4. КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ. КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО. КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА. СУДОВА ЕКСПЕРТИЗА. ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ. СУДОУСТРІЙ. ПРОКУРАТУРА ТА АДВОКАТУРА

DOI:10.35774/app2022.03.158
УДК343.98

Людмила Будник,
кандидат економічних наук, доцент, доцент кафедри безпеки та правоохоронної діяльності Західноукраїнського національного університету
ORCID: https://orcid.org/0000-0002-1393-9354

Ольга Карапетян,
кандидат економічних наук, доцент, доцент кафедри безпеки та правоохоронної діяльності Західноукраїнського національного університету
ORCID: https://orcid.org/0000-0002-8747-7631

Ігор Метельський,
кандидат юридичних наук, старший викладач кафедри кримінального права та процесу
ORCID: https://orcid.org/0000-0001-8518-9321

КІБЕРЗЛОЧИНИ: ТИПОЛОГІЇ, ФІНАНСОВА РОЗВІДКА, ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ

Обґрунтовано необхідність використання спеціальних знань для розслідування кіберзлочинів; визначено послідовність завдань комп'ютерно-технічного дослідження з використанням спеціальних знань у процесі розслідування кіберзлочинів, а саме: ідентифікація баз даних спеціалізованої програми; ідентифікація програм для

створення систем податкової звітності та електронного документообігу; виявлення інформації про платежі, здійснені з використанням мережевих технологій; зроблено висновок, що в процесі дослідження речових доказів у кримінальних справах щодо розслідування економічних кіберзлочинів найбільш ефективним результатом буде комплексна експертиза за спільною участю експертів у галузі економіки та комп'ютерних технологій, оскільки комплексність – це найбільш ефективна форма застосування спеціальних знань.

Ключові слова: *кіберзлочин, типологія, фінансова розвідка, спеціальні знання, судова експертиза, економічна експертиза, комп'ютерно технічна експертиза.*

Budnyk L., Karapetian O., Metelskyi I.

Cybercrimes: types, financial intelligence, use of special knowledge

It was determined that the investigation of cybercrimes remains a difficult task for investigative bodies, which is due to the specificity of this type of crime; the difficulties of summarizing the investigative and judicial materials under consideration; the lack of methodological recommendations regarding the organization of the investigation of criminal acts and the tactics of operational and investigative activities; insufficient qualifications of investigators to work with specific sources of evidenceThe necessity of using special knowledge in the investigation of cybercrimes is substantiated; the sequence of tasks of computer and technical research using special knowledge in the process of investigating cybercrimes is determined, namely: identification of databases of a specialized program; identification of programs for creating tax reporting and electronic document management systems; detection of information about payments made using network technologies. Involvement of an expert or specialist is the investigator's right, not an obligation. When investigating cybercrimes in the economic sphere, the problem arises of systematizing methodical approaches to the study of economic information in automated management systems in the light of complex computer-technical and economic expertise. It was concluded that when examining physical evidence in criminal cases regarding the investigation of economic cybercrimes, the most effective result will be a complex examination with the joint participation of experts in the field of economics and computer technology, since complexity is the most effective form of application of special knowledge. The requirements for the formulation of questions for research by an expert are important. An algorithm of tasks to be investigated using special knowledge in the investigation of cybercrimes in the field of economy is given. A typical task facing an expert is to search for databases with which work was performed, as well as to identify users who had access to one or another database, methods of approaching this task are highlighted.

