УДК 311.21:004.65:355.40
JEL: C55; C81; D83; H56
DOI: https://doi.org/10.32983/2222-4459-2026-6-86-95

OSINT У ЦИФРОВІЙ АНАЛІТИЧНІЙ ІНФРАСТРУКТУРІ: ВІД ВІДКРИТИХ ДАНИХ ДО УПРАВЛІНСЬКИХ РІШЕНЬ

©2026 ОСАУЛЕНКО О. Г., ГОРОБЕЦЬ О. О., ГРИНЧАК Н. А.

УДК 311.21:004.65:355.40
JEL: C55; C81; D83; H56

Осауленко О. Г., Горобець О. О., Гринчак Н. А. OSINT у цифровій аналітичній інфраструктурі: від відкритих даних до управлінських рішень

У статті досліджено роль OSINT-аналітики (Open Source Intelligence) в умовах стрімкого розвитку цифрової економіки, технологій Big Data, Data Science та штучного інтелекту. Показано, що зростання обсягів відкритих даних, поширення цифрових платформ, соціальних мереж, геопросторових сервісів та відкритих державних реєстрів сприяє трансформації OSINT із інструменту пошуку інформації у важливий елемент сучасної цифрової аналітичної інфраструктури. Проаналізовано еволюцію наукових підходів до розуміння OSINT, узагальнено сучасні підходи до його трактування та визначено місце відкритих джерел інформації в екосистемі Big Data. Обґрунтовано необхідність інтеграції відкритих даних, технологій Data Science та статистичних методів для підтримки процесів прийняття управлінських рішень. На основі концепції DIKW (Data – Information – Knowledge – Wisdom) розроблено авторську концептуальну модель інтеграції OSINT у процес перетворення відкритих даних у джерело підтримки прийняття управлінських рішень. Запропонована модель відображає послідовний перехід від даних до інформації, знань, аналітичних висновків та управлінських рішень і визначає функціональне місце OSINT між відкритими джерелами інформації та сучасними аналітичними технологіями. Особливу увагу приділено статистичній складовій OSINT-аналітики та можливостям застосування методів аналізу часових рядів, кластерного аналізу, мережевого аналізу, геостатистики та машинного навчання для роботи з великими масивами відкритих даних. Установлено, що в умовах російсько-української війни OSINT став одним із ключових інструментів забезпечення ситуаційної обізнаності, протидії дезінформації та підтримки управлінських рішень у сфері національної безпеки. Доведено, що статистичні методи виступають механізмом трансформації відкритих даних у знання та аналітичні висновки, придатні для використання в системах data-driven decision making.

Ключові слова: *OSINT; Big Data; Data Science; відкриті дані; державні реєстри; статистичний аналіз; штучний інтелект; управлінські рішення; національна безпека; російсько-українська війна.*
Рис.: *1.* ***Табл.:*** *1.* ***Бібл.:*** *15.*

Осауленко Олександр Григорович *– доктор наук з державного управління, професор, академік НАН України, ректор Національної академії статистики, обліку та аудиту (вул. Підгірна, 1, Київ, 04107, Україна)*
E-mail: *ivanenko@university.ua*
ORCID: *https://orcid.org/0000-0002-7100-7176*

Горобець Олена Олександрівна *– кандидат економічних наук, доцент, проректор з інформаційно-комунікаційної діяльності та цифрової трансформації Національної академії статистики, обліку та аудиту (вул. Підгірна, 1, Київ, 04107, Україна)*
E-mail: *babutska@ukr.net*
ORCID: *https://orcid.org/0000-0001-5433-6448*

Гринчак Наталія Анатоліївна *– кандидат економічних наук, доцент, завідувачка кафедри статистики та математичних методів в економіці, Національна академія статистики, обліку та аудиту (вул. Підгірна, 1, Київ, 04107, Україна)*
E-mail: *nahrynchak@nasoa.edu.ua*
ORCID: *https://orcid.org/0000-0002-2046-6014*

UDC 311.21:004.65:355.40
JEL: C55; C81; D83; H56

Osaulenko O. H., Horobets O. O., Hrynchak N. A. OSINT in Digital Analytical Infrastructure: From Open Data to Managerial Decision-Making

The article examines the role of Open Source Intelligence (OSINT) analytics in the context of the rapid development of the digital economy, Big Data technologies, Data Science, and artificial intelligence. It is demonstrated that the growing volume of open data, along with the expansion of digital platforms, social media, geospatial services, and open government registries, has transformed OSINT from a tool for information retrieval into a significant component of modern digital analytical infrastructure. The study analyzes the evolution of scientific approaches to understanding OSINT, summarizes contemporary interpretations of the concept, and identifies the place of open information sources within the Big Data ecosystem. The necessity of integrating open data, Data Science technologies, and statistical methods to support managerial decision-making processes is substantiated. Based on the Data–Information–Knowledge–Wisdom (DIKW) framework, the article proposes an original conceptual model for integrating OSINT into the process of transforming open data into a source of managerial decision support. The proposed model illustrates the sequential transition from data to information, knowledge, analytical insights, and managerial decisions, while defining the functional position of OSINT between open information sources and modern analytical technologies. Particular attention is paid to the statistical dimension of OSINT analytics and the application of time series analysis, cluster analysis, network analysis, geostatistics, and machine learning methods for processing large volumes of open data. The study finds that, in the context of the Russian–Ukrainian war, OSINT has become one of the key instruments for ensuring situational awareness, countering disinformation, and supporting decision-making processes in the field of national security. It is demonstrated that statistical methods serve as a mechanism for transforming open data into knowledge and analytical insights suitable for use within data-driven decision-making systems.

