Кримінальний процес та криміналістика, судова експертиза,
оперативно-розшукова діяльність

УДК 343.14

Антонюк Анастасія Борисівна
кандидат юридичних наук,
доцент кафедри кримінального процесу та криміналістики
Університет державної фіскальної служби України
Антонюк Анастасия Борисовна
кандидат юридических наук,
доцент кафедры уголовного процесса и криминалистики
Университет государственной фискальной службы Украины
Antoniuk Anastasiia
Candidate of Law, Associate Professor of the
Department of Criminal Procedure and Criminology
University of the State Fiscal Service of Ukraine

Русецька Валерія Артурівна
здобувач другого (магістерського) рівня вищої освіти
Університету державної фіскальної служби України
Русецкая Валерия Артуровна
соискатель второго (магистерского) уровня высшего образования
Университета государственной фискальной службы Украины
Rusetska Valeriia
Student of the second (Master's) level of higher education of
University of the State Fiscal Service of Ukraine

ЕЛЕКТРОННІ ДОКАЗИ В КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ
ЭЛЕКТРОННЫЕ ДОКАЗАТЕЛЬСТВА В УГОЛОВНОМ ПРОИЗВОДСТВЕ

ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS

Анотація. *Дана стаття присвячена розгляду теоретичних питань, пов'язаних із запровадженням в Україні інституту електронних доказів кримінального провадження. Також в статті підіймається питання шляхів отримання електронних доказів. У статті зазначається, що у сучасному розвинутому світі з'являються все нові і нові види злочинів. В даному контексті ми розглянемо злочини, що тісно пов'язані з використанням інформаційних технологій. Доказування таких злочинів викликає декотрі труднощі. На сьогоднішній день актуальним є закріплення поняття електронних доказів у Кримінально-процесуальному кодексі України та формування методики їх вивчення. Також автор статті зазначає, що серед невирішених та проблемних аспектів використання електронних доказів у кримінальному провадженні України вчені виділяють: відсутність чіткого процесуального порядку їх отримання відповідно до Кримінально-процесуального кодексу України; відсутність розробленої методології вивчення таких доказів; труднощі з виявленням та фіксацією електронних доказів через відсутність спеціалізованих знань у слідчих, що обумовлює необхідність залучення спеціалістів для ведення судового провадження; відсутність підстав для визнання електронних доказів неприйнятними; відсутність однорідної термінології та регулювання на законодавчому рівні.*

В статті визначено, що також для ефективної імплементації норм міжнародного права в сфері боротьби з кіберзлочинністю доцільно обґрунтувати необхідність законодавчого визначення електронних доказів, джерел їх формування, допустимості міжнародного співробітництва шляхом обміну електронними доказами, доцільність використання електронних способів напряму запитів і відповідей про їх

виконання, можливість застосування контрольної поставки інформації для розслідування транснаціональних комп'ютерних злочинів.

Виходячи з вищесказаного, автор пропонує власне визначення електронних доказів. Зроблено висновок про необхідність її законодавчого закріплення терміну «електронні докази» та продовження вивчення категорії, важливість розробки методології вивчення електронних доказів, порядок їх збору та фіксації.

Ключові слова: *докази, електронні докази, комп'ютерні дані, дані про інформаційні потоки, міжнародне співробітництво, кримінальне процесуальне право, кримінальний процесуальний кодекс України.*

Аннотация. *Данная статья посвящена рассмотрению теоретических вопросов, связанных с введением в Украине института электронных доказательств уголовного производства. Также в статье поднимается вопрос путей получения электронных доказательств. В статье отмечается, что в современном развитом мире появляются все новые и новые виды преступлений. В данном контексте мы рассмотрим преступления, тесно связанные с использованием информационных технологий. Доказывание таких преступлений вызывает некоторые трудности. На сегодняшний день актуальным является закрепление понятия электронных доказательств в Уголовно-процессуальном кодексе Украины и формирование методики их изучения. Также автор статьи отмечает, что среди нерешенных и проблемных аспектов использования электронных доказательств в уголовном производстве Украины ученые выделяют: отсутствие четкого процессуального порядка их получения в соответствии с уголовно-процессуальным кодексом Украины; отсутствие оснований для признания электронных доказательств неприемлемыми; трудности с выявлением и фиксацией электронных доказательств из-за отсутствия специализированных знаний у*

следователей, что обусловливает необходимость привлечения специалистов для ведения судебного производства; отсутствие разработанной методологии изучения таких доказательств; отсутствие однородной терминологии и регулирования на законодательном уровне.

В статье определено, что также для эффективной имплементации норм международного права в сфере борьбы с киберпреступностью целесообразно обосновать необходимость законодательного определения электронных доказательств, источников их формирования, допустимости международного сотрудничества путем обмена электронными доказательствами, целесообразность использования электронных способов направления запросов и ответов об их выполнении, возможность применения контрольной поставки информации для расследования транснациональных компьютерных преступлений.

