

ЖУРНАЛІСТИКА



Стаття та будь-який пов'язаний з нею опублікований матеріал поширюється за ліцензією Creative Commons Attribution License (CC BY 4.0).
The article and any related published material are licensed under the Creative Commons Attribution License (CC BY 4.0).

УДК 355.432.1(477-651.2:470.323):316.716.23+004.056"2024"

DOI: <https://doi.org/10.17721/1728-2217.2026.67.100-107>

Наталія РОЖНЯТІВСЬКА, ад'юнкнт

ORCID ID: 0009-0005-8613-779X

e-mail: rozhnativska.natali@knu.ua

Київський національний університет імені Тараса Шевченка, Київ, Україна

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ПЕРЕДУМОВА СТРАТЕГІЧНОГО УСПІХУ ВІЙСЬКОВИХ ОПЕРАЦІЙ: ДОСВІД КУРСЬКОЇ ОПЕРАЦІЇ

Вступ. Стаття присвячена аналізу ролі інформаційної безпеки як стратегічного інструменту планування та реалізації військових операцій на прикладі Курської операції Збройних Сил України (серпень – грудень 2024 року). Обґрунтовано актуальність балансування між запитом суспільства на правду й вимогами інформаційної безпеки в умовах гібридної війни. Метою дослідження є аналіз механізмів забезпечення інформаційної безпеки й реалізації комунікаційних стратегій під час підготовки та проведення бойових дій на прикладі Курської операції.

Методи. Застосовано три взаємодоповнювальні методи: нормативно-документальний аналіз п'яти ключових правових актів і стандартів НАТО; контент-аналіз медіаматеріалів за серпень – грудень 2024 року (загалом проаналізовано понад 40 медіаматеріалів і понад 15 аналітичних звітів та експертних публікацій з офіційних повідомлень ЗСУ, українських і міжнародних медіа та російських пропагандистських джерел); порівняльний метод для зіставлення реального перебігу бойових дій із їх медійним висвітленням у трьох сегментах інформаційного простору.

Результати. Проаналізовано чотири взаємопов'язані виміри проблеми: нормативно-правову базу (включно зі стандартами НАТО); структуру медіасередовища з трьома цільовими аудиторіями; підготовчий етап у режимі інформаційної тиші та протидію загрозам OSINT-розвідки; результати інформаційної кампанії після офіційного визнання операції. Установлено, що режим інформаційної тиші забезпечив не лише тактичний успіх, а й перетворення локальної військової перемоги на вагомий зовнішньополітичний результат для України. Виявлено, що стратегія медійної ізоляції позбавила російську сторону інформаційної ініціативи та контролю над поясненням подій, а Україні забезпечила монополію на перше офіційне повідомлення і контроль над глобальним наративом. Для міжнародних партнерів операція стала підставою переглянути сприйняття України як держави, спроможної самостійно планувати складні наступальні операції.

Висновки. Інформаційна безпека в умовах сучасної війни трансформувалася в самостійний вид стратегічного озброєння. Стратегічне управління інформацією є невід'ємною частиною військової операції, у якій інформаційна тиша стає зброєю та підставою для глобального визнання результату, досягнутого завдяки інтеграції правових, організаційних і комунікаційних інструментів.

Ключові слова: інформаційна безпека, Курська операція, стратегічні комунікації, інформаційна тиша, OSINT, медіапростір, інформаційна війна, стратегічна раптовість.

Вступ

У сучасній високотехнологічній війні інформація про успіх на фронті є не лише засобом інформування суспільства, а й критичним ресурсом зміцнення національної стійкості й утвердження міжнародної суб'єктності держави. Водночас оперативне висвітлення подій бойових дій постійно ставить владу перед дилемою між запитом суспільства на правду та вимогами інформаційної безпеки: надмірна публічність здатна розкрити задум операції, поставити під загрозу життя військових і нівелювати результати ще до її завершення.

Наукова значущість обраної проблематики визначається об'єктивною потребою суспільства у систематичному отриманні відомостей про перебіг подій на лінії зіткнення. Повідомлення про успіхи формують почуття гордості за військо й усвідомлення причетності до спільної справи, а інформація про невдачі мобілізує суспільство й водночас сигналізує про загрози персональній безпеці, особливо для мешканців прифронтових територій. Натомість успішне проведення військових операцій безпосередньо залежить від дотримання режиму інформаційної тиші: чим пізніше противник дізнається про напрямок просування, чисельність сил і масштаб успіху, тим більше можливостей закріпитися

на захопленій території з мінімальними втратами. Для України, яка з 2014 року протидіє збройній агресії Російської Федерації, забезпечення такого балансу є особливо актуальним.

Метою статті є аналіз механізмів забезпечення інформаційної безпеки й реалізації комунікаційних стратегій під час підготовки та проведення бойових дій на прикладі Курської операції.

Огляд літератури. Теоретичну основу дослідження становлять праці в кількох взаємопов'язаних напрямках: нормативно-правове регулювання інформаційної безпеки, стратегічні комунікації в умовах збройного конфлікту, OSINT як інструмент сучасної розвідки та інформаційне протистояння в цифровому середовищі.

У сфері інформаційної безпеки та стратегічних комунікацій фундаментальне значення має монографія дослідниці А. Башук (2019), у якій систематизовано комунікаційні стратегії державної влади в умовах інформаційного суспільства й обґрунтовано поняття комунікаційної стратегії як довгострокового системного плану дій, орієнтованого на оптимальне використання комунікаційних ресурсів. Це визначення є базовим для аналізу режиму інформаційної тиші як активної, а не пасивної стратегії. В. Ліпкан (2022) розробив концепцію

© Рожнятівська Наталія, 2026

інформаційної безпеки України в контексті сучасних геополітичних реалій, сформулювавши ключову тезу про те, що в умовах війни інформаційна безпека – це не закритість, а хірургічна точність у дозуванні правди. Дослідниця О. Ільницька (2017) дослідила механізми протидії деструктивному контенту й обґрунтувала необхідність системного захисту національного інформаційного простору від загроз, здатних підірвати державні інтереси.

Питання стратегічних комунікацій у гібридній війні розробляє Г. Почепцов (2024), який аналізує роль інформаційних пауз у формуванні суспільного сприйняття і доводить, що вакуум в інформаційному просторі створює напругу, яку надалі заповнює той, хто першим надає структуровану інтерпретацію подій. О. Курбан (2023) досліджує специфіку інформаційних воєн у цифровому середовищі, наголошуючи на тому, що ефективна протидія інформаційним загрозам вимагає від Збройних Сил глибокого розуміння інтерактивного характеру комунікації із цільовими аудиторіями.

Окремий масив літератури присвячений OSINT як інструменту сучасної збройної боротьби. Дослідники American Security Project (2024) документують, як російсько-українська війна перетворила OSINT на повноцінний інструмент військової розвідки, що чинить вплив на оперативнотактичному й геополітичному рівнях. С. Коултарт (2026) з Університету Олбані ставить під сумнів тезу про безперешкодну ефективність OSINT, стверджуючи, що учасники сучасних збройних конфліктів поступово виробляють дієві методи протидії відкритому моніторингу – спостереження, яке безпосередньо підтверджується досвідом Курської операції. Матеріали аналітичної платформи Babel Street (2024) фіксують парадоксальну закономірність: відкритість цифрового середовища стає загрозою передусім для тієї сторони, яка втрачає контроль над власними комунікаційними каналами.

