УДК 343.1
DOI https://doi.org/10.32844/2618-1258.2022.3.48

ТАРАСЕНКО О.С.

ЗАСОБИ ПОШУКУ ПІД ЧАС ВИЯВЛЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ З ОБІГОМ ПРОТИПРАВНОГО КОНТЕНТУ В МЕРЕЖІ ІНТЕРНЕТ

MEANS OF SEARCH DURING THE DETECTION OF CRIMINAL OFFENSES RELATED TO THE CIRCULATION OF ILLEGAL CONTENT ON THE INTERNET

Актуальність статті полягає в тому, що викрадення особистих даних особи, даних кредитних карток, відомості про особисте життя, інформація щодо роботи установи – це дії, які мають на меті вчинення інших кримінальних правопорушень, оскільки, отримуючи доступ до особистих даних особи, можна не лише викрасти кошти, які знаходяться на рахунках, а й приймати розпорядчі рішення, подавати відомості до державних установ тощо. У більшості випадків на момент отримання такого доступу ще не можливо констатувати факт кримінального правопорушення – а отже, немає підстав для здійснення оперативно-розшукових заходів або початку досудового розслідування. Зазначене та ряд інших проблемних питань значно утруднює використання технічних, пошукових засобів у процесі виявлення. Метою статті є виокремити засоби, що можуть бути використані під час виявлення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет та визначення допустимості їх використання в процесі пошукової діяльності. У статті зазначається, що з метою ефективного виявлення фактів вчинення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, необхідно запровадження у правоохоронну діяльність підрозділів Національної поліції України пошукових програм (систем), передусім Інтернет-технологій, які можна поділити на: технології великих даних (BigData Technologies); технології Інтернету речей (Internet of Things Technologies); хмарні технології (Cloud Technologies), які дозволяють більш ефективно проводити пошук протиправного контенту в мережі Інтернет, а також спрямовані на збір, узагальнення, аналіз, зберігання та використання в оперативно-розшуковій діяльності та кримінальному судочинстві кримінологічно значимої інформації. У результаті аналізу визначено низку проблемних питань, пов'язаних з використанням в оперативно-розшуковій діяльності та кримінальному провадженні результатів, здобутих під час використання пошукових програм, оскільки в правоохоронних органах та на законодавчому рівні відсутня можливість повноцінного використання пошукових програм з метою пошуку протиправного контенту в мережі Інтернет; відсутні правові підстави проведення пошуку інформації в мережі Інтернет з використанням пошукових програм.

Ключові слова: *мережа Інтернет, протиправний контент, обіг, кримінальні правопорушення, виявлення, засоби пошуку, пошукові програми.*

The relevance of the article is that the theft of personal data, credit card data, personal information, information about the work of the institution – these are actions aimed at committing other criminal offenses, because gaining access to personal data, you can not only steal funds in accounts, but also make administrative decisions, submit information to government agencies, etc. In most cases, at the time of obtaining such access, it is not yet possible to ascertain the fact of a criminal offense – and therefore, there are no grounds for carrying out operational and investigative measures or initiating a pre-trial investigation. This and a number of other problematic issues significantly complicate

© ТАРАСЕНКО О.С. – доктор юридичних наук, доцент, професор кафедри оперативно-розшукової діяльності (Національна академія внутрішніх справ)

the use of technical, search tools in the detection process. The purpose of the article is to identify the tools that can be used in the detection of criminal offenses related to the circulation of illegal content on the Internet and determine the admissibility of their use in the search process. The article notes that in order to effectively identify the facts of criminal offenses related to the circulation of illegal content on the Internet, it is necessary to introduce into law enforcement activities of the National Police of Ukraine search programs (systems), especially Internet technologies, which can be divided into: BigData Technologies; Internet of Things technologies (Internet of Things Technologies); Cloud Technologies, which allows you to more effectively search for illegal content on the Internet, as well as aimed at collecting, summarizing, analyzing, storing and using in operational and investigative activities and criminal proceedings criminologically relevant information. The analysis identified a number of issues related to the use in operational and investigative activities and criminal proceedings of the results obtained during the use of search programs, as law enforcement agencies and the legislative level do not have the opportunity to fully use search engines to search for illegal content. Internet networks; there are no legal grounds for searching for information on the Internet using search engines.