Исходя из вышесказанного, автор предлагает собственное определение электронных доказательств. Сделан вывод о необходимости ее законодательного закрепления термина «электронные доказательства» и продолжение изучения категории, важность разработки методологии изучения электронных доказательств, порядок их сбора и фиксации.

Ключевые слова: *доказательства, электронные доказательства, компьютерные данные, данные об информационных потоках, международное сотрудничество, уголовное процессуальное право, уголовный процессуальный кодекс Украины*

Summary. *This article is devoted to the consideration of theoretical issues related to the introduction in Ukraine of the institution of electronic evidence of criminal proceedings. The article also raises the question of ways to obtain electronic evidence. The article notes that in the modern developed world there are more and more new types of crimes. In this context, we will consider crimes*

closely related to the use of information technology. Proving such crimes raises some difficulties. To date, it is relevant to consolidate the concept of electronic evidence in the Criminal Procedure Code of Ukraine and the formation of a methodology for their study. Also, the author of the article notes that among the unresolved and problematic aspects of using electronic evidence in criminal proceedings in Ukraine, scientists distinguish: the lack of a clear procedural procedure for obtaining them in accordance with the Criminal Procedure Code of Ukraine; lack of grounds for declaring electronic evidence inadmissible; difficulties in identifying and fixing electronic evidence due to the lack of specialized knowledge among investigators, which necessitates the involvement of specialists for conducting legal proceedings; lack of a developed methodology for studying such evidence; lack of uniform terminology and regulation at the legislative level.

It is determined in the article that for the effective implementation of international law in the field of combating cybercrime, it is advisable to substantiate the need for a legislative definition of electronic evidence, sources of their formation, the admissibility of international cooperation through the exchange of electronic evidence, the expediency of using electronic methods of sending requests and responses about their implementation, the possibility application of control information supply for investigation of transnational computer crimes.

Based on the above, the author offers his own definition of electronic evidence. It is concluded that it is necessary to legislatively consolidate the term "electronic evidence" and continue to study the category, the importance of developing a methodology for studying electronic evidence, the procedure for collecting and recording them.

Key words: *evidence, electronic evidence, computer data, data on information flows, international cooperation, criminal procedural law, criminal procedure code of Ukraine.*

Мета статті полягає у дослідженні окремих аспектів електронних доказів у кримінальному провадженні.

Постановка проблеми. На думку С. Джобса, тільки інновація відрізняє лідера від наздоганяючого [8]. Науково-технічний прогрес проникає в усі сфери людської діяльності, в тому числі і сферу кримінального судочинства. Сучасні засоби, методи, спеціальні знання завжди ретельно досліджувалися криміналістами на предмет можливого використання їх для виявлення і фіксації доказів. Г. Гросс класифікував докази на «формальні» і «універсальні», або «непідкупні». Під першими він розумів показання свідків, за якими можна отримати лише «формальну» істину, відзначаючи: «Зла воля і обман, помилки і омана, а найчастіше власні висновки свідка і його впевненість, що він говорить лише про те, що бачив і чув, впливають настільки нескінченно багато, що ми лише в найрідкісніших випадках можемо визнати показання свідка об'єктивними, абсолютно вірними і ні в якій мірі не навіяними». Предмет вивчення криміналістики Г. Гросс визначає так: «Яким способом ми можемо знайти ті чи інші докази, як дійти до них, як їх охороняти і як їх використовувати - все це настільки ж важливо, як важливий і той результат, якого ми досягаємо відправленням правосуддя. Знайдені і використані сліди злочинця, акуратно складене креслення, хоча б і нескладне, який-небудь мікроскопічний препарат, розшифроване листування, фотографічні знімки, татуювання, відновлений обвуглений лист, яке-небудь точне вимірювання і тисячі подібних реальностей - не що інше, як непідкупні свідки, які не допускають спростування, і в той же час

допускають постійну перевірку, свідки, щодо яких виключається можливість помилки, одностороннє розуміння, зла воля, наклеп і подібне. З кожним успіхом криміналістики <… > Підвищується значення універсальних доказів» [7].

У 1898 р. в передмові до третього видання книги «Керівництво для судових слідчих як система криміналістики» Г. Гросс передбачав: «Криміналістика, ще настільки молода наука, не може передбачити, до яких кінцевих підсумків вона неодмінно повинна привести, але їй відомо, що ці майбутні зміни також не залишаться постійними, що постійність взагалі ніколи не буде досягнуто, що єдино вічним буде стан безперервного руху» [7].

Відповідно до ст. 22 Угоди про асоціацію України з Європейським Союзом сторони домовились, зокрема, боротися з кіберзлочинністю (п. «f» ч. 2) [1]. Для цього в Україні створено правову базу побудови інформаційного суспільства - прийняті закони України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 рр.», «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про електронний цифровий підпис», «Про основні засади забезпечення кібербезпеки України» які регулюють суспільні відносини у сфері створення інформаційних електронних ресурсів, захист інтелектуальної власності, впровадження електронного документообігу.