Результати Курської операції в інформаційному вимірі аналізують експерти RAND Corporation (2024), які оцінили медіаефект від неї як надзвичайно потужний і порівнянний з ефектом вибуху. Аналітики Atlantic Council (2024) досліджують стратегічний вимір операційної секретності, роблячи висновок, що рішення не інформувати союзників було свідомим і стало демонстрацією здатності України до самостійного стратегічного планування. Дослідження у галузі міжнародної безпеки (European Journal of International Security, 2024) підтверджують, що розширення можливостей аналітики відкритих даних суттєво трансформує логіку сучасних збройних протистоянь, а The Washington Quarterly (2025) фіксує формування цілеспрямованої протидії практикам відкритого моніторингу з боку учасників конфліктів.

Незважаючи на значний обсяг напрацювань у суміжних напрямках, комплексного дослідження, яке б інтегрувало нормативно-правовий, медіасередовищний та OSINT-вимір інформаційної безпеки на прикладі конкретної наступальної операції ЗСУ, у вітчизняній науковій літературі досі не представлено. Це й визначає наукову новизну та практичну значущість пропонованого дослідження.

Методи

Дослідження ґрунтується на комплексному підході, що поєднує три взаємодоповнювальні методи.

Перший – нормативно-документальний аналіз. Опрацьовано чинну нормативно-правову базу України у сфері інформаційної безпеки та стратегічних комунікацій: Доктрину "Військові зв'язки з громадськістю" (2026), Доктрину зі стратегічних комунікацій Сил оборони України (2020), наказ Головнокомандувача ЗСУ № 73 (2022), Проєкт Концепції інформаційної безпеки України

(ОБСЕ), а також стандарт НАТО AJP-3.10 (Allied Joint Doctrine for Strategic Communications, 2023). Додатково проаналізовано фундаментальні наукові праці вітчизняних і зарубіжних дослідників у галузі інформаційної безпеки, стратегічних комунікацій та OSINT.

Другий – контент-аналіз медіаматеріалів за період серпень – грудень 2024 року. Емпіричну базу становлять: офіційні повідомлення Генерального штабу ЗСУ, Президента й Головнокомандувача ЗСУ; матеріали провідних українських медіа (Суспільне, TSN, Espresso.TV, "Є питання"); публікації російських пропагандистських ресурсів і Z-блогерів, задокументовані виданням "Детектор медіа"; матеріали міжнародних медіа (Reuters, CNN, The Washington Post, The Economist); аналітичні звіти провідних think-tank (RAND Corporation, Atlantic Council) та експертні публікації. Одиницями аналізу слугували тематичні повідомлення, наративи та їх хронологічна динаміка у трьох сегментах інформаційного простору – українському, російському й міжнародному.

Процедуру контент-аналізу формалізовано за такими параметрами. Критеріями відбору матеріалів слугували: тематична релевантність Курської операції; належність джерела до одного з трьох сегментів інформаційного простору; наявність датування, що уможливило відтворення хронологічної динаміки. Систему категорій кодування становили п'ять аналітичних рубрик: 1) тип джерела (офіційне, медійне, пропагандистське, експертно-аналітичне); 2) сегмент аудиторії (українська, російська, міжнародна); 3) домінуючий наратив; 4) фаза інформаційної кампанії (інформаційний вакуум, офіційне визнання); 5) тональність повідомлення. Одиницею кодування було окреме тематичне повідомлення (допис, сюжет, публікація). Інтерпретація даних здійснювалася шляхом зіставлення частотності та хронологічної динаміки наративів у межах кожної категорії.

Третій – порівняльний метод. Застосовано для зіставлення реального перебігу бойових дій (за даними відкритих джерел) із темпами та змістом їх медійного висвітлення в кожному з трьох сегментів. Це дало змогу виявити розриви між подією та її публічним відображенням, оцінити ефективність режиму інформаційної тиші та встановити момент і механізм комунікаційного перелому після офіційного визнання операції.

Результати

Першим методологічним кроком у дослідженні є реконструкція нормативно-правового поля, у якому реалізовувалася Курська операція, що розпочалася 6 серпня 2024 року. Поєднання суворого режиму секретності з дотриманням норм міжнародного права створило правові передумови для досягнення ефекту стратегічної раптовості. Аналіз нормативної бази дає змогу визначити, які саме принципи інформаційно-комунікаційної діяльності Збройних Сил України були покладені в основу операції.

Чинна нормативно-правова база зазнала суттєвих трансформацій, адаптуючись до викликів повномасштабного вторгнення. Згідно з Доктриною "Військові зв'язки з громадськістю" інформаційна безпека визначається як стан захищеності інформації, розголошення якої може призвести до обізнаності противника про дії Збройних Сил України й негативно вплинути на виконання завдань за призначенням (Генеральний штаб Збройних Сил України, 2026). У Проєкті Концепції інформаційної безпеки України, розробленому за участю експертів ОБСЕ, поняття трактується ширше – як стан гарантованого захисту життєво важливих інтересів особи, громадянського суспільства й державних інсти-

туцій від загроз у процесі обміну, зберігання, оброблення та поширення інформації (Проект Концепції інформаційної безпеки України, б. д.). У контексті Курської операції цей захист набуває подвійного значення: з одного боку, держава зобов'язана забезпечити конституційне право громадян на достовірну інформацію про хід війни, з іншого – гарантувати безпеку військових підрозділів через обмеження передчасного розголошення оперативної чутливих даних.

Базовим документом, який заклав фундамент взаємодії військових і цивільних медіаструктур, є Доктрина зі стратегічних комунікацій Сил оборони України (2020). Документ визначає стратегічні комунікації як скоординоване й належне використання комунікативних можливостей держави для просування її цілей і цінностей (Доктрина зі стратегічних комунікацій..., 2020). У ньому прямо зазначено, що ефективність операції прямо пропорційна здатності командування мінімізувати неконтрольовані потоки інформації на тактичному рівні (Доктрина зі стратегічних комунікацій..., 2020, с. 14). У науковій літературі комунікаційна стратегія плується як довгостроковий, системний план дій, спрямований на досягнення конкретних цілей завдяки оптимальному використанню комунікаційних ресурсів та інструментів (Башук, 2019). Саме в такому розумінні режим інформаційної тиші є не пасивним мовчанням, а активною комунікаційною стратегією, що передбачає чітке планування моменту, форми та змісту майбутнього публічного повідомлення.

Не менш важливою є імплементація стандартів НАТО, передусім Спільної доктрини сил Альянсу зі стратегічних комунікацій (AJP-3.10) (Спільна доктрина..., 2023). Цей документ запроваджує ключове для нашого дослідження поняття безпеки операцій (Operations Security, OPSEC) – аналітичного процесу, що передбачає ідентифікацію критичної інформації, оцінку можливості її виявлення розвідкою противника та розроблення заходів із приховування чи захисту цієї інформації заради збереження раптовості й досягнення успіху операції. Окремого значення набули внутрішні документи оперативного рівня, зокрема наказ Головнокомандувача ЗСУ № 73, що регламентує порядок взаємодії Збройних Сил зі ЗМІ в умовах воєнного стану (Головнокомандувач ЗСУ, 2022). Запровадження жорстких обмежень на роботу журналістів у "червоних зонах", заборона на використання особовим складом засобів стільникового зв'язку й оприлюднення геолокаційних даних створили правові передумови для досягнення стратегічної раптовості.

