УДК 343.148 (477)
HTTPS://ORCID.ORG/0000-00033710-1318
Дунаєва Тетяна Євгенівна,
кандидат юридичних наук, науковий співробітник
відділу дослідження проблем кримінального процесу та судоустрою
Науково-дослідний інститут вивчення проблем злочинності
імені академіка В.В. Сташиса НАПрН України,
м. Харків, Україна

ОСОБЛИВОСТІ ПРЕДМЕТУ ДОКАЗУВАННЯ КІБЕРЗЛОЧИНІВ В УКРАЇНІ ПІД ЧАС ВОЄННОГО СТАНУ[1]

Анотація. *У статті досліджено особливості предмету доказування кіберзлочинів в Україні під час воєнного стану. Обґрунтовано, що особливого значення набувають збирання доказів, їх оцінка та закріплення під час воєнних дій, що є важливим етапом при розслідуванні кримінальних проваджень щодо злочинів, вчинених в Інтернет-мережі. Проведення всебічного та швидкого досудового розслідування під час дії воєнного стану для подальшого встановлення наявності або відсутності вини особи у вчиненні кримінального правопорушення є важливими для подальшого підвищення ефективності судового розгляду та забезпечення єдності судової практики, верховенства права, ефективного захисту прав людини, що слугують додатковим юридичним аргументом під час прийняття рішень у разі виявлення недоліків, помилок, прогалин у чинному законодавстві. Досліджено процес доказування (збирання, перевірка та оцінка доказів) кіберзлочинів. Доведено необхідність проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, експертиз, залучення експертів та спеціалістів, застосування заходів забезпечення кримінального провадження та здійснення міжнародного співробітництва.*

Постає питання про підвищення якості кримінального процесуального законодавства України шляхом застосування цифровізації кримінального провадження, при збиранні доказів, їх закріплення та внесення відповідних змін до кримінального процесуального законодавства України.

Ключові слова: кіберзлочин, доказування, докази, розслідування, кримінальне провадження, цифровізація кримінального процесу.

Anotation. *The article examines the peculiarities of the subject of proving cybercrimes in Ukraine during martial law. It is substantiated that the collection of evidence, their evaluation and consolidation during military operations, which is an important stage in the investigation of criminal proceedings regarding crimes committed on the Internet, acquire special importance. Conducting a comprehensive and quick pre-trial investigation during martial law to further establish the presence or absence of a person's guilt in committing a criminal offense is important for further increasing the effectiveness of judicial proceedings and ensuring the unity of judicial practice, the rule of law, effective protection of human rights, which serve as an additional legal argument during decision-making in case of detection of shortcomings, errors, gaps in the current legislation. The process of proving (collection, verification and evaluation of evidence) of cybercrimes has been studied. The need to conduct investigative (search) actions and covert investigative (search) actions, examinations, involvement of experts and specialists, use of measures to ensure criminal proceedings and implementation of international cooperation has been proven.*

Therefore, the question arises about improving the quality of the criminal procedural legislation of Ukraine by applying digitalization of criminal proceedings, when collecting evidence, consolidating it and making appropriate changes to the criminal procedural legislation of Ukraine. I support a number of timely and appropriate changes to the Criminal Procedure Code of Ukraine, which correspond to the realities of life during

[1] Підготовлено на виконання фундаментальної теми «Теоретико-правові проблеми цифровізації кримінального провадження в Україні», що досліджується в НДІ вивчення проблем злочинності імені академіка В.В.Сташиса НАПрН України (№ державної реєстрації в УкрІНТЕІ 0121U114401).

martial law: paragraph 2 of Article 170; paragraph 2, part 6 of Article 236; Part 2 of Article 237; Part 5 of Article 268.

Key words: cybercrime, evidence, investigation, criminal proceedings, digitalization of the criminal process.

Постановка проблеми. У всьому світі злочини у кіберпросторі щороку завдають збитків на десятки мільярдів доларів США як державам, так і приватним компаніям [1]. Щодо статистичних даних про кількість кібератак, збільшення нападів під час воєнного стану збільшилась у понад 3 рази. Статистичні дані свідчать, що у 2020 році було зафіксовано майже 800 кібератак, у 2021 р. - 1400, то у 2022 р. - кількість кібернападів зросла у понад 3 рази. Наразі країна-агресор завдає в середньому понад 10 кібератак на добу, здебільшого по об'єктах критичної інфраструктури, зокрема енергетичному комплексу, логістиці, зв'язку, військовим об'єктам, а також в його зоні уваги реєстри і бази даних органів влади [2]. За даними журналу Cybercrime Magazine, до 2025 р. прогнозована вартість кіберзлочинності для світової економіки становитиме 10,5 трильйонів доларів США щорічно. Кіберзлочинна діяльність також може поставити під загрозу життя. Раніше хакери загрожували водопостачанню невеликого міста, що викликало занепокоєння щодо впливу кіберзлочинців на здоров'я та безпеку всього населення. Ці загрози підкреслюють важливість розслідувань кіберзлочинів та їх роль у тому, щоб зробити Інтернет безпечнішим місцем для суспільства та бізнесу [3].