В сучасних умовах комп'ютеризації одним з дискусійних питань кримінального процесу та криміналістики є використання електронних доказів як в національному законодавстві, так і в сфері надання міжнародної правової допомоги.

Аналіз останніх досліджень і публікацій. Дослідженню електронних доказів присвячені роботи Д.О. Алєксєєвої-Процюк [5], А.Г. Волєводз [6], О.В. Сіренко [14], В. В. Мурадов [12], О. І. Котляревський [10], Д. М. Киценко [10] та ін. Зважаючи на те, що нормативне регулювання електронних доказів лише розпочато, багато питань як наукового, так і нормативного характеру залишаються невирішеними.

Формулювання цілей статті (постановка завдання). З урахуванням глобалізації комп'ютерного простору необхідно провести уніфікацію законодавства, що регламентує розслідування, оцінку доказів і міжнародне співробітництво при використанні електронних доказів. Як справедливо зазначає А. Волєводз, практика міжнародної співпраці в боротьбі зі злочинністю свідчить, з одного боку, про появу і все більш широке поширення злочинів у сфері комп'ютерної інформації, а з іншого - про зростання ролі нових методів отримання доказів і перспективності використання високих технологій в цій діяльності [5, с. 9]. Для ефективної імплементації норм міжнародного права в сфері боротьби з кіберзлочинністю доцільно обґрунтувати необхідність законодавчого визначення електронних доказів, джерел їх формування, допустимості міжнародного співробітництва шляхом обміну електронними доказами, доцільність використання електронних способів напряму запитів і відповідей про їх виконання, можливість застосування контрольної поставки інформації для розслідування транснаціональних комп'ютерних злочинів.

Виклад основного матеріалу. Відповідно до ст. 84 Кримінального процесуального кодексу України (далі - КПК України) доказами являються фактичні дані, отримані в установленому порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність або відсутність фактів і обставин, що мають значення для кримінального

провадження і підлягають доказуванню. Процесуальними джерелами доказів є свідчення, речові докази, документи, висновки експертів. При цьому документами визнаються спеціально створені з метою збереження інформації матеріальні об'єкти, що містять зафіксовані за допомогою письмових знаків, звуку, зображення і так далі відомості, які можуть бути використані як докази факту або обставини, що встановлюється в рамках кримінального судочинства (ст. 99 КПК України). В п. 1 ч. 2 ст. 99 КПК України міститься вказівка на те, що документами можуть бути визнані матеріали фотозйомки, звукозапис, відеозапис та інші носії інформації, в тому числі електронні. Незважаючи на розширення сфери використання електронних документів, в тому числі і при вчиненні злочинів, Кримінальний процесуальний кодекс України, прийнятий в 2012 р., що не містить спеціального розділу, присвяченого поняттю, збору, фіксації та оцінці даного виду доказів [2]. Законодавець обмежився лише фрагментарною згадкою про використання такого виду доказів. Так, одним з видів негласних слідчих (розшукових) дій є втручання в приватне спілкування, при цьому його різновидами є аудіо-, відеоконтроль особи, арешт, огляд і виїмка кореспонденції, зняття інформації з транспортних телекомунікаційних систем, зняття інформації з електронних інформаційних систем (ч. 4 ст. 258 КПК України).

На законодавчому рівні закріплено, що пошук, виявлення і фіксація відомостей, що містяться в електронній інформаційній системі, або її частинах, доступ до електронної інформаційної системи або її частин, а також отримання таких відомостей без відома їх власника, володільця або утримувача може здійснюватися на підставі ухвали слідчого судді при існуванні відомостей про наявність інформації в електронній системі або її частині, що має значення для певного досудового розслідування. Не потребує дозволу слідчого судді на отримання відомостей з електронних

інформаційних систем, доступ до яких не обмежується їх власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту. У визначенні слідчого судді додатково повинні бути вказані ідентифікаційні ознаки електронної інформаційної системи, в якій може здійснюватися втручання в приватне спілкування (ст. 264 КПК України).

Згідно ч. 2 ст. 265 КПК України зміст інформації, отриманої внаслідок зняття відомостей з електронних інформаційних систем або їх частин, фіксується на відповідному носії особою, що здійснювала зняття, та яка зобов'язана забезпечити обробку, збереження і передачу інформації.

Дослідження інформації, отриманої при застосуванні технічних засобів, в разі необхідності здійснюється за участю фахівців. Технічні засоби, що застосовувалися під час проведення негласних слідчих (розшукових) дій, а також первинні носії отриманої інформації повинні зберігатися до набрання вироком законної сили. Зазначені носії інформації можуть бути предметом дослідження відповідних спеціалістів або експертів (ст. 266 КПК України).