Keywords: *cybercrime, types, financial intelligence, special knowledge, forensic expertise, economic expertise, computer-technical expertise.*

Постановка проблеми. Стрімкий розвиток інформаційних технологій в Україні в останнє десятиліття, неминуче супроводжується динамічним розвитком злочинності у цій сфері. Будь-який прогрес, який приносив людству блага цивілізації та нові можливості, завжди супроводжувався негативними явищами. Не є винятком масова комп'ютеризація та бурхливий розвиток діджитал технологій, які значно спростили життя людини. Кіберзлочинність – це найбільш динамічна група суспільно небезпечних видів діяльності, оскільки щороку вона набуває масового характеру. На сучасному етапі багато фахівців у сфері інформаційних технологій усвідомлюють, що ситуація з кіберзлочинністю у світі загострюється. Організована злочинність все частіше використовує Інтернет для приховування своєї діяльності. За даними ГУНП України, за останній рік кількість організованих злочинних груп та організацій, які вчиняють злочини з використанням діджітал-технологій, зросла на 36% [1].

Аспект переслідування кіберзлочинців переважно стосується кримінальної відповідальності осіб, які вчинили кіберзлочин. Так, згідно з Кримінальним кодексом України у сфері використання комп'ютерів, комп'ютерних систем і мереж розслідуються такі категорії злочинів за статтями 361, 361-1, 361-2, 362, 363, 363-1 [2]. Згідно з результатами досліджень переважну більшість у структурі досліджуваних кіберзлочинів становлять ті злочини, відповідальність за які передбачено ст. 362 Кримінального кодексу України (ККУ) (46,5%) (рис. 1).

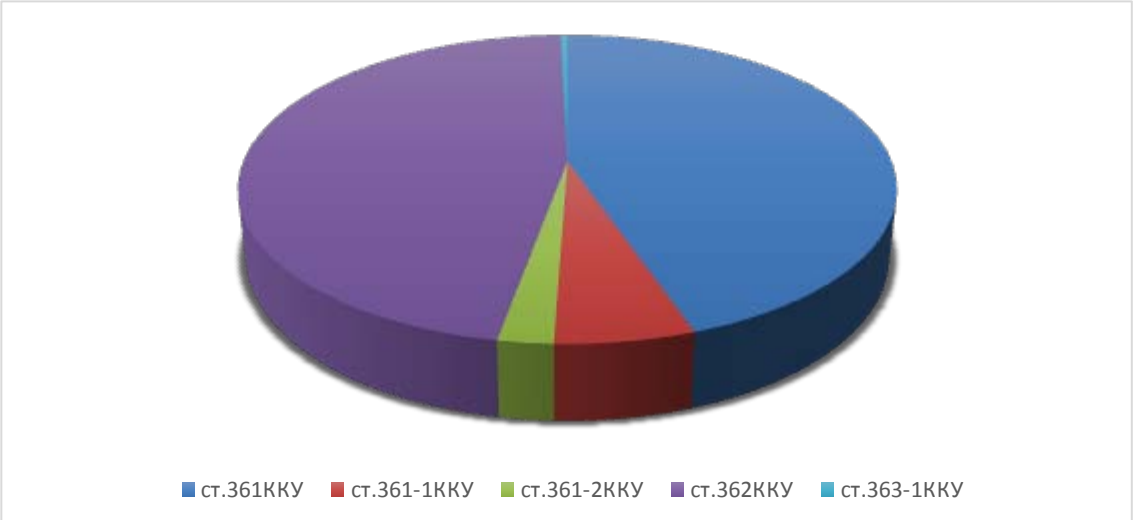

Рис. 1. Структура злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [3].

Розслідування кіберзлочинів – складне завдання для слідчих органів, що зумовлено специфікою цього виду злочинів; труднощами узагальнення слідчих та судових матеріалів, що розглядається; відсутністю методичних рекомендацій щодо організації розслідування злочинних діянь та тактики проведення оперативно-розшукової діяльності; недостатньою кваліфікацією слідчих для роботи з конкретними джерелами доказів.

