ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ТЕХНІЧНОЇ ДІЯЛЬНОСТІ ПОЛІЦІЇ

УДК 343.98:004.822:351.746 (477)
DOI https://doi.org/10.32782/2709-9261-2025-4-16-30

Габорець Ольга Андріївна,
доктор філософії в галузі освіти, доцент,
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки
Навчально-наукового інституту підготовки фахівців
для підрозділів кримінальної поліції імені Е.О. Дідоренка
(Донецький державний університет внутрішніх справ, м. Кропивницький)
ORCID: https://orcid.org/0000-0001-7791-6795

Волобоєв Артур Олегович,
доктор філософії в галузі права,
начальник відділу організації освітнього процесу
(Донецький державний університет внутрішніх справ, м. Кропивницький)
ORCID: https://orcid.org/0000-0002-7138-5847

ІННОВАЦІЙНІ ПІДХОДИ ДО ВИКОРИСТАННЯ ARTELLENCE У СУЧАСНОМУ КРИМІНАЛЬНОМУ АНАЛІЗІ

У статті здійснено всебічне дослідження функціональних можливостей аналітичної платформи "Artellence", що є прикладом сучасного когнітивного інструменту для кримінального аналізу в цифровому середовищі. Розкрито архітектуру системи, модульний склад і технічні аспекти, зокрема елементи екосистеми "BigDataPeople 2". Описано практичне застосування таких модулів, як фотопошук, семантичне профілювання, побудова графів зв'язків, геопозиціонування, класифікація ідеологічної орієнтації та часовий аналіз цифрової активності. Наведено кейс-аналіз роботи системи в умовах розпізнавання особи за зображенням, побудови аналітичного профілю, визначення взаємодій, а також оцінювання лексичних маркерів та інформаційних кластерів. Висвітлено інтерфейсні рішення та точнісні показники, що підтверджують ефективність інструменту. Визначено потенціал Artellence у побудові доказових гіпотез, верифікації цифрових слідів, оперативній і стратегічній підтримці досудового розслідування та розробленні аналітичних моделей злочинної поведінки з урахуванням міжнародних підходів.

Ключові слова: *кримінальний аналіз, Artellence, Big People 2, BigDataPeople 2, OSINT, аналітична платформа, штучний інтелект, досудове розслідування, кримінальне провадження.*

Постановка проблеми. У сучасних умовах динамічної трансформації форм і методів злочинності – як у структурному, так і у функціональному аспекті – традиційні підходи до кримінального аналізу втрачають свою ефективність. Правоохоронні органи дедалі частіше стикаються з необхідністю оперативного опрацювання гетерогенних джерел інформації, включаючи цифрові сліди, облікові записи в соціальних мережах, дані з відкритих платформ, результати відеоспостереження та інших неструктурованих джерел. У зв'язку із

цим постає об'єктивна потреба в упровадженні високотехнологічних аналітичних систем, здатних до автоматизованого аналізу великих обсягів даних у реальному часі з дотриманням вимог процесуального законодавства.

Особливої актуальності набувають аналітичні платформи, які не лише обробляють інформацію, а й формують на її основі обґрунтовані аналітичні гіпотези, виявляють приховані зв'язки між об'єктами, передбачають імовірні події та ідентифікують ризикові патерни поведінки. У цьому контексті система "Artellence", локалізована для потреб українських правоохоронних структур у партнерстві з компанією "Big People 2" [1], становить приклад технології, яка синтезує алгоритмічну потужність, багатошарову OSINT-аналітику й архітектуру цифрового профілювання суб'єктів. Ця платформа репрезентує перехід від реактивних моделей розслідування до проактивних стратегій превентивної аналітики, що відповідає сучасним тенденціям розвитку правоохоронних систем у країнах Європейського Союзу та Північної Америки.

Однак упровадження таких рішень висуває низку теоретико-методологічних і юридичних викликів. Зокрема, ідеться про допустимість використання автоматизованих засобів у кримінальному процесі, достовірність даних, отриманих без прямої участі людини, а також дотримання принципів справедливого судочинства. Як результат, виникає додаткова проблематика щодо алгоритмічної прозорості – здатності штучного інтелекту (далі – ШІ) надавати зрозумілі пояснення своїх рішень.

Теоретичним підґрунтям для розуміння таких аспектів слугує концепція поліцейської діяльності на основі доказів (evidence-based policing), яку в 1998 р. сформулював Л.В. Шерман [2]. Він обґрунтував необхідність використання найкращих наукових досліджень для ухвалення рішень у правоохоронній сфері замість покладання на традиції або інтуїцію [2, с. 4]. Цей підхід передбачає систематичне застосування емпірично верифікованих методів, що дозволяє підвищити ефективність правоохоронної діяльності та забезпечити її відповідність стандартам доказування. Саме ці аспекти й зумовлюють потребу у ґрунтовному науковому аналізі зазначеної теми дослідження.