Варто відзначити той факт, що за допомогою комп’ютерних технологій може бути скоєно безліч злочинів (загроза терористичного акту, виготовлення порнографічної продукції, фінансові злочини і інші), а це обумовлює необхідність проводити огляд комп'ютерної техніки, обшук, що супроводжується специфічної процедурою фіксації і вилучення, дослідження електронних доказів. Відсутність чіткого законодавчого закріплення поняття електронних доказів, їх видів, джерел, допустимості призводить до низького рівня розкриття окремих видів злочинів, до невизнання їх в суді. Зокрема, кібератаки представляють серйозну загрозу банківській системі України. Однак офіційні дані Державної судової адміністрації України свідчать, що до судів з обвинувальними актами

доходить незначна кількість кримінальних проваджень. Так, в 2019 р. за злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), комп'ютерних систем і систем електрозв'язку в судах України розглянуто 101 кримінальне провадження щодо 66 осіб; обвинувальні вироки постановлені лише по 67 кримінальним провадженням. По 6 справах затверджені угоди про примирення, по 30 справах - про визнання провини, 27 виробництв закрито та ні одного не спрямовано на додаткове розслідування [9].

Європейська конвенція про кіберзлочинність від 23.11.2001 р. (далі - Конвенція) визначила зміст декількох дефініцій: «комп'ютерні дані» - будь-яке представлення фактів, відомостей або концепцій у формі, придатній для обробки за допомогою до комп'ютерних систем, в тому числі програми, призначені для виконання комп'ютерної системою певних дій; «Дані трафіку» - будь-які комп'ютерні дані, пов'язані з передачею інформації за допомогою комп'ютерної системи, які створені комп'ютерною системою, що була частиною ланцюга передачі даних, і вказує на джерело повідомлення, його призначення, маршрут, час, дату, розмір, тривалість або тип лежить в його основі послуги [3]. Слід зазначити, що зазначені терміни не є вичерпними. В даному випадку український законодавець при формуванні національного стандарту комп'ютерних доказів стикається з релятивізмом, оскільки особливістю міжнародних актів є лише загальне закріплення понять, що не обмежує законотворчу діяльність і особливість внутрішнього права країни.

Підписанти Конвенції взяли на себе зобов'язання вжити таких законодавчих та інших заходів, які можуть знадобитися для встановлення повноважень і процедур, передбачених в цілях проведення певних кримінальних розслідувань або розглядів, а саме: 1) до кримінальних злочинів, передбаченими ст.ст. 2-11 Конвенції (незаконний доступ;

незаконний перехоплення, втручання в дані, втручання в систему, неналежне використання пристроїв; підроблення комп'ютерних даних; комп'ютерне шахрайство, злочини, пов'язані з дитячою порнографією; злочини, пов'язані з порушеннями авторського права і суміжних прав; замах, пособництво і підбурювання); 2) до інших кримінальних злочинів, скоєних за допомогою комп'ютерної системи; 3) до збору доказів у кримінальному злочині в електронній формі.

Згідно ст. 19 Конвенції кожна зі сторін вживатиме таких законодавчих та інших заходів, які можуть знадобитися для того, щоб дозволити своїм компетентним органам шляхом проведження обшуку або подібним чином отримувати доступ на її території до комп'ютерної системи в цілому або окремої її частини, що зберігаються там комп'ютерним даним, а також до носію комп'ютерних даних, на якому можуть зберігатися комп'ютерні дані. Ці заходи повинні включати в себе такі повноваження: а) по конфіскації або вилученню комп’ютерної системи або її частини, носія комп'ютерних даних; б) по виготовленню і збереженню копії таких комп'ютерних даних; в) по підтримці цілісності відповідних збережених комп'ютерних даних; г) по припиненню доступу до цих комп'ютерних даних в комп'ютерній системі, до якої отримано доступ, або видалення їх з цієї системи.

Конвенція в ст. 20 передбачає право збору комп’ютерних даних в режимі реального часу. Кожна з сторін вживатиме таких законодавчих та інших заходів, які можуть знадобитися для того, щоб дозволити її компетентним органам збирати або записувати (за допомогою застосування технічних засобів на території даної сторони), а також примушувати постачальника послуг (в межах його існуючих технічних можливостей) збирати або записувати (шляхом застосування технічних засобів на територій цієї сторони) або співпрацювати з компетентними

органами і допомагати їм збирати або записувати в режимі реального часу дані трафіку, пов'язані з певними операціями з передачі даних на її території, здійснюваними за допомогою комп'ютерної системи.

Варто відзначити можливість перехоплення даних змісту інформації (ст. 21 Конвенції) у відношенні ряду серйозних злочинів, визначених відповідно до національного законодавства, які дозволили б компетентним органам збирати або записувати шляхом застосування технічних засобів на території цієї сторони і примушувати постачальника послуг (в межах його існуючих технічних можливостей) збирати або записувати (шляхом застосування технічних засобів на території цієї сторони) або співпрацювати з компетентними органами і допомагати їм збирати або записувати в режимі реального часу дані змісту певних передач інформації на території держави, що здійснюються за допомогою комп'ютерної системи.