Keywords: *OSINT; Big Data; Data Science; open data; government registries; statistical analysis; artificial intelligence; managerial decision-making; national security; Russian-Ukrainian war.*
Fig.: *1.* ***Tabl.:*** *1.* ***Bibl.:*** *15.*

Osaulenko Oleksandr H. *– D. Sc. (Public Administration), Professor, Academician of NAS of Ukraine, Rector of the National Academy of Statistics, Accounting and Auditing (1 Pidhirna Str., Kyiv, 04107, Ukraine)*
E-mail: *ivanenko@university.ua*
ORCID: *https://orcid.org/0000-0002-7100-7176*
Horobets Olena O. *– PhD (Economics), Associate Professor, Pro-rector for Information and Communication Activities and Digital Transformation of the National Academy of Statistics, Accounting and Auditing (1 Pidhirna Str., Kyiv, 04107, Ukraine)*
E-mail: *babutska@ukr.net*
ORCID: *https://orcid.org/0000-0001-5433-6448*
Hrynchak Nataliia A. *– PhD (Economics), Associate Professor, Head of the Department of Statistics and Mathematical Methods in Economics, The National Academy of Statistics, Accounting and Auditing (1 Pidhirna Str., Kyiv, 04107, Ukraine)*
E-mail: *nahrynchak@nasoa.edu.ua*
ORCID: *https://orcid.org/0000-0002-2046-6014*

У XXI столітті дані є одним із ключових ресурсів розвитку цифрової економіки, формуючи основу для функціонування державного управління, бізнесу, науки та суспільства загалом.

Стрімке поширення цифрових технологій, розвиток мережевих комунікацій, електронних сервісів, мобільних платформ, соціальних мереж та інтернету речей супроводжуються безперервним зростанням обсягів інформації, що генерується в цифровому середовищі. За таких умов дані стають не лише об'єктом накопичення, але й стратегічним активом, від якого дедалі більше залежить конкурентоспроможність держав, організацій та окремих суб'єктів економічної діяльності.

Зростання обсягів, різноманітності та швидкості надходження інформації сприяло формуванню концепції Big Data, яка стала однією з ключових парадигм цифрової епохи.

На відміну від традиційних підходів до роботи з даними Big Data передбачає використання спеціалізованих технологій збирання, зберігання, оброблення та аналізу великих масивів структурованої та неструктурованої потокової інформації. Водночас цінність даних визначається не лише їхнім обсягом, а й можливістю перетворення інформації у знання, а знань – у практичні рішення. Саме тому сучасні системи управління дедалі активніше інтегрують інструменти Data Science, штучного інтелекту та аналітики великих даних для підтримки процесів прийняття рішень.

Одночасно з розвитком технологій Big Data відбулося й суттєве розширення доступності відкритих джерел інформації. Протягом останніх десятиліть уряди багатьох країн реалізують політику відкритих даних (Open Data), спрямовану на забезпечення прозорості діяльності державних інституцій та підвищення доступності інформаційних ресурсів для громадян, бізнесу та дослідницької спільноти. Відкриті державні реєстри, статистичні бази даних, електронні кадастри, портали відкритих даних, системи електронних закупівель та цифрові сервіси формують нову інформаційну екосистему, у якій накопичуються значні масиви суспільно значущих даних.

Також важливими джерелами цифрової інформації стають соціальні мережі, новинні ресурси, форуми, блоги, геопросторові сервіси, супутникові системи спостереження та різноманітні цифрові платформи. Сукупність таких джерел формує складну багаторівневу екосистему відкритих даних, що характеризується високою динамічністю, різноманітністю форматів та значним аналітичним потенціалом. У такому середовищі активно розвивається концепція OSINT (*Open Source Intelligence*), яка передбачає систематичне збирання, інтеграцію, перевірку та аналіз інформації з відкритих джерел з метою отримання нових знань і формування аналітичних висновків.

OSINT, або розвідка на основі відкритих джерел, – це не нова ідея. Вона виникла ще на початку 1900-х років, під час Першої світової війни, коли країни почали аналізувати публічну інформацію, таку як газети та радіопередачі, для збирання тих чи інших відомостей про об'єкт зацікавлення.

Під час Другої світової війни розвідник Вільям Донован заснував Управління стратегічних служб, яке згодом стало Центральним розвідувальним управлінням (ЦРУ) – службою зовнішньої розвідки США. У цій організації спеціальний підрозділ мав завдання аналізувати загальнодоступну інформацію та збирати необхідні дані з газет, журналів та радіопередач з усього світу [1].

Пізніше OSINT набула більш офіційного статусу завдяки створенню такої структури, як Служба відстеження іноземного мовлення (FBIS) у США, діяльність якої була розгорнута для моніторингу та аналізу зарубіжних радіопрограм.

З поширенням інтернетизації обсяг доступної інформації колосально зріс, що зробило OSINT надзвичайно важливим елементом сучасної розвідувальної діяльності [2].

У сучасних умовах OSINT суттєво виходить за межі традиційного розуміння інструменту інформаційного пошуку або розвідувальної діяльності. Завдяки інтеграції з технологіями Data Science, Big Data та штучного інтелекту OSINT поступово трансформувався в комплексну аналітичну систему роботи з великими масивами різнорідних даних. Використання алгоритмів обробки природної мови, комп'ютерного бачення, автоматизованого аналізу соціальних мереж, геопросторової аналітики та великих мовних моделей дозволяє здійснювати аналіз інформації в режимі реального часу, виявляти приховані закономірності, прогнозувати тенденції та підтримувати процеси прийняття рішень у різних сферах діяльності.

Особливого значення в OSINT набувають відкриті державні реєстри та набори відкритих даних. На відміну від значної частини контенту соціальних медіа, який характеризується високою варіативністю, неструктурованістю та ризиками дезінформації, реєстрові дані зазвичай мають формалізований характер, регулярно оновлюються та забезпечують вищий рівень достовірності. У зв'язку з цим відкриті реєстри можуть розглядатися як важливий інструмент інтеграції традиційних підходів офіційної статистики із сучасними технологіями OSINT-аналітики. Більше того, розвиток електронного урядування поступово трансформує державні реєстри з адміністративних інформаційних систем у важливий компонент цифрової аналітичної інфраструктури.

