УДК 34:004.056.5
DOI https://doi.org/10.32689/2617-9660-2025-1(33)-6-11

Аганін Богдан Юрійович,
кандидат юридичних наук, головний спеціаліст Управління моніторингу дотримання прав людини Міністерства внутрішніх справ України, вул. Академіка Богомольця, 10, м. Київ, 01601; https//orcid.org/0000-0002-8654-3940

ОКРЕМІ ВИДИ НЕБЕЗПЕКИ У ПРОЦЕСІ РОЗМІЩЕННЯ ВІДКРИТОЇ ІНФОРМАЦІЇ У РІЗНОМАНІТНИХ ДЖЕРЕЛАХ ТА І МЕРЕЖІ ІНТЕРНЕТ

Анотація. *У науковій статті встановлено, що сучасний стан обміну і отримання інформації кардинально відрізняється від систем, які використовувалися два-три десятиліття раніше. Такі зміни пов'язані з швидким розвитком мережі Інтернет та інших засобів отримання інформації включно зі супутниковими системами.*

У статті обґрунтовано, що виокремлення технології OSINT має досить великий вплив на систему інформації в цілому, а також на розвиток наукових досліджень та технічних рішень в окремих галузях. Крім того використання відкритих джерел інформації дає можливість оцінки ризиків інвестицій та інших фінансових операцій, проте якщо так інформація є правдивою.

Проте разом з позитивними аспектами використання відкритих джерел інформації у зазначеній системі є досить вагомі недоліки. Перш за все що відкрита інформація може змінюватися з метою ведення інформаційної війни, що широко використовується засобами масової інформації Російської Федерації під час повномасштабного вторгнення в Україну.

З іншого боку використання відкритих джерел та застосування технологій штучного інтелекту можуть сприяти отриманню повної інформації про ті чи інші об'єкти і зазначена інформація може використовуватися для нанесення ударів по таким об'єктам за допомогою дронів або ракет.

Обґрунтовано, що з метою убезпечення форм і методів використання технології OSINT тобто інформації з відкритих джерел необхідно перш за все вдосконалювати систему правового регулювання і впливу на недобросовісних отримувачів відкритої інформації. З цією метою в Європейському Союзі вже прийняті окремі нормативні документи, які треба вивчити і в разі можливості використання в Україні підготувати відповідні пропозиції.

Зроблено висновки, що основними напрямами підвищення рівня безпеки у сфері використання відкритої інформації є крім правового регулювання можливість зменшення обсягу відкритої інформації, особливо у сфері оборони та інших сферах, які стосуються військових об'єктів та інфраструктурних об'єктів.

Ключові слова: *національна безпека України, OSINT, система отримання відкритої інформації, Інтернет, інформаційні мережі, зміни при використанні відкритої інформації, правове регулювання використання відкритої інформації, безпека окремих осіб.*

Ahanin Bohdan Yuriyovych,
Candidate of Legal Sciences, Chief Specialist at the Human Rights Monitoring Department of the Ministry of Internal Affairs of Ukraine, 10, Akademika Bohomoltsia Str., Kyiv, 01601; https//orcid.org/0000-0002-8654-3940

CERTAIN TYPES OF DANGERS IN THE PROCESS OF POSTING OPEN INFORMATION IN VARIOUS SOURCES AND ON THE INTERNET

Abstract. *The scientific article establishes that the current state of information exchange and acquisition is fundamentally different from the systems that were used two or three decades earlier. Such changes are associated with the rapid development of the Internet and other means of obtaining information, including satellite systems.*

The article substantiates that the isolation of OSINT technology has a fairly large impact on the information system as a whole, as well as on the development of scientific research and technical solutions in certain industries. In addition, the use of open sources of information makes it possible to assess the risks of investments and other financial transactions, but if so, the information is true.

However, along with the positive aspects of the use of open sources of information in the specified system, there are quite significant disadvantages. First of all, open information can be changed for the purpose of waging information warfare, which is widely used by the Russian Federation media during the full-scale invasion of Ukraine.

On the other hand, the use of open sources and the application of artificial intelligence technologies can contribute to obtaining complete information about certain objects, and this information can be used to strike such objects using drones or missiles.