Особливу увагу приділено питанням юрисдикції, оскільки кожна зі сторін вживатиме таких законодавчих та інших заходів, які можуть знадобитися, щоб встановити юрисдикцію по будь-якому із злочинів, передбачених ст. ст. 2-11 Конвенції, якщо воно вчинене на її території, на борту судна під прапором даної сторони, на борту повітряного судна, зареєстрованого згідно із законами даної сторони, або одним з підданих даної сторони, якщо правопорушення підпадає під дію кримінального законодавства на території, де воно було вчинено, або ж якщо право-порушення вчинено поза територіальною юрисдикцією будь-якої держави (ст. 20 Конвенції).

Згідно ст. 23 Конвенції з метою розслідування або судового переслідування кримінальних злочинів, пов'язаних з комп'ютерними системами і даними, а також з метою збору доказів в кримінальних злочинах в електронній формі сторони повинні здійснювати найширше

співробітництво один з одним через застосування відповідних міжнародних договорів про міжнародне співробітництво в сфері боротьби зі злочинністю, домовленостей, досягнутих на основі єдиного чи взаємозобов'язаного законодавства, а також національних законів.

У Кримінальному процесуальному кодексі України передбачається, що в рамках міжнародного співробітництва запит направляється поштою, а в невідкладних випадках - електронним, факсимільним або іншим способом. В такому випадку оригінал запиту надсилається поштою пізніше трьох днів з моменту його передачі електронною поштою. Виконання такого запиту здійснюється виключно за умови підтвердження його оригіналом (ч. 4 ст. 548 КПК України). Направлення компетентному органу іноземної держави матеріалів виконання запиту можливе лише після отримання українською стороною оригіналу запиту (ч. 5 ст. 548 КПК України). Очевидним є закріплення в законі обов'язковості існування електронного і письмового запиту, що вказує на обмежену правову дію першого, що полягає лише у виконанні вимог, але не зобов'язує надати інформацію іншій державі. Прерогативою користується тільки письмовий запит, який має двовекторну обов'язковість.

Існуючу прогалину в КПК України щодо електронних доказів логічно повинно було усунути в спеціальному Законі України «Про боротьбу з кіберзлочинністю», проект якого містить поняття кібершпигунство, комп'ютерних даних, даних про інформаційні потоки і так далі [4]. З аналізу норм закону вбачається відсутність вказівок на джерела електронних доказів. У цій частині проект належить доповнити нормою такого змісту: «Джерелами електронних доказів є електронні пристрої: комп'ютери та периферійні пристрої, комп'ютерні мережі, мобільні телефони, цифрові камери і інші портативні пристрої, в тому

числі пристрої для зберігання інформації, а також мережа Інтернет. Інформація з цих джерел не має відокремленої фізичної форми».

Зокрема, Сіренко О. В. вважає, що електронні докази - це дані про обставини, що мають значення для кримінального провадження й існують у нематеріальному вигляді в межах технічного носія чи каналу зв'язку та сприйняття і дослідження яких можливе за допомогою технічних засобів і програмного забезпечення [11, с. 211].

В. В. Мурадов під електронними доказами визнає сукупність інформації, яка зберігається в електронному вигляді на будь-яких типах електронних носіїв та в електронних засобах [12, с. 8]. Цієї ж позиції притримуються О. І. Котляревський, Д. М. Киценко [10].

Електронні докази в чому схожі з традиційними, проте мають вони і ряд унікальних характеристик:

1) їх не видно неозброєним оком: витягти їх може тільки фахівець;

2) вони дуже нестійкі: на деяких пристроях або в певних обставинах під час звичайної експлуатації пристрою інформація в його пам'яті (а тобто, і докази, які воно містить) може змінюватись. Наприклад, при розрядці пристрою або нестачі пам'яті система накладає (записує) нову інформацію поверх старої. Комп'ютерна пам'ять може бути пошкоджена або знищена під впливом фізичних факторів (великої вологості або високої температури) і електромагнітних полів;

3) вони можуть бути змінені або знищені в процесі звичайної експлуатації пристрою: пам'ять комп'ютерних пристроїв постійно змінюється за запитом користувачів («зберегти документ», «скопіювати файл») або операційної системи;

4) їх можна копіювати без втрати якості: цифрові дані можна копіювати необмежену кількість разів, і кожна наступна копія нічим не

буде відрізнятися від оригіналу. Завдяки цій унікальній особливості різні фахівці можуть паралельно і незалежно один від одного досліджувати різні копії одного і того ж електронного докази, не зачіпаючи при цьому оригінал;

5) стрімка еволюція джерел електронних доказів: нові технології з'являються і розвиваються з неймовірною швидкістю, тому методи і процедури по роботі з електронними доказами потрібно постійно переглядати і оновлювати [13].