Окреслене вище нормативне поле реалізовувалося в конкретному медіасередовищі, особливості якого безпосередньо визначали можливості й обмеження інформаційної кампанії. Будь-яка військова операція сьогодні розгортається у комунікаційному просторі, що характеризується миттєвим поширенням контенту, мультимедійністю і глобальною доступністю. Як зазначає О. Курбан, протистояння в цифровому середовищі вимагає від Збройних Сил не лише володіння зброєю, а й глибокого розуміння інтерактивного характеру комунікації із цільовими аудиторіями (Курбан, 2023, с. 212).

Особливістю інформаційного простору навколо Курської операції стала його єдність: повідомлення українських, російських і міжнародних медіа поширювалися в одному цифровому полі, у якому одночасно перебувають принципово різні аудиторії з різними потребами та інтерпретаційними рамками. Споживачі інформації є сегментованими, і для ефективної комуніка-

ційної стратегії важливо враховувати специфіку кожного сегмента окремо.

Українська (внутрішня) аудиторія розглядається передусім як цільова група, для якої метою комунікації є підтримка морального духу, утвердження відчуття історичної справедливості та підтвердження бойових спроможностей Збройних Сил. Для військовослужбовців та їхніх родин до цього додається потреба у фаховій та особистій інформації – про побратимів, долю рідних, перебіг бойових завдань. Саме ця аудиторія найбільше реагує на офіційні комунікації Президента та Головнокомандувача.

Міжнародна аудиторія (західні партнери та світова спільнота) є ключовою для досягнення стратегічних, а не лише тактичних результатів операції. Меседжі, орієнтовані на цю аудиторію, спрямовані на підтвердження ефективності використання військової допомоги, демонстрацію спроможності України нав'язувати ініціативу та легітимізацію наступальних дій на території противника. Від реакції цієї аудиторії значною мірою залежать продовження військово-технічної підтримки й політична позиція України на переговорах.

Ворожа аудиторія (російське населення та військово-політичне керівництво РФ) виступає об'єктом інформаційно-психологічного впливу. Метою комунікації щодо неї є створення інформаційного хаосу, посилення паніки серед військовослужбовців, дискредитація центральної влади й руйнування базового пропагандистського наративу про "недоторканість російських кордонів".

Усвідомлення тривимірної структури медіасередовища дало змогу українському командуванню розробити ефективну комунікаційну стратегію, у межах якої кожна аудиторія отримувала повідомлення у потрібний для досягнення стратегічних цілей момент.

Підготовчий етап: режим інформаційної тиші та протидія OSINT-загрозам. Розуміння нормативної бази та структури медіасередовища дає змогу перейти до аналізу того, як саме принципи інформаційної безпеки були реалізовані на етапі підготовки Курської операції. Успішна реалізація операції стала можливою лише завдяки системному підходу до планування, що базувався на режимі суцільної інформаційної тиші. Інформаційна тиша була не епізодичним заходом, а наскрізною стратегією, яка послідовно застосовувалася на всіх рівнях підготовки – від обмеження кола обізнаних осіб до унеможливлення зовнішнього моніторингу пересувань військ.

Першочерговим кроком стало максимальне звуження кола осіб, допущених до планування операції. Розроблення планів здійснювалося під безпосереднім керівництвом Головнокомандувача ЗСУ за участю вузької групи командирів у режимі суворого секретності, а ключові питання обговорювалися Головнокомандувачем із Президентом сам на сам, без участі штабу. За даними відкритих джерел, на момент початку операції з її планом були ознайомлені лише три-чотири вищих офіцери; офіцери середнього рівня отримали інформацію за три доби до наступу, а рядовий склад – лише за добу. До операції залучалися військові з різних бригад і родів військ, причому з кожної частини відбиралися окремі підрозділи й невеликі групи особового складу, що додатково знижувало ризик витоку інформації. Самі учасники операції згодом розповіли: "Операція планувалася в таємниці й ніхто не розумів, що готується. Було зрозуміло, що нас очікують штурмові дії. Можна було логічно зрозуміти, що планується певний наступ, але де це буде, ніхто до кінця не знав" (Суспільне Суми, 2024).

Принципово важливим є те, що навіть ключові західні союзники не отримали попереднього повідомлення про заплановане вторгнення на територію Російської Федерації. За оцінками аналітичного центру Atlantic Council, відсутність попереджень партнерів була свідомим рішенням, спрямованим на запобігання витокам, що траплялися у попередніх операціях (Atlantic Council, 2024). Таке рішення усувало ризик розголошення задуму через людський фактор або перехоплення каналів зв'язку на стратегічному рівні. Хоча воно й створило певну напругу в дипломатичних відносинах, водночас засвідчило здатність України до самостійного стратегічного планування та забезпечило максимальний ефект раптовості.

Паралельно з фізичним переміщенням військ здійснювалася підготовка інформаційно-психологічних операцій (ІПСО) як інтегрованого складника комунікаційної стратегії. Підрозділи Сил спеціальних операцій, реалізуючи операцію під кодовою назвою "Сенека", зосередилися на впливі на російське військове командування та армійські підрозділи противника. Завданням цих заходів було поширення дезінформації, нагнітання паніки серед військовослужбовців противника й дезорганізація його управління (Громадське, 2024). Дезінформаційні заходи в межах OPSEC передбачали відволікаючі маневри, що мали приховати зосередження ударних сил саме на Сумському напрямку. Поєднання класичних військових дій із психологічними операціями та інформаційними кампаніями становить характерну ознаку сучасної гібридної війни, у якій інформаційний вплив на противника здійснюється паралельно з фізичними операціями, а не як окремий ізольований процес.

Окремим важливим аспектом підготовки стала протидія загрозам у сфері розвідки на основі відкритих джерел – OSINT (Open Source Intelligence). У сучасному розумінні OSINT – це систематичний процес збирання, аналізу й верифікації інформації з публічно доступних джерел (соціальних мереж, державних реєстрів, медіа, супутникових сервісів) задля отримання нових розвідувальних даних. Російсько-українська війна стала каталізатором розвитку цього напрямку як повноцінного інструменту військової розвідки: за оцінками American Security Project, вона перетворила OSINT на дієвий чинник впливу на оперативно-тактичному й геополітичному рівнях (American Security Project, 2024).