It is substantiated that in order to secure the forms and methods of using OSINT technology, that is, information from open sources, it is necessary, first of all, to improve the system of legal regulation and influence on unscrupulous recipients of open information. For this purpose, the European Union has already adopted separate regulatory documents that need to be studied and, if possible, to prepare appropriate proposals for use in Ukraine.

It was concluded that the main areas of increasing the level of security in the field of using open information are, in addition to legal regulation, the possibility of reducing the volume of open information, especially in the field of defense and other areas related to military facilities and infrastructure facilities.

Key words: *national security of Ukraine, OSINT, system for obtaining open information, Internet, information networks, changes in the use of open information, legal regulation of the use of open information, security of individuals.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Сучасний стан використання інформації та її отримання відрізняється від попередніх форм і методів радикально. Розвідувальні органи всіх держав вже не використовують в переважній більшості агентурну та дипломатичну розвідку. Всі питання отримання інформації покладені на мережу Інтернет та інші мережі.

Особливе занепокоєння на сьогодні викликає використання інформації, яка є у вільному доступі і може використовуватися будь-ким.

Висвітлено основні проблеми у сфері використання відкритої інформації та інші впливу на безпеку окремих осіб, а також на національну безпеку.

Аналіз показує, що особливої уваги вимагають питання використання відкритої інформації з метою розвідувальних заходів а також з метою дискредитації та формування негативного іміджу як окремих осіб так і підприємств, установ та організацій.

Запропоновано розробляти окремі форми і методи правового регулювання відкритої інформації, а також відповідних технічних можливостей з метою запобігання і протидії використання інформації для спричинення шкоди

Подальший ефективний розвиток використання відкритої інформації має стимулюватися всіма форми і методами, проте встановлення певних обмежень є необхідним

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор, виділення не вирішених раніше частин загальної проблеми, котрим присвячується означена стаття. Теоретичною основою статті є певний спектр наукових і законодавчих джерел. Основними з них є закони України, окремі програми та інші нормативно-правові акти. Використовується також інформаційно-аналітичний матеріал, який висвітлює різні позитивні аспекти використання технології OSINT з метою підвищення ефективності розвитку науки і техніки. У статті використовувалися дослідження таких авторів як Жмур Н. В, Пик С., Клімушин П.С та ряд інших. Водночас, аналізувалися роботи таких дослідників як Легомінова С.В. та інші, які розробляли напрями щодо шкідливості технології OSINT.

Використовувалися іноземні джерела та окремі нормативні акти Європейського Союзу.

Формулювання цілей статті (постановка завдання). Метою пропонованого наукового дослідження є обгрунтування більш зваженого підходу до висвітлення та використання інформації у відкритих джерелах з метою запобігання негативного впливу такої інформації як на окремих осіб, так і на національну безпеку України.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. З часу виникнення людського суспільства та держав у світі безперервно точиться боротьба за отримання інформації, яка б давала змогу отримати певну перевагу однієї з держав над іншою, послаблення її, виникнення можливості отримання прибутку від тих чи інших джерел. При цьому використовувалась різноманітна інформація, але найбільш цінною виявлялася інформація, яка була отримана шляхом розвідки та таємних операцій.

Досить вдало питання розвідки та отримання інформації було висвітлено в підручнику, який

був підготовлений науково-педагогічним колективом Навчально-наукового інституту права ім. князя Володимира Великого Міжрегіональної академії управління персоналом «Оперативно-розшукова діяльність» [1]. У підручнику наведено посилання на Біблію де автори пишуть, що вже в Стародавні часи з метою встановлення могутності держави Ханаан Моісей відправляв своїх прибічників до зазначеної держави, які проводили опитування жителів Ханаану, змальовували його мапу та т. ін. [2]. Одним з творів який присвячений мистецтв розвідки став також трактат китайського полководця Сунь-Дзи [3]. Разом з тим він писав про військову розвідку як специфічного типу розвідки. Окремі питання розвитку розвідки висвітлені також і у статті Сушка О. [4].

З розвитком держав постійно розвивалась і розвідка, вдосконалювалися її форми і методи. В переважній більшості розвідка у різних державах будувалася для потреб війни, тому діяльності поширеною була також теорія ведення війни та розвідки з метою ведення війни К. фон Клаузевица «Про війну» [5].

