УДК 004:343.98 (477)(045)

Лунгол Ольга Миколаївна, доктор філософії, доцент, доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки Донецького державного університету внутрішніх справ, м. Кропивницький, вул. Велика Перспективна 1, e-mail: olyalungol@gmail.com, https://orcid.org/0000-0001-8128-0072

Габорець Ольга Андріївна, доктор філософії, доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки Донецького державного університету внутрішніх справ, м. Кропивницький, вул. Велика Перспективна 1, e-mail: olga-gaborets@ukr.net, https://orcid.org/0000-0001-7791-6795

ІННОВАЦІЙНІ МЕТОДИ ТА ЦИФРОВІ ТЕХНОЛОГІЇ В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ

Анотація. Цифрові технології переломно змінюють парадигму та методологію проведення оперативно-розшукової діяльності, резонуючи вдосконалену ефективність та раціональну швидкість цього процесу. У сучасному світі, де зростає рівень небезпеки як у реальному, так і у віртуальному світі, особливого значення набуває актуальність інноваційних рішень і цифрових технологій в галузі оперативно-розшукової діяльності. Сучасні цифрові технології розширили можливості оперативних служб у сфері обробки та аналізу великих обсягів інформації, що відкриває нові перспективи у виявленні та розслідуванні злочинів. Інноваційні методи, доступні правоохоронним органам, дозволяють здійснювати швидке та результативне відстеження комунікацій, проводити глибокий аналіз великих обсягів даних, вивчати активність у соціальних мережах та застосовувати високорівневу аналітику для отримання критично важливої інформації. Ці засоби сприяють підвищенню ефективності та розширенню можливостей правоохоронних органів у проведенні операцій та розслідуванні сучасних злочинних явищ. Автори статті розглядають інноваційні продукти вітчизняних науковців, а також можливості аналітичних інструментів на основі штучного інтелекту та машинного навчання для виявлення потенційних загроз та можливих злочинів. В роботі відзначається авторами, що кримінальні групи та загрози можуть приймати глобальний характер, а використання цифрових технологій надає можливість оперативним службам ефективно співпрацювати та обмінюватися інформацією на міжнародному рівні. У сучасному світі оперативно-розшукова діяльність стикається з великими викликами і можливостями, які пропонують інноваційні методи та цифрові технології. Для забезпечення безпеки та зменшення злочинності важливо використовувати ці засоби на користь суспільства, забезпечуючи захист прав громадян та ефективну боротьбу з злочинністю. Як приклад, автори наводять особливості використання OSINT-технологій в оперативно-розшуковій діяльності правоохоронних органів для збору інформації з відкритих джерел, таких як веб-сайти, соціальні мережі, форуми, блоги, новини та інші публічно доступні ресурси, для розкриття злочинів, виявлення злочинців та збору доказів;

аналізу велиих обсягів даних для виявлення зв’язків, шаблонів та інших важливих відомостей для створення портретів злочинців, виявлення їхнього місця перебування та діяльності; ідентифікації осіб за допомогою цифрових слідів, які залишаються в Інтернеті; моніторингу діяльності груп, організацій та індивідів в мережі для виявлення та запобігання злочинів, зокрема тероризму та організованої злочинності; збереження та аналізу доказів для підтримки розслідувань; попередження злочинів через відстеження ознак, які можуть свідчити про планування злочинів.

Ключові слова: правоохоронна діяльність, OSINT (Open Source Intelligence), аналіз, розвідка, розпізнавання облич.

Lunhol Olha, PhD in Pedagogical Sciences, Docent, Associate Professor of the Department of Operational-search Activities and Information Security of Donetsk State University of Internal Affairs, Kropyvnytskyi, Velyka Perspektyvna 1, e-mail: olyalungol@gmail.com, https://orcid.org/0000-0001-8128-0072

Haborets Olha, PhD in Pedagogical Sciences, Associate Professor of the Department of Operational-search Activities and Information Security of Donetsk State University of Internal Affairs, Kropyvnytskyi, Velyka Perspektyvna 1, e-mail: olga-gaborets@ukr.net, https://orcid.org/0000-0001-7791-6795