Високий рівень інформаційної прозорості формує глобальне OSINT-середовище – інформаційний простір, насичений безпрецедентними масивами загальнодоступних цифрових даних та інструментами для їх автоматизованого аналізу. За оцінками, до 2025 року глобальний обсяг згенерованих даних подвоївся і досяг приблизно 150 зетабайтів (Coulthart, 2026). Аналітичні звіти провідних OSINT-платформ свідчать про парадоксальну закономірність: відкритість інформаційного середовища стає загрозою передусім для тієї воюючої сторони, яка втрачає контроль над власними комунікаційними каналами (Babel Street, 2024). У випадку Курської операції командування ЗСУ продемонструвало здатність ефективно протидіяти цим загрозам шляхом запровадження жорсткого режиму інформаційної тиші й багаторівневої системи допуску до інформації. Як зазначає дослідник С. Коултарт з Університету Олбані, початковий етап повномасштабного вторгнення 2022–2023 років міг виявитися кульмінаційною точкою безперешкодної ефективності OSINT, оскільки сторони війни поступово навчилися адаптуватися до відкритого моніторингу та протидіяти йому (Coulthart, 2026). Курська операція підтверджує цю тенденцію: попри високу техно-

логічну розвиненість сучасних OSINT-інструментів, українському командуванню вдалося зберегти стратегічну раптовість, що стало вагомим аргументом надійності України як партнера для міжнародних союзників.

Логічним продовженням аналізу підготовчого етапу є оцінка результатів, яких досягла оборона комунікаційна стратегія після початку активної фази операції. Хронологія публічних подій 6–27 серпня 2024 року дає змогу виокремити два чітко розмежовані етапи: етап інформаційного вакууму (6–8 серпня), коли українська сторона повністю утримувала тишу, та етап усвідомлення масштабів і офіційного визнання операції (9–12 серпня), що завершився перебудовою інформаційного поля на користь української сторони. Подальший виклад послідовно розкриває, як саме оборона стратегії позначилася на трьох ключових сегментах аудиторії – російському, українському й міжнародному.

Етап інформаційного вакууму (6–8 серпня 2024 року). 6 серпня 2024 року Міністерство оборони Російської Федерації заявило про нібито спробу прориву кордону в районі населених пунктів Миколаєво-Дар'їно та Олешня Курської області. Того самого дня міжнародне агентство Reuters, посилаючись на заяви місцевого губернатора, опублікувало матеріал про обстріли міста Суджа (Reuters, 2024). Показово, що в іноземних медіа акцент зміщувався переважно на удари безпілотних літальних апаратів, а не на масштабну наземну операцію, оскільки реальні масштаби прориву залишалися прихованими.

У перші дні Російська Федерація фактично виявилася єдиним джерелом інформації для світових ЗМІ, проте її повідомлення були хаотичними та внутрішньо суперечливими. Це підтверджується аналітичним дослідженням видання "Детектор медіа" ("Курський хаос. Моніторинг росЗМІ за 5–11 серпня 2024 року"), згідно з яким події в Курській області миттєво перетворилися на домінуючу тему російського інформаційного простору і спровокували системні суперечності всередині пропагандистської машини (Детектор медіа, 2024). Уже 7 серпня вище керівництво РФ було змушене публічно реагувати на кризу: Володимир Путін уперше назвав дії ЗСУ "масштабною провокацією".

В умовах повної відсутності офіційних коментарів з боку Генерального штабу ЗСУ українські медіа працювали в режимі жорстких інформаційних обмежень. Зокрема, телеканал "1+1" у перших оглядових сюжетах був змушений посилатися виключно на російські пабліки та джерела агресора, підкреслюючи відсутність офіційної інформації від українського командування (ТСН, 2024). Цей офіційний вакуум частково заповнювався повідомленнями в соціальних мережах. Зокрема, генеральний директор "Укрпошти" Ігор Смілянський іронічно анонсував у Facebook гіпотетичне відкриття нового відділення у Суджі. Журналіст і волонтер Сергій Стерненко припустив, що українське командування ухвалило рішення атакувати одне з найслабших місць у противника, оскільки за повідомленнями самих росіян, ними було втрачено вже 11 населених пунктів, а ефект несподіванки був досягнутий завдяки відсутності витоків інформації.

Натомість у російських пабліках паралельно розгорталася повна паніка, зафіксована, зокрема, у репортажах українського YouTube-каналу "Є питання" на основі моніторингу відкритих відеоматеріалів ("Є питання", 2024). Тотальне мовчання офіційного Києва дестабілізувало внутрішній простір противника: поки Міноборони РФ намагалася нівелювати загрозу заявами про "ефективне відбиття атак", російські Z-блогери відкрито описували стрімке просування бронетехніки ЗСУ вглиб російської

території. У таких умовах "туману війни" провідні західні медіа опинилися в ситуації браку верифікованих даних і змушені були спиратися переважно на повідомлення російських мілітарних блогерів.

Така стратегія дала змогу Україні повторити успішний сценарій медійної ізоляції бойових дій, апробований раніше під час рейдів РДК на Белгород. Тоді Україна також не надавала інформації щодо своєї причетності, попри те, що на сайті РДК було вказано, що вони діють під керівництвом українського командування.

Водночас режим тривалого тотального мовчання офіційних джерел не є безризиковою "ідеальною моделлю" і має зворотний бік, який доцільно враховувати під час оцінювання його ефективності. Передусім ідеться про внутрішню (українську) аудиторію прифронтових областей: затяжний інформаційний вакуум здатний породжувати щонайменше дві групи ризиків. По-перше, відповідно до закономірності, описаної Г. Почепцовим (2024), незаповнена інформаційна порожнечка неминуче заповнюється сторонніми інтерпретаціями – за відсутності офіційних повідомлень її можуть посісти чутки, панічні наративи в соціальних мережах або цілеспрямована ворожа дезінформація, спрямована на дестабілізацію тилу. По-друге, брак верифікованих відомостей про перебіг бойових дій підвищує рівень тривожності місцевого населення та ускладнює ухвалення ним обґрунтованих рішень щодо особистої безпеки. Таким чином, режим інформаційної тиші доцільно розглядати не як універсальне благо, а як інструмент, ефективність якого зумовлена точним балансуванням між вимогами OPSEC і конституційним правом громадян на достовірну інформацію; саме таке балансування становить ключову управлінську дилему стратегічних комунікацій.

Етап офіційного визнання та комунікаційного перелому (9–12 серпня 2024 року). Із 9 серпня приховувати присутність українських військ ставало дедалі важче. Радник Президента вперше визнав факт вторгнення 8 серпня, не підтверджуючи безпосередньої ролі України. 10 серпня Володимир Зеленський у вечірньому зверненні зробив перші зауваження заяві про те, що війна "повертається туди, звідки прийшла", уникаючи деталізації. У мережі почали з'являтися перші відео українських військових у селах Курської області.

Ліше 12 серпня вперше з'явилася офіційна заява про наступальну операцію ЗСУ в Курській області від Президента України та Головнокомандувача ЗСУ. Уже 27 серпня стало відомо про звільнення близько 100 населених пунктів (Суспільне новини, 2024). Поступова ескалація офіційних заяв створила наростаючий інформаційний ефект, який утримував увагу світових ЗМІ та міжнародної аудиторії впродовж тривалого часу. У цей самий день Путін провів публічну нараду щодо ситуації у прикордонні з демонстрацією роздратування та наказом "вибити противника" з Курської області, а російська пропаганда перевела увагу суспільства на тему евакуації біженців і формування образу "гуманітарної катастрофи".