Особливої актуальності питання розвитку OSINT-аналітики набули в умовах російсько-української війни. Війна в Україні стала одним із найбільш досліджуваних прикладів використання відкритих джерел інформації в сучасних збройних конфліктах. Також наголошується на суттєвому зростанні ролі відкритої розвідки в документуванні воєнних подій, перевірці інформації, протидії дезінформації та аналізі ситуації на полі бою [3; 4].

Крім того, відкриті джерела активно використовуються для документування воєнних злочинів, фіксації руйнувань інфраструктури, моніторингу гуманітарної ситуації та формування доказової бази для міжнародних розслідувань [5].

Водночас розширення використання відкритих даних супроводжується низкою викликів, пов'язаних із достовірністю інформації, інформаційним перевантаженням, алгоритмічними викривленнями, поширенням фейків, використанням бот-мереж і ризиками маніпуляції суспільною думкою. У цих умовах ефективність OSINT визначається не лише обсягом доступної інформації, а й здатністю інтегрувати різнорідні джерела даних, оцінювати їхню надійність і трансформувати потоки даних у релевантні аналітичні висновки для підтримки процесів прийняття рішень.

Аналіз останніх досліджень та публікацій. Палата представників США свого часу визначила OSINT як розвіддані, вироблені з публічно доступної інформації, які збираються, опрацьовуються та поширюються своєчасно для відповідної аудиторії з метою задоволення конкретної розвідувальної потреби.

Пуйвельде Д. і Табарес Рієнсі Ф. пояснювали OSINT як сукупність практик, що включають збір, перевірку та використання загальнодоступних даних та інформації для задоволення інформаційних потреб [6].

Гіоні Р. та ін. стверджували, що розвідка на основі відкритих джерел становить від 70% до 90% усіх сучасних розвідувальних матеріалів. Таким чином, OSINT здатний задовольнити більшість інформаційних потреб правоохоронних органів та розвідувальних служб [7].

Європейський союз трактує поняття OSINT як «практику збирання та аналізу інформації, отриманої з відкритих джерел, для створення практичних розвідувальних даних». Зазначаючи при цьому, що «ці розвідувальні дані можуть бути корисними, наприклад, для національної безпеки, правоохоронних органів та бізнес-розвідки». Також у публікації [8] представлені шість категорій інформаційних потоків відкритих джерел, які доцільно використовувати для OSINT-розслідувань:

- *суспільні ЗМІ* (друковані газети, журнали та телебачення);
- *інтернет* (онлайн-видання та блоги, дискусійні групи, такі як форуми, та соціальні мережі);
- *дані державного управління* (звіти, бюджети, інформація з прес-конференцій, слухання та промови);
- *академічні публікації* (наукові журнали, конференції, дисертації та ін.);
- *комерційні дані* (комерційні зображення, фінансові оцінки, а також різноманітні бази даних);
- *«сіра» література* (технічні звіти, патенти, ділова документація, неопубліковані роботи та інформаційні бюлетені).

Разом із тим, концепція OSINT характеризується певною методологічною специфікою, оскільки передбачає отримання нових знань про об'єкти дослідження шляхом аналізу відкритої інформації.

Міністерство оборони США (наразі – Міністерство війни США) класифікувало п'ять основних розвідувальних дисциплін на основі використовуваних для розвідки джерел інформації:

- *HUMINT (розвідка, отримана з використанням людських ресурсів)* – у сфері громадської безпеки та військової справи HUMINT є цінним інструментом для збирання інформації, яку неможливо отримати іншими способами [9], передбачає збирання інформації, недоступної для інших методів, від ключових осіб – офіцерів, агентів чи інформаторів;
- *IMINT (розвідка зображень)* – розвідувальні дані збираються за допомогою аеро/супутникових знімків та геопросторової інформації;
- *SIGINT (сигнальна розвідка)* – розвідувальні дані збираються шляхом перехоплення та аналізу електромагнітних сигналів;
- *MASINT (вимірювальний і сигнатурний інтелект)* – використання датчиків, сенсорів, спектрометрів тощо з метою документування фізичних параметрів об'єкта, що підтверджує або спростовує інформацію з відкритих джерел;
- *OSINT (розвідка з відкритих джерел)* – розвідувальна інформація, зібрана з різних джерел, доступних широкому загалу, таких як засоби масової інформації, комерційна інформація та візуальні зображення, офіційні урядові звіти, експертні звіти та соціальні мережі [10].

Дортон С. та ін. у своїй роботі [11], з-поміж іншого, наголошують, що всі джерела, які використовуються в межах збирання інформації, потрібно тріангулювати, тобто інформація, знайдена в одному джерелі, повинна бути підтверджена іншим джерелом, щоб уникнути упередженості або дезінформації та полегшити контекстуальне розуміння даних. Тому, незважаючи на значний потенціал, використання OSINT пов'язане з ризиками інформаційного шуму, дезінформації, deepfake-технологій, алгоритмічної упередженості та нерепрезентативності окремих джерел.

Незважаючи на значну кількість досліджень у сфері Big Data, Data Science та цифрової аналітики, більшість наукових праць розглядають OSINT переважно як інструмент кібербезпеки, журналістських розслідувань або інформаційної розвідки. Водночас недостатньо дослідженими залишаються питання інтеграції OSINT у екосистему Big Data, використання відкритих державних реєстрів як джерела аналітичної інформації, а також роль OSINT у підтримці процесів прийняття управлінських рішень на основі великих даних. Це зумовлює необхідність формування комплексного наукового підходу до розуміння OSINT як складової сучасної цифрової аналітичної інфраструктури.

Метою статті є дослідження місця та ролі OSINT-аналітики в екосистемі Big Data, розроблення концептуальної моделі інтеграції відкритих джерел даних, технологій Data Science та статистичних методів у процес підтримки прийняття управлінських рішень, а також обґрунтування практичного значення OSINT в умовах цифрового суспільства та сучасних безпекових викликів, зокрема російсько-української війни.

Методологічною основою дослідження стали методи системного аналізу, структурно-логічного моделювання, порівняльного аналізу наукових підходів до OSINT, Big Data та Data Science, а також концепція DIKW.