Key words: *Internet, illegal content, circulation, criminal offenses, detection, search tools, search programs.*

Постановка проблеми. Здатність мережі Інтернет відображати соціальні факти та процеси, а також певні соціально значимі дії фізичних та юридичних осіб призвела до поширення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет. При цьому злочинці постійно удосконалюють технічні й програмні засоби для полегшення вчинення таких кримінальних правопорушень – тобто переваги сучасного цифрового світу та розвиток інформаційних технологій обумовив виникнення нових загроз національній та міжнародній безпеці [1, с. 42]. Практично сформувалося нове поле протистояння – кіберпростір, протиправні дії у якому значно відрізняються від традиційних видів злочинних дій, що обумовлено розвитком інформаційно-комунікаційних систем, високим рівнем технічного забезпечення злочинних дій, їх латентністю, використанням при вчиненні міжрегіональних і міжнародних зв'язків, стійкою тенденцією до виникнення та розповсюдження нових способів протиправних діянь, пов'язаних з недоліками регулювання обігу контенту у мережі Інтернет. В процесі розміщення та обігу протиправного контенту злочинцями здійснюється низка дій, які залишаються латентними практично до моменту настання злочинних наслідків у вигляді вчинення кримінальних правопорушень, пов'язаних саме з обігом зазначеного контенту. Якщо раніше мова йшла про можливість використання інструментарію оперативно-розшукової діяльності (заходів оперативного пошуку) для виявлення фактів підготовки до вчинення кримінальних правопорушень (або їх вчиненні в умовах неочевидності – коли факт вчинення невідомий), то тепер це завдання ще ускладнилося. Адже факт розміщення або забезпечення обігу протиправного контенту – це ще не факт вчинення кримінального правопорушення (а також і підготовки до нього – оскільки невідомо, з якою саме метою цей контент розміщується). Ситуація ускладнюється тим, що нові форми отримання, передачі та опрацювання інформації розвиваються постійно, також щодня удосконалюються та розвиваються різноманітні інформаційні ресурси, комунікатори зв'язку, загалом комп'ютерні технології та мережа Інтернет. Сьогодні достатньо мати смартфон з під'єднанням до мережі Інтернет, для того щоб можна було здійснити оплату в магазині, замовити доставку товару, відправити та отримати електронну пошту, отримати інформацію з Інтернет ресурсів, спілкуватися за допомогою соціальних сторінок, в тому числі у форматі відеоконференції, навіть ставити цифровий підпис. На перший погляд, усі ці аспекти спрощують та покращують існування громадян, утім, користуючись персональним комп'ютером, смартфоном тощо, – особа піддається певним ризикам щодо захисту своїх даних, які можуть використовуватися з метою підготовки до вчинення кримінального правопорушення іншими особами. Викрадення особистих даних особи, даних кредитних карток, відомості про особисте життя, інформація щодо роботи установи – це дії, які мають на меті вчинення інших кримінальних правопорушень, оскільки, отримуючи доступ до особистих даних особи, можна не лише викрасти кошти, які знаходяться на рахунках, а й приймати розпорядчі рішення, подавати відомості до державних установ тощо [2, с. 85–86]. У більшості випадків на момент отримання такого доступу ще не можливо констатувати факт кримінального

правопорушення – а отже, немає підстав для здійснення оперативно-розшукових заходів або початку досудового розслідування. Зазначене та ряд інших проблемних питань значно утруднює використання технічних, пошукових засобів у процесі виявлення.

Стан наукових досліджень. Ряд науковців вивчали проблематику допустимості використання певних технічних, пошукових заходів під час виявлення ознак латентних кримінальних правопорушень. В. І.Школьніков відзначів недосконаліть ст. 8 Закону України «Про оперативно-розшукову діяльність» [3], яка не надає права оперативним підрозділам проводити аналітичну розвідку для виконання завдань оперативно-розшукової діяльності і вважає, що саме відсутність такої норми може викликати проблеми при оцінці судом результатів кримінального аналізу [4, с. 343]. О. В. Калиновський, аналізуючи вимоги кримінального процесуального законодавства щодо можливості використання пошукових програм як засобів виявлення ознак кіберзлочинів, повязує проблематику їх застосування, з одного боку – з вимогами ст. 99 КПК України, яка встановлює, що матеріали, в яких зафіксовано фактичні дані про протиправні діяння окремих осіб та груп осіб, зібрані оперативними підрозділами з дотриманням вимог Закону України «Про оперативно-розшукову діяльність», за умови відповідності вимогам цієї статті, є документами та можуть використовуватися в кримінальному провадженні як докази [5, с. 300-303], а з іншого – відсутністю чіткої регламентації переліку та реквізитів документів, що повинні складатися за результатами застосування певних засобів під час пошукової діяльності. Науковці також зазначають, що застосування пошукових програм (систем) у правоохоронній діяльності обмежене, оскільки відповідно до ст. 25 Закону України «Про Національну поліцію» поліція здійснює лише інформаційно-аналітичну діяльність, в рамках якої також здійснює інформаційно-пошукову та інформаційно-аналітичну роботу [6, с. 273].