При цьому якщо навіть в 20 сторіччі ще до Другої світової війни в більшості випадків використовувалась так звана «агентурна розвідка» та «дипломатична розвідка», тобто направлення своїх агентів на території інших країн з метою добування певної інформації, або підготовка спеціальних дипломатів для ведення розвідки, то вже у кінці 20 сторіччя зазначені форми отримання інформації поступово стали непотрібними.

В цілому можна виокремити декілька видів отримання таємної інформації, які використовувалися в процесі розвитку розвідки. Окремі дослідники визначають такі види:

– агентурна розвідка, тобто введення до країни, в якій у іншої країн є інтереси спеціально підготовлених осіб, які повинні збирати як таємну так і іншу інформацію та передавати її до спеціальних служб;

– дипломатична розвідка, направлення до певних країн дипломатів, які мають спеціальну підготовку та займаються відповідним збиранням інформації;

– технічна розвідка, тобто збирання інформації за допомогою різноманітних технічних пристроїв [6].

Поступово на заміну використання агентів, резидентів та просто шпигунів прийшли радіоелектронні та інші технічні засоби та пристрої. На сьогодні практично кожна країна, яка має супутники, може практично відслідковувати всі предмети, а також транспорт, будівництво та інші речі на території іншої країни.

Якщо розглядати Україну то можна констатувати, що у нас майже не має на жаль супутників – шпіонів, проте є досить розвинена система Інтернету та інших соціальних мереж, які дозволяють здійснювати відповідні заходи щодо проведення розвідки.

Проте на сьогодні у світі сформувалась досить цікава система яка має назву розвідки з відкритих джерел (Open source intelligence, OSINT) [7]. Одним з напрямів зазначеної діяльності вже зараз виділяється IMINT (imagery intelligence) видова розвідка. Ця система ставить за мету збір різноманітної розвідувальної інформації, яка отримана за допомогою фотографічної, оптико-електронної або радіолокаційної апаратури [1]. Основними джерелами отримання інформації є аерозйомка та космічна зйомка. При цьому інформація визначається на основі детального та ретельного аналізу великої кількості зображень, які отримані за допомогою зазначених видів зйомки.

Разом з тим на сьогодні є досить велика кількість інформації, що стосується економічної, соціальної , політичної, культурної та духовної сфер і яка є у відкритому доступі. В Україні є відповідні нормативні акти які регулюють види інформації, що можуть бути засекречені. У першу чергу до них відноситься Закон України «Про державну таємницю», у якому визначені основні напрями та види інформації, яка може бути засекречена. До сфер інформації, яка може бути засекречена відносяться:

– оборона та діяльності щодо забезпечення оборони держави;

– стан економіки держави;

– дослідження у сфері науки і техніки;

– відомості про зовнішні відносини держави;

– відомості щодо державної безпеки та питань охорони правопорядку [8].

Щодо відкритої так званої публічної інформації то у згаданому законі та в Законі України «Про доступ до публічної інформації» вказано, до неї відносяться дані: які відображають стан довкілля, вплив на життя і здоров'я громадян, якість продуктів, надзвичайні події , які впливають на стан життя і здоров'я громадян, або загрожують їхній безпеці, стан медичного обслуговування, стан освіти та охорони правопорядку [9].

На сьогодні збереження інформації та її нерозповсюдження є особливо важливим у зв'язку з повномасштабним вторгненням Російської Федерації та війною в Україні. Окремі питання

щодо дотримання відповідних норм стосовно розповсюдження інформації внесені також до Закону України «Про основи національного спротиву» [10] та до ряду інших нормативних актів.

Проте на практиці досить часто відбуваються порушення зазначено законодавства. Якщо засоби масової інформації повідомляють про такі небезпечні події, які викликані наприклад, діями тих чи інших керівників підприємств, установ та організацій і виникли у певному районі то для осіб, які моніторять ситуацію і роблять висновки що у даному районі розташовані наприклад, підприємства, які пов'язані з ядерною енергетикою та т. ін. не складає особливих проблем моніторити ситуацію в цьому районі. Тим більше вона пов'язана з впливом на стан життя і здоров'я людей.

Крім того працівники засоби масової інформації обов'язково проведуть опитування громадян та висвітлять карту та місцезнаходження об'єктів, які стали причиною надзвичайних ситуацій. Не треба бути дуже розумним, щоб зробити відповідні висновки де і як працювало підприємство. Особливо важливим є також питання притягнення до відповідальності осіб, які винні у створенні надзвичайних ситуацій.