Аналіз останніх досліджень та публікацій. Результати аналізу наукових публікацій вказують на те, що питання розслідування правопорушень у сфері кібербезпеки – це предмет досліджень українських та іноземних науковців: А. І. Марущака, В. О. Болгова, В. Бутузов, О. М. Миколенко, М. Д. Гудман, С. В. Бреннер, П. Вілліамс та ін. Вчені обґрунтовують теоретичні основи боротьби з кіберзлочинністю в глобальному масштабі та розслідування кіберзлочинів. Однак у наукових працях іноземних та вітчизняних науковців не достатньо уваги приділено використанню спеціальних знань у процесі розслідування кіберзлочинів.

Мета дослідження – обґрунтування специфіки розслідування кіберзлочинів з урахуванням основних теоретичних положень науки криміналістики, визначення завдань дослідження з використанням спеціальних знань у процесі розслідування таких злочинів; дослідження проблем взаємодії слідчого та експерта в процесі розслідування кіберзлочинів у справах економічного спрямування.

Виклад основного матеріалу дослідження. У процесі розслідування кіберзлочинів використовується робота експертів зі спеціальними знаннями в цій галузі. Під поняттям «спеціальні знання» розуміються наукові, технічні чи інші знання, отримані в результаті спеціальної підготовки та практики суб'єктом, процесуальний статус якого визначено як експерт або прирівнюється до спеціаліста. У ході розслідування кримінальних злочинів застосовують три процесуальні форми використання спеціальних знань: 1) залучення спеціаліста для надання письмової консультації; 2) залучення спеціаліста для надання безпосередньої технічної допомоги під час здійснення процесуальних дій; 3) залучення експерта для проведення судової експертизи. Крім того, слідча практика довела ефективність таких непроцесуальних форм використання спеціальних знань, як: усна консультація слідчого зі спеціалістом; залучення спеціаліста під час перевірки оперативної інформації про вчинення або підготовку злочину [4].

Аналіз наукової літератури та практичних матеріалів дає змогу виокремити кілька можливостей для залучення до розслідування кіберзлочинів обізнаних осіб, серед яких: 1) працівники експертних установ Міністерства юстиції чи Міністерства внутрішніх справ України, які мають знання, необхідні для пошуку, збереження, відновлення та дослідження комп'ютерних слідів злочину; мають документи, що підтверджують кваліфікацію; проходять періодичну професійну перепідготовку та підвищення кваліфікації; не мають особистого інтересу в конкретному провадженні; 2) ІТ-спеціалісти інших підприємств, організацій, установ, для яких доцільно створити постійний перелік, його періодично переглядати та оновлювати за відповідними критеріями. Такий фахівець може виявити встановлені власником на комп'ютері спеціальні інструменти для знищення інформації в разі несанкціонованого доступу; встановити необхідний пароль

для доступу до інформації, дізнатися, які правила її використання та чи призведе порушення цих правил до знищення файлів тощо.

Під час розслідування всіх класифікаційних груп і підгруп злочинів, вчинених у кіберпросторі, як правило, призначаються судові експертизи апаратно-програмного забезпечення комп'ютерів. На практиці для опису цієї експертизи використовується комп'ютерно-технічна експертиза. Залежно від завдання, специфіки дослідження та видів об'єктів дослідження теоретично виокремлюють різні види, а саме: апаратно-комп'ютерну експертизу, програмно-комп'ютерну експертизу; дослідження даних (інформаційних та комп'ютерних); комп'ютерна та мережева експертиза; комплекс цих досліджень. Об'єктом комп'ютерної технічної експертизи є комп'ютери з носіями інформації (усі пристрої зберігання інформації – дискети, жорсткі диски, компакт-диски, флеш-карти тощо), програмне забезпечення та інше комп'ютерне обладнання (наприклад, мобільні телефони, банкомати, ігрові автомати, картрідери), електронні блокноти, принтери та ін.), а також документація на обладнання [5].

Нормативними документами щодо встановлення приблизного переліку питань, пов'язаних з проведенням комп'ютерно-технічної експертизи, є Інструкція про призначення та проведення судових експертиз і експертних досліджень», та Науково-методичні рекомендації щодо підготовки та призначення судових експертиз та експертних досліджень [6; 7].

