ВІЙСЬКОВІ НАУКИ

DOI: https://doi.org/10.32839/2304-5809/2020-5-81-40
УДК 351.746.1

Фаріон О.Б.
Національна академія Державної прикордонної служби України

МЕТОДОЛОГІЧНІ ОСНОВИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ РОЗВІДКИ В ГЛОБАЛЬНІЙ МЕРЕЖІ ІНТЕРНЕТ ОПЕРАТИВНИМИ ПІДРОЗДІЛАМИ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

Анотація. Розроблено методологічні основи інформаційно-аналітичної розвідки в глобальній мережі Інтернет оперативними підрозділами Державної прикордонної служби України. Представлено окремі інструменти пошуку інформації в Інтернеті. Запропоновано певну послідовність етапів та методів інформаційно-аналітичної розвідки. Рекомендовано поглиблений аналіз отриманої інформації здійснювати із використанням спеціального програмного забезпечення. Для практичного застосування запропонований механізм інформаційно-аналітичної розвідки в глобальній мережі Інтернет надасть можливість оперуповноваженим оперативних підрозділів отримувати інформацію, яка має оперативний інтерес, та покращити аналітичні дослідження в рамках проведення заходів з протидії злочинності на кордоні України.

Ключові слова: інформаційно-аналітична розвідка, інформація, аналіз, Інтернет, оперативний підрозділ.

Farion Oleg
National Academy of the State Border Guard Service of Ukraine

METHODOLOGICAL BASES OF THE INFORMATIONAL AND ANALYTICAL INTELLIGENCE IN THE GLOBAL INTERNET NETWORK BY OPERATIONAL UNITS OF THE STATE BORDER GUARD SERVICE OF UKRAINE

Summary. In the scientific article the methodological bases of informational and analytical intelligence in the global Internet network by operational units of the State Border Guard Service of Ukraine are developed. The sequence of actions (stages) is proposed, aimed at the implementation of informational and analytical intelligence in the global Internet network: the definition of the purpose (goals) and the formation of the information request; review of intelligence resources; search procedure planning; implementation of search strategy (plan); accumulation and processing of the obtained information based by the results of informational and analytical intelligence; formation of analytical products. It is noted that obtaining (extracting) information (data) necessary for operational and investigative activities, is recommended to carry out both from open and hidden resources of the global Internet network. Some tools for searching indexed and non-indexed information (data) by Internet search systems are presented. The usage of various informational and analytical intelligence tools allows analysts of operational units of the State Border Guard Service of Ukraine to check the information obtained from the global Internet network. Advanced analysis of the received information is recommended to do using special software iBase, Analyst's Notebook, etc. For each type of search methods of informational and analytical intelligence are proposed. The principle of legality must be ahead while choosing and applying informational and analytical intelligence tools. The reliable data of the facts of illegal activity of individuals or groups of individuals obtained as a result of informational and analytical intelligence can be used as evidence in criminal proceedings. The practical value of the obtained scientific result is that the proposed toolkit will enable operatives of operational units of the State Border Guard Service of Ukraine to obtain information which has operational interest for taking measures to resist crime at the state border. In addition, developed methodological bases of informational and analytical intelligence in the global Internet network are a tool for improving analytical research.

Keywords: informational and analytical intelligence, information, analysis, Internet, operational unit.

Постановка проблеми. В сучасних умовах глобалізації інформаційних і комунікаційних технологій (Інтернет-технологій) у світі поширюється електронне середовище, а мережеві форми організації та відповідні механізми управління різними сферами діяльності суспільства стають більш домінуючими. Такі досягнення дають зловмисникам нові можливості для здійснення і поширення протиправної діяльності із використанням більш досконалих способів та методів анонімного спілкування та прихованого обміну інформацією.

За даними держав ЄС поширення Інтернет-технологій забезпечує стійкість організованої злочинності до превентивних заходів правоохоронних органів [1]. Так, організовані злочинні угруповання для переміщення заборонених товарів (наприклад, засобів терору, наркотичних засобів) до пунктів призначення стали використовують все більш доступні та розвинути види транспортного сполучення – інфраструктуру портів, контейнеровози, вантажні автомобілі, приватні човни, літаки, квадрокоптери тощо. Разом із тим, використання ними ресурсів Інтернету дозволило приховано отримувати незаконно здобуті доходи, накопичувати, легалізовувати та використовувати їх у подальшій протиправній діяльності. Ресурсами глобальної мережі Інтер-

нету є сукупність інтегрованих технічних, програмно-апаратних засобів та інформації, призначеної для публікації в текстовій, графічній та мультимедійній формах [2].