Проблема полягає в тому, що в умовах *цифровізації* життя, доцільно і удосконалити збір та збереження **доказів**, що стосуються **кіберзлочинності**. Тому постає питання про підвищення якості кримінального процесуального законодавства України шляхом внесення відповідних змін до КПК України у частині підвищення ефективності **доказування кіберзлочинів**.

Важливим завданням є встановлення необхідності у швидкому реагуванні на вчинення **кіберзлочинів**, володіння особи, яка проводить досудове **розслідування**, знаннями та навичаками у зазначеній сфері незаконної діяльності особи. Особливу увагу необхідно приділити удосконаленим способам збирання **доказів** при **розслідуванні кіберзлочинів**.

Інша проблема в тому, що через процесуальні складнощі при потребі вилучення даних через електронні мережі з віддалених носіїв інформації, до яких у правоохоронних органів немає безпосереднього доступу [4, с. 50].

Аналіз останніх досліджень та публікацій. Питання **доказування та розслідування кіберзлочинів,** якості кримінального процесуального законодавства України, досліджували вітчизняні та зарубіжні науковці, зокрема: О. В. Амелін, П. Д. Біленчук, М. В. Бутузов, Н. В. Глинська, М. В. Гуцалюк, І. В. Колесников, Л. М. Лобойко, Г. В. Муляр, Є. О. Наливайко, М. І. Пашковський, І. Л. Петрухін, М. А. Погорецький, Є. В. Пряхін, О. А. Самойленко, В. М. Тертишник, Л. Д. Удалова, О. С. Ховпун, Р. Ф. Черниш, В. Ю. Шепітько, О. Г. Шило, K.-S. Choi, P. Gladyshev, A. Patel, T. J. Holt, G. E. Higgins, P. Watters, тощо.

Зокрема, стаття "Формалізація обмеження часу події в цифрових розслідуваннях" (P. Gladyshev, A. Patel "Formalising event time bounding in digital investigations", 2005) визначає обмеження часу події як математичну задачу та представляє алгоритм її вирішення [5].

Мета. Метою статті є проведення аналізу наукових праць і норм чинного кримінального процесуального законодавства щодо особливостей предмету доказування кіберзлочинів під час воєнного стану в Україні.

Виклад основного матеріалу. Під час воєнного стану в Україні набувають особливого значення збирання доказів, їх оцінка та закріплення, що є важливим етапом при **розслідуванні кримінальних проваджень** у сфері **кіберзлочинності**, а також проведення всебічного та швидкого досудового **розслідування** для подальшого встановлення наявності або відсутності вини особи. Про велику кількість кібератак на Україну відомо ще з початку війни, а несанкціоноване втручання у роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж передбачає достатній рівень загрози, а наслідки можуть не проявлятися або не

реалізовуватися з причин, що не залежать від суб'єкта вчинення. Додатково це спрощує здійснення провадження, оскільки перелік обставин, які підлягають **доказуванню** у процесі, зменшується. **Кіберзлочини** вчиняють особи, які мають певні знання у сфері ІТ-технологій, що дозволяє їм уникати кримінального покарання, тому ці злочини високолатентні. У 2020 р. в Україні суди ухвалили близько 100 обвинувальних вироків, пов'язаних із кіберзлочинами [6]. Виявлення та **розслідування** кіберзлочинів становить цілу програму поетапно здійснених заходів, передбачених кримінально-процесуальним законодавством. **Доказування** на етапі збирання **доказів** здійснюється шляхом: проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій; витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок; здійснення міжнародного співробітництва під час **кримінального провадження**; проведення інших дій, передбачених КПК України [7, с. 137].