INNOVATIVE METHODS AND DIGITAL TECHNOLOGIES IN OPERATIONAL AND INVESTIGATIVE ACTIVITIES

Abstract. Digital technologies are fundamentally reshaping the paradigm and methodology of operational and investigative activities, resonating with enhanced efficiency and heightened speed in this process. In the modern world, where the level of danger is increasing in both the physical and virtual realms, the relevance of innovative solutions and digital technologies in the field of operational and investigative activities becomes particularly significant. Contemporary digital technologies have expanded the capabilities of law enforcement agencies in processing and analyzing vast volumes of information, opening new horizons in the detection and investigation of crimes. Innovative methods accessible to law enforcement allow for rapid and effective monitoring of communications, deep analysis of extensive datasets, examination of social media activity, and the application of advanced analytics to acquire critically important information. These tools contribute to the increased efficiency and extended capabilities of law enforcement agencies in conducting operations and investigating contemporary criminal phenomena. The authors of this article explore innovative products by domestic scientists and the potential of analytical tools based on artificial intelligence and machine learning for the detection of potential threats and possible crimes. In the paper, the authors note that criminal groups and threats can take on a global nature, and the use of digital technologies enables law enforcement agencies to effectively cooperate and exchange information at an international level. In the modern world, operational and investigative activities face significant challenges and opportunities provided by innovative methods and digital technologies. To ensure

security and reduce crime, it is crucial to use these tools for the benefit of society, safeguarding citizens' rights and effectively combating criminality. As an example, the authors highlight the specificities of employing OSINT-technologies in the operational and investigative activities of law enforcement agencies to gather information from open sources such as websites, social networks, forums, blogs, news, and other publicly available resources for crime detection, criminal identification, and evidence collection. These tools also involve analyzing extensive datasets to identify connections, patterns, and other critical information for creating profiles of criminals, discovering their whereabouts and activities, identifying individuals through digital traces left on the internet, monitoring the activities of groups, organizations, and individuals online to detect and prevent crimes, including terrorism and organized crime, preserving and analyzing evidence to support investigations, and preventing crimes by tracking signs that may indicate criminal planning.

Keywords: law enforcement, OSINT (Open Source Intelligence), analysis, intelligence, facial recognition.

Постановка проблеми. Необхідність у використанні правоохоронними органами передових підходів та інструментів для боротьби з кримінальною діяльністю й забезпечення громадської безпеки, пов'язана із зростанням обсягу даних та збільшенням кількості кіберзлочинів, адаптацією методів та стратегій злочинців до сучасних технологій, глобалізацією злочинності. З активною цифровізацією суспільства та зростанням кількості цифрових слідів у віртуальному просторі, правоохоронні органи мають постійно адаптуватися до нових умов та застосовувати інноваційні методи й цифрові технології для ефективного проведення оперативно-розшукової роботи. Застосування інновацій дозволяє правоохоронцям забезпечити швидке виявлення злочинів, збільшити точність розслідувань, зменшити вплив злочинців як у фізичному, так і у віртуальному просторі, підвищити рівень кібербезпеки.

У сучасному світі інформаційні технології настільки проникли в усі сфери життя, що злочинці також активно використовують цифрові інструменти для своїх цілей. Зростаюча кількість кіберзлочинів, таких як хакерські атаки, шахрайство в Інтернеті, кібершпигунство, фішинг тощо створює потребу у розробці спеціалізованих методів та технологій для їх виявлення та запобігання. Це вимагає від правоохоронних органів навчання та застосування сучасних цифрових технологій для виявлення та розслідування відповідних злочинів. Як результат, дослідження і впровадження інноваційних методів та цифрових технологій у сферу оперативно-розшукової діяльності стає необхідним для забезпечення ефективної роботи правоохоронних органів у сучасних умовах.

Аналіз останніх досліджень і публікацій. Питанню використання інноваційних методів та цифрових технологій в оперативно-розшуковій діяльності присвячені роботи як вітчизняних, так і зарубіжних науковців та практиків. Так, під час міжнародного «круглого столу» [1] «Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці» були висвітлені питання розроблення і використання інноваційних методів та цифрових технологій в криміналістиці, судовій експертизі і

юридичній практиці. Серед іншого були представлені інноваційні продукти, розроблені співробітниками НДІ вивчення проблем злочинності імені академіка В. В. Сташиса спільно з науковцями кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого [1, с. 6 – 10]: «Пристрій для виміру швидкості балістичного об'єкта», «Автоматизоване робоче місце (АРМ) слідчого «Інсайт», «Польова» мініфотолабораторія», «Спосіб формування суб'єктивного портрету «RAIPS-портрет» (комп'ютерного фотороботу)», комп'ютерна системи «База даних «Практика слідчого», інформаційно-пошукова система «Слідчий прецедент» та ін.

Севрук В. Г. у своїх дослідженнях [2] зазначає, що в даний час Україною здійснюється взаємодія з Генеральним Секретаріатом Інтерполу в рамках наступних інноваційних проєктів: «Мілленіум» (тисячоліття) – проєкт, запроваджений для збору та аналізу інформації про транснаціональну євразійську організовану злочинність; «Брідж» (міст) – проєкт щодо протидії нелегальній міграції; «Сідраг» – проєкт щодо збору інформації про розповсюдження синтетичних наркотиків; «Червоні шляхи» – проєкт щодо припинення функціонування каналів торгівлі жінками з країн Східної Європи з метою сексуальної експлуатації до західноєвропейського регіону.