Як зазначає Г. Почепцов, "пауза в інформаційному просторі створює напругу, яку згодом заповнює той, хто першим надає структуровану подію" (Почепцов, 2024, с. 92). Коли вакуум заповнюється не чутками, а заздалегідь підготовленими і верифікованими фактами, виникає ефект інформаційного домінування. Замість рефлекторної реакції на хаотичні викиди противника Сили оборони отримали монополію на перше офіційне повідомлення, що сформувало глобальну рамку сприйняття операції як професійної та переможної (Центр протидії

дезінформації, 2024). Після офіційної заяви Україна почала конструювати власну картинку в медіапросторі. Вона почала допускати західних журналістів (CNN, The Washington Post, італійського RAI тощо) на контрольовані території, що спричинило обурення Російської Федерації та порушення кримінальних справ проти іноземних репортерів.

Обмеження проросійського використання платформи Telegram, що збіглося із цим періодом, додатково посилює здатність української сторони диктувати наратив навколо Курської операції (RAND Corporation, 2024). Ексклюзивний репортаж Espresso.TV із Суджі продемонстрував повний контроль ЗСУ над містом (Espresso.TV, 2024). Зазначене відповідає теоретичній моделі інформаційного домінування, згідно з якою стратегічну перевагу в медійному протистоянні здобуває та сторона, що першою формує цілісний наратив і забезпечує його трансляцію через контрольовані канали. О. Ільницька обґрунтовує, що система захисту національного інформаційного простору має бути орієнтована саме на нейтралізацію деструктивного контенту, здатного підривати державні інтереси (Ільницька, 2017).

Результати для російської сторони. Для російської сторони обрана Україною стратегія обернулася втратою інформаційної ініціативи та контролю над поясненням подій, що супроводжувалося появою взаємосуперечливих версій у межах її власного інформаційного простору. Будучи фактично єдиним джерелом інформації у перші дні, російські структури через шок і нерозуміння реальної ситуації подавали її в хаотичний спосіб. Російська пропаганда, що роками формувала наратив "армії-визволительки", виявилася неспроможною швидко пояснити, як іноземні війська увійшли на власну територію РФ. Офіційні структури намагалися применшити масштаб подій, кваліфікуючи їх як "диверсію", однак реальні відео біженців і поширення паніки в місцевих Telegram-каналах підривали довіру до влади (The Moscow Times, 2024). Провладні російські медіа намагалися подати операцію як другорядну диверсію, що нібито не впливає на головний напрямок бойових дій у Донецькій і Луганській областях; офіційні зведення фокусувалися на "успішних ударах авіації" по українських резервах, а втрата Суджі замовчувалася або подавалася як "тимчасове тактичне ускладнення".

Ключовою причиною інформаційної поразки російської сторони стала концептуальна неспроможність запропонувати альтернативний цілісний наратив. Якщо армія декларується як визволителька, то її присутність на чужій території логічно вписується у пропагандистську рамку, натомість входження інших військ на власну територію руйнує цю рамку зсередини. Спостерігалось своєрідне інформаційне ухиляння: уникнення фактологічних повідомлень компенсувалося апеляціями до "контролю Путіна над ситуацією", обіцянками завершення "спецоперації" до кінця року, а також залякуванням партнерів України загрозою пошкодження атомних електростанцій – Курської та Запорізької. У підсумку інформаційний простір противника зазнав дефрагментації: влада втратила монополію на пояснення подій, а суспільство отримало розбіжні версії з різних рівнів пропагандистської машини.

Результати для української сторони. 12 серпня 2024 року, після офіційної заяви Президента, відбувся комунікаційний злам. Витримавши тривалу паузу, Україна отримала монополію на перше офіційне пояснення подій і запропонувала чіткий переможний наратив: Збройні Сили України здатні ефективно вести насту-

пальні дії на території держави-агресорки (Центр протидії дезінформації, 2024). Цей наратив був принципово сильнішим за російську версію подій із кількох причин.

По-перше, він підтверджував спроможність України не лише захищати власну територію, а й планувати та реалізовувати складні наступальні операції на території противника, причому з використанням значною мірою власного озброєння. По-друге, він демонтував російську пропагандистську рамку "визволителя", оскільки операція довела, що ЗСУ можуть діяти там, де декларована "недоторканість кордонів" виявилася фікцією. По-третє, він закріпив за Україною позицію сторони, яка не лише потребує допомоги, а й здатна пропонувати союзникам власний військовий досвід і зразки озброєння, особливо дрони – передусім ті, що були створені та випробувані під час війни.

Серед ознак успішної інформаційної кампанії варто виокремити: повний контроль над наративом після зняття режиму тиші, масове цитування українських офіційних повідомлень провідними світовими медіа, активну присутність ЗСУ в цифровому полі (включно з відеоматеріалами із Суджі в TikTok, що мали виразний деморалізуючий ефект (ТСН, 2024)), а також змістове перевизначення ролі України у війні – з країни-жертви на країну-партнера, спроможну ділитися досвідом.

Результати для міжнародних партнерів. Для міжнародних партнерів Курська операція стала підставою для перегляду парадигми сприйняття України. Інформаційна кампанія засвідчила, що Україна є не лише державою, яка потребує військово-технічної допомоги, а й професійним партнером, здатним планувати й реалізовувати складні наступальні маневри з дотриманням високого рівня операційної безпеки. Експерти RAND Corporation оцінили інформаційний ефект операції як надзвичайно потужний, порівнявши його вплив на глобальний медіапростір з ефектом вибуху незалежно від тривалості суто військового складника вторгнення (RAND Corporation, 2024). Збереження стратегічної раптовості в умовах прозорого цифрового поля стало вагомим аргументом для союзників щодо продовження фінансового й матеріально-технічного забезпечення.

Опосередкованим, але важливим результатом стала зміна тональності публікацій провідних західних видань. Якщо в перші дні матеріали будувалися на російських джерелах і припущеннях мілітарних блогерів, то після офіційного визнання операції західні медіа почали отримувати дозволи на роботу безпосередньо з контрольованої українськими силами території і цитувати українські офіційні повідомлення як першоджерело. У грудні 2024 року Головнокомандувач ЗСУ публічно охарактеризував Курську операцію як успіх, досягнутий завдяки ефекту раптовості, забезпеченому збереженою інформаційною тишею (Суспільне новини, 2024). В. Ліпкан із цього приводу влучно зауважує, що "інформаційна безпека в умовах війни – це не закритість, а хірургічна точність у дозуванні правди" (Ліпкан, 2022, с. 152). Конкретним виявом цієї зміни стали репортажі CNN та The Washington Post із контрольованих Силами оборони територій Курської області, у яких українські офіційні повідомлення вперше виступили першоджерелом фактів, а не об'єктом спростування (O'Grady, Burianova, & Ram, 2024; Paton Walsh, 2024).