Аналіз останніх досліджень та публікацій. Проблематика використання цифрових технологій у кримінальному аналізі останніми роками стала об'єктом інтенсивного міждисциплінарного вивчення як в Україні, так і за кордоном. Особливу увагу дослідників привертають питання методології кримінальної аналітики, допустимості цифрових доказів, етичних меж застосування ШІ у правозастосовній діяльності, а також операційної ефективності аналітичних платформ.

У вітчизняному науковому дискурсі варто відзначити праці І.А. Федчака, який систематизував базові категорії аналітичної діяльності, окреслив завдання, структуру аналітичного процесу та принципи взаємодії між оперативними, аналітичними й слідчими підрозділами [3]. Автор також наголошує на необхідності інтеграції інформаційно-аналітичних платформ у повсякденній діяльності органів Національної поліції України [3, с. 27], з урахуванням принципів інформаційної безпеки [4, с. 96–97].

Поряд з вітчизняними напрацюваннями, міжнародний досвід демонструє активне впровадження аналітичної платформи "Palantir Gotham", що використовується розвідувальними службами Сполучених Штатів Америки та поліцейськими відомствами європейських країн [5]. Ця практика актуалізує питання балансу між ефективністю кримінального аналізу та захистом прав людини.

Окрім того, усе частіше в науковій площині висвітлюються питання, пов'язані з отриманням інформації з відкритих джерел у розслідуванні злочинів, зокрема вчинених у кіберпросторі [6, с. 88–106]. З огляду на це Б. Ахгар, П.С. Баєрл, Ф. Семпсон слушно акцентують на стратегічному підході інтеграції OSINT, наголошують на ключовій відмінності інформації від доказів [7, с. 145–148]. Суть доказів в електронній формі та їх належність до конкретного виду процесуальних джерел у кримінальному провадженні детально розкрито В.М. Фігурським [8]. Автор обґрунтованого дійшов висновку про те, що докази в електронній формі є новим соціально-правовим явищем в інформаційну епоху. Порівняно з доказами в позаелектронній формі, вони мають власну природу, яка зумовлює їхні особливості, потребують іншого механізму доказування, що свідчить про самостійне місце в системі процесуальних джерел доказів [8, с. 97, 100–101].

Питання алгоритмічної прозорості, що є критично важливим для використання ШІ у правоохоронній діяльності, детально розкрила С. Рудін [9]. Науковиця стверджує, що для високоризикових застосувань не варто використовувати непрозорі алгоритми («чорні скриньки»), коли існує інтерпретована модель з порівнянною точністю, оскільки пояснення результатів роботи «чорних скриньок» post factum є принципово недостатнім [9, с. 206–210].

Міжнародні стандарти етичного використання ШІ також відіграють важливу роль у регулюванні аналітичних платформ. Рекомендація UNESCO щодо етики ШІ встановлює ключові принципи: повагу до прав людини й людської гідності, прозорість, підзвітність, багатостороннє управління та нагляд людини над системами ШІ [10], а керівні принципи Ради Європи щодо розпізнавання облич наголошують на конкретних заходах для забезпечення дотримання принципів захисту даних [11, с. 17].

Правову рамку для масштабних систем спостереження визначив Європейський суд з прав людини у справі "Big Brother Watch v. UK" (заяви № № 58170/13, 62322/14 та 24960/15) [12], встановивши необхідність «наскрізних гарантій»: незалежної авторизації, контролю пропорційності й ефективних засобів правового захисту. Рішення підкреслює, що законність масового спостереження залежить від існування чітких процесуальних гарантій [12, § § 334–362].

Попри збільшення кількості публікацій, досі відсутнє комплексне дослідження, яке б узагальнювало функціональні, юридичні й аналітичні характеристики платформи "Artellence" як конкретного прикладу впровадження цифрової аналітики у кримінальний процес України. Саме ця прогалина зумовлює актуальність і наукову доцільність нашого дослідження.

Метою статті є дослідження інструментальних можливостей аналітичної платформи "Artellence" як прикладу впровадження сучасних цифрових рішень у сферу кримінального аналізу.

Виклад основного матеріалу. Аналітична платформа "Artellence" є інструментом нового покоління в арсеналі кримінального аналізу, що поєднує технології ШІ, мережеву аналітику, OSINT-інструментарій і моделі прогнозування. Вона реалізована як багатокомпонентна цифрова система, орієнтована на аналітичну підтримку досудового розслідування, оперативно-розшукової діяльності й інформаційно-аналітичного забезпечення керівництва підрозділів. Архітектура системи побудована за принципом модульності, що дозволяє поєднувати в єдиному середовищі інструменти пошуку, фільтрації,

верифікації, аналітичного моделювання, прогнозування та генерації візуалізованих звітів. Така архітектура забезпечує гнучкість системи, дозволяє адаптувати її функціонал до спеціальних потреб конкретних правоохоронних органів без необхідності повної реконфігурації платформи.