На важливості й актуальності використання в правоохоронній діяльності програм для розпізнавання обличчя (комп'ютерних програм або систем штучного інтелекту, які розроблені для ідентифікації та аналізу облич людей на фотографіях або відео) наголошує доцентка кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ Злагода О.В. [3]. Науковиця зазначає, що на сьогодні найбільш поширеним у світі методом розшуку особи є розпізнання і пошук схожих осіб. Як приклад, детально розглядає програмний комплекс «Face-Інтелект» – систему автоматичного розпізнавання облич, яка включає два модулі: модуль розпізнання облич та модуль пошуку схожих облич у відеоархіву.

На актуальності використання штучного інтелекту в правоохоронній діяльності наголошують науковці Львівського державного університету внутрішніх справ Зачек О.І., Дмитрик Ю.І. та Сеник В.В. [4]. Вони зазначають, що використання штучного інтелекту правоохоронними органами дозволяє відстежувати злочинців та злочинні групи, визначати місцезнаходження злочинців, аналізувати відео- та аудіозаписи, шукати співвідношення між різними злочинами та правопорушниками тощо. Як результат, використання штучного інтелекту допомагає поліпшити ефективність розслідувань, знизити кількість помилок та зайвих витрат часу і зусиль, а також допомагає аналізувати великі обсяги інформації і виявляти можливі зв'язки між різними фактами, що можуть мати ключове значення для розслідування злочинів.

Проблеми та перспективи використання штучного інтелекту в правоохоронній діяльності також аналізують у своїх дослідженнях Благута Р.І. [5], Мовчан А.В. [5], Бугера О.І. [6], Бортник С.М. [7], Макаринська А.В. [8], Лисенко О.В. [9], Просвіріна Т.В. [10] та ін.

Значний інтерес наукової спільности до питання впровадження інноваційних технологій в роботу оперативно-розшукової діяльності

підкреслюють його важливість у сучасному світі з численними викликами та загрозами. Тому, **метою** даної **статті** є вивчення та аналіз інноваційних методів та цифрових технологій, які використовуються в оперативно-розшуковій діяльності в процесі пошуку і фіксації фактичних даних про протиправні діяння окремих осіб та груп, а також отримання інформації в інтересах безпеки громадян, суспільства і держави.

Виклад основного матеріалу. Проаналізувавши роботи вище зазначених науковців, ми встановили, що одним із інноваційних методів, який знаходить широке застосування в оперативно-розшуковій діяльності є автоматичне розпізнавання облич. Воно значно полегшує пошук та ідентифікацію підозрюваних осіб на великих областях або в потоці людей. В режимі реального часу системи розпізнавання облич можуть відстежувати рух осіб та надавати інформацію оперативним службам про можливі підозрілі дії. Системи автоматичного розпізнавання облич можуть зберігати дані та записи, які в подальшому можуть бути використані для розслідувань злочинів або інцидентів. Шляхом встановлення осіб за допомогою автоматичного розпізнавання облич, правоохоронні органи можуть попереджати можливі злочини через виявлення підозрілих або розшукуваних осіб на громадських заходах або в інших місцях.

Для автоматичного розпізнавання облич у світі також використовують наступні програмні комплекси і технології:

- Open Source Computer Vision Library (OpenCV) – це бібліотека з відкритим вихідним кодом для розпізнавання облич та обробки зображень. Вона надає інструменти для створення програм, які можуть виявляти та розпізнавати обличчя на фотографіях та відео.
- Microsoft Azure Face API – платформа від Microsoft надає API для розпізнавання облич та ідентифікації осіб на зображеннях та відео. Вона використовує розширені алгоритми для точного розпізнавання та аналізу облич.
- Amazon Rekognition – хмарна служба від Amazon, яка надає можливість розпізнавання обличчя на фотографіях та відео. Вона також підтримує інші завдання ком’ютерного зору, такі як виявлення об’єктів та тексту.
- IBM Watson Visual Recognition – інструмент для розпізнавання облич та відкритих об’єктів на зображеннях. Він використовує штучний інтелект для аналізу та класифікації зображень.
- Face++ (Megvii) – це китайська компанія, яка надає API для розпізнавання облич та обробки зображень. Їхні технології використовуються для багатьох застосувань, включаючи безпеку та ідентифікацію користувачів.
- Kairos – компанія, яка спеціалізується на розпізнаванні облич та обробці зображень. Вони надають інструменти для розпізнавання облич на зображеннях та відео.