Залучення експерта чи спеціаліста – це право слідчого, а не обов'язок. Коли розслідують кіберзлочини в економічній сфері, виникає проблема систематизації методичних підходів до дослідження економічної інформації в автоматизованих системах управління в контексті комплексних комп'ютерно-технічних та економічних експертиз. Ця проблема доволі складна. Адже навіть розпочавши та провівши комплексне дослідження, фахівці різних галузей знань не можуть сформувати загальний висновок, і тоді кожен з них дає власний висновок за результатами своїх досліджень. Щоб цього не сталося, для вирішення комплексної експертизи варто подати 1-2 ключових питання, які стосуються деяких суміжних аспектів різних галузей знань. Питання ідентифікації та відтворення всієї інформації, що міститься на електронних носіях, входить до компетенції експерта комп'ютерно технічної експертизи і зазвичай не є для нього проблемою. Проте пошук економічно значущої інформації неможливо здійснювати без урахування думки експерта-економіста, який формулює висновок до системи у форматі, який запропонував експерт комп'ютерно-технічної експертизи. У процесі дослідження речових доказів у кримінальних справах щодо притягнення до відповідальності за економічні кіберзлочини найбільш ефективний результат дає дослідження за спільною участю експертів, як у галузі економіки, так і комп'ютерних технологій. Комплексність – це найбільш ефективна форма застосування спеціальних знань, оскільки під час комплексної експертизи експерти спільно вирішують проблеми, що виникають[8].

Важливе значення мають вимоги до формулювання питань для дослідження експертом. На рис. 2 подано алгоритм завдань, які підлягають дослідженню з використанням спеціальних знань у розслідуванні кіберзлочинів у галузі економіки.

Завдання проведення контекстного пошуку за ключовими словами дає змогу експерту ідентифікувати електронні документи, що містять певні слова чи фрази. Це може бути назва документа, посада, прізвище, назва суб'єкта господарювання, а також будь-які інші ключові слова, які допоможуть слідчому вибрати з великої кількості інформації потрібну йому. Окрім власне вмісту документа, експерт також отримує інформацію про метадані файлу: дату створення, останньої зміни, дату друку, останнього доступу.

Рис. 2. Алгоритм завдань дослідження з використанням спеціальних знань

Для вирішення проблеми можуть використовуватися різні способи: від простого покрокового перегляду каталогів і використання невеликих спеціалізованих програм до використання спеціалізованих апаратно-програмних комплексів. Вибір методу залежить від результату, який хоче отримати експерт. Метод контекстного пошуку базується на використанні невеликих спеціалізованих програм (AVSearch, Archivarius 3000 та ін.), які працюють на основі індексування інформації та подальшого контекстного пошуку в базі даних (індекс) [9]. Бази для застосування спеціальних знань у галузі криміналістичної техніки для цілей контекстного пошуку практично немає. Основною перевагою експертів для самостійного вирішення завдання контекстного пошуку в процесі перегляду комп'ютерних носіїв є фактор часу. І тут мова йде не тільки і не стільки про тимчасові витрати на процедуру призначення та огляду. Експерт, який не має у своєму розпорядженні всіх матеріалів справи, вирішує суто технічне завдання контекстного пошуку і позбавлений можливості оцінити корисність тієї чи іншої знайденої інформації.