В переважній більшості суд є відкритим, працівники засоби масової інформації висвітлюють всі події коментують та т. ін. Для осіб, які зацікавлені у тому, щоб встановити, яке підприємство розташоване на зазначений території, його нам діяльності та т. ін. не становить особливої проблеми все це встановити. А якщо пов'язати отримані дані з даними космічної розвідки, то всі спроби, щось сховати стають марними.

На сьогодні вже є цілий ряд публікацій, які вказують, що використання OSINT перш за все небезпечне як для окремих галузей народного господарства так і для національної безпеки в цілому. Легомінова С.В. разом з кількома авторами проаналізували шкідливість технології OSINT [11] і довели, що її використання повинно бути певною мірою обмежене.

Вони довели, що вимагає вирішення питання про етичність та законність використання технології OSINT. Особливо важливим є використання технології відкритого збору інформації в комерційних цілях. Якщо у Європейському Союзі існують певні механізми, які встановлюють обмеження використання відкритих баз даних для збору відповідної інформації, то в Україні ще цього немає.

Окремо слід зазначити, що на даний час в Україні йде повномасштабна війна у ході якої Російська Федерація використовує всі форми і методи та засоби. Пропагандистами Російської Федерації досить часто використовуються відкриті джерела інформації для створення ІПСО. При цьому відкрита інформація певною мірою змінюється перекручуються різні факти. Зазначені спеціальні операції спрямовані на населення України так і на населення інших країн. За допомогою таких операцій наприклад, формуються негативні риси більшості заходів, які проводяться в Україні наприклад, таких як мобілізація, робота державних органів та т. ін.

Відповідно треба розробляти заходи протидії таким ІПСО.

Крім того необхідно розробляти відповідні законодавчі акти, які б передбачали, що якщо інформація знаходиться у публічному доступі, то це не дає підстав для її використання у зміненому вигляді або поширення в неповному обсязі чи перекручено. Користувачі мають поважати конфіденційність, особливо особистої інформації, яка є наприклад, у соціальних мережах. На сьогодні вже цілий ряд країн починають вживати заходи для захисту від неправомірного використання відкритих баз даних для формування впливу чи створення негативного контенту.

Клімушин П. С. та Білобров А. В аналізуючи технології OSINT, показують, що їх використання є корисним для оперативно-розшукової діяльності, проте необхідно виключити питання упередженого використання відкритої інформації та чітке розуміння аналізу, який проводиться [12].

Про позитивний вплив на ефективність використання технології OSINT пишуть і інші автори [13, 14]. Разом з тим у наукових працях існують окремі висновки, що технології OSINT є певною мірою небезпечними як для громадян так і для національної безпеки України в цілому.

Легомінова С. стверджує, що не існує універсального інструменту який можна використовувати з метою захисту від збору відкритих даних про особу чи організацію. Разом з тим вона пропонує ряд окремих превентивних заходів які в окремих випадках дозволяють перш за все зменшити шкідливість неправомірного чи неправильного використання технології OSINT.

Серед пропозицій можна виокремлювати такі:

– обмеження висвітлення особистої інформації у соціальних мережах для громадян;

– навчання та підвищення рівня відповідальності персоналу організацій щодо висвітлення інформації, яка в подальшому може бути використана з шкідливою метою

– проведення відповідного моніторингу з метою отримання розуміння того, яка інформація, може бути використана з негативною метою;

– розроблення відповідних заходів щодо усунення наслідків шкідливого використання відкритої інформації;

– впровадження окремих форм і методів дезінформації, особливо у сфері безпеки та оборони, або поширення різноманітної інформації, яка може використовуватися, але тільки в обмеженому вигляді;

– зменшення доступу представників засобів масової інформації особливо на місця надзвичайних ситуацій та пряма заборона проведення зйомок і інших заходів щодо місця та результатів надзвичайних ситуацій [11].

Проте зазначені заходи необхідно використовувати з посиланням на від нормативні акти, які треба прийняти.

Таким чином, впровадження ефективних заходів захисту від збору інформації за допомогою відкритих джерел є невід'ємною складовою стратегії забезпечення кібербезпеки для сучасних організацій.

Висновки та перспективи подальших досліджень:

1. Використання технології OSINT має позитивний вплив на розвиток наукових досліджень у всьому світ в тому числі і в Україні, адже сучасні соціальні мережі та Інтернет містять досить багато інформації, яка може бути використана як науковцями так і практиками.