Результати. Аналіз наукових джерел дозволяє стверджувати, що сучасна OSINT-аналітика поступово еволюціонує від інструменту пошуку інформації до важливого елемента цифрової аналітичної інфраструктури.

Водночас у науковій літературі недостатньо уваги приділено поясненню того, яким чином відкриті дані проходять шлях від первинних інформаційних масивів до формування знань та обґрунтованих управлінських рішень. Для усунення зазначеної прогалини та відображення логіки взаємодії між відкритими джерелами даних, OSINT, аналітичними технологіями та процесом прийняття рішень запропоновано авторську концептуальну модель, представлену на *рис. 1*.

Запропонована модель частково ґрунтується на концепції DIKW (Data – Information – Knowledge – Wisdom) [12], відповідно до якої процес прийняття рішень розглядається як послідовна трансформація даних у знання. У запропонованому підході OSINT виконує функцію переходу від даних до інформації, тоді як аналітичні технології забезпечують формування знань і аналітичних висновків.

На рис. 1 представлено авторську концептуальну модель інтеграції OSINT-аналітики у процес трансформації відкритих даних в управлінські рішення. Модель відображає послідовний ланцюг перетворення даних на знання та демонструє функціональне місце OSINT між відкритими джерелами інформації та сучасними аналітичними технологіями.

В основі моделі знаходяться відкриті джерела даних, які розглядаються як складова екосистеми Big Data. До них віднесено відкриті державні реєстри, соціальні медіа, супутникові дані, геопросторові ресурси, вебресурси та цифрові платформи. Саме ці джерела формують інформаційну основу сучасної OSINT-аналітики та забезпечують доступ до значних масивів структурованих і неструктурованих даних. Водночас модель акцентує увагу на

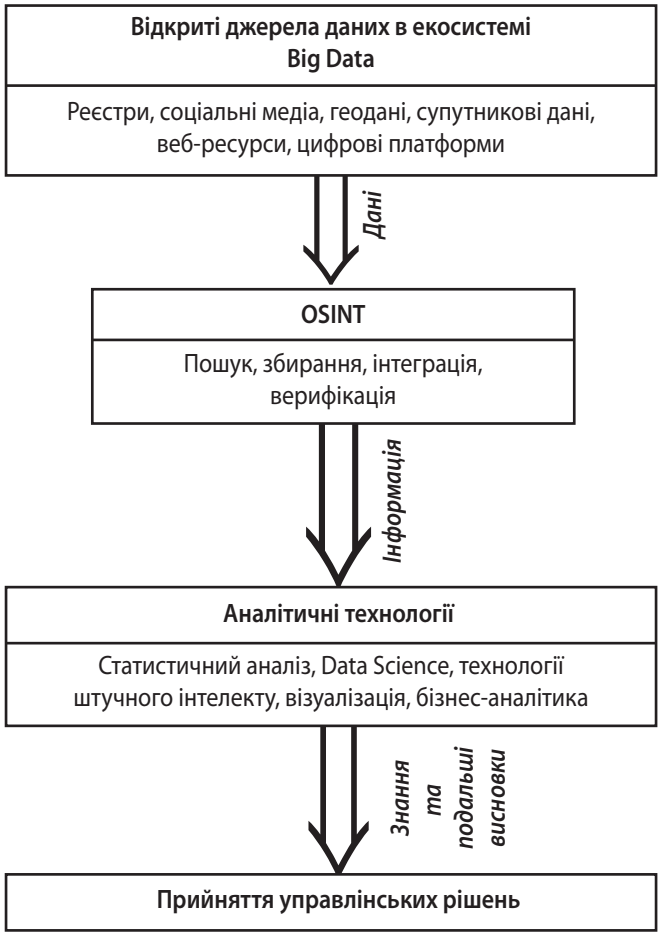

Рис. 1. Концептуальна модель інтеграції OSINT у процес підтримки прийняття рішень

Джерело: авторська розробка.

тому, що предметом OSINT виступає не вся екосистема Big Data, а лише її відкрита частина, доступна для законного збору та використання.

Першим етапом аналітичного процесу є формування масиву даних (*Data*), які надходять із відкритих джерел. На цьому рівні інформація існує у вигляді окремих фактів, повідомлень, записів реєстрів, геопросторових координат, мультимедійного контенту або статистичних показників. Незважаючи на значний обсяг і різноманітність, такі дані ще не мають достатньої аналітичної цінності для підтримки прийняття рішень.

Центральне місце в моделі займає *OSINT*, який розглядається не як окрема технологія аналізу даних, а як методологія роботи з відкритою інформацією. До основних функцій OSINT віднесено: пошук, збирання, інтеграцію та верифікацію даних. Саме на цьому етапі відбувається відбір релевантної інформації, її перевірка на достовірність, усунення дублювання та поєднання даних із різних джерел. У результаті первинні дані трансформуються в інформацію (*Information*), яка вже може бути використана для подальшого аналітичного опрацювання. Таким чином, OSINT виступає інтеграційною ланкою між відкритими джерелами даних та інструментами цифрової аналітики.

Наступний рівень моделі представлений сукупністю *аналітичних технологій*, до яких належать статистичний аналіз, Data Science, технології штучного інтелекту, машинне навчання, засоби візуалізації та бізнес-аналітики. На відміну від OSINT, який забезпечує формування якісної інформаційної бази, аналітичні технології виконують функції виявлення закономірностей, побудови моделей, прогнозування, класифікації, кластеризації та візуалізації результатів аналізу. Саме на цьому етапі відбувається перехід від інформації до знань (*Knowledge*), що характеризуються виявленням нових закономірностей, взаємозв'язків та аналітичних інтерпретацій.

Особливістю запропонованої моделі є виокремлення категорії «висновки», яка виступає проміжною ланкою між знаннями та управлінськими рішеннями. Це дозволяє врахувати той факт, що знання самі по собі не завжди безпосередньо трансформуються в рішення. Для

прийняття управлінських рішень необхідне формування інтерпретованих висновків, орієнтованих на конкретні цілі, ризики та потреби суб'єкта управління. У такому контексті висновки можна розглядати як результат інтелектуального опрацювання знань та їх адаптації до потреб процесу управління.