Збільшення ємності пам'яті та розвиток мережевих технологій означає, що сучасний персональний комп'ютер може працювати з десятками баз даних. За найбільш загального підходу до класифікації баз даних їх можна поділити на локальні та мережеві. Локальні знаходяться на диску перевіреного комп'ютера, яким можуть користуватися користувачі, які мають облікові записи лише на цьому комп'ютері. Мережеві бази даних можуть розташовуватися як на персональному комп'ютері, так і на будь-якому мережевому ресурсі (іншому комп'ютері, сервері локальної мережі, сервері глобальної мережі). Багато користувачів, які мають доступ до ресурсу, на якому встановлена база даних, можуть працювати з такою базою одночасно. Типовим завданням для експерта є пошук баз даних, з якими виконувалася робота людей, а також виявлення користувачів, які мали доступ до тієї чи іншої бази даних. Є кілька способів підходу до цього завдання. Перший спосіб полягає в пошуку розширень файлів у базах даних. Ефективність безпосереднього використання першого методу пошуку експертом можна позитивно оцінити лише тоді, коли він впевнений, що база даних зберігається на зламаному комп'ютері, а її виявлення не потребує значних витрат часу та зусиль. Ця впевненість може ґрунтуватися на показаннях свідків, обвинувачених, результатах обшуків і т. д. В інших випадках розглядуваний спосіб варто використовувати в поєднанні з іншими. Другий спосіб виявлення баз даних полягає в безпосередньому дослідженні файлів програмного комплексу, а також файлів реєстру операційної системи. Таке дослідження дає змогу визначити конкретний перелік баз даних, з якими працювала програма, встановлена на досліджуваному носії. Основу таких досліджень становить властивість програм зберігати робочі налаштування в деяких файлах [10].

Оцінюючи рівень знань, необхідний для здійснення описаного пошуку, очевидно, що необхідно знати структуру реєстру операційних систем Microsoft Windows, уміння працювати з файлами реєстру та основи організації локальних мереж. Крім того, залежно від параметрів політики безпеки доступ до файлів системного реєстру може бути закритий або обмежений. Тому також необхідно мати знання для доступу до захищеної інформації. Сукупність вищезазначених даних належить до спеціальних знань, що зумовлює необхідність залучення до процедури перевірки спеціаліста з комп'ютерних технологій.

Часто слідчий має не тільки проаналізувати звітність, а й визначити, чи підготовлені податкові декларації для відправлення до податкового органу з урахуванням наявної бухгалтерської звітності. Для цього експерт має вирішити питання щодо визначення програм для підготовки податкової звітності та електронного обміну інформацією з податковими органами. Особливість вивчення програм податкової звітності та програм електронного документообігу полягає в тому, що більшість таких програм зберігає необхідну інформацію у вигляді внутрішніх спеціалізованих баз даних. Це означає, що інформація, яка зберігається в такій базі даних, доступна лише тоді, коли запущена програма. Програма може бути запущена тільки в працюючій операційній системі, що суперечить принципу збереження незмінності інформації – запуск операційної системи викликає незворотні зміни інформації, наявної на носії. Описана проблема найчастіше вирішується за допомогою систем віртуалізації (так званих «віртуальних машин»). Найпопулярнішими інструментами в цій сфері є VMware і VirtualBox. Зокрема, цей метод також можна використовувати для пошуку баз даних, з якими працював користувач.

Отримати таку інформацію можна, запустивши виконуваний модуль програмного комплексу. Після запуску програмного комплексу на екрані з'являється діалогове вікно зі списком раніше опрацьованих баз даних і користувачеві пропонується вибрати зі списку базу даних для подальшої роботи. Список баз даних складається з назви бази даних і шляху до них. При пошуку інформації за допомогою систем віртуалізації слід враховувати, чи програма працювала з апаратним ключем безпеки, тому що, якщо такого ключа немає у віртуальній машині, програма виведе повідомлення про помилку. Таку реєстраційну інформацію можна отримати лише шляхом проведення необхідних слідчих або розшукових заходів. Як видно з

опису методу, його застосування вимагає від експерта певних навичок роботи з графічними файлами та знання нюансів налаштування віртуальної машини, а також певної кількості часу. Всі ці знання не можна назвати загальновідомими, тому що вони вимагають професійних знань принципів роботи, завантаження операційних систем.