Отже, зазначені обставини ускладнюють діяльність правоохоронних органів щодо протидії організованій злочинності та обумовлюють необхідність застосування більш дієвих інструментів отримання інформації (даних) з глобальної мережі Інтернету.

Аналіз останніх досліджень і публікацій. Дослідженням окремих питань щодо пошуку та отримання з Інтернету правоохоронними органами інформації щодо протиправної діяльності займались вітчизняні та закордонні вчені, зокрема: Базилевич В.М., Дика Є.О., Зачек О.І., Знахур С. В., Nithyanand Rishab, Cai Xiang, Johnson Rob, Wang Tao, Goldberg Ian, Marc Juarez, Mohsen Imani, Mike Perry [3–9] та інші. Разом з тим, із появою нових прийомів та способів застосування ресурсів Інтернету для скоєння злочинів, наявні наукові розробки та методичні рекомендації щодо протидії злочинам стають менш ефективними в діяльності правоохоронних органів. Тому пошук нових або удосконалення розроблених інструментальних засобів отримання інформації з глобальної мережі Інтернет є актуальним для протидії злочинності та обумовлює важливість обраної теми.

Метою статті є розробка методологічних основ інформаційно-аналітичної розвідки в глобальній мережі Інтернет оперативними підрозділами Державної прикордонної служби України.

Виклад основного матеріалу дослідження. З метою запобігання та припинення кримінальних правопорушень оперативними підрозділами Державної прикордонної служби (далі – ДПС) України проводяться комплекс заходів, спрямованих на пошук і фіксацію фактичних даних про протиправну діяльність осіб (груп осіб), виявлення, установлення місцезнаходження розшукуваних осіб [10]. Одним із таких заходів є оперативна ідентифікація (ототожнення) осіб, предметів тощо за окремими ознаками, властивостями та іншими даними, що у поєднані з аналізом отриманих даних є процесами інформаційно-аналітичної розвідки [11].

В оперативних підрозділах ДПС України інформаційно-аналітичною розвідкою (далі – ІАР) є спеціальний метод оперативного (ініціативного) пошуку, призначений для цілеспрямованого пошуку та отримання нових або додаткових даних про об'єкти, які становлять оперативний інтерес і встановлення причинно-наслідкових зв'язків між ними. ІАР полягає у здійсненні пошуку, виявленні, зборі, обробці, систематизації і накопиченні інформації та отримані на основі комплексного її аналізу нових або додаткових відомостей про об'єкти, події, факти та явища, що становлять оперативний інтерес. Вона спрямована на комплексне дослідження інформації за допомогою багатофакторного аналізу розрізнених відомостей про об'єкти, що вивчаються, шляхом їх системної обробки з використанням різноманітних прийомів і методів.

Правоохоронними органами Федеративної Республіки Німеччини та Сполучених Штатів Америки ІАР широко застосовується для пошуку інформації в глобальній мережі Інтернет в рамках проведення заходів щодо боротьби з організованою злочинністю та тероризмом.

За оцінками інформаційно-аналітичної компанії IDC (*International Data Corporation*) обсяги цифрової інформації в мережі Інтернет по завершенню 2020 року може досягти 40 зеттабайт, з яких до 80% буде становити так звана погано-, слабоструктурована інформація, що циркулює у вигляді інтервальних медіа-потоків, інформації соціальних мереж, медіа-мереж, мережних мобільних пристроїв тощо [12]. Тенденції поширення структурованої й слабоструктурованої інформації в глобальній мережі Інтернет з 2000 року представлено на рисунку 1.

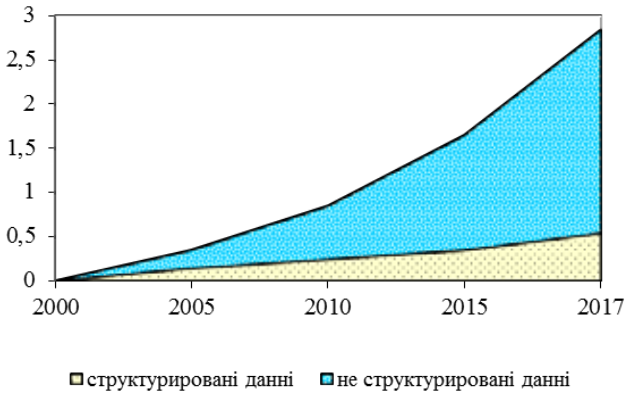

Рис. 1. Тенденції поширення структурованої й слабоструктурованої інформації в глобальній мережі Інтернеті з 2000 року

Інформація, яку можна отримати з різних загальнодоступних сайтів Інтернету, є відкритою та індексованою пошуковими системами, такими, як, наприклад, Google, Yahoo, Yandex.