Згідно з технічною документацією до BigDataPeople 2, яка становить складову частину екосистеми "Artellence", платформа забезпечує автоматизовану обробку відкритих даних із цифрового середовища: соціальних мереж, відеохостингів, месенджерів, публічних баз оголошень і спеціалізованих OSINT-ресурсів [13]. Серед основних модулів платформи варто виділити:

– модуль фотопошуку – забезпечує можливість завантаження зображення та автоматичного виявлення збігів із профілями осіб у відкритому інтернет-просторі на основі алгоритмів комп'ютерного зору та розпізнання біометричних характеристик обличчя;

– модуль профілювання – виконує семантичний аналіз цифрових акаунтів, виявляє належність до ідеологічних груп, зв'язків з іншими суб'єктами, а також динаміку цифрової активності в часовому вимірі з використання методів обробки природної мови (Natural Language Processing – NLP);

– модуль зв'язків – будує графи міжособистісних або організаційних взаємозв'язків на основі спільної участі в інформаційних подіях або просторово-часових перетинів, застосовує алгоритми мережевого аналізу;

– інструмент геопозиціонування – призначений для зіставлення цифрової присутності об'єкта з географічним простором чи часовими межами подій.

Локалізована версія Artellence, адаптована компанією "Big People 2", підтримує український і англомовний інтерфейс, інтегрується з державними реєстрами, аналітичними сервісами, а також дозволяє створення звітів відповідно до вимог кримінального процесуального законодавства. Зазначене робить платформу придатною для використання не лише в рамках процесуальних дій і оперативно-розшукових заходів, а і як інструмент доказової аналітики в межах кримінального провадження.

Практичне застосування Artellence ілюструється кейсом із використанням модуля фотопошуку (рис. 1). Аналітик завантажує фотографію невідомої особи, отриману з місця події. Система в автоматичному режимі проводить зіставлення з базами публічних зображень, після чого формує профіль особи з наявними відкритими даними: акаунтами в соціальних мережах, геотегованими зображеннями, контактними зв'язками.

На наступному етапі виконується побудова мережі з визначенням центральних вузлів, щільності зв'язків і потенційно ризикових контактів. Аналітик отримує візуалізований результат, на основі якого формує аналітичний звіт із зазначенням ступеня достовірності й посиланням на джерела. Такий звіт може бути долучений до матеріалів кримінального провадження як джерело аналітичної інформації, що підлягає подальшій процесуальній перевірці й оцінюванню.

Ключовою перевагою системи є можливість одночасної роботи з великим обсягом цифрових об'єктів і виявлення нелінійних залежностей, які не є очевидними в ручному аналізі. Кожен модуль BigDataPeople 2 має окреме інтерфейсне представлення, оптимізоване для спеціальних аналітичних завдань, де: фотопошук виводить результати як галерею з відповідними посиланнями; модуль зв'язків – як інтерактивний граф з можливістю фільтрації за категоріями (профілі, сторінки, контент); аналітична панель – як таблицю з можливістю сортування, експортом у форматах CSV та PDF; а профільна картка користувача надає зведену інформацію щодо активності, лексики, тем, що домінують, контекстів появи особи, дат і геолокації (рис. 2).

Під час тестування платформи була підтверджена ефективність класифікатора ідеологічної орієнтації – система здатна автоматично ідентифікувати наративи, до яких тяжіє користувач. Це відкриває можливості для поглибленої аналітики соціальних кластерів, деструктивних груп і кримінальних мереж. Класифікатор використовує методи обробки природної мови для виявлення семантичних патернів, характерних для окремих ідеологічних дискурсів. Завдяки цьому Artellence функціонує як когнітивний інструмент, що підтримує ухвалення управлінських рішень, виявлення кримінальних загроз і конструювання доказових гіпотез на основі цифрового середовища.