Ці програмні комплекси використовують різні алгоритми та технології, включаючи нейронні мережі, щоб розпізнавати обличчя та ідентифікувати осіб на зображеннях та відео. Проаналізувавши принципи роботи різних програмних комплексів розпізнавання обличчя, ми встановили спільні кроки в алгоритмах їх роботи:

1. *Збір інформації або вхідних даних*. Зазвичай це фотографії або відео, які можуть бути отримані з камер спостереження, веб-камер, смартфонів або інших джерел.

2. *Виявлення обличчя.* Програма проводить аналіз вхідних даних для визначення місця розташування обличчя на зображенні. Цей процес включає в себе пошук основних рис, таких як очі, ніс, рот і контури обличчя.

3. *Екстракція особливостей*. Після виявлення обличчя, програма екстрагує основні особливості, такі як розмір і форма обличчя, положення очей, рота та інші антропометричні параметри.

4. *Порівняння*. Отримані дані порівнюються із зразками або базою даних облич. Система може порівнювати виявлене обличчя з фотографіями або шаблонами вже ідентифікованих осіб.

5. *Визначення та ідентифікація*. Якщо знайдено відповідність, програма визначає ім'я або ідентифікатор особи, якій належить виявлене обличчя. Якщо збіг не знайдено, система може розглядати обличчя як невідому особу або може вимагати подальшої ідентифікації.

6. *Оцінка точності*. Програми для розпізнавання обличчя оцінюють точність ідентифікації на основі різних факторів, таких як якість вихідних даних, якість алгоритмів розпізнавання та кількість даних для порівняння.

7. *Використання результатів.*

Значна увага як вітчизняних, так і зарубіжних наукоців [4-10] приділяється можливостям використання штучного інтелекту та машинного навчання. Узагальнивши дослідження вищезазначених науковців [4-10], ми прийшли до висновку, що штучний інтелект (ШІ) вже активно використовується в правоохоронній діяльності для поліпшення різних аспектів роботи правоохоронних органів, а саме:

1. ШІ допомагає аналізувати великі обсяги даних для виявлення злочинів та їх розкриття, зокрема шляхом обробки відеоматеріалів, аналізу телефонних дзвінків, текстових повідомлень та іншої інформації.

2. Системи передбачення злочинності використовують дані та алгоритми для визначення можливих зон ризику та виявлення патернів, що можуть свідчити про можливі злочини. Наприклад, відома PredPol (Predictive Policing) – це система передбачення злочинності, яка використовує алгоритми і аналітику для передбачення місць і часів можливих злочинів. Система базується на великих обсягах даних, включаючи історичні дані про злочини, географічні координати, час і типи злочинів. Основні риси і функції PredPol включають: аналіз даних (PredPol аналізує історичні дані про злочини, зокрема злочинні звіти, що містять інформацію про дату, місце та типи злочинів); прогнозування злочинів (система використовує алгоритми передбачення, щоб ідентифікувати патерни та тенденції в злочинності в певних районах і на певні часи); генерація гарячих точок (PredPol генерує мапи «гарячих точок», де ймовірність злочинів найвища, і рекомендує правоохоронним органам зосередити увагу на цих районах); повідомлення та рекомендації (система надає рекомендації правоохоронцям щодо оптимальних маршрутів патрулювання та роботи в певних районах для зменшення злочинності); регулярні оновлення (PredPol постійно аналізує нові дані та

оновлює свої прогнози, щоб враховувати зміни в злочинності); застосування в реальному часі (система може бути використана для спрогнозування злочинів в реальному часі, що дозволяє правоохоронцям реагувати на потенційні загрози миттєво); підвищення ефективності ресурсів (PredPol допомагає правоохоронцям ефективніше розподіляти ресурси та забезпечити більшу видимість і присутність в тих районах, де ймовірність вчинення злочинів вища). PredPol використовується багатьма поліцейськими департаментами в Сполучених Штатах та інших країнах як інструмент для підвищення ефективності правоохоронних заходів і зменшення злочинності.

3. Відслідковування злочинців через розпізнавання обличчя, розпізнавання голосу і аналіз соціальних мереж.

4. ШІ використовується для виявлення кіберзлочинців, моніторингу мереж і виявлення загроз в Інтернеті. Включає в себе виявлення шкідливих програм, блокування шкідливих веб-сайтів і аналіз потоків даних.

5. ШІ може аналізувати дані про дорожні умови, інформацію про дорожні пригоди та погодні умови, щоб прогнозувати можливість дорожніх подій і аварій.

6. ШІ автоматизує виконанні рутинних завдань, таких як обробка документів та аналіз інформації з баз даних, що економить час правоохоронців на роботу з більш важливими справами.

