КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНАЛЬНИЙ ПРОЦЕС

УДК 343.148 https://doi.org/10.31548/law2019.03.017

ОСОБЛИВОСТІ ДОКАЗУВАННЯ КІБЕРЗЛОЧИНІВ

Г. В. МУЛЯР, *кандидат історичних наук, доцент*
кафедри кримінального права, процесу та криміналістики,
Академія праці, соціальних відносин і туризму
E-mail: Box0007@meta.ua
О. С. ХОВПУН, *кандидат юридичних наук, завідувач*
кафедри кримінального права, процесу та криміналістики,
Академія праці, соціальних відносин і туризму
E-mail: Khovpun3322@gmail.com

Анотація. *У науковій статті розглядається питання збирання, використання та застосування доказів під час доказування злочинів, які вчиняються через мережу Інтернет (кіберзлочинів). Особлива увага приділяється проведенню всебічного, повного, об'єктивного та швидкого досудового розслідування по кримінальним провадженням щодо вчинення кіберзлочинів, збір та закріплення усіх необхідних доказів, збереження юридичних властивостей доказів та в подальшому встановлення наявності або відсутності вини особи. Розглядається поетапно процес доказування (збирання, перевірка та оцінка доказів) кіберзлочинів та можливі труднощі, з якими може зіштовхнутись слідчий/прокурор, під час розслідування. Встановляються необхідність проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, проведення експертиз, залучення експертів та спеціалістів до консультацій, застосування заходів забезпечення кримінального провадження та налагодження міжнародного співробітництва з метою притягнення винних до кримінальної відповідальності за кіберзлочини. Окрема увага надається особам, які вчиняють кіберзлочини, оскільки останні мають досить високий інтелектуальний рівень та володіють знаннями та навичками у користуванні комп'ютерними технологіями та програмами.*

Ключові слова: *докази, процес доказування, кіберзлочини, кіберзлочинність, розслідування, кримінальне провадження*

Актуальність.

Боротьба з кіберзлочинами займає важливе місце серед інших злочинів, оскільки кіберзлочини носять більш латентний характер та постійно вдосконалюють механізм їх вчинення. У зв'язку із розвитком комп'ютерних систем та технологій, злочини у вказаній сфері розвиваються досить швидко, а процес доказування становить окремий механізм, який необхідно постійно вдосконалювати та вносити корективи, відповідно до змін та доповнень законодавства. Сфера кіберзлочинності посягає в певній мірі на права та свободи людини у інформаційному просторі, а інформація та комп'ютерна техніка можуть виступати предметом злочинних посягань.

Процес доказування складається із стадій, які нерозривно пов'язані та являє собою збирання доказів, їх оцінку та вірне закріплення, являючись при цьому важливим етапом при розслідуванні кримінальних проваджень у сфері кіберзлочинності. Докази кіберзлочинів досить важко отримати, оскільки інформаційний простір є масштабним полем для діяльності осіб, які посягають на кібер-свободу громадян.

Під час розслідування кіберзлочинів актуальним залишається питання проведення всебічного та швидкого досудового розслідування по вказаним кримінальним провадженням, збір та закріплення усіх необхідних доказів, збереження юридичних властивостей доказів та в подальшому встановлення наявності або відсутності вини особи. Високу увагу під час проведення досудового розслідування у кримінальному провадженні займають особливості доказування кіберзлочинів, встановлення механізму доказування та визначення джерел доказів.

Аналіз останніх досліджень та публікацій.

Основою даної статті стали праці таких українських науковців як: Р.С. Бєлкіна, Т.В. Варфаломеєвої, В.Т. Маляренка, М.М. Михеєнка, І.Л. Петрухіна, О.Р. Ратінова, В.М. Тертишника, Л.Д. Удалової, В.Ю. Шепітька, а також інших науковців, які зробили вагомий внесок у дослідження проблематики розслідування кіберзлочинів, проведенні досудового розслідування з метою притягнення винних осіб до відповідальності за вказаний різновид злочинів. Незважаючи на це, вищевказане питання залишається актуальним та необхідним для дослідження. Саме тому окремі аспекти потребують більш детального вивчення.

Метою статті є дослідження питання особливостей доказування кіберзлочинів за допомогою використання належним чином зібраних доказів. Розглядаються особливості механізму процесу доказування та доведення або спростування вини особи. 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 способам збирання доказів при розслідуванні кіберзлочинів та вірного визначення особи, яка вчинила злочин.

Результати.