Більш складною для пошуку є прихована від загального користування інформація, методи (способи) роботи з якої є специфічними. Тому в протиправній діяльності прихована інформація набула широкого розповсюдження та активно використовується. Обмін такого роду інформацією здійснюється зловмисниками в «Deep Web» та «Dark Web» за допомогою спеціальних технологій (наприклад, «Darknet», «TahoeLAFS», «Freenet»).

Подальше вивчення досвіду діяльності уповноважених органів зазначених держав дозволило сформувати етапи ІАР в глобальній мережі Інтернет для отримання (добування) інформації в інтересах оперативно-розшукової діяльності оперативних підрозділів ДПС України:

1. Визначення мети (цілей) та формування інформаційного запиту. Тут здійснюється цілеспрямоване обмеження і конкретизація завдань пошуку.

2. Огляд розвідувальних ресурсів. Цей етап полягає у виборі елементів Інтернет-ресурсів та інструментів виконання завдань ІАР.

3. Планування пошукової процедури. Основна мета цього процесу – визначення шляхів і способів раціонального вирішення пошукового завдання. Цей етап включає розробку конкретних пошукових стратегій відповідно до пріоритетів виконання кожного завдання із урахуванням набору вимог.

4. Реалізація стратегії (плану) пошуку. Технологічне вирішення пошукового завдання із використанням емулятору, наприклад Nox, App, Player.

4.1. Застосування ІАР для пошуку та отримання відкритої (індексованої) інформації в глобальні мережі Інтернету із використанням:

а) людського інтелекту, на основі застосування окремих інструментів HUMINT, з використанням різних методів обміну інформацією через інших (підставних) осіб, фірм тощо;

б) соціальної медіа-аналітики, на основі застосування окремих інструментів SOCMINT, з використанням нав'язування тощо або не інтрузивних засобів;

в) аналізу зображень, фотографій, рисунків тощо, на основі застосування окремих інструментів IMINT;

г) інтелектуального аналізу електронних сигналів, на основі аналізу сигналів комунікації (наприклад, про iP-адреси) за допомогою окремих інструментів SIGINT;

д) геопросторовий інтелект-аналіз, на основі отримання і аналізу інформації (даних) про місце знаходження об'єкта у просторі за допомогою окремих інструментів GEOINT.

Для пошуку інформації (даних) з відкритим вихідним кодом в глобальній мережі Інтернет можуть застосовуватись такі інструменти:

SpiderFoot – дозволяє автоматично використовувати запити значної кількості джерел для збору інформації про електронні листи, іменах, IP-адреси, доменні імена та інші дані, пов'язані між собою.

Creepy – це інструмент, за допомогою якого збирається інформація про геолокацію з використанням різних соціальних мереж і сервісів розміщення зображень. Надає можливість отримати звіти про точне місцезнаходження на карті і дату для експорту та додаткового аналізу.

Snitch – це інструмент на основі Python, який дозволяє автоматизувати процес збору інформації для певного домену, використовуючи вбудовані Доркі.

Maltego – це інструмент для отримання інформації про IP-адреси, ідентифікації автономної системи і місця розташування об'єкта пошуку.

TheHarvester – це інструмент для пошуку e-mail адрес, імен піддоменів, віртуальних хостів, відкритих портів-банерів, IP-адрес тощо.

Recon-ng – інструмент для реалізації соціальної інженерії та отримання відомостей про адреси електронної пошти, пов'язаних з доменом.

Sudomy – це інструмент, створений з використанням bash-script для швидкого і всебічного аналізу доменів і збору піддоменів.

4.2. Застосування ІАР для пошуку та отримання неіндексованої інформації в глобальній мережі Інтернету із використанням спеціальних методів (способів) та програмного забезпечення. Пошук та отримання такого роду інформації в «Deep Web» або «Dark Web» може здійснюватись з використанням низки інструментів (пошукових систем), зокрема:

Pipl – дозволяє із використанням програм-роботів знаходити в прихованих базах даних та завантажувати контактні данні та іншу інформацію з особистого профілю об'єкта пошуку.