Слід зазначити, що окремі правові положення щодо електронних джерел доказової інформації діють в кримінальному процесі вже сьогодні. Так, використання електронних документів в якості процесуальних джерел **доказів** передбачене ст. 99 КПК України; допускається електронна форма фіксації окремих слідчих розшукових дій (зокрема відеозапис в ході проведення обшуку, огляду, допиту, слідчого експерименту, електронні додатки до протоколів С(Р)Д в порядку ст. 104, 105 КПК України), проведення допиту, впізнання в режимі відеоконференції тощо. Втім, ні правове регулювання, ні ступінь наукової розробленості проблем, пов'язаних з **електронними доказами** не відповідають вимогам практики. Зокрема, не працює в електронних реаліях закріплений в ч. 1 ст. 99 КПК України принцип прив'язки документу до матеріального носія інформації. За такого підходу, документом в процесуальному значенні буде вважатися не окремий електронний файл, що містить відомості, які мають значення для **кримінального провадження**, а фізичний носій електронної інформації, що містить згаданий файл. При цьому, сучасні фізичні носії електронної інформації здатні містити мільйони файлів різного формату та розміру одночасно, лише одиниці з яких можуть мати відношення до **кримінального провадження**. Через згаданий принцип також виникають процесуальні складнощі при потребі вилучення даних через електронні мережі з віддалених носіїв інформації, до яких у правоохоронних органів немає безпосереднього доступу [4, с. 50].

У зв'язку зі стрімким зростанням кількості злочинів, скоєних за допомогою інформаційних технологій, постає проблема їх швидкого, якісного та ефективного **розслідування та доказування**. **Розслідування кіберзлочинів** розпочинається з моменту внесення відомостей до Єдиного реєстру досудових розслідувань про факт виявлення такого порушення та закінчується складанням обвинувального акту відносно винної особи та направлення до суду, або відповідно закриття **кримінального провадження**. Під час проведення досудового **розслідування** слідчий/прокурор застосовують усі необхідні заходи щодо притягнення винних до кримінальної відповідальності за **кіберзлочини** шляхом проведення гласних та негласних слідчих (розшукових) дій, експертиз, міжнародного співробітництва тощо.

Особливу увагу під час проведення **розслідування кіберзлочинів** приділяють збиранню **доказів**. Сторона обвинувачення здійснює збирання **доказів** шляхом: проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій; витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок; здійснення міжнародного співробітництва під час **кримінального провадження**; проведення інших дій, передбачених КПК України. Першочерговим завданням слідчого на початковому етапі **розслідування кіберзлочинів** є аналіз інформаційного середовища вчинення злочину (визначення типу носія, де зберігалася або оброблялася комп'ютерна інформація, до якої здійснено неправомірний доступ, що визначить напрямок всього подальшого **розслідування**); встановлення типу операційної системи комп'ютера (сервера), до якого здійснено неправомірний доступ, а також використаного для вчинення злочину програмного забезпечення, що значною мірою допоможе звузити коло можливих підозрюваних;

визначення апаратного та програмного забезпечення, яке піддалося впливу під час неправомірного доступу, а також інформації про засоби і знаряддя вчинення такого доступу, що дозволить скласти об'єктивну картину слідів злочину [8, с. 179].

Слід зазначити, що законодавець прийняв такі Закони України як: «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового **розслідування** «за гарячими слідами» та протидії кібератакам» № 2137-IX від 15.03.2022 р.; «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24.03.2022 р. Так, було внесено такі зміни у кримінальне процесуальне законодавство зміни, які покращили його ефективність та якість, а також процесуальної економії, як: у абз. 2 ст. 170 КПК України передбачена можливість накладання арешту на комп'ютерні системи чи їх частини, якщо вони отримані внаслідок вчинення кримінального правопорушення або є засобом його вчинення, або необхідні для проведення експертного дослідження, а також якщо доступ до них обмежується власником; У абз. 2 ч. 6 ст. 236 КПК України передбачається, що під час обшуку слідчий, прокурор зможе отримувати доступ до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку без попереднього дозволу, за умови, що інформація, яка на них міститься, має значення для встановлення обставин у **кримінальному провадженні**. У ч. 2 ст. 237 КПК України зазначено, що огляд комп'ютерних даних проводиться слідчим, прокурором шляхом відображення у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (фото, відео тощо). А ст. 245-1 КПК України запроваджується нова слідча (розшукова) дія - зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису, яка проводиться на підставі постанови слідчого, прокурора. У ч. 5 ст. 268 КПК України вказано, що установлення місцезнаходження радіообладнання (радіоелектронного засобу) тепер за заявою його власника не потребує дозволу слідчого судді [9].