Типовим завданням для слідчих є виявлення програм віддаленого доступу до розрахункових рахунків кредитних організацій, встановлення організацій, що надають такий доступ, а також найменувань кредитних організацій (банків) і номерів рахунків. Протягом тривалого часу в банківській системі використовується система «Банк-клієнт», яка охоплює програмне забезпечення для встановлення захищеного каналу зв'язку між комп'ютером користувача (клієнта) та сервером банку та клієнтом банку, автоматизоване робоче місце (АРМ). Наявність такого ARM-клієнта можна виявити, перевіривши системний каталог Program Files у поєднанні з перевіркою файлів системного реєстру. Вивчення файлів реєстру, як уже зазначалося, вимагає знання структури реєстру операційних систем Microsoft Windows, навичок роботи з файлами реєстру. Перший спосіб не вимагає спеціальних знань і доступний для дослідження. Другий спосіб вимагає використання таких програм, як Belkasoft Evidence Center Ultimate або Internet Evidence Finder, які недоступні для слідчого. Відповідно, вилучення інформації зазначеним способом без застосування спеціальних знань і залучення експерта неможливо.

Висновки. Результати дослідження дають змогу зробити такі висновки щодо необхідності використання спеціальних знань у розслідуванні кіберзлочинів.

1. Під час розслідування всіх класифікаційних груп та підгруп злочинів, вчинених у кіберпросторі, доцільно призначати судову експертизу комп'ютерної техніки та програмних продуктів.

2. Доцільно проводити таку послідовність вирішення завдань комп'ютерно-технічного дослідження з використанням спеціальних знань у процесі розслідування кіберзлочинів: ідентифікація баз даних спеціалізованої програми; ідентифікація програм для створення систем податкової звітності та електронного документообігу; виявлення інформації про платежі, здійснені з використанням мережевих технологій.

3. У процесі дослідження речових доказів у кримінальних справах щодо розслідування економічних кіберзлочинів найбільш ефективним результатом буде комплексна експертиза за спільною участю експертів у галузі економіки та комп'ютерних технологій. Комплексність – це найбільш ефективнп форма застосування спеціальних знань.

Проблема використання спеціальних знань у процесі розслідування кіберзлочинів багатоаспектною і існує достатній простір для дослідження та розробки шляхів її вирішення.

Список використаних джерел

1. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606 (дата звернення: 12.08.2022).
2. Кримінальний кодекс України : Закон України від 5.04. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 26.08.2022).
3. Єдиний звіт про кримінальні правопорушення по державі. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2 (дата звернення: 22.08.2022).
4. Самойленко О. А. Виявлення та розслідування кіберзлочинів : навчально-методичний посібник. Одеса, 2020. 112 с.
5. Климчук М. П., Комісарчук Ю. А., Марко С. І., Стецик Б. В. Судова комп'ютерно-технічна експертиза у кримінальному провадженні : навч. посіб. Львів : Львівський державний університет внутрішніх справ, 2022. 112 с.
6. Інструкція про призначення та проведення судових експертиз і експертних досліджень, затверджена наказом Міністерства юстиції України від 10.08.98 р. 53/5 у редакції наказу Міністерства юстиції України від 26.12.2012 № 1950/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 15.08.2022).
7. Науково-методичні рекомендації щодо підготовки та призначення судових експертиз та експертних досліджень у редакції наказу Міністерства юстиції України від 26.12.2012. № 1950/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 15.08.2022).
8. Коваленко І. Окремі види експертиз як обов'язкові слідчі (розшукові) дії під час розслідування шахрайства у сфері банківських електронних платежів. *Підприємництво, господарство і право*. 2020. № 12. С. 262–266.

9. Довгань О., Тарасюк А. Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні. *Інформація і право*. 2018. № 3(26). С. 94–103.
10. Войтович О. П., Вітюк В. О., Каплун В. А. Особливості дослідження ознак шкідливого програмного забезпечення без наявності вихідних кодів. *Інформаційні технології та комп'ютерна інженерія*. 2013. № 3. С. 4–9.