7. Використання ШІ сприяє збору та обробці інформації, що полегшує обмін даними між правоохоронцями на різних рівнях та в різних відділах.

8. ШІ використовує аналітику та алгоритми для прогнозування, де ймовірно виникнуть злочини в майбутньому на основі аналізу попередніх даних.

Інтеграція штучного інтелекту в правоохоронну діяльність допомагає значно підвищити ефективність та точність роботи правоохоронних органів, що в свою чергу сприяє підвищенню безпеки та якості життя громади.

Одним із інноваційних методів в оперативно-розшуковій діяльності є отримання інформації про незаконну діяльність за допомогою відкритих джерел (OSINT). OSINT (Open Source Intelligence) – це процес збору, аналізу та використання інформації, яка є відкритою і доступною громадськості через різні відкриті джерела. Ця інформація може включати в себе дані з веб-сайтів, соціальних мереж, новинних джерел, форумів, блогів, Інтернет-видань та інших джерел. OSINT використовується для здійснення різних видів аналізу, розвідки, досліджень та іншої інформаційної діяльності з метою розуміння певної ситуації, ідентифікації загроз або використання інформації у різних цілях, включаючи безпеку та розслідування. OSINT грає важливу роль в сферах розвідки, кібербезпеки, правоохоронної діяльності та інших галузях, де інформація має стратегічне значення. OSINT є надзвичайно корисним інструментом і в оперативно-розшуковій діяльності правоохоронних органів. До основних напрямків використання OSINT в оперативно-розшуковій діяльності ми відносимо:

1. Збір відкритої інформації про підозрюваних – правоохоронці можуть використовувати OSINT для збору інформації про осіб, щодо яких вони проводять розшук або розслідування. Ця інформація може включати в себе

адреси, номери телефонів, профілі у соціальних мережах та інші дані, які допоможуть встановити місцезнаходження або спільнокримінальні зв'язки.

2. Моніторинг соціальних мереж, оскільки підозрювані часто залишають сліди своєї діяльності у соціальних мережах. За допомогою OSINT правоохоронці можуть відстежувати активності підозрюваних, спостерігати за змінами в статусі та взаємодії з іншими користувачами.

3. Аналіз геоданих через інформацію з мобільних додатків і сервісів, таких як картографічні додатки та фотографії з геотегами, що може надати важливі дані про місцезнаходження підозрюваних або потенційних свідків подій.

4. Моніторинг новин та інших джерел – онлайн-новини, блоги та форуми можуть надати важливі вказівки, що стосуються подій або осіб, що фігурують у справах. Вони можуть слугувати джерелом нової інформації або підтвердженням існуючих даних.

5. Виявлення відомостей про транспорт – через визначення власників транспорту, перевірку страхових полісів, водійських посвідчень та інших транспортних документів.

6. Аналіз зображень і відео – для виявлення доказів та інформації про злочини чи підозрюваних.

Як практичний посібник для правоохоронців, що використовують відкриті цифрові дані в оперативно-розшуковій діяльності, може бути використаний Протокол Берклі [11]. В цьому документі описані вимоги та настанови з питань пошуку, збору, зберігання, перевірки та аналізу інформації з соціальних мереж та інших відкритих ресурсів. Він також включає міжнародні стандарти для проведення розслідувань в онлайн-середовищі, і надає детальні вказівки щодо методів і процедур збирання, аналізу та зберігання цифрової інформації відповідно до вимог професійної, правової та етичної поведінки. Крім того, посібник містить рекомендації для слідчих, які здійснюють пошук інформації в Інтернеті, щодо забезпечення своєї фізичної та психологічної безпеки, а також захисту інших осіб, включаючи свідків, потерпілих, громадян, активістів і журналістів.

Потужним інструментом, який може бути використаний в оперативно-розшуковій діяльності для аналізу відкритих джерел інформації є OSINT Framework [12]. Пошук інформації з відкритих джерел за іменем користувача є однією з ключових функцій OSINT. Такий пошук досить зручно здійснювати засобами OSINT Framework. Серед ресурсів та можливостей OSINT Framework для пошуку інформації за іменем користувача з відкритих джерел ми виділяємо:

- Ресурс Namechk – це інструмент, який дозволяє перевіряти доступність конкретного імені користувача або назви на різноманітних популярних платформах, соціальних мережах, ресурсах тощо. Ресурс проводить одноразовий пошук на декількох ресурсах одночасно, з'ясовуючи, чи доступне обране ім'я користувача на кожному з них. Namechk охоплює багато різних веб-сайтів і сервісів, включаючи соціальні мережі, форуми, блог-платформи і багато інших майданчиків для взаємодії в Інтернеті. Є можливість налаштувати пошук, щоб врахувати спеціальні символи або певний формат імені користувача.