Ретельна підготовка операцій і слідчих дій зі збору електронних доказів охоплює вирішення деяких питань. По-перше, необхідно знати місцезнаходження даних (фізичне розміщення), оскільки не виключається знаходження обладнання в одному місці, а даних - в іншому. Якщо не враховувати таку ймовірність, то вже після прибуття на місце може виявитися, що для подальших дій потрібен дозвіл компетентного органу (особливо якщо дані знаходяться в іншій юрисдикції) або додаткові технічні навички / обладнання.

По-друге, рекомендується заздалегідь встановити професійні навички підозрюваного. Для цього необхідно зібрати якомога більше інформації про підозрюваного. Якщо він добре розбирається в комп'ютерних технологіях, то він може здійснити маніпуляції, які допомагають йому «замести сліди» своїх діянь або перешкодити вилученню обладнання та даних, наприклад, поставити на пристрій пароль або встановити програму незворотного знищення ключових даних. Потрібно підготуватися до подібних ситуацій, тобто зробити контрзаходи. Підозрюваний може зберігати дані в хмарному сховищі або на інших онлайн-ресурсах, і тоді на самому устаткуванні не буде ніякої інформації.

По-третє, слідчий не повинен ігнорувати наявність альтернативних джерел доказів. Перш ніж приступати до будь-яких дій, які передбачають

прямий контакт з підозрюваним і виїмку даних або обладнання, на підготовчому етапі потрібно перевірити, чи існують інші, більш кращі джерела тієї ж інформації. Наприклад, для отримання даних про електронні повідомленні можна звернутися до іншої сторони - адресату повідомлення або третьої сторони - постачальнику інтернет-послуг або онлайн-послуг [13].

Слідчий повинен прийняти тактичне рішення, де шукати дані: у підозрюваного або в іншого власника цієї ж інформації. У деяких країнах закон вимагає від компаній повідомляти клієнтів про будь-які запити про надання даних, а це може насторожити підозрюваного, він може заховати або знищити докази. Особи, які ведуть розслідування, повинні оцінити, яким чином процедура витребування доказів у третіх осіб може вплинути на його ефективність, особливо якщо дані зберігаються на території іншої держави. Крім того, важливо визначити оптимальне джерело доказів, яке допоможе отримати найбільш важливу інформацію.

У процесі підготовки до обшуку необхідно встановити, які пристрої інформації або комунікаційне та мережеве обладнання можуть бути виявлені на місці обшуку; хто відповідає за комп'ютерні пристрої; скільки одиниць обладнання може бути виявлено; який обсяг даних, які потрібно буде скопіювати; чи існує резервна копія даних і на якому носії вона зберігається.

Іноді в отриманні доказів може допомогти нотаріус або аналогічний фахівець. У романо-германських правових системах однією з функцій нотаріуса є перевірка і засвідчення справжності певних юридичних документів і угод, які надаються в якості судових доказів. Нотаріус може увійти в Інтернет через свій комп'ютер, оглянути необхідні веб-сайти або сторінки, після чого формально засвідчити їх справжність. Що стосується

міжнародного співробітництва, то багато країн уклали угоди про взаємне визнання нотаріально завірених документів.

Конвенція передбачає можливість транскордонного доступу до комп'ютерних даних, які знаходяться в системах загального доступу, або при отриманні відповідного дозволу (ст. 32). Будь-яка зі сторін має право, без згоди іншої сторони, одержувати доступ до комп'ютерних даних з відкритих джерел, які знаходяться в системах загального доступу, незалежно від територіального місцезнаходження цих даних; а також за допомогою комп'ютерної системи на своїй території отримувати доступ до комп'ютерних даних, розташованим на території іншої сторони, при отриманні правомірної і добровільної згоди з боку особи, яка має законне право на надання даних цій стороні за допомогою вищезгаданої комп’ютерної системи [4].

Незважаючи на наявність конвенційних зобов'язань, національне законодавство України та інших країн не містить пряму регламентацію їх реалізації. В законодавстві України це питання не вирішене, оскільки міжнародне співробітництво в рамках кримінальної провадження має здійснюватися через уповноважені на те органи. Прикладом спроби реалізації права на отримання правоохоронними органами інформації від особи, яка має законне право на надання даних іншої країни, минаючи направлення запиту до центрального органу досудового розслідування, є досвід Бельгії в розслідуванні комп'ютерного шахрайства [11]. Так, на території цієї країни було скоєно одночасно декілька злочинів в сфері фінансового шахрайства з використанням комп'ютерних систем. Визначивши загальні ознаки, прокуратура Бельгії об'єднала всі епізоди в одне провадження на підставі того, що всі потерпілі напередодні «атаки» отримували листи від незнайомця через систему «Yahoo». Оскільки Директорат «Yahoo» знаходиться в Каліфорнії, прокурор для прискорення

отримання IP-адрес підозрюваних направив електронний запит безпосередньо директорату, а не в прокуратуру США. Компанія «Yahoo» відмовилася виконувати запит, спрямований прокурором іншої країни, що створило перешкоди для ефективного розслідування злочину. Суд Бельгії задовільнив позов прокурора Бельгії до Директорату «Yahoo» про накладення штрафу за невиконання припису прокурора про надання інформації, наявної в розпорядженні власника, необхідної для виробництва в рамках кримінального переслідування.