Дискусія і висновки

Отримані результати доцільно співвіднести з наявними теоретичними моделями, аби чіткіше окреслити, у чому саме досвід Курської операції доповнює, видозмінює або заперечує попередні висновки. Класичні моделі медійної прозорості цифрової епохи здебільшого

виходять із тези про невідворотне зростання ролі відкритих даних і поступову втрату можливості досягати стратегічної раптовості. Досвід Курської операції не стільки підтверджує, скільки коригує цю тезу: він емпірично ілюструє припущення С. Коултартта про те, що пік безперешкодної ефективності OSINT, імовірно, уже пройдено, а сторони конфлікту виробляють дієві контрзаходи (Coulthart, 2026). У цьому сенсі дослідження вступає в полеміку з оптимістичними оцінками "тотальної прозорості": інституційна дисципліна та режим інформаційної тиші виявляються спроможними тимчасово нейтралізувати технологічну перевагу відкритого моніторингу. Водночас концепт "інформаційної паузи" Г. Почепцова (Почепцов, 2024) у матеріалах Курської операції набуває уточнення – пауза є стратегічним ресурсом лише за умови, що сторона здатна вчасно й першою заповнити її верифікованим наративом, інакше той самий механізм обертається проти неї, що й сталося з російським інформаційним простором.

Окремого дискусійного осмислення потребує нормативна межа між демократичним правом суспільства на інформацію та жорстким обмеженням свободи слова, запровадженим, зокрема, наказом Головнокомандувача ЗСУ № 73 (Головнокомандувач Збройних Сил України, 2022). З одного боку, обмеження роботи журналістів у "червоних зонах" і заборона геолокаційних даних є виправданими вимогами OPSEC, які прямо вплинули на успіх операції. З іншого боку, тривалі обмеження створюють ризик нормалізації непрозорості та послаблення суспільного контролю, на що звертають увагу медіадослідники. Однозначного розв'язання цієї дилеми наявна література не пропонує: підходи коливаються від пріоритету безпеки операцій до пріоритету права на інформацію. Позиція, обстоювана в цьому дослідженні, полягає в тому, що йдеться не про вибір одного полюса, а про динамічне регулювання – звуження публічності на етапі підготовки з її подальшим контрольованим розширенням після досягнення оперативних цілей. Саме така постановка питання продуктивніша за бінарне протиставлення безпеки й відкритості та потребує подальшої наукової верифікації на ширшому масиві операцій.

Проведене дослідження дає змогу стверджувати, що інформаційна безпека в умовах сучасної війни трансформувалася в самостійний вид стратегічного озброєння, ефективність якого підтверджується на прикладі Курської операції. Чотири взаємопов'язані аспекти – нормативно-правова база, структура медіасередовища, підготовка операції та результати інформаційної кампанії – утворюють цілісний механізм, у якому жодний елемент не може бути замінений іншим без втрати загальної ефективності.

По-перше, чинна нормативно-правова база України, доповнена стандартами НАТО (зокрема концепцією OPSEC), створила інституційні передумови для запровадження режиму інформаційної тиші як легітимної комунікаційної стратегії. По-друге, тривимірна структура аудиторії – українська, російська й міжнародна – зумовила потребу в диференційованому інформаційному впливі. По-третє, на етапі підготовки операції режим інформаційної тиші довів свою спроможність нейтралізувати загрози OSINT-розвідки навіть в умовах загальної прозорості цифрового простору. По-четверте, результати кампанії продемонстрували: чим довше зберігається режим тиші, тим потужнішим є медіаефект перемоги на етапі офіційного оголошення.

На прикладі Курської операції підтверджено: стратегічне управління інформацією, що поширюється у відкриті джерела, є невід'ємною частиною військової опера-

ції, у якій тиша стає зброєю та водночас підставою для глобального визнання її результату. Перетворення локальної військової перемоги на вагомий зовнішньополітичний результат стало можливим завдяки інтеграції правових, організаційних і комунікаційних інструментів.

Наукова новизна одержаних результатів полягає в інтеграції нормативно-правового, медіасередовищного й OSINT-вимірів інформаційної безпеки в межах єдиної аналітичної моделі, застосованої до конкретної наступальної операції Збройних Сил України, що раніше у вітчизняній науковій літературі комплексно не здійснювалося. Поставлену мету дослідження досягнуто: механізми забезпечення інформаційної безпеки та реалізації комунікаційних стратегій Курської операції розкрито на всіх чотирьох виокремлених рівнях, а ключову тезу про режим інформаційної тиші як активну комунікаційну стратегію верифіковано емпіричним матеріалом контент-аналізу.

Перспективи подальших досліджень пов'язані щонайменше з трьома напрямками. Перший – розроблення нових форматів співпраці із цивільними медіа, які забезпечили б оперативне інформування світу про події на передовій без розкриття позицій підрозділів. Другий – формування етичних кодексів для OSINT-спільноти й журналістів, що працюють у зоні бойових дій, оскільки публікація даних із відкритих джерел дедалі частіше створює дилему між правом суспільства на інформацію та безпекою військових (American Security Project, 2024). Третій – порівняльний аналіз українського досвіду інформаційного забезпечення наступальних операцій із досвідом інших країн, що дасть змогу виокремити універсальні моделі стратегічних комунікацій у сучасних збройних конфліктах (European Journal of International Security, 2024; The Washington Quarterly, 2025). Курська операція стала одним із найяскравіших прикладів такої успішної протидії прозорості цифрової епохи.

Джерела фінансування. Це дослідження не отримало жодного гранту від фінансової установи в державному, комерційному або некомерційному секторах.

Список використаних джерел

- Башук, А. І. (2019). *Комунікаційні стратегії державної влади в умовах інформаційного суспільства*. ТОВ "Друкарня "Рута". https://scc.knu.ua/upload/iblock/3a4/dis_Bashuk.pdf
- Генеральний штаб Збройних Сил України. (2026). *Військові зв'язки з громадянськістю*. Доктрина від 15.01.2026 № 340.
- Головнокомандувач Збройних Сил України. (2020). *Доктрина зі стратегічних комунікацій Сил оборони України*. Наказ від 20.10.2020 № 121. <https://sprotyvg7.com.ua/wp-content/uploads/2022/04/%D0%92%D0%9A%D0%9F-10-0049.01-%D0%94%D0%BE%D0%BA%D1%82%D1%80%D0%B8%D0%BD%D0%B0-%D0%B7%D1%96-%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%87%D0%BD%D0%B8%D1%85-%D0%BA%D0%BE%D0%BC%D1%83%D0%BD%D1%96%D0%BA%D0%B0%D1%86%D1%96%D0%B8%CC%86.pdf>
- Головнокомандувач Збройних Сил України. (2022). *Про організацію взаємодії між Збройними Силами України, іншими складовими сил оборони та представниками медіа на час дії правового режиму воєнного стану*. Наказ від 03.03.2022 № 73. <https://mod.gov.ua/diyalnist/normativno-pravova-baza/nakaz-golovnokomanduvacha-zsu-vid-03-03-2022-roku-73-zi-zminami>
- Громадське. (2024). *ССО розповіли, як починалася Курська операція та чому вдалося швидко просуватися*. <https://hromadske.ua/viyna/239238-ss0-rozpovily-iak-pochynalasja-kurska-operatsiia>
- Детектор медіа. (2024). *Курський хаос. Моніторинг росЗМІ за 5–11 серпня 2024 року*. <https://detector.media/infospace/article/230925/2024-08-15-kursky-khaos-monitoryng-roszmi-za-511-serpnya-2024-roku/>
- "Є питання". (2024). *Наступ на Курськ: Курська АЕС, стратегічний газопіп і колишня українська столиця Суджа*. <https://www.youtube.com/watch?v=3QNZPo2Z27o>
- Ільницька, О. М. (2017). *Інформаційна безпека України: сучасні виклики, загрози та механізми протидії*. Наукове видання Львівської політехніки. <https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/lnicka0.pdf>
- Курбан, О. В. (2023). *Інформаційні війни у цифровому середовищі*. Інститут журналістики.