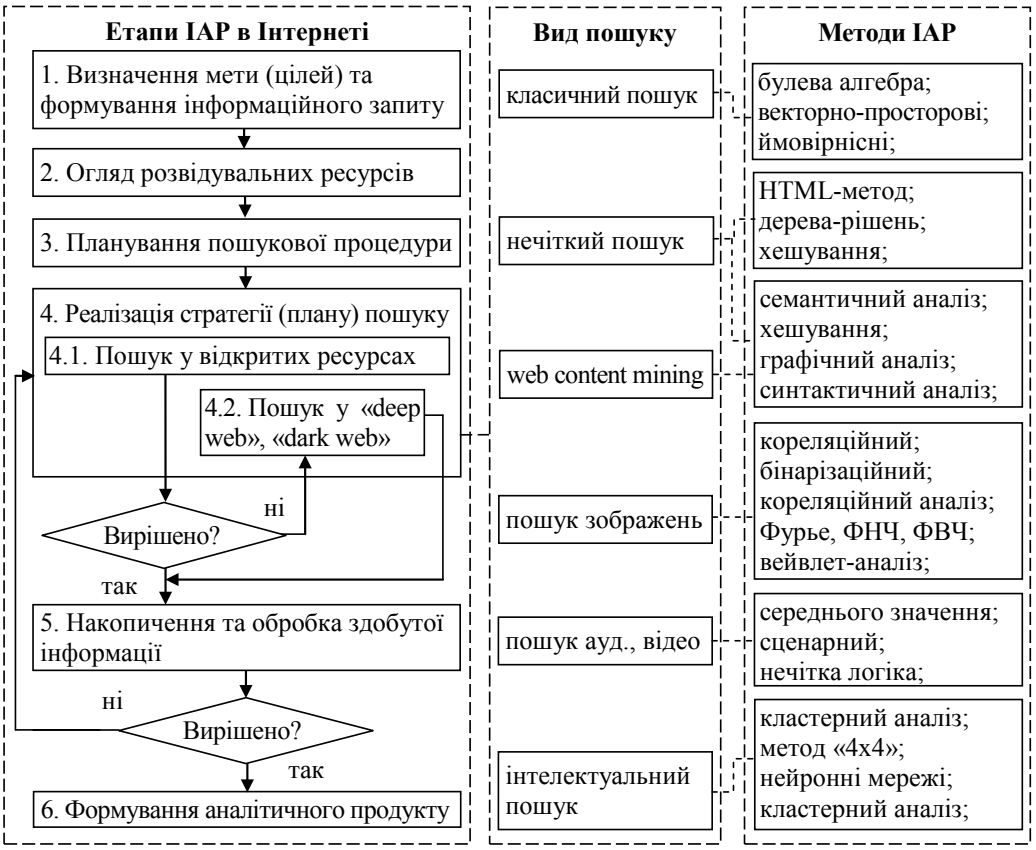

Рис. 2. Методологічні основи інформаційно-аналітичної розвідки в глобальній мережі Інтернет оперативними підрозділами Державної прикордонної служби України

Mylife – дозволяє отримати дані про об'єкт пошуку (наприклад, вік, минулі і поточні місця проживання, номери телефонів, адреси електронної пошти, місця роботи, інструкції, фотографії, родичів).

DuckDuckgo – дозволяє генерувати результати пошуку з значної кількості окремих джерел, включаючи пошукові системи Bing, Yahoo, Yandex і Yummly.

Fazzle.com – дозволяє отримати інформацію за результатами перегляду значної кількості змінених мета-веб-індексів.

Start Page – це інструмент пошуку, який на відміну від інших пошукових систем не записує IP-адресу особи, яка здійснює пошук інформації.

Spokeo – дозволяє отримати адресу електронної пошти, профілі з соціальних мереж, відомості про судимість та іншу інформацію про об'єкт пошуку.

Для отримання інформації використовується спеціальне програмне забезпечення, наприклад: «Tor», «Advanced IP scanner», «NMAP», «NESKA».

Використання різних інструментів ІАР надасть можливість аналітикам оперативних підрозділів перевіряти інформацію, отриману з Інтернету.

5. Накопичення та обробка здобутої інформації за результатами ІАР. На цьому етапі отримана інформації зіставляється, систематизується і завантажується для подальшого поглибленого дослідження з використанням спеціального програмного забезпечення (наприклад, iBase, Analyst's Notebook).

6. Формування аналітичних продуктів за результатами ІАР. За результатами обробки розробляється аналітичний продукт (аналітичний звіт).