2. Поряд з позитивними рисами використання технології OSINT визначаються і певні застереження, адже відкриті джерела інформації дають можливість одну й ту ж саму інформацію використовувати в різних цілях. Особливо часто інформація у перекрученому вигляді використовується засобами масової інформації Російської Федерації для створення інформаційно-пропагандистських завдань, які стосуються як окремих громадян так і держави в цілому. Таким чином відкрита інформація перетворюється на відверту пропаганду. Можуть необхідно розробити відповідні дії, щоб зміни які додаються до відкритої інформації або її перекручування, яке потім тиражують окремі засоби масової інформації підлягали відповідний кваліфікації в особи, які розповсюджують зазначену інформацію могли притягатися до відповідальності.

3. Є також необхідність підготовки окремих законодавчих актів щодо правового регулювання використання відкритої інформації та її змінення з метою дискредитації чи іншої шкоди.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Оперативно-розшукова діяльність. Навчальний посібник автори С. В. Князєв, А. М. Кислий., І. А., Козаченко О. І., Ільницький В. Я., Марець Б. М., Кислий А. М., Демедюк С. В. та ін. Нац. поліція України. Київ: Людмила, 2019. 239 с.
2. Біблія Книги Старого Завіту. Четверта книга Мойсеєя. Глава 13, ст. 3, 18–30, 1990 р.
3. Сунь-дзи. Мистецтво війни; пер. С. Лесняк. Львів : Видавництво Старого Лева, 2016. 103 с.
4. Сушко О. Поняття розвідки та особливості її ведення в антсько-візантійських конфліктах VI століття. *Наукові праці Міжрегіональної Академії управління персоналом. Юридичнінауки*,2024.4(72),43–48.https://doi.org/10.32689/2522-4603.2024.4.8
5. Клаузевіц К. Найважливіші принципи ведення війни; пер. С. Іванчук. Київ : Арій, 2023. 384 с
6. Пик С. Розвідувальна діяльність у сучасному світі та її пріоритети. *Вісник Львівського університету. Серія міжнародні відносини*. 2013. Випуск 32. URL: https://intrel.lnu.edu.ua/wpcontent/uploads/2015/10/VLNU_Mv_2013_32_12.pdf
7. Жмур Н. В. Історія становлення та сучасний стан технології пошуку інформації. *OSINT Юридичний вісник НАУ*. 2022. 3 (64)
8. Про державну таємницю Закон України від 21 січня 1994 року № 3855-XII. Відомості Верховної Ради України (ВВР), 1994, № 16, ст.93
9. Про доступ до публічної інформації Закон України від 13 січня 2011 року № 2939-VI Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314
10. Про основи національного спротиву Закон України від 16 липня 2021 року № 1702-IX Відомості Верховної Ради (ВВР), 2021, № 41, ст.339
11. Легомінова С. В. Небезпека інструментів OSINT та способи пом'якшення наслідків їх використання для організації. Кібербезпека. *Освіта, наука, техніка* № 1 (25) 2024.
12. Клімушин П. С., Білобров А. В. Використання технологій OSINT для отримання інформації. Протидія кіберзлочинності та торгівлі людьми Харків 2020. URL: https://www.univd.edu.ua/general/publishing/konf/27_05_2020/pdf/39.pdf
13. Ісмайлов К. Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. Південноукраїнський правничий часопис. 2016. № 2. С. 110–113.
14. Жарков Я. М, Васильєв А. О. Наукові підходи щодо визначення суті розвідки з відкритих джерел. Вісник Київського національного університету імені Тараса Шевченка. 2013. Вип. ЗО. С. 38–41.
15. Мірошниченко О. І., Ланде Д. В. Роль методів OSINT та їх застосування під час воєнних конфліктів Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених. URL: https://ela.kpi.ua/server/api/core/bitstreams/a04460d3-93d9-48b7-ba83 f5bace2083ec/content

REFERENCES:

