Foreign Malign Influence Activity: Joint Cybersecurity Advisory*. Washington, DC: Federal Bureau of Investigation.

17. Ukraina. (2021, March 25). Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Pro Stratehiiu voiennoi bezpeky Ukrainy" No. 121/2021 [Decision of the National Security and Defense Council of Ukraine "On the Military Security Strategy of Ukraine" No. 121/2021]. *Ofitsiinyi visnyk Ukrainy*, no. 28, Art. 1132. Available at: https://zakon.rada.gov.ua/go/121/2021 (accessed February 4, 2026).

18. Ukraina. (2021, October 15). Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Pro Stratehiiu informatsiinoi bezpeky Ukrainy" No. 685/2021 [Decision of the National Security and Defense Council of Ukraine "On the Information Security Strategy of Ukraine" No. 685/2021]. *Ofitsiinyi visnyk Ukrainy*, no. 82, Art. 3284. Available at: https://zakon.rada.gov.ua/go/685/2021 (accessed February 4, 2026).

19. Ukraina. (2021, May 14). Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Pro Stratehiiu kiberbezpeky Ukrainy" No. 447/2021 [Decision of the National Security and Defense Council of Ukraine "On the Cybersecurity Strategy of Ukraine" No. 447/2021]. *Ofitsiinyi visnyk Ukrainy*, no. 45, Art. 1789. Available at: https://zakon.rada.gov.ua/go/447/2021 (accessed February 4, 2026).

20. Ukraina. (2021, August 20). Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Pro Stratehichnyi oboronnyi biuleten Ukrainy" No. 473/2021 [Decision of the National Security and Defense Council of Ukraine "On the Strategic Defense Bulletin of Ukraine" No. 473/2021]. *Ofitsiinyi visnyk Ukrainy*, no. 68, Art. 2698. Available at: https://zakon.rada.gov.ua/go/473/2021 (accessed February 4, 2026).

Стаття отримана: 05.02.2026
Стаття прийнята: 02.03.2026
Стаття опублікована: 09.04.2026