Завершальним етапом моделі є *прийняття управлінських рішень*. Таким чином, запропонована концепція відображає повний цикл трансформації відкритих даних у практичні управлінські рішення через послідовність:

Дані → Інформація → Знання → Висновки → Управлінські рішення

На відміну від традиційних підходів, у яких OSINT розглядається переважно як інструмент інформаційного пошуку або розвідки, запропонована модель дозволяє інтерпретувати його як важливий елемент сучасної аналітичної інфраструктури, що забезпечує інтеграцію відкритих даних екосистеми Big Data з інструментами Data Science, штучного інтелекту та аналітичної підтримки прийняття рішень.

Практична значущість запропонованої концептуальної моделі особливо яскраво проявляється в умовах російсько-української війни, яка стала безпрецедентним прикладом використання відкритих даних для забезпечення національної безпеки та підтримки процесів прийняття рішень. На відміну від більшості попередніх воєнних конфліктів, сучасна війна супроводжується постійним генеруванням величезних обсягів цифрової інформації, що надходить із соціальних мереж, супутникових систем спостереження, геоінформаційних сервісів, електронних реєстрів, платформ моніторингу повітряної обстановки та інших відкритих джерел.

Російсько-українська війна стала підґрунтям для формування масштабних OSINT-масивів даних. Так, Й. Ніу та ін. за період із січня 2022 р. по липень 2023 р. за допомогою соціальної мережі Twitter (нині – X) було сформовано новий OSINT-датасет щодо російсько-української війни, який ґрунтується на початковому пошуку користувачів, які публікували OSINT-матеріали, та подальшому підході «снігової кулі» для виявлення інших авторів. Фінальний датасет містить майже 2 млн твітів, опублікованих 1040 користувачами [13] та відкривають можливості для застосування статистичних методів аналізу великих даних, мережевої аналітики та виявлення дезінформаційних кампаній.

У цих умовах OSINT виступає механізмом оперативного збирання та верифікації інформації, тоді як статистичні методи забезпечують її узагальнення, аналіз, кількісну оцінку невизначеності, перевірку гіпотез, оцінювання достовірності інформації та трансформацію у знання, придатні для прийняття управлінських рішень. Водночас ефективність використання відкритих даних у сфері національної безпеки визначається не лише наявністю інформації, а й можливістю застосування до неї відповідних статистичних і аналітичних методів. Різноманітність джерел OSINT обумовлює необхідність використання широкого спектра інструментів аналізу – від класичних статистичних методів до сучасних технологій штучного інтелекту, машинного навчання та мережевої аналітики. Узагальнення можливих напрямів використання відкритих даних, відповідних методів аналізу та їхнього прикладного значення для підтримки управлінських рішень у сфері національної безпеки наведено в *табл. 1*.

Зазначене в табл. 1 свідчить про міждисциплінарний характер сучасної OSINT-аналітики, яка поєднує методи статистики, Data Science, геоінформаційного аналізу, комп'ютерного бачення та штучного інтелекту. Аналіз представлених напрямів використання OSINT дозволяє виокремити кілька ключових тенденцій. Зокрема, переважна більшість завдань пов'язана з опрацюванням великих масивів різнорідних даних, що обумовлює необхідність застосування автоматизованих методів аналізу. Суттєве значення мають просторово-часові аспекти інформації, що пояснює активне використання геостатистичних підходів, аналізу часових рядів та геоінформаційних систем. Також важливою складовою сучасного інформаційного простору є аналіз соціальних медіа і цифрових комунікацій, де ключову роль відіграють методи мережевого аналізу, кластеризації та обробки природної мови.

Таким чином, статистичні методи в системі OSINT виконують не допоміжну, а системоутворювальну функцію, забезпечуючи перехід від масивів відкритих даних до знань, прогнозів та управлінських рішень в умовах високої невизначеності та динамічності безпекового середовища.

Одним із прикладів використання статистичних методів є аналіз часових рядів повідомлень із відкритих джерел. Узагальнення інформації про ракетні удари, активність безпілотних літальних апаратів, переміщення військової техніки або інтенсивність інформаційних кампаній дозволяє виявляти закономірності, сезонність, циклічність та аномалії, які можуть бути використані для прогнозування подальшого розвитку подій.

Важливу роль відіграє просторова статистика та геоаналітика. В умовах бойових дій критично важливим є доступ до достовірної та актуальної інформації, яка слугує основою для ухвалення оперативних рішень [14]. Використання супутникових знімків, геопросторових сервісів і відкритих кар-

Таблиця 1

Статистичний аналіз та інші аналітичні методи до використання OSINT-даних у системі підтримки рішень у сфері національної безпеки