У законодавстві України в рамках міжнародного співробітництва передбачається «контрольна поставка» (ст. 569 КПК України), але тільки в разі виявлення контрабанди. На нашу думку, цей метод необхідно поширити і при зборі електронних даних в разі виявлення ознак підготовки до вчинення хакерських атак, хаквітізма (злочинів, які зазіхають на конфіденційність інформації), деструктивних кіберзлочинів з території іншої держави. Такий підхід пояснюється тим, що кіберпростір - це змодельований за допомогою комп'ютера інформаційний простір, в якому знаходяться дані про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символічному чи іншому вигляді і знаходяться в процесі руху по локальних і глобальних комп'ютерних мереж, або відомості, які зберігаються в пам'яті будь-якого фізичного або віртуального пристосування, а також іншого носія, спеціально призначеного для їх зберігання, обробки і передачі, унікальне середовище, що не розміщене в географічному просторі, але доступне кожному в будь-якій точці світу за допомогою доступу в Інтернет.

Неврегульованими та проблемними аспектами використання електронних доказів у кримінальному судочинстві України науковці виокремлюють: відсутність чіткого процесуального порядку їхнього отримання відповідно до Кримінального процесуального кодексу України;

складності у слідчих під час виявлення та фіксації електронних доказів через недостатність спеціальних знань у слідчих, що зумовлює необхідність залучення спеціалістів для проведення процесуальних дій; відсутність підстав визнання електронних доказів недопустимими; відсутність однотипної термінології та урегульованості на законодавчому рівні; відсутність сформованої методики дослідження таких доказів [5, с. 248–249].

Висновки. В контексті євроінтеграції України актуалізується проблема вивчення досвіду становлення інформаційного суспільства в країнах-членах Європейського Союзу, а також імплементації норм правових актів Європейського Союзу в інформаційне законодавство України. У переліку пріоритетів стратегічного розвитку України особливе місце повинні займати захист прав, свобод та безпеки в інформаційній сфері, відмова від ідей тотального інформаційного контролю. З цією метою необхідно в законодавстві визначити поняття «електронний доказ» як дані, що підтверджують факти, інформацію або концепцію в формі, пристосованої для обробки за допомогою комп'ютерної системи, в тому числі програми виконання комп'ютерною системою тих чи інших дій. Джерелами електронних доказів доцільно визнати електронні пристрої: комп'ютери та периферійні пристрої, комп’ютерні мережі, мобільні телефони, цифрові камери і інші портативні пристрої, в тому числі пристрої для зберігання інформації, а також мережу Інтернет. Інформація з цих джерел не має відокремленої фізичної форми. В рамках міжнародного співробітництва необхідно інтенсифікувати використання електронних способів передачі інформації, яка запитується, а не тільки направлення запитів. На думку А.Л. Шатлен, існує соціальний запит на створення нового напрямку в сфері виявлення, фіксації, дослідження електронних

доказів - цифрової криміналістики, що займається обробкою електронних доказів для їх законного використання в суді [15].

Література

1. Угода про асоціацію між Україною та Європейським Союзом від 27.06.2014 р. : ратифікована Законом України від 16.09.2014 р. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення: 23.10.2020)
2. Кримінальний процесуальний кодекс України від 13.04.2012 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 23.10.2020)
3. Конвенція про кіберзлочинність від 23.11.2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 23.10.2020)
4. Про основні засади забезпечення кібербезпеки України від 05.10.2017 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19/ed20200703#Text (дата звернення: 27.10.2020)
5. Алєксєєва-Процюк Д. О. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування // Науковий вісник публічного та приватного права. 2018. Випуск 2. С. 247–253.
6. Волеводз А. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2002. 496 с.
7. Гросс Г. Руководство для судебных следователей как система криминалистики. М.: ЛексЭст, 2002. 1088 с.
8. Джобс С. Афоризмы, цитаты, высказывания. URL: http://aphorism-citation.ru/index/0-783 (дата звернення: 28.10.2020)