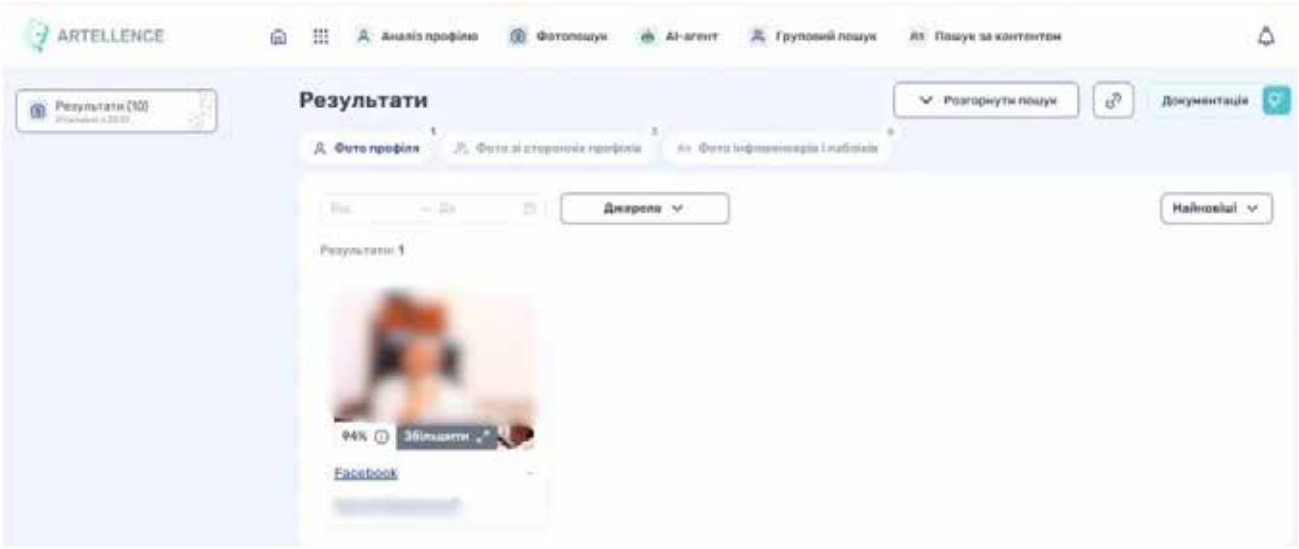

Рис. 1. Результат фотопошуку в Artellence: одиничний збіг із соціальним профілем за зовнішністю, що дозволяє ідентифікувати особу та перейти до пов'язаних відкритих джерел

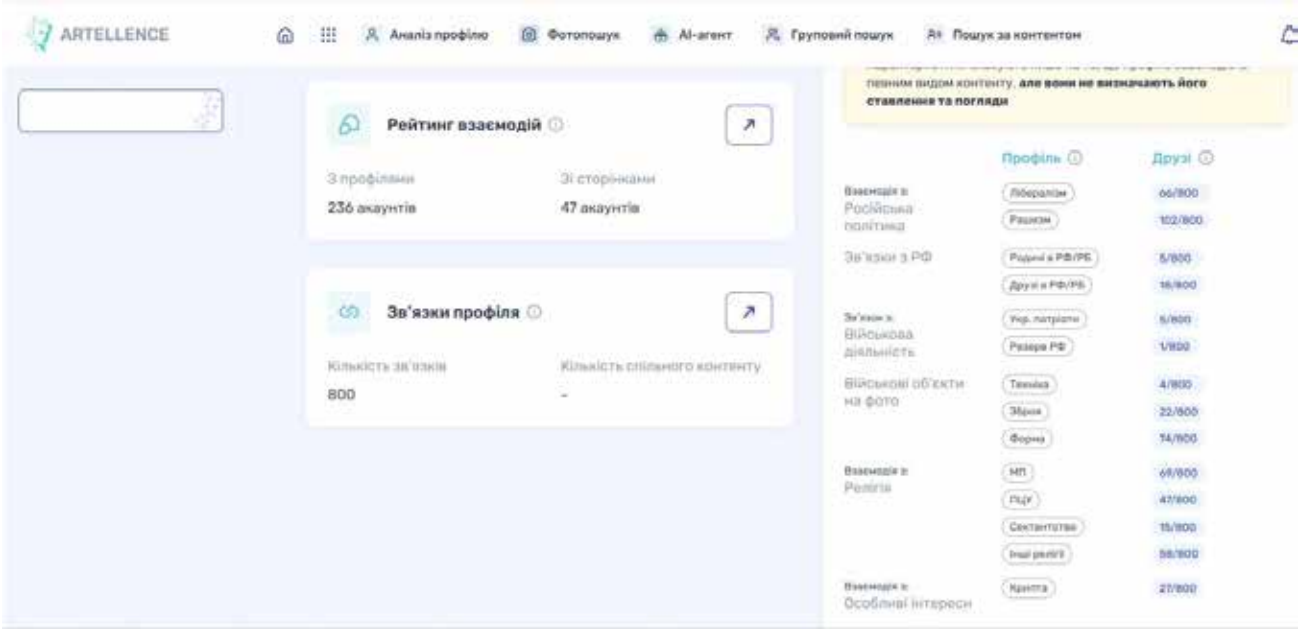

Рис. 2. Інтерфейс Artellence із модулями «Рейтинг взаємодій» та «Зв'язки профілю»: приклад структури цифрової активності об'єкта дослідження за політичними, релігійними та соціальними тематиками

У межах документації до BigDataPeople 2 також визначено важливість використання функціоналу платформи для ідентифікації повторюваних шаблонів поведінки, які можуть свідчити про потенційні загрози. Зокрема, модуль часової лінії активності дозволяє відстежувати динаміку комунікаційної активності суб'єкта впродовж визначеного періоду, фіксувати пікові моменти, типи взаємодії (публікації, поширення, коментарі) та тематику залучених джерел. Це дозволяє виявляти аномальні патерни поведінки, як-от різке зростання активності перед визначеними подіями або синхронізована діяльність групи акаунтів, що може свідчити про координовані дії. Ця інформації створює основу для побудови прогнозу поведінки або гіпотези щодо намірів.