Мета статті – виокремити засоби, що можуть бути використані під час виявлення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет та визначення допустимості їх використання в процесі пошукової діяльності.

Основний зміст. У процесі виявлення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, застосовуються переважно заходи, що передбачають використання певних технічних засобів, переважна більшість яких є специфічною з точки зору можливості використання саме для сфери комп'ютерних технологій.

Перш за все необхідно відмітити пошукові системи (програми), що можуть бути використані у процесі виявлення ознак кримінального правопорушення. У цьому сенсі необхідно відмітити систему Security i2 Analyst's Notebook від компанії IBM [7], це інструмент візуального аналізу, що допомагає перетворити дані в осмислену (графічну) інформацію. Рішення включає інноваційні функції, такі як візуалізація взаємопов'язаних мереж, аналіз соціальних мереж, просторові й тимчасові уявлення, які дозволяють виявляти приховані зв'язки і закономірності в даних. Застосування Security i2 Analyst's Notebook надає можливість супроводжувати та підтримувати оперативно-розшукову діяльність (упорядкування інформації, її оцінка, представлення результатів аналізу, пошук інформації з власних баз тощо) при цьому вказана система здатна автоматично проаналізувати накопичені дані, розплутувати складні зв'язки в мережах, що відображають взаємодію об'єктів різної природи. Так, під час здійснення аналізу телефонних роздруківок використання Security i2 Analyst's Notebook дозволяє: перевірити, підтвердити чи спростувати робочі оперативні версії; визначити ймовірну роль участі контактів при вчиненні протиправної діяльності; встановити зв'язки з особами, які раніше потрапляли у поле зору; визначити місця імовірного проживання об'єктів аналізу, їх спільних контактів; установлення інших телефонних трубок і карток, що використовуються об'єктами, особливостей їх використання; визначення нових об'єктів, які доцільно взяти до уваги при здійсненні оперативно-розшукової діяльності, тощо [8, с. 70]. Необхідно зауважити, що програма IBM i2 Analyst`s Notebook (та інші подібні аналітичні продукти, які здебільшого використовуються в діяльності правоохоронних органів), має обмежені можливості в питанні об'єму інформації, що обробляється та аналізується. Тому для таких завдань – обробки та аналізу великого масиву даних, а також отримання інформації з мережі Інтернет – аналітики використовують спеціально створені для виконання таких завдань мови програмування, на кшталт Python. Варто відмітити, що можливо використовувати й інші мови програмування, але Python є найбільш придатною за функціоналом та легкістю розуміння мовою програмування саме для аналізу великого масиву даних та *веб-скрапінгу* (або парсинг) [9, с. 5]. Окрім аналізу даних та вебскрапінгу за допомогою мови програмування Python також можливо отримувати інформацію з *API веб-сайтів*. **Прикладний програмний інтерфейс** (англ. *Application Programming Interface*, скорочено *API*) – це сукупність засобів та правил, що вможливлюють взаємодію між окремими складниками програмного