Напрям використання OSINT	Джерела відкритих даних	Статистичний / аналітичний метод	Аналітичне завдання	Аналітичний результат	Потенційна сфера застосування
Моніторинг ракетних атак і повітряних загроз	Повідомлення моніторингових каналів, відкриті карти повітряних тривог, соціальні мережі	Аналіз часових рядів, виявлення аномалій	Виявлення трендів, циклічності та часових закономірностей	Прогнозування інтенсивності атак та оцінювання ризиків	Оперативне реагування, цивільний захист
Аналіз супутникових знімків і геопросторових даних	Супутникові знімки, відкриті картографічні сервіси, геопортали	Просторова статистика, геоінформаційний аналіз	Оцінювання просторового розподілу подій та об'єктів	Виявлення зон концентрації військової активності та змін інфраструктури	Моніторинг бойових дій, оцінювання руйнувань
Виявлення бот-мереж і координованих інформаційних кампаній	Соціальні мережі, месенджери, форуми	Мережевий аналіз (Social Network Analysis)	Дослідження структури взаємодії між акаунтами	Ідентифікація координованих мереж впливу та ботів	Інформаційна безпека, протидія дезінформації
Аналіз повідомлень соціальних мереж	Telegram, X, Facebook, YouTube та інші новинні ресурси	Методи NLP, кластеризація, тематичне моделювання	Виявлення тематичних груп, наративів та емоційних патернів	Ідентифікація інформаційних операцій та дезінформаційних кампаній	Стратегічні комунікації, інформаційна політика
Оцінювання безпекових ризиків	Комплексні OSINT-масиви даних	Прогностичне моделювання, сценарний аналіз	Прогнозування розвитку подій та оцінювання ризиків	Формування прогнозних сценаріїв та оцінка ймовірних наслідків	Підтримка управлінських рішень
Аналіз військової активності противника	Фото- та відеоматеріали, супутникові дані, повідомлення очевидців	Комп'ютерне бачення, класифікація об'єктів, статистичне узагальнення	Ідентифікація техніки та оцінювання інтенсивності переміщень	Виявлення змін у дислокації сил і засобів	Ситуаційна обізнаність
Документування воєнних злочинів	Фото, відео, геопросторові дані, відкриті реєстри	Геолокаційний аналіз, просторово-часова верифікація	Підтвердження фактів і встановлення просторово-часових зв'язків	Формування доказової бази	Міжнародні розслідування
Моніторинг гуманітарної ситуації	Відкриті державні реєстри, гуманітарні платформи, соціальні мережі	Описова статистика, аналіз динаміки показників	Оцінювання змін соціально-економічної ситуації	Виявлення кризових територій та груп населення	Гуманітарне реагування
Аналіз економічної безпеки	Відкриті реєстри підприємств, закупівель, санкційні списки	Кореляційний аналіз, кластеризація, мережевий аналіз	Виявлення прихованих зв'язків та аномалій	Ідентифікація ризикових суб'єктів та схем	Фінансовий моніторинг, санкційна політика
Моніторинг інформаційного середовища	Новинні ресурси, соціальні мережі, блоги	Контент-аналіз, аналіз тональності (sentiment analysis)	Оцінювання суспільних настроїв та інформаційних тенденцій	Виявлення інформаційних загроз та змін громадської думки	Стратегічне планування та кризові комунікації

Джерело: сформовано авторами.

тографічних ресурсів дає можливість здійснювати статистичне оцінювання просторової концентрації військової активності, виявляти зміни в розташуванні техніки, оцінювати масштаби руйнувань інфраструктури та аналізувати територіальні закономірності розвитку бойових дій.

Суттєве значення мають також методи мережевого аналізу, які використовуються для дослідження інформаційного простору. Аналіз структури взаємодії між акаунтами в соціальних мережах дозволяє виявляти координовані інформаційні кампанії, бот-мережі та центри поширення дезінформації. У цьому випадку статистичні показники центральності, щільності мережі та інтенсивності комунікацій виступають індикаторами потенційних інформаційних загроз.

Кластерний аналіз та алгоритми машинного навчання забезпечують можливість автоматизованого групування великих масивів повідомлень за тематикою, джерелами походження або характеристиками інформаційного впливу. Це дозволяє значно підвищити ефективність OSINT-аналітики в умовах інформаційного перевантаження та зростання обсягів цифрових даних.

Робота з великими обсягами даних дає змогу за допомогою штучного інтелекту робити певні висновки: з переміщення військ, інтенсивності бойових дій, а також з ідентифікації об'єктів. Штучний інтелект має розпізнавати військові та цивільні об'єкти, медичну службу, пресу за фото і відео, до того ж за лічені секунди [15]. Незалежно від конкретного програмного забезпечення чи джерела надходження інформації ключовим елементом таких систем залишається статистичне узагальнення, оцінювання ризиків, виявлення закономірностей та прогнозування розвитку ситуації.

У цьому контексті OSINT доцільно розглядати не лише як інструмент отримання інформації, а як важливий елемент сучасної системи data-driven security, у якій статистичні методи, технології Data Science та штучного інтелекту забезпечують перетворення відкритих даних на аналітичні висновки для підтримки управлінських рішень у сфері національної безпеки. У цих умовах статистика перестає виконувати виключно функцію опису даних і трансформується в інструмент оперативного виявлення закономірностей, оцінювання ризиків, прогнозування подій та забезпечення ситуаційної обізнаності у сфері національної безпеки.

ВИСНОВКИ

У результаті дослідження встановлено, що в умовах цифрової трансформації суспільства OSINT виходить за межі традиційного інструменту інформаційного пошуку та перетворюється на важливий елемент сучасної аналітичної інфраструктури. Відкриті джерела даних формують значну частину екосистеми Big Data та створюють інформаційну основу для здійснення аналітичних досліджень у державному управлінні, бізнесі та сфері національної безпеки. Запропонована концептуальна модель інтеграції OSINT у процес підтримки прийняття рішень демонструє послідовність трансформації відкритих даних в інформацію, знання, аналітичні висновки та управлінські рішення. Доведено, що ключову роль у цьому процесі відіграють статистичні методи, які забезпечують узагальнення, верифікацію, моделювання та інтерпретацію даних.

Російсько-українська війна стала одним із перших масштабних прикладів практичної інтеграції OSINT, Big Data, геопросторової аналітики, штучного інтелекту та статистичних підходів у єдину систему підтримки рішень. Це підтверджує перспективність використання OSINT як складової сучасних data-driven систем управління та безпеки. ■