- ThatsThem – це онлайн-ресурс і пошуковий інструмент, який надає можливість шукати інформацію про осіб за допомогою їхнього імені, адреси електронної пошти, номера телефону або адреси. Цей ресурс в основному спеціалізується на пошуку контактних даних та публічної інформації про осіб у Сполучених Штатах Америки. Основні функції та можливості ThatsThem включають: пошук за іменем, що дозволяє отримати інформацію про адресу, номер телефону, можливих родичів та інші контактні дані особи; пошук за адресою електронної пошти; пошук за номером телефону.

- Check Usernames – це онлайн-інструмент, який призначений для перевірки доступності користувацьких імен або нікнеймів на різних популярних платформах і соціальних мережах. Основні функції та можливості Check Usernames включають: пошук доступності імен користувачів, робота зі списоком платформ, які підтримуються для перевірки імен користувачів (Twitter, Instagram, Facebook, GitHub, Reddit, YouTube, і багато інших), рекомендації щодо імен користувачів тощо.

OSINT Framework пропонує значні можливості для роботи з IP-адресами: визначення приблизної геолокації IP-адреси, аналіз IP-адреси на предмет загроз або інцидентів, таких як історія атак чи злочинних дій; пошук пов'язаних доменів та служб, а також інші служби, які можуть використовуватися на цій IP-адресі; моніторинг активності та статус IP-адреси в мережі; зв'язок із суміжними інформаційними джерелами, тобто OSINT Framework може надати посилання на інші додаткові ресурси, такі як блоги, форуми або соціальні мережі; аналіз історії IP-адреси для інформації щодо її реєстрації та власника.

Blacklists у контексті OSINT Framework вказують на списки IP-адрес, доменів, а також URL-адрес, які розглядаються як небажані або потенційно небезпечні. Ці списки містять інформацію про об'єкти, що можуть бути пов'язані зі спамом, шахрайством, кіберзлочинністю або іншими видами шкідливої діяльності в Інтернеті. OSINT Framework має вбудовані інструменти та ресурси для роботи з цими чорними списками та регулярно оновлює їх, щоб користувачі мали доступ до актуальної інформації, надає користувачам посилання на інші інструменти та ресурси, які дозволяють докладніше досліджувати IP-адреси або домени, виявлені в чорних списках, створює умови для автоматизації перевірки IP-адрес та доменів на предмет наявності в чорних списках. Чорні списки OSINT Framework дозволяють оперативно виявляти й ідентифікувати потенційно небезпечні об'єкти та сприяють підвищенню рівня безпеки в Інтернеті.

BGP, або Border Gateway Protocol, в контексті OSINT Framework, вказує на інструменти та ресурси, які дозволяють збирати та аналізувати інформацію про маршрутизацію мережі та активність систем, які використовують протокол BGP. Серед можливостей BGP в рамках OSINT Framework виділяємо: пошук інформації про конкретне Autonomous System, включаючи інформацію про власників, географічне розташування та інші характеристики; моніторинг маршрутів BGP, що може бути корисним для виявлення аномалій чи атак на мережу; аналіз AS-відносин для визначення потенційних точок відмови чи атак на мережу; визначення геолокації AS та вивчення, де саме відбувається маршрутизація мережевих пакетів; пошук інформації про BGP-підприємства та

інтернет-постачальників, що може бути корисним для аналізу мережевих інфраструктур; пошук потенційних точок відмови тощо.

Images в OSINT Framework вказують на можливості та ресурси, які допомагають аналізувати та збирати інформацію зображень, включаючи фотографії, знімки відео та інший мультимедійні вміст. OSINT Framework дозволяє проаналізувати метадані, які вбудовані в зображення (EXIF-дані), такі як географічні координати, дату та час створення, модель камери та інші параметри. Є можливість здійснювати реверсний пошук зображень, що дозволяє визначити джерело, де це зображення було раніше опубліковане в Інтернеті. Засоби Images дозволяють визначити місце на зображенні (геолокацію), об'єкти та їхні характеристики. Засоби пошуку схожих зображень допомагають виявити дублікати або подібні матеріали зображень в соціальних мережах та інших онлайн-ресурсах. Перевірка на аутентичність зображень полегшує виявлення ознак фотошопу або монтажу.