забезпечення або між програмним та апаратним забезпеченням. Простими словами − це спеціальний алгоритм, який дозволяє власникам вебсайтів автоматично завантажувати інформацію. В розумінні теорії відкритих даних API надає можливість користувачу отримувати дані від володільців вебсайтів, які добровільно надали згоду на отримання та обробку таких даних. Наприклад, такі іноземні вебсайти, як Facebook, Twitter, Reddit тощо, а також низка вітчизняних вебсайтів (www.data.gov.ua, www.spending.gov.ua, www.rada.gov.ua тощо) пропонують кожному користувачу мережі Інтернет API для завантаження даних з їхніх веб-сайтів. Головною перевагою даних отриманих з API – це зручний формат обробки та аналізу таких даних. Тобто це використання форматів даних, які придатні для автоматизованої обробки її засобами обчислювальної техніки. Як правило, це такі формати, як *CSV*, *XML*, *JSON*, *RDFa*, *HTML Microdata* тощо. Суть роботи з API полягає в надсиланні за допомогою мови програмування запиту на отримання інформації та миттєвого отримання відповіді від вебсервера. Перевагою використання API є: можливість отримувати актуальні дані в автоматичному режимі без необхідності кожен раз завантажувати оновлений набір даних; можливість обирати конкретний тип даних (наприклад, тільки коментарі користувачів соціальних мереж), що дає можливість не завантажувати великі об'єми даних; можливість створення власних програм, в тому числі аналітичних, для виконання конкретних завдань. Саме мова програмування Python дозволяє повноцінно використовувати всі переваги API вебсайтів. Для того, щоб правильно інсталювати, використовувати мову програмування Python для здобуття інформації в мережі Інтернет та зрозуміти всі її переваги необхідно визначити поняття та надати основи, характерні ознаки даної мови програмування [9, с. 5–6].

Поряд з вказаними пошуковими програмами (системами) науковці пропонують використовувати програмне забезпечення, яке було розроблене) з метою протидії відмиванню грошей, корупції та іншим видам організованої злочинності, але може бути використано з метою виявлення кримінальних правопорушень, пов'язаних з обігом протиправного контенту у мережі Інтернет [10]. Пропонується наступне програмне забезпечення: ***goAML*** (збір та аналіз інформації про фінансові операції та угоди); ***goPRS*** (підозрілі операції та угоди); ***goCASE*** (аналіз інформації, отриманої у ході оперативних і досудових розслідувань); ***goTRACE*** (оперативний обмін зашифрованими даними конфіденційного характеру, виявлення зв'язків між особами, адресами і контактними даними) [11, с. 81–85].

Наступний технічний засіб – це Інтернет-технології, що можуть бути використані під час виявлення окремих видів кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет.

Технології великих даних – це набори стратегій та технологій, які дозволяють охоплювати, зберігати, обробляти, аналізувати та візуалізувати складні набори даних. Технології великих даних здатні забезпечити можливість швидко та достовірно проводити автоматизований збір, фільтрацію, сортування та структурування величезних обсягів даних, і складаються з трьох елементів – дані, аналітика, технології. При цьому вони характеризуються наступними ознаками: об'єм (накопичення та обробка величезного об'єму інформації за будь-який проміжок часу); швидкість (можливість надшвидкісного накопичення та обробки інформації); різноманітність (аналіз інформації в різних форматах: текстові повідомлення, відеофайли, аудіозаписи та ін.) [12]. С. В. Пеньков та В. В. Шендрик зазначають, що практичне використання в оперативно-розшуковій діяльності та досудовому розслідуванні технологій великих даних, дозволяє вирішувати широкий спектр завдань: забезпечити пошук, збирання та систематизацію інформації щодо суб'єктів оперативної уваги; фіксувати соціальну активність певної категорії осіб, виникнення та зміни їх мережевих зв'язків, аналізувати ступінь їх інтересів до конкретних тем, що обговорюються в місцях мережевого спілкування; відстежувати появу в мережі Інтернет інформації із характеристиками, що вказують на високу ймовірність підготовки або вчинення кримінальних правопорушень, із наступним реагування на таку інформації; виявляти угруповання кримінальної спрямованості, визначати їх спеціалізацію, ступінь організованості, розподіл ролей, характер неочевидних зв'язків між фігурантами та їх причетність до тих чи інших подій; будувати «поведінкові профілі» для осіб, які вчиняють злочини певних видів, і формувати на цій основі поведінкові гіпотези; покращувати планування оперативно-розшукових дій за допомогою обліку складної сукупності численних факторів, що впливають на розвиток конкретної оперативно-тактичної ситуації; визначати оптимальні варіанти ефективного управляючого впливу на виявлені в соціальних мережах спільноти і групи кримінальної спрямованості на основі моделювання характеристик таких груп; формувати комплекс методичних рекомендацій на основі аналізу інформаційного масиву великих даних всіх оперативно-розшукових ситуацій і варіантів їх розвитку [13, с. 83–84].