Окрім того, у системі реалізовано можливість оцінювання лінгвістичних маркерів – визначення риторичних патернів, полярності висловлювань, частоти вживання окремих термінів, ключових концептів і фреймів. Такі інструменти є особливо цінними в розслідуваннях злочинів з елементами пропаганди, радикалізації або вербування. Лінгвістичний аналіз базується на побудові словників ключових термінів, що асоціюються з певними типами незаконної діяльності, та виявленні контекстуальних зв'язків між ними.

Платформа підтримує побудову «розширених профілів» – коли в рамках одного об'єкта здійснюється збирання інформації не лише щодо цифрової активності, а й щодо місць роботи, навчання, участі у групах, прив'язки до географічних зон і періодів підвищеної активності. Це дозволяє створити багатовимірну модель суб'єкта, яка значно підвищує якість оцінки його зв'язків і ризиків участі у кримінальній діяльності. Багатовимірність профілю забезпечується інтеграцією даних з гетерогенних джерел і їх консолідацією на основі унікальних ідентифікаторів, що дозволяє формувати цілісне уявлення про об'єкт аналізу.

У сукупності ці чинники свідчать про високий рівень інституційної корисності платформи для кримінальної юстиції України.

Також застосування Artellence уможливлює створення аналітичної моделі злочинної діяльності не лише на рівні окремого інциденту, а й у масштабі групи, регіону чи категорії правопорушень. Наприклад, під час аналізу злочинів, що скоєні в умовах воєнного стану або мають ознаки диверсійної діяльності, система здатна агрегувати дані про інформаційну активність груп користувачів, їхню територіальну локалізацію, реакцію на інформаційні приводи, виявляти ознаки координованих дій. Це дозволяє формувати стратегічні аналітичні продукти для керівництва силових структур.

Окрім того, інтеграція Artellence із системами відеоспостереження та розпізнавання облич дозволяє використовувати платформу для оперативного реагування на події в публічних місцях. У разі фіксації злочину або правопорушення платформа може здійснити ідентифікацію особи за фото- або відеофрагментом, виявити її цифровий слід, уточнити маршрут пересування та ідентифікувати осіб, із якими вона контактувала до або після інциденту.

На особливу увагу заслуговує функція порівняльного аналізу між об'єктами. Аналітик може ініціювати побудову порівняльного профілю двох і більше осіб, з можливістю визначення збігів у поведінці, місцях перебування, спільних контактів, вживаної лексики й ознак участі в тих самих інформаційних кластерах. Такий аналіз є цінним для виявлення фіктивних акаунтів, інформаційних ботів або для підтвердження ознак змови.

Тобто Artellence забезпечує не лише оперативну, а й глибоку аналітичну підтримку в роботі правоохоронних органів, створює умови для переходу від реагування на злочин до його превентивного виявлення.

Практична реалізація цих функцій яскраво ілюструється безпосередньо в інтерфейсі системи. Зокрема, модуль «Рейтинг взаємодій» дозволяє аналітику визначити інтенсивність комунікаційного обміну між об'єктом дослідження та іншими цифровими профілями – у формі таблиці з точними числовими індикаторами реакцій і коментарів. Це дозволяє фіксувати навіть опосередкова-

ні соціальні зв'язки, важливі для побудови мережевих моделей.

Зауважимо, що метрики взаємодії включають не лише кількісні показники (лайки, коментарі, репости), а і якісні характеристики – тональність комунікації, частоту контактів, сталість взаємодії в часі.

У вікні «Профільна карта користувача» систематизовано ключову інформацію щодо демографії, географічного положення, наявності освіти, роботи, належності до спільнот, тематики контенту та цифрових слідів. Вкладки щодо цифрової поведінки містять деталізовані візуалізації – включно із частотою появи в окремих інформаційних середовищах, зв'язками з контентом політичного, релігійного, військового й ідеологічного змісту.

Модуль «Фотоаналітики» відображає результати зіставлення візуальних матеріалів (фотографій), згрупованих за ступенем відповідності. Аналітик може верифікувати автентичність особи або встановити належність до конкретного цифрового кластера на основі присутності в масивах публікацій. Фотографії з різних джерел – зокрема й Telegram-каналів або Instagram-сторінок – упорядковуються за хронологією та ступенем відповідності. Це дозволяє швидко встановити участь об'єкта в інформаційних подіях або фізичну присутність на окремих заходах (рис. 3).