- Ліпкан, В. А. (2022). *Інформаційна безпека України в умовах сучасних геополітичних реалій*. КНТ.
- Почепцов, Г. Г. (2024). *Стратегічні комунікації в умовах гібридних зароз. Вид. дім "Києво-Могилянська академія"*.
- Проект Концепції інформаційної безпеки України. (б. д.). ОБСЄ. <https://www.osce.org/files/f/documents/0/2/175056.pdf>
- Суспільне новини. (2024). *"Уперше поставили РФ в оборону на власній території": Сирський розкрив деталі Курської операції*. <https://susplne.media/1073487-uperse-postavili-ih-v-oboronu-na-vlasnij-teritorii-sirskij-rozkryv-detali-kurskoj-operacii/>
- Суспільне Суми. (2024). *"Ми перенесли війну на територію Росії" – як планувалася і розгорталася Курська операція*. <https://susplne.media/sumy/912943-mi-perenesli-vijnu-na-teritoriu-rosii-ak-planuvalasja-i-rozgortalasa-kurska-operacia/>
- TCH. (2024). *"Х*охлі вошли, учите гімн України!" Місто Суджа: де воно і чому його обрали для наступу*. <https://www.youtube.com/watch?v=KEMpwU9ubnM>
- Центр протидії дезінформації при РНБО України. (2024). *Аналіз маніпулятивних наративів РФ під час Курської операції*. <https://cpd.gov.ua/articles/yak-ukrayinskyj-nastup-u-kurskij-oblasti-vplyvaye-na-putina-i-rosiyan/>
- Espresso.TV. (2024). *Ексклюзивний репортаж з Курської області*. https://www.youtube.com/watch?v=FUo1H62_2Nc
- Reuters. (2024, серпень 6). *П'ятеро поранено внаслідок обстрілу Курської області з боку України*. <https://www.reuters.com/world/europe/five-injured-ukraine-shelling-russias-kursk-region-26-drones-downed-governor-2024-08-06/>
- Allied Joint Doctrine for Strategic Communications (AJP-3.10). (2023). NATO Standardization Committee.
- American Security Project. (2024). *How OSINT has shaped the war in Ukraine*. <https://www.americansecurityproject.org/osint-in-ukraine/>
- Atlantic Council. (2024). *Ukraine's Kursk offensive proves surprise is still possible in modern war*. <https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-kursk-offensive-proves-surprise-is-still-possible-in-modern-war/>
- Babel Street. (2024). *The Ukraine-Russia war confirms the value of OSINT*. <https://www.babelstreet.com/blog/the-ukraine-russia-war-confirms-the-value-of-osint>
- Coulthart, S. (2026). *Lessons from Ukraine: How OSINT networks are changing war*. Centrum Balticum, Baltic Rim Economies. <https://centrumbalticum.org/stephen-coulthart-lessons-from-ukraine-how-osint-networks-are-changing-war>
- European Journal of International Security. (2024). *The rise of open-source intelligence*. Cambridge Core. <https://www.cambridge.org/core/journals/european-journal-of-international-security/article/rise-of-opensource-intelligence/21122432399ECB8078BF0D89A76D0586>
- O'Grady, S., Burianova, T., & Ram, E. (2024, August 18). *In Ukraine-controlled Sudzha, stranded Russian civilians question what's next*. *The Washington Post*. <https://www.washingtonpost.com/world/2024/08/18/ukraine-russia-sudzha-kursk/>
- Paton Walsh, N. (2024, August 16). *Sudzha, Kursk: Russian residents take shelter as Ukraine advances*. *CNN*. <https://edition.cnn.com/2024/08/16/europe/sudzha-russia-ukraine-streets-intl-latam>
- RAND Corporation. (2024). *Ukraine may be winning the information war in Kursk*. <https://www.rand.org/pubs/commentary/2024/09/ukraine-may-be-winning-the-information-war-in-kursk.html>
- The Moscow Times. (2024). *Kursk incursion rages for a third month*. <https://www.themoscowtimes.com/2024/10/15/as-ukraines-kursk-incursion-rages-for-a-third-month>
- The Washington Quarterly. (2025). *The war on open-source intelligence*. Taylor & Francis. <https://www.tandfonline.com/doi/full/10.1080/0163660X.2025.2554477>

References

- "There is a question". (2024). *The offensive on Kursk: Kursk NPP, strategic gas pipeline and the former Ukrainian capital Sudzha* [in Ukrainian]. <https://www.youtube.com/watch?v=3QNZPo2Z27o>
- Alliance Joint Force Doctrine on Strategic Communications (AJP-3.10). (2023). NATO Standardization Committee [in Ukrainian].
- Allied Joint Doctrine for Strategic Communications (AJP-3.10). (2023). NATO Standardization Committee.
- American Security Project. (2024). *How OSINT has shaped the war in Ukraine*. <https://www.americansecurityproject.org/osint-in-ukraine/>
- Atlantic Council. (2024). *Ukraine's Kursk offensive proves surprise is still possible in modern war*. <https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-kursk-offensive-proves-surprise-is-still-possible-in-modern-war/>
- Babel Street. (2024). *The Ukraine-Russia war confirms the value of OSINT*. <https://www.babelstreet.com/blog/the-ukraine-russia-war-confirms-the-value-of-osint>
- Bashuk, A. I. (2019). *Communication strategies of state power in the conditions of the information society*. LLC "Printing House "Ruta" [in Ukrainian]. https://scc.knu.ua/upload/iblock/3a4/dis_Bashuk.pdf
- Center for Countering Disinformation at the National Security and Defense Council of Ukraine. (2024). *Analysis of the Russian Federation's manipulative narratives during the Kursk operation* [in Ukrainian]. <https://cpd.gov.ua/articles/yak-ukrayinskyj-nastup-u-kurskij-oblasti-vplyvaye-na-putina-i-rosiyan/>
- Commander-in-Chief of the Armed Forces of Ukraine. (2020). *Doctrine on strategic communications of the Defense Forces of Ukraine*. Order dated 10/20/2020 No. 121 [in Ukrainian]. <https://sprotyvg7.com.ua/wp-content/>

uploads/2022/04/%D0%92%D0%9A%D0%9F-10-0049.01-%D0%94%D0%BE%D0%BA%D1%82%D1%80%D0%B8%D0%BD%D0%B0-%D0%B7%D1%96-%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%87%D0%BD%D0%B8%D1%85-%D0%BA%D0%BE%D0%BC%D1%83%D0%BD%D1%96%D0%BA%D0%B0%D1%86%D1%96%D0%B8%CC%86.pdf