1. Operatyvno-rozshukova diialnist [Operational and investigative activities Textbook] (2019). authors S. V. Knyazev, A. M. Kyslyi., I. A., Kozachenko O. I., Ilnytskyi V. Ya., Marets B. M., Kyslyi A. M., Demedyuk S. V. and others. National Police of Ukraine. Kyiv: Lyudmila, 239 p.
2. Bibliia Knyhy Staroho Zavitu [Bible Books of the Old Testament] (1990). The Fourth Book of Moses. Chapter 13, p. 3, 18–30.
3. Sun, Tzu. (2016). Mystetstvo viiny [The Art of War]. trans S. Lesnyak. Lviv: Old Lion Publishing House, 103 p.
4. Sushko, O. (2024). Poniattia rozvidky ta osoblyvosti yii vedennia v antsko-vizantiiskykh konfliktakh VI stolittia [The concept of intelligence and features of its conduct in the Anti-Byzantine conflicts of the VI century]. *Scientific works of the Interregional Academy of Personnel Management. Legal Sciences*, 4 (72), 43–48. https://doi.org/10.32689/2522-4603.2024.4.8
5. Clausewitz, K. (2023). Naivazhlyvishi pryntsypy vedennia viiny [The most important principles of warfare]. trans S. Ivanchuk. Kyiv: Ariy, 384 p
6. Pyk, S. (2013). Rozviduvalna diialnist u suchasnomu sviti ta yii priorytety [Intelligence activity in the modern world and its priorities Bulletin of Lviv University]. *International relations series.* Issue 32. Retrieved from: https://intrel.lnu.edu.ua/wpcontent/uploads/2015/10/VLNU_Mv_2013_32_12.pdf
7. Zhmur, N. V. (2022). Istoriia stanovlennia ta suchasnyi stan tekhnolohii poshuku informatsii [History of formation and current state of information retrieval technologies]. *OSINT Legal Bulletin of NAU* 3 (64).
8. Pro derzhavnu taiemnytsiu Zakon Ukrainy [On State Secrets Law of Ukraine] dated January 21, 1994 № 3855-XII Bulletin of the Verkhovna Rada of Ukraine (VVR), 1994, No. 16, p. 93.
9. Pro dostup do publichnoi informatsii Zakon Ukrainy [On Access to Public Information Law of Ukraine] dated January 13, 2011 No. 2939-VI Bulletin of the Verkhovna Rada of Ukraine (VVR), 2011, No. 32, p. 314.
10. Pro osnovy natsionalnoho sprotyvu Zakon Ukrainy [On the Foundations of National Resistance Law of Ukraine] dated July 16, 2021 No. 1702-IX Bulletin of the Verkhovna Rada (VVR), 2021, No. 41, p. 339.
11. Legominova, S.V. (2024). Nebezpeka instrumentiv OSINT ta sposoby pomiakshennia naslidkiv yikh vykorystannia dlia orhanizatsii [The Danger of OSINT Tools and Ways to Mitigate the Consequences of Their Use for the Organization]. Cybersecurity. Education, Science, Technology No. 1 (25).
12. Klimushyn, P. S., Bilobrov, A. V. (2020). Vykorystannia tekhnolohii OSINT dlia otrymannia informatsii [Using OSINT technologies to obtain information]. Counteraction to cybercrime and human trafficking Kharkiv. Retrieved from: https://www.univd.edu.ua/general/publishing/konf/27_05_2020/pdf/39.pdf
13. Ismailov, K. Yu. (2016). Osoblyvosti kryminalnoi rozvidky z vidkrytykh dzherel yak instrument zbyrannia operatyvnoi informatsii [Peculiarities of criminal intelligence from open sources as a tool for collecting operational information]. *South Ukrainian Law Journal*. No. 2. P. 110–113.
14. Zharkov, Ya. M., Vasyliev, A. O. (2013). Naukovi pidkhody shchodo vyznachennia suti rozvidky z vidkrytykh dzherel [Scientific approaches to determining the essence of intelligence from open sources]. *Bulletin of the Taras Shevchenko National University of Kyiv.* Issue 30. P. 38–41.
15. Miroshnychenko, O. I., Lande, D. V. Rol metodiv OSINT ta yikh zastosuvannia pid chas voiennykh konfliktiv Vseukrainska naukovo-praktychna konferentsiia studentiv, aspirantiv ta molodykh vchenykh [The role of OSINT methods and their application during military conflicts All-Ukrainian scientific and practical conference of students, postgraduates and young scientists] Retrieved from: https://ela.kpi.ua/server/api/core/bitstreams/a04460d3-93d9-48b7-ba83f5bace2083ec/content