Зазначені функціональні модулі, реалізовані у формі інтерактивних панелей, таблиць, карт і блоків з аналітичними фільтрами, дозволяють опрацьовувати сотні профілів одночасно, автоматизують рутинну частину аналітичної роботи та звільняють фахівця для ухвалення рішень на підставі вже агрегованих і візуалізованих даних.

На особливу увагу заслуговує функціонал групового аналізу. За допомогою функції «груповий пошук» аналітик має змогу виявляти суб'єктів, які демонструють синхронізовану активність, як-от: коментування тих самих публікацій в однаковий проміжок часу, участь у подібних дискусіях або публікація контенту зі схожими геомітками. Ця функція дозволяє не лише ідентифікувати потенційних співучасників злочинної діяльності, але й аналізувати структури координації в межах інформаційних операцій.

З технічного боку Artellence базується на високоточних алгоритмах розпізнавання образів, лексичного аналізу та багатофакторної перевірки. За результатами тестувань, точність розпізнавання облич за якісного вхідного зображення сягає 96%, а обробка текстів і семантичне групування демонструє стабільність класифікації понад 90%. Система підтримує автоматичне оновлення індексу даних щогодини, що забезпечує постійну актуальність інформації. Це особливо важливо в умовах швидкозмінного цифрового середовища та необхідності своєчасного реагування правоохоронних органів на інформаційні виклики. Висока частота оновлення індексу досягається завдяки використанню розподіленої архітектури обробки даних і оптимізованих алгоритмів інкрементального індексування, які дозволяють додавати нову інформацію без необхідності повної переіндексації всієї бази даних.

Водночас технічна досконалість платформи не вичерпує всіх аспектів її впровадження. Залишаються відкритими питання щодо правової регламентації та процесуальних гарантів, які мають забезпечити баланс між ефективністю розслідування та захистом прав людини.

Висновки. Аналітична платформа "Artellence" демонструє високий рівень адаптованості до потреб кримінального аналізу в умовах цифрової трансформації правоохоронної діяльності. Комплексна структура системи, багатомодульна архітектура, гнучкість у побудові зв'язків та здатність до обробки мультимодальних даних забезпечують її ефективність як у межах оперативно-розшукової діяльності, так і на етапі досудового розслідування.

Використання Artellence дозволяє реалізовувати повний цикл цифрового аналітичного дослідження – від ідентифікації цифрових слідів до побудови аналітичної гіпотези з подальшою її верифікацією. На особливу увагу заслуговують інструменти фотопошуку, побудови

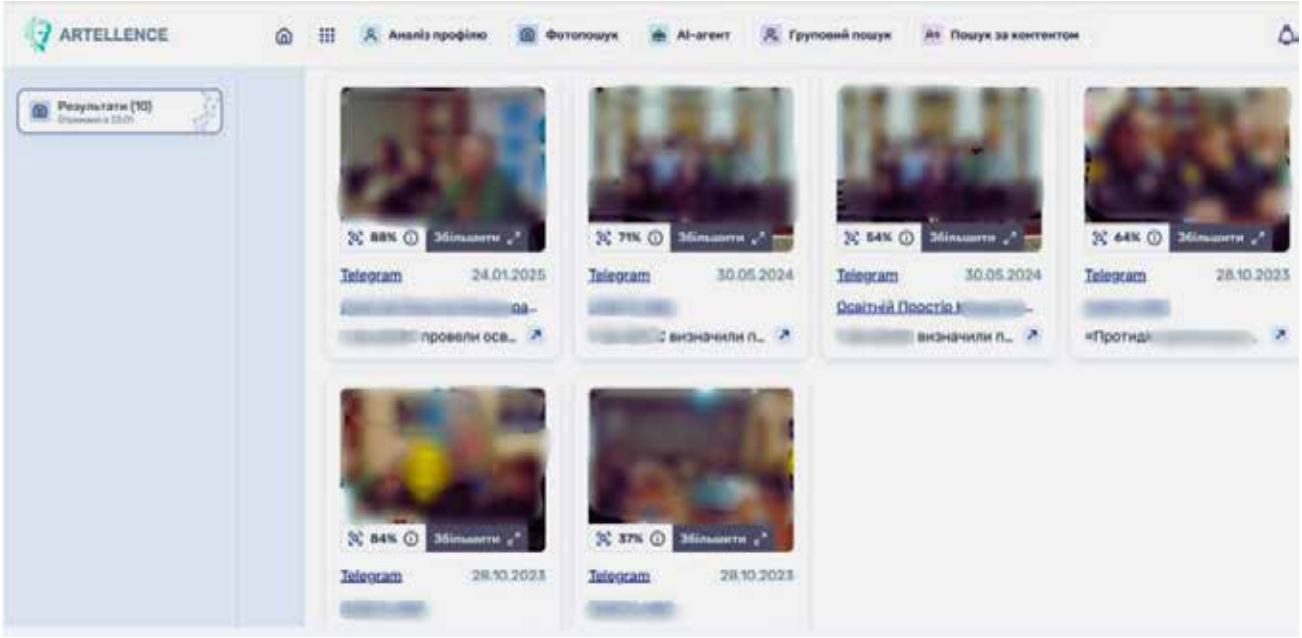

Рис. 3. Результати фотопошуку в Artellence: приклади збігів із Telegram-каналами та соціальними мережами за датами, джерелом і ступенем відповідності