References

1. *Kiberzlochynnist v Ukrayini. Era tsyfrovykh tekhnolohiy – era novykh zlochyniv [Cybercrime in Ukraine. The era of digital technologies is the era of new crimes]*. Retrieved from https://uz.ligazakon.ua/ua/magazine_article/EA013606 [in Ukrainian].
2. *Kryminalnyi kodeks Ukrayiny: Zakon Ukrayiny vid 5.04. 2001 r. № 2341-III. [Criminal Code of Ukraine. Law of Ukraine dated April 5 2001 No. 2341-III]*: Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14 [in Ukrainian].
3. *Yedynyi zvit pro kryminalni pravoporushennya po derzhavi [Unified report on criminal offenses by state]*. Retrieved from https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2 [in Ukrainian].
4. Samoylenko, O. A. (2020). *Vyyavlennya ta rozsliduvannya kiberzlochyniv: navchal'no-metodychnyy posibnyk [Detection and investigation of cybercrimes]*. Odesa, 112 p. [in Ukrainian].
5. Klymchuk, M. P., Komissarchuk, Yu. A., Marko, S. I., Stetsyk, B. V. (2022). *Sudova kompyuterno-tekhnichna ekspertyza u kryminalnomu provadzhenni: navch. posib. [Forensic computer-technical expertise in criminal proceedings]*. Lviv: Lvivskyi derzhavnyi universytet vnutrishnikh sprav [in Ukrainian].
6. *Instruktsiya pro pryznachennya ta provedennya sudovykh ekspertyz i ekspertnykh doslidzhen, zatverdzhena nakazom Ministerstva yustytsiyi Ukrayiny 10.08.98 n. 53/5 u redaktsiyi nakazu Ministerstva yustytsiyi Ukrayiny 26.12.2012 № 1950/5 [Instructions on the appointment and conduct of forensic examinations and expert studies]*. Retrieved from https://zakon.rada.gov.ua/laws/show/z0705-98#Text [in Ukrainian].
7. *Naukovo-metodychni rekomendatsiyi shchodo pidhotovky ta pryznachennya sudovykh ekspertyz ta ekspertnykh doslidzhen' u redaktsiyi nakazu Ministerstva yustytsiyi Ukrayiny 26.12.2012 № 1950/5. [Scientific and methodological recommendations on the preparation and appointment of forensic examinations and expert studies]*. Retrieved from https://zakon.rada.gov.ua/laws/show/z0705-98#Text [in Ukrainian
8. Kovalenko, I. (2020). Okremi vydy ekspertyz yak obovyazkovi slidchi (rozshukovi) diyi pid chas rozsliduvannya shakhraystva u sferi bankivs′kykh elektronnykh platezhiv [Certain types of examinations as mandatory investigative (research) actions during the investigation of fraud in the field of bank electronic payments]. *Pidpryyemnytstvo, hospodarstvo i pravo – Entrepreneurship, economy and law, 12,* 262-266 [in Ukrainian].
9. Dovhan, O. & Tarasyuk, A. (2018). Hlobalna kultura kiberbezpeky v systemi zapobihannya kiberzlochynnosti v Ukrayini [Global culture of cyber security in the system of cybercrime prevention in Ukraine]. *Informatsiya i pravo – Information and Law, 3 (26),* 94-103 [in Ukrainian].
10. Voytovych, O. P., Vityuk, V. O. & Kaplun, V. A. (2013). Osoblyvosti doslidzhennya oznak shkidlyvoho prohramnoho zabezpechennya bez nayavnosti vykhidnykh kodiv [Peculiarities of studying the signs of malicious software without the presence of source codes]. *Informatsiyni tekhnolohiyi ta kompyuterna inzheneriya – Information technologies and computer engineering, 3*, 4-9 [in Ukrainian].

Стаття надійшла до редакції 15.09.2022.