Videos в OSINT Framework вказують на можливості та ресурси, які допомагають аналізувати та збирати інформацію з відеозаписів та мультимедійних матеріалів, включаючи відеоматеріали, опубліковані в Інтернеті. OSINT Framework дозволяє аналізувати метадані відеозаписів, такі як дата та час створення, власник відео, географічні координати, модель камери, а також інші параметри. Є засоби для проведення реверсного пошуку відео для визначення джерела, де відеозапис був раніше опублікований в Інтернеті. Засоби Videos в OSINT Framework надають можливість визначити місце та об'єкти, які зображені на відео, включаючи геолокацію та розпізнавання облич, виявлення звідки було отримано або опубліковано відео, можливість аналізу аудіо-слідів відео для ідентифікації розмов, музики, а також інших звукових даних, визначення слідів фотошопу або монтажу, пошук відеозаписів, які схожі на вказане відео, що може бути корисно для виявлення дублікатів або аналізу подібних матеріалів.

Images та Videos в OSINT Framework є сучасними та зручними засобами для проведення оперативно-розшукової діяльності через аналіз змісту фото та відеоматеріалів.

У своїй сукупності засоби OSINT Framework, такі як Malicious File Analysis, Digital Currency, Mobile Emulation, Metadata, Geolocation Tools / Maps, Transportation, Business and Public Records, Telephone Numbers, Social Networks, Images / Videos / Docs, IP Address та інші, є корисним інструментом у сфері оперативно-розшукової діяльності для збору відкритої інформації з використанням різноманітних джерел та ресурсів. Ці інноваційні засоби дозволяють збирати інформацію про осіб, включаючи їхні імена, контактну інформацію, адреси, соціальні мережі, родину та інші персональні дані; відстежувати активність осіб на соціальних мережах, аналізувати їхні публікації, фотографії та зв'язки; визначати місцезнаходження осіб чи об'єктів; аналізувати IP-адреси, визначати їхні власників, геолокацію та зв'язок з іншими даними; проводити аналіз відео та фотографій для виявлення об'єктів, подій чи здійснення реверсного пошуку для встановлення походження зображень; шукати інформацію на веб-сайтах, форумах, блогах та інших ресурсах; досліджувати

аудіо-файли для ідентифікації голосів, розмов та іншої аудіо-інформації; проводити моніторинг і аналіз відкритих джерел на можливі загрози чи аномалії, пов’язані з певними особами або подіями.

OSINT Framework в правоохоронній діяльності надає можливості для ретроспективного та реального аналізу відкритих джерел інформації, що може бути корисним у розслідуваннях, оперативно-розшуковій діяльності, контролі за додержанням законів та безпекою.

Висновки. Цифрові технології відзначаються значущим впливом на еволюцію оперативно-розшукової діяльності, створюючи нові можливості та парадигми в її методології. У сучасному світі, де наростає загроза як у фізичному, так і в віртуальному середовищі, важливість і актуальність використання інновацій та цифрових технологій в галузі оперативно-розшукової діяльності надзвичайно великі. Сучасні цифрові технології значно розширили можливості оперативних служб, особливо в обробці та аналізі значних обсягів інформації, що відкриває нові перспективи для виявлення та розслідування злочинів. Інноваційні методи, доступні правоохоронним органам, надають змогу здійснювати швидке та результативне відстеження комунікацій, проводити глибокий аналіз великих обсягів даних, вивчати активність у соціальних мережах та використовувати високорівневу аналітику для отримання критично важливої інформації. Інноваційні методи та цифрові технології сприяють підвищенню ефективності й розширенню можливостей правоохоронних органів у проведенні операцій та розслідуванні злочинів.

1. Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці : матеріали міжнар. «круглого столу» (Харків, 12 груд. 2019 р.). Харків : Право, 2019. 164 с.
2. Севрук В. Г. Зарубіжний досвід використання інформаційно-аналітичного забезпечення протидії злочинам, що вчиняються організованими групами і злочинними організаціями, які сформовані на етнічній основі. Протидія злочинності: проблеми практики та науково-методичне забезпечення. Південноукраїнський правничий часопис. № 1, 2021. С. 61 – 66. DOI: https://doi.org/10.32850/sulj.2021.1.10.
3. Злагода О.В., Курінний О.В. Аспекти ефективності розшуку безвісно зниклих осіб. 2021. С. 59 – 61. URL: http://elar.naiau.kiev.ua (Дата звернення: 18.08.2023).
4. Зачек О.І., Дмитрик Ю.І., Сеник В.В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. Науковий вісник Львівського державного університету внутрішніх справ. № 3. 2023. С. 148 – 156. DOI: https://doi.org/10.32782/2311-8040/2023-3-19.
5. Благута Р.І., Мовчан А.В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с.
6. Бугера О.І. Використання штучного інтелекту для запобігання злочинності. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. Том 32(71). № 6. 2021. С. 82–86. URL: https://www.juris.vernadskyjournals.in.ua/journals/2021/6_2021/15.pdf (дата звернення: 12.04.2023).
7. Бортник С.М. Особливості регулювання використання штучного інтелекту у правоохоронної системі. Застосування інформаційних технологій у діяльності правоохоронних органів: матеріали круглого столу (м. Харків, 14 грудня 2021 р.) / МВС України, Харк. нац. ун-т внутр. справ., Каф. кібербезпеки та DATA-технологій. Харків: ХНУВС, 2021. С. 28–31.