графів зв'язків, аналізу мовних патернів, групової активності та прогнозування цифрової поведінки.

Система не лише інтегрується із чинними джерелами OSINT, а й формує принципово новий рівень аналітичної практики, заснованої на автоматизованому виявленні прихованих закономірностей, міжособистісних структур, а також на оцінюванні ризиків, пов'язаних з ідеологічними, комунікаційними та поведінковими характеристиками об'єкта.

Наявність автоматизованого алгоритму, візуалізацій, цифрової трасології та можливостей багатофакторної ідентифікації створює підґрунтя для широкого впровадження Artellence у діяльність аналітичних підрозділів Національної поліції України, Служби безпеки України й органів прокуратури. За умови належного нормативного супроводу, зокрема ухвалення відомчих нормативних актів, що регулюють порядок використання результатів аналітичних платформ, а також забезпечення прозорості процедур використання через механізми аудиту алгоритмів і контролю за дотриманням прав людини відповідно до стандартів Європейського суду з прав людини, установлених у справі "Big Brother Watch v. UK" [12, § 361], – платформа може стати ефективним інструментом кримінального аналізу, а її результати – процесуально допустимим джерелом доказів у кримінальному провадженні.

Список використаних джерел

1. Artellence. *Seeds of bravery. European Innovation Council.* URL: https://seedsofbravery.eu/startups/bigdatapeople-2/.
2. Sherman L. W. Evidence-based policing. Ideas in American policing. Washington, DC : Police Foundation, 1998. P. 1–16. URL: https://www.policinginstitute.org/wp-content/uploads/2015/06/Sherman-1998-Evidence-Based-Policing.pdf
3. Федчак І. А. Основи кримінального аналізу : навчальний посібник. Львів : ЛьвДУВС, 2021. 288 с.
4. Волобоєв А. О., Зеленський С. М. Правові та організаційні засади забезпечення інформаційної безпеки України. *Українська поліцеїстика: теорія, законодавство, практика*. 2025. Вип. № 2 (14). С. 95.–99. DOI: 10.32782/2709-9261-2025-2-14-17
5. Gotham. *Palantir.* URL: https://www.palantir.com/platforms/gotham/
6. Організація розкриття шахрайств, учинених у кіберпросторі : монографія / А. В. Шевчишен та ін. ; за заг. ред С. С. Вітвіцького. Київ : Алерта, 2023. 200 с.
7. Akhgar B., Bayerl P.S., Sampson F. Open Source Intelligence Investigation: From Strategy to Implementation. Cham : Springer International Publishing, 2016. 304 p. DOI: 10.1007/978-3-319-47671-1
8. Фігурський В. М. Докази в електронній формі у кримінальному провадженні. *Галицькі студії: Юридичні науки.* 2023. Вип. № 4. С. 97–105. DOI: 10.32782/galician_studies/law-2023-4-14
9. Rudin C. Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence.* 2019. Vol. 1. P. 206–215. DOI: 10.48550/arXiv.1811.10154
10. Recommendation on the Ethics of Artificial Intelligence. *UNESCO.* URL: https://www.unesco.org/ru/artificial-intelligence/recommendation-ethics
11. Guidelines on facial recognition. Strasbourg : Council of Europe, 2021. 29 p. URL: https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html
12. Рішення Європейського суду з прав людини у справі "Big Brother Watch v. UK". Заяви № № 58170/13, 62322/14, 24960/15. *European Court of Human Rights.* URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-210077%22]}
13. Artellence. *Аналітична платформа*. URL: https://artellence.com/ua