Для запобігання поширення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, також використовується технологія Інтернету речей. Технологічно це концепція мережі, яка окрім датчиків, може мати виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через дротові чи бездротові мережі. Ці взаємопов'язані пристрої мають функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів. Загалом основною концепцією Інтернету речей є можливість підключення різних об'єктів (речей), які людина може використовувати в повсякденному житті, наприклад, кондиціонер, автомобіль, велосипед та ін. Всі ці об'єкти (речі) повинні бути оснащені вбудованими давачами або сенсорами, які мають можливість обробляти інформацію, що надходить з навколишнього середовища, обмінюватися нею і виконувати різні дії залежно від отриманої інформації [14, с. 295–296]. Використання Інтернету речей передбачається як для розслідування злочинів, так і для їх запобігання. Це досягається насамперед тим, що міська інфраструктура стає більш «розумнішою» та з'єднаною. А це, своєю чергою, дозволяє отримувати інформацію в режимі реального часу, починаючи від камер відеоспостереження до спеціальних датчиків. При цьому рівень технічних можливостей відеокамер, звукових та інших датчиків суттєво підвищився. Так, камери нового покоління здатні краще сканувати номерні знаки на автомобілях, здійснювати розпізнавання обличчя для пошуку потенційних злочинців або зниклих людей, а також автоматично виявляти підозрілі ситуації, якот залишені без нагляду різноманітні предмети в публічних місцях та ін. Відеоспостереження дозволяє також аналізувати поведінку людини [15; 16, с. 14–16].

Для виявлення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, можливим є також використання хмарних технологій – технологій мережевого доступу до даних. Модель хмарних технологій або обчислень складається із зовнішньої і внутрішньої частини. Ці два елементи з'єднані через мережу Інтернет. За допомогою зовнішньої частини користувач взаємодіє з системою; внутрішня частина – це власне хмара. Зовнішня частина складається з клієнтського комп'ютера або мережі комп'ютерів і додатків, що використовуються для доступу до хмари. Хмарні технології дають можливість користувачеві зберігати файли та користуватися програмами без необхідності мати спеціальні локальні програми. Користувач працює через мережу Інтернет, де і зберігається інформація [17].

Хмарні технології можуть бути використані для інформатизації кримінологічної діяльності, і зокрема, щодо оптимізації збору та обробки інформації, яка містить протиправний контент та подальше використання хмарних технологій для автоматизованого обміну інформацією між підрозділами правоохоронних органів [18]. Так, наприклад, в Управлінні інформаційно-аналітичного забезпечення області спільно з кафедрою штучного інтелекту Харківського національного університету радіоелектроніки розроблено інформаційно-аналітичний комплекс «Realtime intelligen cecrimeanalytics system» – інтелектуальну систему кримінального аналізу у реальному часі «RICAS». Вказана інтелектуальна система кримінального аналізу даних здатна здійснювати аналітичний пошук у реальному часі, що дозволяє значно підвищити ефективність і результативність розкриття кримінальних правопорушень за «гарячими слідами» і нерозкритих раніше кримінальних правопорушень.

Разом з тим, за наявності технічних можливостей, науковці зазначають і ми підтримуємо їх думку [4, с. 343], що на сьогодні наявна низка проблемних питань, пов'язаних з використанням в оперативно-розшуковій діяльності та кримінальному провадженні результатів, здобутих під час використання пошукових програм, оскільки в правоохоронних органах та на законодавчому рівні відсутня можливість повноцінного використання пошукових програм з метою пошуку протиправного контенту в мережі Інтернет; відсутні правові підстави проведення пошуку інформації в мережі Інтернет з використанням пошукових програм; оперативним працівникам і слідчим бракує знань, вмінь і навичок щодо використання пошукових програм.

Таким чином, з метою ефективного виявлення фактів вчинення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет, необхідно запровадження у правоохоронну діяльність підрозділів Національної поліції України пошукових програм (систем), передусім Інтернет-технологій, які можна поділити на: технології великих даних (BigData Technologies); технології Інтернету речей (Internet of Things Technologies); хмарні технології (Cloud Technologies), які дозволяють більш ефективно проводити пошук протиправного контенту в мережі Інтернет, а також спрямовані на збір, узагальнення, аналіз, зберігання та використання в оперативно-розшуковій діяльності та кримінальному судочинстві кримінологічно значимої інформації.