8. Макаринська А.В., Лунгол О.М. Modern digital technologies in criminal analysis. Матеріали Всеукраїнської науково-практичної «Актуальні питання діяльності підрозділів кримінальної поліції» (14 квітня 2023 року, м. Кропивницький). Кропивницький: ДонДУВС, 2023. С. 357 – 360.

9. Lysenko O.V., Lunhol O.M., Haborets O.A. Law enforcement information and analytical support. Current issues in modern science. Issue № 3(9) 2023. Pp. 281-291. DOI: https://doi.org/10.52058/2786-6300-2023-3(9)-281-291.

10. Prosvirina T., Haborets O., Lunhol O. Analysis of the organization of information and analytical support of police activities / T. Prosvirina, O. Haborets, O. Lunhol// Наукові інновації та передові технології. № 1(15). 2023. Pp. 319 – 327. DOI: https://doi.org/10.52058/2786-5274-2023-1(15)-319-327.

11. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. Практичний посібник. Нью-Йорк і Женева, 2020. 119 с. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (Дата звернення: 15.08.2023).

12. OSINT Framework. URL: https://osintframework.com (Дата звернення: 15.08.2023).

References:

1. *Innovative methods and digital technologies in forensics, forensic examination, and legal practice:* Proceedings of the International Roundtable (2019). Kharkiv: Pravo.

2. Sevruk, V. H. (2021). *Zarubizhnyi dosvid vykorystannia informatsiino-analitychnoho zabezpechennia protydii zlochynam, shcho vchyniaiutsia orhanizovanymy hrupamy i zlochynnymy orhanizatsiiamy, yaki sformovani na etnichnii osnovi*. Protydiia zlochynnosti: problemy praktyky ta naukovo-metodychne zabezpechennia. Pivdennoukrainskyi pravnychyi chasopys [in Ukrainian].

3. Zlahoda, O.V., & Kurinnyi, O.V. (2021). *Aspekty efektyvnosti rozshuku bezvisno znyklykh osib [Aspects of the efficiency of missing persons search*]. Kyiv: NAIAU [in Ukrainian].

4. Zachek, O.I., Dmytryk, Yu.I., & Senyk V.V. (2023). *Rol shtuchnoho intelektu v pidvyshchenni efektyvnosti pravookhoronnoi diialnosti [The role of artificial intelligence in enhancing law enforcement efficiency]*. Lviv: Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav [in Ukrainian].

5. Blahuta, R.I., & Movchan, A.V. (2020). *Novitni tekhnolohii u rozsliduvanni zlochyniv: suchasnyi stan i problemy vykorystannia [Modern technologies in crime investigation: current state and usage challenges]*. Lviv: LvDUVS [in Ukrainian].

6. Buhera, O.I. (2021).*Vykorystannia shtuchnoho intelektu dlia zapobihannia zlochynnosti. Vcheni zapysky TNU imeni V.I. Vernadskoho [Utilizing artificial intelligence for crime prevention]*. Vcheni zapysky TNU imeni V.I. Vernadskoho [in Ukrainian].

7. Bortnyk, S.M. (2021). *Osoblyvosti rehuliuvannia vykorystannia shtuchnoho intelektu u pravookhoronnoi systemi [Regulation Features of Artificial Intelligence Usage in Law Enforcement System]*. Kharkiv, Khark. nats. un-t vnutr. Sprav [in Ukrainian].

8. Makarynska, A.V., & Lunhol, O.M. (2023). *Modern digital technologies in criminal analysis*. Kropyvnytskyi: DonDUVS [in English].

9. Lysenko, O.V., Lunhol, O.M., & Haborets, O.A. (2023). *Law enforcement information and analytical support.* Current issues in modern science [in English].

10. Prosvirina, T., Haborets, O., & Lunhol, O. (2023). *Analysis of the organization of information and analytical support of police activities.* Naukovi innovatsii ta peredovi tekhnolohii [in English].

11. *Protokol Berkli z vedennia rozsliduvan z vykorystanniam vidkrytykh tsyfrovykh danykh*. Berkeley Protocol on Digital Open Source Investigations (2020). New York and Geneva [in Ukrainian].

12. *OSINT Framework* (2023) [in English].