References

1. Artellence. (n.d.). *Seeds of bravery. European Innovation Council*. Retrieved from https://seedsofbravery.eu/startups/bigdatapeople-2/ [in English].
2. Sherman, L. W. (1998). Evidence-based policing. *Ideas in American policing* (pp. 1–16). Washington, DC: Police Foundation. Retrieved from https://www.policinginstitute.org/wp-content/uploads/2015/06/Sherman-1998-Evidence-Based-Policing.pdf [in English].
3. Fedchak, I. A. (2021). Osnovy kryminalnoho analizu [Fundamentals of criminal analysis]. Lviv: LvDUVS [in Ukrainian].
4. Voloboiev, A. O., & Zelenskyi, S. M. (2025). Pravovi ta orhanizatsiini zasady zabezpechennia informatsiinoi bezpeky Ukrainy [Legal and organizational principles of ensuring information security of Ukraine]. *Ukrainska politseistyka: teoriia, zakonodavstvo, praktyka*, 2 (14), 95–99. https://doi.org/10.32782/2709-9261-2025-2-14-17 [in Ukrainian].
5. Gotham. (n.d.). *Palantir.* Retrieved from https://www.palantir.com/platforms/gotham/ [in English].
6. Shevchyshen, A. V., Romanov, M. Yu., Voloboiev, A. O., Lunhol, O. M., Haborets, O. A., & Holovkin, S. V. (2023). Orhanizatsiia rozkryttia shakhraitstv, uchinenykh v kiberprostori [Organization of fraud detection committed in cyberspace]. Kyiv: Alerta [in Ukrainian].
7. Akhgar, B., Bayerl, P. S., & Sampson, F. (2016). Open Source Intelligence Investigation: From Strategy to Implementation. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-47671-1 [in English].
8. Fihurskyi, V. M. (2023). Dokazy v elektronnii formi u kryminalnomu provadzhenni [Evidence in electronic form in criminal proceedings]. *Halytski studii. Yurydychni nauky,* 4, 97–105. https://doi.org/10.32782/galician_studies/law-2023-4-14 [in Ukrainian].
9. Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence*, 1, 206–215. https://doi.org/10.48550/arXiv.1811.10154 [in English].
10. Recommendation on the Ethics of Artificial Intelligence. (n.d.). *UNESCO.* Retrieved from https://www.unesco.org/ru/artificial-intelligence/recommendation-ethics [in English].
11. Guidelines on facial recognition. (2021). *Strasbourg: Council of Europe.* Retrieved from https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html [in English].
12. Big Brother Watch v. UK, Applications nos. 58170/13, 62322/14, 24960/15. *European Court of Human Rights.* Retrieved from https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-210077%22]} [in English].
13. Artellence. *Analitychna platforma [Analytical platform].* (n.d.). Retrieved from https://artellence.com/ua [in Ukrainian].

Haborets Olha,
PhD in Educational and Pedagogical Sciences, Associate Professor,
Associate Professor at the Department of Operational and
Investigative Activities and Information Security
(Donetsk State University of Internal Affairs, Kropyvnytskyi)
ORCID: https://orcid.org/0000-0001-7791-6795

Voloboiev Arthur,
PhD in Law,
Head of the Department for the Organization of the Educational Process
(Donetsk State University of Internal Affairs, Kropyvnytskyi)
ORCID: https://orcid.org/0000-0002-7138-5847

INNOVATIVE APPROACHES TO THE USE OF ARTELLENCE IN MODERN CRIMINAL ANALYSIS

In the current context of a significant complication of crime traditional approaches to criminal analysis are losing their effectiveness. Law enforcement agencies increasingly face the need for the rapid processing of heterogeneous sources of information, including digital traces, social media accounts, data from open platforms, video surveillance results, and other unstructured sources. In this regard, there arises an objective need for the implementation of high-tech analytical systems capable of automated real-time analysis of large volumes of data while complying with procedural legislation.

Particularly relevant are analytical platforms that not only process information but also generate substantiated analytical hypotheses based on it, reveal hidden connections between objects, predict probable events, and identify risky behavioral patterns. In this context, the Artellence system, localized for the needs of Ukrainian law enforcement agencies in partnership with Big People 2, represents a technology that synthesizes algorithmic power, multilayered OSINT analytics, and a digital profiling architecture of subjects.

Accordingly, this article provides a comprehensive study of the functional capabilities of the Artellence analytical platform, which serves as an example of a modern cognitive tool for criminal analysis in the digital environment. The architecture of the system, its modular composition, and technical aspects – including elements of the BigDataPeople 2 ecosystem – are disclosed. The practical application of such modules as photo search, semantic profiling, link graph construction, geolocation, ideological orientation classification, and temporal analysis of digital activity is described. A case analysis of the system's operation is presented, illustrating its performance in facial recognition, analytical profiling, interaction mapping, and assessment of lexical markers and information clusters. Interface solutions and accuracy indicators are highlighted, confirming the tool's effectiveness. The potential of Artellence in constructing evidentiary hypotheses, verifying digital traces, providing operational and strategic support for pre-trial investigations, and developing analytical models of criminal behavior in line with international approaches is defined.

Key words: *criminal analysis, Artellence, Big People 2, BigDataPeople 2, OSINT, analytical platform, artificial intelligence, pre-trial investigation, criminal proceedings.*

Надіслано до редколегії 19.11.2025
Рекомендовано до публікації 15.12.2025
Опубліковано 29.12.2025