Список використаних джерел:

1. Довгань О. Д., Доронін І. М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту : монографія. К. : Видавничий дім «АртЕк». 2017. 107 с.

2. Тарасенко О. С. Виявлення шкідливого програмного забезпечення як засіб попередження несанкціонованого втручання в роботу інформаційної системи. *Оперативно-розшукова діяльність Національної поліції*: *проблеми теорії та практики* : матеріали Всеукр. наук.- практ. конф. (Дніпро, 20 жовт. 2017 р.) : у 2-х ч. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2017. Ч. 1. С. 85–86.

3. Про оперативно-розшукову діяльність : Закон України від 18 лют. 1992 р. № 2135-XII. URL: http://zakon2.rada.gov.ua/laws/show/2135-12.

4. Школьніков В. І. Використання результатів кримінального аналізу в кримінальному процесі України. С. 343. URL: http://elar.naiau.kiev.ua/bitstream/123456789/3918/1/11_p340-343.pdf

5. Калиновський О. В., Школьніков В. І. Використання методу кримінального аналізу для протидії організованій злочинності. *Часопис Київського університету права.* 2017. № 1. С. 300–303.

6. Тарасенко О. С. Теорія та практика протидії кримінальним правопорушенням, пов'язаним з обігом протиправного контенту в мережі Інтернет : монографія. Київ : Національна академія внутрішніх справ, 2021. 426 с.

7. IBM Security i2 Analyst's Notebook. https://www.ibm.com/ru-ru/products/i2-analysts-notebook

8. Кіреєва О. С. Використання альтернативних аналітичних інструментів у кримінальному аналізі. *Збірник наукових праць Національної академії Державної прикордонної служби України*. *Серія : Військові та технічні науки* / за ред. Б. М. Олексієнка. Хмельницький, 2016. № 4(70). С. 64–76.

9. Школьніков В. І., Орлов Ю. Ю., Корнейко О. В., Вознюк А. А. Здобуття доказової інформації в мережі Інтернет із використанням можливостей мови програмування Python : метод. рек. К. : Нац. акад. внутр. справ, 2019. 58 с.

10. Кржечковськис І., Тацієнко В. В., Стрільців О. М. та ін. Європейський досвід протидії корупції: теорія та практика: аналіт. огляд. К. : Нац. акад. внутр. справ, 2016. 170 с.

11. Тарасенко О. С. Використання пошукових програм (систем) підрозділами Національної поліції під час виявлення протиправного контенту. *Становлення та розвиток наукових досліджень*: матеріали І Міжнар. наук.-практ. конф., присвяченої Дню науки України (м. Київ, 20−21 трав. 2016 р.). Київ : ГО «Фундація науковців та освітян», 2016. С. 81–85.

12. Що таке Big Data? URL: http://inlimited.com.ua/ukr/content/bigdata. php

13. Пеньков С. В., Шендрик В. В. Впровадження інтернет-технологій у діяльність Національної поліції України для отримання оперативно-розшукової інформації. *Право і безпека.* 2017. № 2 (65). С. 83–84. URL: http://pb.univd. edu.ua/?action=publications&pub_id=411139&mid=8&year=2017

14. Бугера О. Інтернет речей та запобігання злочинності. *Підприємство, господарство і право*. 2018. № 6. С. 295–296 ; Інтернет речей. URL: https://uk.wikipedia.org/ wiki/Інтернет_речей

15. Faggella D. AI for Crime Prevention and Detection – 5 Current Applications. URL: https://www.techemergence.com/ ai-crime- prevention-5-current-applications/

16. Бугера О. І. Кримінологічні засади використання мережі Інтернет для запобігання злочинності : автореф. дис. ... д.ю.н. за спец. 12.00.08 – кримінальне право та кримінологія ; кримінально-виконавче право. К. : Ін-т держ. і права ім. В. М. Корецького НАН України, 2020. 36 с.

17. Облачные технологии. URL: http://www.wikireality.ru/wiki/

18. Минин А. Я. Информатизация криминологической деятельности. URL: http://www.books.google.com.ua/books