БІБЛІОГРАФІЯ

1. Colquhoun C. A Brief History of Open Source Intelligence. *Bellingcat*. 2016. URL: https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/
2. Gurbanov M., Gurbanova G., Mikayilli G. et al. AI for OSINT: Challenges, opportunities, and future directions. In: *Proceedings of the 9th International Azerbaijan Congress on Life, Engineering, Mathematical, and Applied Sciences*. 2024. P. 1524–1530. URL: https://bib.opensourceintelligence.biz/STORAGE/2024.%20ai%20for%20osint.pdf
3. Van Puyvelde D. Open-source research and the war in Ukraine: Intelligence for the people by the people? *Leiden University*. 2023–2024. URL: https://www.universiteitleiden.nl/en/research/research-projects/governance-and-global-affairs/open-source-research-and-the-war-in-ukraine-intelligence-for-the-people-by-the-people
4. Fleischman A. Effective Use of OSINT in the Russo-Ukrainian War: Collection and Disclosure of Reliable Information along with Refuting False Information. *American Intelligence Journal*. 2022. Vol. 39. Iss. 2. P. 66–79. URL: https://www.jstor.org/stable/27369383
5. Toler A. How Ukraine is Crowdsourcing Digital Evidence of War Crimes. *UC Berkeley*. 2022, April 19. URL: https://humanrights.berkeley.edu/hrc-in-the-news/how-ukraine-is-crowdsourcing-digital-evidence-of-war-crimes/
6. Van Puyvelde D., Tabárez Rienzi F. The rise of open-source intelligence. *European Journal of International Security*. 2025. Vol. 10. Iss. 4. P. 530–544. DOI: https://doi.org/10.1017/eis.2024.61

7. Ghioni R., Taddeo M., Floridi L. Open source intelligence and AI: A systematic review of the GELSI literature. *AI & Society*. 2023. Vol. 39. Iss. 4. P. 1827–1842. DOI: https://doi.org/10.1007/s00146-023-01628-x
8. European data. What is OSINT: Open-source intelligence? *European Union*. 2022, May 2. URL: https://data.europa.eu/en/publications/datastories/what-osint-open-source-intelligence
9. Trisolini M. Intelligence di polizia: Le forze dell'ordine come human sensors. *Società Italiana di Intelligence*. 2020. DOI: https://doi.org/10.36182/2020.14
10. Scuro V. Open-Source Intelligence (OSINT) for Researchers and Practitioners. In: Smith E., Austin S. (eds). *Researching a Rigged Game: Digital Approaches to Tracing the Illicit Trade in Cultural Objects. Studies in Art, Heritage, Law and the Market*. 2026. Vol. 11. DOI: https://doi.org/10.1007/978-3-032-02014-7_2
11. Dorton S. L., Frommer I. D., Garrison T. M. A Theoretical Model for Assessing Information Validity from Multiple Observers. In: *2019 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)* (8–11 April 2019). P. 52–58. DOI:https://doi.org/10.1109/COGSIMA.2019.8724242
12. Baskarada S., Koronios A. Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension. *Australasian Journal of Information Systems*. 2013. Vol. 18. Iss. 1. P. 5–24. DOI: https://doi.org/10.3127/ajis.v18i1.748
13. Niu J., Stillman M., Seeberger P., Kruspe A. A Dataset of Open Source Intelligence (OSINT) Tweets about the Russo-Ukrainian War. In: *Proceedings of the 21st International Conference on Information Systems for Crisis Response and Management (ISCRAM 2024)*. DOI: https://doi.org/10.59297/377r3945
14. Кобзан С. М., Поморцева О. Є., Паньків В. В. та ін. Військові геоінформаційні системи. Шляхи застосування та перспективи розвитку. *Випробування та сертифікація*. 2025. № 1. С. 67–75. DOI: https://doi.org/10.37701/ts.07.2025.08
15. Кобзан С. М., Поморцева О. Є., Паньків В. В., Андронов В. В. Погляди щодо побудови геоінформаційної системи для використання у Збройних Силах України. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України*. 2024. № 3. С. 40–46. DOI: https://doi.org/10.33099/2304-2745/2024-3-83/40-46

REFERENCES

Baskarada S. & Koronios A. (2013). Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension. *Australasian Journal of Information Systems, 1*(18), 5–24. https://doi.org/10.3127/ajis.v18i1.748

Colquhoun C. (2016). A Brief History of Open Source Intelligence. *Bellingcat*. https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/

Dorton S. L., Frommer I. D. & Garrison T. M. (2019). A Theoretical Model for Assessing Information Validity from Multiple Observers. *2019 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)* (p. 52–58). https://doi.org/10.1109/COGSIMA.2019.8724242

European Union. (2022, May 2). *What is OSINT: Open-source intelligence?* https://data.europa.eu/en/publications/datastories/what-osint-open-source-intelligence

Fleischman A. (2022). Effective Use of OSINT in the Russo-Ukrainian War: Collection and Disclosure of Reliable Information along with Refuting False Information. *American Intelligence Journal, 2*(39), 66–79. https://www.jstor.org/stable/27369383

Ghioni R., Taddeo M. & Floridi L. (2023). Open source intelligence and AI: A systematic review of the GELSI literature. *AI & Society, 4*(39), 1827–1842. https://doi.org/10.1007/s00146-023-01628-x

Gurbanov M., Gurbanova G. & Mikayilli G. (2024). AI for OSINT: Challenges, opportunities, and future directions. *Proceedings of the 9th International Azerbaijan Congress on Life, Engineering, Mathematical, and Applied Sciences* (p. 1524–1530). https://bib.opensourceintelligence.biz/STORAGE/2024.%20ai%20for%20osint.pdf

Kobzan S. M., Pomortseva O. Ye. & Pankiv V. V. (2025). Viiskovi heoinformatsiini systemy. Shliakhy zastosuvannia ta perspektyvy rozvytku [Military geographic information systems. Ways of application and prospects for development]. *Vyprobuvannia ta sertyfikatsiia, 1*, 67–75. https://doi.org/10.37701/ts.07.2025.08

Kobzan S. M., Pomortseva O. Ye., Pankiv V. V. & Andronov V. V. (2024). Pohliady shchodo pobudovy heoinformatsiinoi systemy dlia vykorystannia u Zbroinykh Sylakh Ukrainy [Views on building a geographic information system for use in the Armed Forces of Ukraine]. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy, 3*, 40–46. https://doi.org/10.33099/2304-2745/2024-3-83/40-46