На основі проведеного дослідження [13; 14] та інших джерел розроблено методологічні основи ІАР в глобальній мережі Інтернеті оперативними підрозділами ДПС України (див. рис. 1).

Під час вибору та застосування інструментів ІАР необхідно дотримуватись принципу законності.

Отримані за результатами ІАР достовірні данні про факти протиправних діянь окремих осіб або груп осіб можуть використовуватись як докази в кримінальному провадженні.

Висновки з даного дослідження і перспективи. Таким чином, розроблено методологічні основи ІАР в глобальній мережі Інтернет оперативними підрозділами ДПС України.

На практиці запропонований механізм ІАР в глобальній мережі Інтернет надасть можливість оперуповноваженим оперативних підрозділів отримувати інформацію, яка має оперативний інтерес, та покращити аналітичні дослідження в рамках проведення заходів з протидії злочинності на державному кордоні України.

У подальшому дослідженні необхідно деталізувати інструментарій ІАР в глобальній мережі Інтернет відповідно до специфіки завдань, покладених законодавством на оперативні підрозділи ДПС України.

Список літератури:

1. Freedom and security. URL: https://www.europol.europa.eu/events/freedom-and-security (дата звернення: 07.04.2020).
2. Бородій Н.А. Інтернет-ресурси: поняття, види, їх цільова аудиторія. URL: https://prezi.com/p/f3mf-nqs3r4n/presentation/ (дата звернення: 13.04.2020).
3. Базилевич В.М. Недоліки анонімних Інтернет-сервісів на прикладі мережі Tor. *Новітні технології у науковій діяльності і навчальному процесі* : зб. тез доп. Всеукр. наук.-практ. конф., м. Чернігів, 18-19 травн. 2016 р. Чернігів : ЧНТУ, 2016. 314 с.
4. Дика Є.О. Щодо ефективності Державного бюро розслідувань у протидії злочинності. *Державне бюро розслідувань: на шляху розбудови* : матеріали міжн. наук.-пр. конф., м. Одеса, 16 червн. 2018 р. Одеса : Юридична література, 2018. 432 с.
5. Зачек О.І. Протидія комп'ютерним злочинцям, що перебувають поза зоною досяжності правоохоронних органів України. *Теоретичні та практичні засади протидії злочинності в сучасних умовах* : зб. тез доп. міжнар. наук.-практ. конф., м. Львів, 16 жовт. 2015 р. Львів : ЛДУВС, 2015. 260 с.
6. Знахур С.В. Особливості реалізації інтелектуальної системи на базі azure machine learning системи обробки інформації : зб. наук. пр. 2(148). Харків : ХНУПС, 2017. 148 с.
7. Nithyanand Rishab, Cai Xiang, Johnson Rob. Glove: A Bespoke Website Fingerprinting Defense / 13th Workshop on Privacy in the Electronic Society. Scottsdale, Arizona, USA, 2014. P. 131–134.
8. Wang Tao, Goldberg Ian. Walkie-Talkie: An Effective and Efficient Defense against Website Fingerprinting / 21st European Symposium on Research in Computer Security. 2015.
9. Toward an Efficient Website Fingerprinting Defense / Marc Juarez, Mohsen Imani, Mike Perry et al. / 21st European Symposium on Research in Computer Security. 2016. P. 27–46.
10. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 р. № 2135-XII. Дата оновлення: 28.08.2019. URL: http://zakonl.rada.gov.ua/laws/show/2135-12/page (дата звернення: 12.09.2019).
11. Харабєрюш О.І. Оперативно-розшукове забезпечення протидії контрабанді в Україні : автореф. дис. ... д-ра юрид. наук : 12.00.09. Дніпро, 2016. 36 с.
12. Гула Л.Ф. Оптимізація інформаційно-аналітичного забезпечення оперативних підрозділів у протидії злочинам, що вчиняються організованими злочинними групами : зб. наук. статей і матеріалів доп. між нар. наук.-практ. конф., м. Львів, 22 груд. 2017 р. Львів : ЛівДУВС, 2018. 407 с.
13. Симанков В.С., Толкачев Д.М. Методы и алгоритмы поиска информации в Интернете : монографія. Москва : БИБЛИО-ГЛОБУС, 2017. 332 с.
14. Болюбаш Ю.Я. Методи та засоби опрацювання інформаційних ресурсів великих даних в системах територіального управління : дис. … канд. технічн. наук : 01.05.03. Нац. університет «Львівська політехніка». Львів, 2017. 234 с.