Слід зазначити, що під час **розслідування кіберзлочинів** доцільно проводити гласні та негласні слідчі (розшукові) дії з метою отримання **доказів**. Допит заявника, потерпілої особи (у разі наявності) та свідків становить необхідний процес отримання **доказів** через показання. Показання – це відомості, які надаються в усній або письмовій формі під час допиту підозрюваним, обвинуваченим, свідком, потерпілим, експертом щодо відомих їм обставин у **кримінальному провадженні**, що мають значення для цього **кримінального провадження** [10, с. 98]. У разі необхідності вилучення документів необхідною дією є проведення тимчасового доступу до речей та документів як заходу забезпечення **кримінального провадження**, тобто надання особою, у володінні якої знаходяться такі речі і документи, можливості стороні кримінального провадження ознайомитися з ними, зробити їх копії та, у разі прийняття відповідного рішення слідчим суддею, судом, провести виїмку. Проведення вказаного заходу забезпечує отримання речей або документів, які можна використати в якості **доказів**, встановивши їх причетність до **кіберзлочину**. Слід погодитись з Г. В. Муляр та О. С. Ховпун щодо можливості проведення таких дій як огляд приміщення, житла або його обшуку. Зазначені слідчі (розшукові) дії проводяться з метою відшукання знарядь та засобів вчинення **кіберзлочину** (комп'ютерної техніки) або особи, яка вчинила злочин. Лише *комплексне (курсив мій - Т.Д.)* проведення усіх заходів допоможе особі, яка проводить досудове **розслідування** притягти винних до кримінальної відповідальності за **кіберзлочини**, відшкодувати шкоду, заподіяну злочином. Експертиза є різновидом **доказів**, а тому займає особливе місце в процесі **доказування кіберзлочинів** [7, с. 136].

Висновки. Отже, предмет **доказування кіберзлочинів** в Україні під час воєнного стану є важливим для подальшого підвищення ефективності досудового **розслідування** та судового розгляду та забезпечення єдності судової практики, верховенства права, ефективного захисту прав людини. У зв'язку з впровадженням цифрових технологій і телекомунікацій в усі сфери суспільного життя доцільно модернізувати правове регулювання та практику застосування кримінального процесуального законодавства.

Підтримую низку своєчасних і доцільних змін до Кримінального процесуального кодексу України, які відповідають реаліям життя під час воєнного стану у країні щодо: 1) можливості накладання арешту на комп'ютерні системи чи їх частини, якщо вони отримані внаслідок вчинення кримінального правопорушення або є засобом його вчинення, або необхідні для проведення експертного дослідження, а також якщо доступ до них обмежується власником (абз. 2 ст. 170); 2) права під час обшуку слідчого, прокурора отримувати доступ до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку без попереднього дозволу (абз. 2 ч. 6 ст. 236); 3) огляду комп'ютерних даних проводиться слідчим, прокурором з відображенням у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (фото, відео тощо) (ч. 2 ст. 237); 4) установлення місцезнаходження радіообладнання (радіоелектронного засобу) (ч. 5 ст. 268).

Література:

1. Кривенко К. Кіберзлочинність: актуальна судова практика. *Лігазакон.* 22.02.2022. URL: https://biz.ligazakon.net/analitycs/209283_kberzlochinnst-aktualna-sudova-praktika.
2. Заремба Т. Щодоби Росія завдає Україні понад 10 кібератак - СБУ. РБК-Україна. 26.12.2022. URL: https://www.rbc.ua/rus/news/shchodobi-rosiya-zavdae-ukrayini-ponad-10-1672081715.html.
3. Cyber crime investigation: making a safer Internet space. *Maryville univercity.* URL: https://online.maryville.edu/blog/cyber-crime-investigation/.
4. Коваленко А.В. Перспективи впровадження категорії «електронні докази» в кримінальний процес України. *Актуальні питання протидії кіберзлочинності та торгівлі людьми*: збірник матеріалів Всеукр. наук.-практ. конф. (23 листопада 2018, м. Харків). МВС України, ХНУВС, Координатор проектів ОБСЄ в Україні. Харків: ХНУВС, 2018. С. 49-51.
5. Gladyshev P., Patel A. Formalising event time bounding in digital investigations. *International Journal of Digital Evidence.* 2005. Vol. 2. № 4. P. 1-14.
6. Якуша В. Олександр Тананакін: розслідування кіберзлочинів часто відбувається за принципом “хто швидше”. *Закон і бізнес.* Вип. № 12 (1518). 20.03.-26.03.2021. URL: https://zib.com.ua/ua/147082.html.
7. Муляр Г.В., Ховпун О.С. Особливості доказування кіберзлочинів. *Право. Людина. Довкілля.* Київ: НУБіП України, 2019. Том 10. № 3. - С. 132-138. URL: http://dglib.nubip.edu.ua/handle/123456789/8430.
8. Бурбело Б.А. Криміналістичні основи протидії кіберзлочинності. *Актуальні питання розслідування кіберзлочинів:* матеріали Міжнародної науково-практичної конференції (Харків, 10 грудня 2013 р.). Харків: Харківський національний університет внутрішніх справ, 2013. С. 179–182.
9. Єрема М., Борисенко А. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. *Юрліга. 13.04.2022.* URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix.
10. Заходи забезпечення кримінального провадження. Зразки та бланки процесуальних документів: практичний посібник-коментар. Київ: «Центр учбової літератури», 2018. 160 с.