Niu J., Stillman M., Seeberger P. & Kruspe A. (2024). A Dataset of Open Source Intelligence (OSINT) Tweets about the Russo-Ukrainian War. *Proceedings of the 21st International Conference on Information Systems for Crisis Response and Management (ISCRAM 2024)*. https://doi.org/10.59297/377r3945

Scuro V. (2026). Open-Source Intelligence (OSINT) for Researchers and Practitioners. *Researching a Rigged Game: Digital Approaches to Tracing the Illicit Trade in Cultural Objects*. https://doi.org/10.1007/978-3-032-02014-7_2

Toler A. (2022, April 19). How Ukraine is Crowdsourcing Digital Evidence of War Crimes. *UC Berkeley*. https://humanrights.berkeley.edu/hrc-in-the-news/how-ukraine-is-crowdsourcing-digital-evidence-of-war-crimes/

Trisolini M. (2020). Intelligence di polizia: Le forze dell'ordine come human sensors. *Società Italiana di Intelligence*. https://doi.org/10.36182/2020.14

Van Puyvelde D. & Tabárez Rienzi F. (2025). The rise of open-source intelligence. *European Journal of International Security, 4*(10), 530–544. https://doi.org/10.1017/eis.2024.61

Van Puyvelde D. (2023). Open-source research and the war in Ukraine: Intelligence for the people by the people? *Leiden University*. https://www.universiteitleiden.nl/en/research/research-projects/governance-and-global-affairs/open-source-research-and-the-war-in-ukraine-intelligence-for-the-people-by-the-people

Дослідження не отримувало зовнішнього фінансування.
Автори заявляють про відсутність конфлікту інтересів.
Інструменти ШІ не застосовувалися при написанні статті.

Стаття надійшла до редакції / Received: 07.06.2026
Статтю прийнято до публікації / Accepted: 20.06.2026
Оприлюднено / Published: 30.07.2026

УДК 338.2:004.9
JEL: O10; O33; O38
DOI: https://doi.org/10.32983/2222-4459-2026-6-95-105

СТРАТЕГІЧНІ МОДЕЛІ УПРАВЛІННЯ ЦИФРОВОЮ ТРАНСФОРМАЦІЄЮ ЕКОНОМІЧНИХ СИСТЕМ ДЕРЖАВИ

©2026 **МІЩЕНКО В. А.**

УДК 338.2:004.9
JEL: O10; O33; O38

Міщенко В. А. Стратегічні моделі управління цифровою трансформацією економічних систем держави

У сучасних умовах прискореної цифровізації економічних систем держави зберігається суттєва наукова прогалина, що полягає у відсутності цілісних інтегрованих підходів до формування стратегічних моделей управління цифровою трансформацією на макрорівні. Існуючі дослідження переважно фокусуються на окремих аспектах цифрового розвитку – цифровому урядуванні, платформних рішеннях або трансформації підприємств, однак недостатньо висвітлюють системну взаємодію між державою, економічними екосистемами та мікрорівнем господарювання. Саме це зумовлює актуальність даного дослідження. Метою статті є теоретичне обґрунтування та систематизація стратегічних моделей управління цифровою трансформацією економічних систем держави, а також розробка інтегрованої багаторівневої моделі цифрового розвитку. У процесі дослідження використано системний, структурно-функціональний і компаративний методи аналізу, а також методи узагальнення наукових підходів до цифрової трансформації та стратегічного управління економічними системами. Результати дослідження дозволили виокремити чотири основні стратегічні моделі цифрової трансформації: ієрархічно-адміністративну, мережеву, платформну та екосистемно-адаптивну. Обґрунтовано, що еволюція цифрового управління відбувається в напрямі переходу від централізованих адміністративних структур до гнучких цифрових екосистем, у яких ключову роль відіграють цифрові платформи, дані та технології штучного інтелекту. Запропоновано інтегровану трирівневу модель управління, що включає макрорівень державного стратегічного управління, мезорівень економічних екосистем і платформ, мікрорівень підприємств і домогосподарств, а також крос-рівневий інтеграційний контур цифрової взаємодії. Наукова новизна полягає у формуванні концептуальної багаторівневої моделі стратегічного управління цифровою трансформацією економічних систем держави, що поєднує інституційний, платформний та екосистемний підходи в єдину аналітичну конструкцію. Практична цінність полягає в можливості застосування запропонованої моделі для розробки державних стратегій цифрового розвитку, удосконалення механізмів цифрового урядування та підвищення ефективності управління національними економічними системами в умовах цифрової економіки.

Ключові слова: *цифрова трансформація; стратегічне управління; економічні системи держави; цифрові платформи; цифрові екосистеми; цифрове урядування; цифрова економіка.*
Табл.: *2.* ***Бібл.:*** *18.*

Міщенко Володимир Артурович *– підприємець, ФОП Харченко В. С. (вул. Дмитра Пругла, 14/2, Полтава, 36019, Україна)*
E-mail: *68mishenko@gmail.com*
ORCID: *https://orcid.org/0009-0007-5853-299X*

UDC 338.2:004.9
JEL: O10; O33; O38

Mishchenko V. A. Strategic Models for Managing the Digital Transformation of State Economic Systems

In the context of accelerated digitalization of national economic systems, a significant research gap is the absence of holistic and integrated approaches to the formation of strategic models for managing digital transformation at the macro level. Existing studies are mainly focused on specific aspects of digital development – such as digital governance, platform solutions, or enterprise transformation – while insufficient attention is paid to the systemic interaction between the State, economic ecosystems, and the micro-level of economic activity. This determines the relevance of the present study. The aim of the article is to provide a theoretical substantiation and systematization of strategic models for managing the digital transformation of national economic systems, as well as to develop an integrated multi-level model of digital development. The study employs systemic, structural-functional, and comparative analysis methods, as well as methods of generalization of scientific approaches to digital transformation and strategic management of economic systems. The results of the study made it possible to identify four main strategic models of digital transformation: hierarchical-administrative, network, platform, and ecosystem-adaptive. It is substantiated that the evolution of digital governance is moving from centralized administrative structures toward flexible digital ecosystems, where digital platforms,