References:

1. Freedom and security. URL: https://www.europol.europa.eu/events/freedom-and-security (data zvernennia: 07.04.2020).
2. Borodii N.A. Internet-resursy: poniattia, vydy, yikh tsilova audytoriia [Internet resources: concepts, types, their target audience]. URL: https://prezi.com/p/f3mf-nqs3r4n/presentation/ (data zvernennia: 13.04.2020).

3. Bazylevych, V.M. (2016). Nedoliky anonimnykh Internet-servisiv na prykladi merezhi Tor [Disadvantages of anonymous Internet services on the example of the Tor network]. *Novitni tekhnolohii u naukovii diialnosti i navchalnomu protsesi*: zb. tez dop. Vseukr. nauk.-prakt. konf., m. Chernihiv, 18-19 travn. 2016 r. Chernihiv: ChNTU, 314 p.
4. Dyka, Ye.O. (2018). Shchodo efektyvnosti Derzhavnoho biuro rozsliduvan u protydii zlochynnosti [Regarding the effectiveness of the State Bureau of Investigation in combating crime]. *Derzhavne biuro rozsliduvan: na shliakhu rozbudovy* : materialy mizhn. nauk.-pr. konf., m. Odesa, 16 chervn. 2018 r. Odesa: Yurydychna literatura, 432 p.
5. Zachek, O.I. (2015). Protydiia kompiuternym zlochyntsiam, shcho perebuvaiut poza zonoiu dosiazhnosti pravookhoronnykh orhaniv Ukrainy [Countering computer criminals who are out of reach of Ukrainian law enforcement agencies]. Teoretychni ta praktychni zasady protydii zlochynnosti v suchasnykh umovakh: zb. tez dop. mizhnar. nauk.-prakt. konf., m. Lviv, 16 zhovt. 2015 r. Lviv: LDUVS, 260 p.
6. Znakhur, S.V. (2017). Osoblyvosti realizatsii intelektualnoi systemy na bazi azure machine learning systemy obrobky informatsii [Features of the implementation of an intelligent system based on azure machine learning information processing system]: zb. nauk. pr. 2(148). Kharkiv: KhNUPS, 148 p.
7. Nithyanand Rishab, Cai Xiang, Johnson Rob (2014). Glove: A Bespoke Website Fingerprinting Defense / 13th Workshop on Privacy in the Electronic Society. Scottsdale, Arizona, USA, pp. 131–134.
8. Wang Tao, Goldberg Ian (2015).Walkie-Talkie: An Effective and Efficient Defense against Website Fingerprinting / 21st European Symposium on Research in Computer Security.
9. Toward an Efficient Website Fingerprinting Defense / Marc Juarez, Mohsen Imani, Mike Perry et al. / 21st European Symposium on Research in Computer Security. 2016. P. 27–46.
10. Pro operatyvno-rozshukovu diialnist [About operative-search activity]: Zakon Ukrainy vid 18.02.1992 r. № 2135-XII. Data onovlennia: 28.08.2019. URL: http://zakonl.rada.gov.ua/laws/show/2135-12/page (accessed: 12.09.2019).
11. Kharaberiush, O.I. (2016). Operatyvno-rozshukove zabezpechennia protydii kontrabandi v Ukraini [Operational and search support of anti-smuggling in Ukraine]: avtoref. dys. ... d-ra yuryd. nauk: 12.00.09. Dnipro, 36 p.
12. Hula, L.F. (2018). Optymizatsiia informatsiino-analitychnoho zabezpechennia operatyvnykh pidrozdiliv u protydii zlochynam, shcho vchyniaiutsia orhanizovanymy zlochynnymy hrupamy [Optimization of information and analytical support of operational units in combating crimes committed by organized criminal groups] : zb. nauk. statei i materialiv dop. mizh nar. nauk.-prakt. konf., m. Lviv, 22 hrud. 2017 r. Lviv: LivDUVS, 407 p.
13. Simankov, V.S., & Tolkachev, D.M. (2017). Metody i algoritmy poiska informatsii v Internete [Internet Information Search Methods and Algorithms]: monografiya. Moskva: BIBLIO-GLOBUS, 332 p. (in Russian)
14. Boliubash, Yu.Ya. (2017). Metody ta zasoby opratsiuvannia informatsiinykh resursiv Velykykh danykh v systemakh terytorialnoho upravlinnia [Methods and means of processing big data information resources in territorial management systems]: dys. … kand. tekhnichn. nauk: 01.05.03. Nats. universytet «Lvivska politekhnika». Lviv, 234 p.