9. Форма №1-к «Звіт судів першої інстанції про розгляд матеріалів кримінального провадження за 2019 рік» : звіт Державної судової адміністрації України за 2019 р. URL: https://court.gov.ua/inshe/sudova_statystyka/rik_2019 (дата звернення: 28.10.2020)
10. Котляревський О. І. Киценко Д. М. Комп'ютерна інформації як речовий доказ у кримінальній справі / О. І. Котляревський // Інформаційні технології та захист інформації : збірник наукових праць. 1998. № 2. С. 70–79.
11. Матеріали семінару для голів судів загальної юрисдикції «Особливості оцінки доказів у справах, пов'язаних з використанням комп'ютерних технологій» (м. Київ, 16 лютого 2011 р.). К.: 2011.
12. Мурадов В. В. Електронні докази: криміналістичний аспект використання // Ефективність державного управління. 2013. Вип. № 3-2. С. 313–315.
13. Руководство по работе с электронными доказательствами для сотрудников полиции, прокуратуры и судов. Отдел по вопросам противодействия киберпреступности // Генеральная дирекция по правам человека и верховенству права. Страсбург, 2020. URL: https://rm.coe.int/09000016809f1fde (дата звернення: 29.10.2020)
14. Сіренко О. В. Електронні докази у кримінальному провадженні. Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика). Вип. 14. 2019. 252 с.
15. Шатлен А.Л. Висновок БДІПЛ/ОБСС щодо проекту Закону України «Про боротьбу з кіберзлочинністю» (2014 р.) та дотримання стандартів прав людини під час розробки законодавства, пов'язаного з кіберзлочинністю // Матеріали Комітету з інформаційної політики Верховної Ради України. 26 березня 2015.

References

1. Ugoda pro asociaciyu mizh Ukrayinoyu ta Yevropejskim Soyuzom vid 27.06.2014 r. : ratifikovana Zakonom Ukrayini vid 16.09.2014 r. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (data zvernennya: 23.10.2020)
2. Kriminalnij procesualnij kodeks Ukrayini vid 13.04.2012 r. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (data zvernennya: 23.10.2020)
3. Konvenciya pro kiberzlochinnist vid 23.11.2001 r. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (data zvernennya: 23.10.2020)
4. Pro osnovni zasadi zabezpechennya kiberbezpeki Ukrayini vid 05.10.2017 r. URL: https://zakon.rada.gov.ua/laws/show/2163-19/ed20200703#Text (data zvernennya: 27.10.2020)
5. Alyeksyeyeva-Procyuk D. O. Elektronni dokazi v kriminalnomu sudochinstvi: ponyattya, oznaki ta problemni aspekti zastosuvannya // Naukovij visnik publichnogo ta privatnogo prava. 2018. Vipusk 2. S. 247–253.
6. Volevodz A. Protivodejstvie kompyuternym pre¬stupleniyam: pravovye osnovy mezhdunarodnogo sotrudniche¬stva. M.: Yurlitinform, 2002. 496 s.
7. Gross G. Rukovodstvo dlya sudebnyh sledovatelej kak sistema kriminalistiki. M.: LeksEst, 2002. 1088 s.
8. Dzhobs S. Aforizmy, citaty, vyskazyvaniya. URL: http://aphorism-citation.ru/index/0-783 (data zvernennya: 28.10.2020)
9. Forma №1-k «Zvit sudiv pershoyi instanciyi pro rozglyad materialiv kriminalnogo provadzhennya za 2019 rik» : zvit Derzhavnoyi sudovoyi administraciyi Ukrayini za 2019 r. URL:

https://court.gov.ua/inshe/sudova_statystyka/rik_2019 (data zvernennya: 28.10.2020)

10. Kotlyarevskij O. I. Kicenko D. M. Komp'yuterna informaciyi yak rechovij dokaz u kriminalnij spravi / O. I. Kotlyarevskij // Informacijni tehnologiyi ta zahist informaciyi : zbirnik naukovih prac. 1998. № 2. C. 70–79.
11. Materiali seminaru dlya goliv sudiv zagalnoyi yurisdikciyi «Osoblivosti ocinki dokaziv u spravah, pov'yazanih z vikoristannyam komp'yuternih tehnologij» (m. Kiyiv, 16 lyutogo 2011 r.). K.: 2011.
12. Muradov V. V. Elektronni dokazi: kriminalistichnij aspekt vikoristannya // Efektivnist derzhavnogo upravlinnya. 2013. Vip. № 3-2. S. 313–315.
13. Rukovodstvo po rabote s elektronnymi dokazatel¬stvami dlya sotrudnikov policii, prokuratury i sudov. Otdel po voprosam protivodejstviya kiberprestupnosti // Generalnaya direkciya po pravam cheloveka i verhovenstvu prava. Strasburg, 2020. URL: https://rm.coe.int/09000016809f1fde (data zvernennya: 29.10.2020)
14. Sirenko O. V. Elektronni dokazi u kriminalnomu provadzhenni. Mizhnarodnij yuridichnij visnik: aktualni problemi suchasnosti (teoriya ta praktika). Vip. 14. 2019. 252 s.
15. Shatlen A.L. Visnovok BDIPL/OBSS shodo proektu Zakonu Ukrayini «Pro borotbu z kiberzlochinnistyu» (2014 r.) ta dotrimannya standartiv prav lyudini pid chas rozrobki zakonodavstva, pov'yazanogo z kiberzlochinnistyu // Materiali Komitetu z informacijnoyi politiki Verhovnoyi Radi Ukrayini. 26 bereznya 2015.