Commander-in-Chief of the Armed Forces of Ukraine. (2022). *On the organization of interaction between the Armed Forces of Ukraine, other components of the defense forces and representatives of the media during the period of the legal regime of martial law*. Order dated 03.03.2022 No. 73 [in Ukrainian]. <https://mod.gov.ua/diyalnist/normativno-pravova-baza/nakaz-golovnokomanduvacha-zsu-vid-03-03-2022-roku-73-zi-zminami>

Coulthart, S. (2026). *Lessons from Ukraine: How OSINT networks are changing war*. Centrum Balticum, Baltic Rim Economies. <https://centrumbalticum.org/stephen-coulthart-lessons-from-ukraine-how-osint-networks-are-changing-war>

Draft Concept of Information Security of Ukraine. (n.d.). OSCE [in Ukrainian]. <https://www.osce.org/files/f/documents/0/2/175056.pdf>

Espresso.TV. (2024). *Exclusive report from the Kursk region* [in Ukrainian]. https://www.youtube.com/watch?v=FUo1H62_2Nc

European Journal of International Security. (2024). *The rise of open-source intelligence*. Cambridge Core. <https://www.cambridge.org/core/journals/european-journal-of-international-security/article/rise-of-open-source-intelligence/21122432399ECB8078BF0D89A76D0586>

General Staff of the Armed Forces of Ukraine. (2026). *Military Public Relations*. Doctrine dated 01/15/2026 No. 340 [in Ukrainian].

Hromadske. (2024). *SSO told how the Kursk operation began and why it was possible to advance quickly* [in Ukrainian]. <https://hromadske.ua/viynal/239238-ss0-rozpovily-iak-pochynalasja-kurska-operatsiia>

Ilnytska, O. M. (2017). *Information Security of Ukraine: Modern Challenges, Threats and Countermeasures*. Scientific Publication of Lviv Polytechnic [in Ukrainian]. <https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf>

Kurban, O. V. (2023). *Information Wars in the Digital Environment*. Institute of Journalism [in Ukrainian].

Lipkan, V. A. (2022). *Information Security of Ukraine in the Conditions of Modern Geopolitical Realities*. KST [in Ukrainian].

Media Detector. (2024). *Kursk chaos. Monitoring of Russian media for August 5–11, 2024* [in Ukrainian]. <https://detector.media/infospace/article/230925/2024-08-15-kursky-khaos-monitoring-rozsmi-za-511-serpnia-2024-roku/>

Nataliia ROZHNIATIVSKA, PhD Student

ORCID ID: 0009-0005-8613-779X

e-mail: rozhniativska.natali@knu.ua

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

O'Grady, S., Burianova, T., & Ram, E. (2024, August 18). In Ukraine-controlled Sudzha, stranded Russian civilians question what's next. *The Washington Post*. <https://www.washingtonpost.com/world/2024/08/18/ukraine-russia-sudzha-kursk/>

Paton Walsh, N. (2024, August 16). Sudzha, Kursk: Russian residents take shelter as Ukraine advances. *CNN*. <https://edition.cnn.com/2024/08/16/europe/sudzha-russia-ukraine-streets-intl-latam>

Pochepstov, G. G. (2024). *Strategic Communications in Conditions of Hybrid Threats*. Publishing House "Kyiv-Mohyla Academy" [in Ukrainian].

Public News. (2024). *"For the first time, the Russian Federation was put on the defensive on its own territory": Syrs kij revealed the details of the Kursk operation* [in Ukrainian]. <https://suspihne.media/1073487-uperse-postavili-ih-v-oboronu-na-vasnij-teritorii-sirskij-rozkryv-detali-kurskoi-operacii/>

Public Sumy. (2024). *"We moved the war to the territory of Russia" – how the Kursk operation was planned and unfolded* [in Ukrainian]. <https://suspihne.media/sumy/912943-mi-perenesli-vijnu-na-teritoriu-rosii-ak-planuvalasa-i-rozgortalasja-kurska-operacia/>

RAND Corporation. (2024). *Ukraine may be winning the information war in Kursk*. <https://www.rand.org/pubs/commentary/2024/09/ukraine-may-be-winning-the-information-war-in-kursk.html>

Reuters. (2024, August 6). *Five people were injured as a result of the shelling of the Kursk region from Ukraine* [in Ukrainian]. <https://www.reuters.com/world/europe/five-injured-ukraine-shelling-russias-kursk-region-26-drones-downed-governor-2024-08-06/>

The Moscow Times. (2024). *Kursk incursion rages for a third month*. <https://www.themoscowtimes.com/2024/10/15/as-ukraines-kursk-incursion-rages-for-a-third-month>

The Washington Quarterly. (2025). *The war on open-source intelligence*. Taylor & Francis. <https://www.tandfonline.com/doi/full/10.1080/0163660X.2025.2554477>

TSN. (2024). *"Fuck you, come in, learn the anthem of Ukraine!" The city of Sudzha: where is it and why was it chosen for the offensive* [in Ukrainian]. <https://www.youtube.com/watch?v=kEMpwU9ubnM>

Отримано редакцією журналу / Received: 08.06.26

Прорецензовано / Revised: 23.06.26

Схвалено до друку / Accepted: 16.07.26

Опубліковано / Published: 21.09.26

INFORMATION SECURITY AS A PREREQUISITE FOR THE STRATEGIC SUCCESS OF MILITARY OPERATIONS: LESSONS FROM THE KURSK OPERATION

Background. The article examines the role of information security as a strategic instrument for planning and conducting military operations, using the Armed Forces of Ukraine's Kursk Operation (August–December 2024) as a case study. It highlights the importance of balancing society's right to information with information-security requirements in hybrid warfare. The aim is to analyse the mechanisms of information security and the implementation of communication strategies during the preparation and conduct of combat operations, using the Kursk Operation as an example.

Methods. Three complementary methods were applied: normative-documentary analysis of five key legal acts and NATO standards; content analysis of media materials for August–December 2024 (in total, over 40 media reports and more than 15 analytical reports and expert publications were analyzed, drawn from official statements by the Armed Forces of Ukraine, Ukrainian and international media, and Russian propaganda sources); and a comparative method to juxtapose the actual course of combat operations with their media coverage across three segments of the information environment.

Results. Four interrelated dimensions of the problem are analysed: the legal framework (including NATO standards); the structure of the media environment with three target audiences; the preparation phase under a regime of information silence and countermeasures against OSINT threats; and the results of the information campaign after the official acknowledgement of the operation. It is established that the information-silence regime ensured not only tactical success but also the transformation of a local military victory into a significant foreign-policy outcome for Ukraine. The strategy of media isolation deprived Russia of the initiative in the information domain and control over the explanation of events, while securing for Ukraine a the exclusive opportunity to issue the first official statement and control over the global narrative. For international partners, the operation became a basis for reassessing the perception of Ukraine as a state capable of independently planning complex offensive operations.

Conclusions. Information security in modern warfare has transformed into an independent type of strategic armament. Strategic management of information is an integral part of a military operation, in which information silence becomes a weapon and the basis for global recognition of its outcome, achieved through the integration of legal, organisational, and communicative instruments.

Keywords: information security, Kursk Operation, strategic communications, information silence, OSINT, media space, information warfare, strategic surprise.

Автор заявляє про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The author declares no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.