Конвенцією про кіберзлочинність (прийняту Радою Європи у 2001 р.) надано визначення терміну «кіберзлочинність» та отримано уявлення про це явище як злочинність у кіберпросторі. Конвенція Ради Європи поділяє

кіберзлочини на наступні групи: 1) злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему); 2) злочини, пов'язані з використанням комп'ютера як засобу скоєння злочинів, а саме – для маніпуляції з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення); 3) злочини, пов'язані з контентом (змістом даних); 4) злочини, пов'язані з порушенням авторського права і суміжних прав; 5) акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж («Конвенцією про кіберзлочинність», 2005).

Кабінет Міністрів України запропонував розмежувати підслідність кіберзлочинів, вчинених у сфері використання комп'ютерів, систем та комп'ютерних мереж, мереж електрозв'язку, державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури, істотно підвищивши при цьому відповідальність за втручання в їх роботу. Законопроектом передбачається збільшення санкцій за кіберзлочини (несанкціоноване втручання в роботу об'єктів критичної інформаційної інфраструктури, створення, розповсюдження та збут шкідливих програм, несанкціонований збут або розповсюдження створеної та захищеної відповідно до чинного законодавства інформації з обмеженим доступом, яка обробляється на об'єктах критичної інформаційної інфраструктури) («Кабмін пропонує…»).

Важливим документом у сфері протидії кіберзлочинам визначається Стратегія розвитку системи Міністерства внутрішніх справ України до 2020 р. (далі – Стратегія), яка в тому числі містить позицію щодо виявлення кіберзлочинів та притягнення винних до кримінальної відповідальності за вказаний різновид злочинів. Основною метою Стратегії є створення безпечного середовища для існування та розвитку вільного суспільства через формування та реалізацію державної політики у сфері внутрішніх справ, зміцнення довіри до органів системи МВС з боку суспільства, продовження розвитку України як безпечної європейської держави, в основі якої лежать інтереси її громадян та висока ефективність усіх складових системи МВС. Реалізація скрадатиметься з послідовних кроків на основі оптимальних рішень, які враховують позитивний досвід і кращі практики провідних країн світу.

До 2020 р. Стратегією визначено основні пріоритети діяльності: безпечне середовище, протидія злочинності, дотримання та забезпечення прав людини органами системи МВС, ефективне інтегроване управління кордонами і збалансована міграційна політика, якість і доступність послуг, ефективне врядування, прозорість і підзвітність, розвиток кадрового потенціалу та соціальний захист працівників. Зазначимо, що протидія кіберзлочинам має зовсім індивідуальну позицію щодо їх попередження та припинення («Стратегія розвитку системи …»).

Одним із способів вчинення протиправних діянь є глобальна мережа Інтернет, за допомогою якої вчиняються не один злочин, передбачений Кримінальним кодексом України (далі – КК України). У КК України Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» присвячений питанню кіберзлочинів, фактично притягненню до відповідальності осіб, які вчинили даний різновид кримінальних правопорушень (злочинів) («Кримінальний кодекс України…», 2016).

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.

Доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому Кримінально-процесуальному кодексі України, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню (ст. 84 ч. 1). Доказування полягає у збиранні, перевірці та оцінці доказів з метою встановлення обставин, що мають значення для кримінального провадження (ст. 91 ч. 2) («Кримінальний процесуальний кодекс України…», 2018).

Метою доказування у кримінальному провадженні є отримання достовірних знань щодо події кримінального правопорушення та винуватості обвинуваченого. Доказування має кримінальне-правову та кримінальне-процесуальне значення. Кримінальне-правове значення доказування полягає в тому, що: завдяки доказуванню встановлюється, чи мало місце кримінальне правопорушення та якою є його кваліфікація; доказування гарантує реалізацію кримінальної відповідальності. Кримінально-процесуальне значення доказування полягає в тому, що: правильне його здійснення дає змогу забезпечити реалізацію прав та законних інтересів усіх учасників кримінального процесу; усі питання, що виникають під час кримінального провадження, можна вирішити лише на підставі достовірно встановлених під час доказування обставин; участь заінтересованих суб'єктів у доказуванні є гарантією реалізації засад кримінального процесу (змагальності, забезпечення права на захист); докази є підставою для прийняття всіх процесуальних рішень у кримінальному провадженні.

Процес доказування – це шлях відтворення реальної картини події кримінального правопорушення, з'ясування її сутності та вироблення на підставі цього відповідних процесуальних рішень. Цей процес формує комплекс процесуальних дій і відносин, які можна згрупувати в окремі відносно самостійні елементи, які є єдиними для всіх кримінальних проваджень («Теорія судових доказів…», 2018: 43).

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 електронно-обчислюваль-

ної машини (носія), де зберігалася або оброблялася комп'ютерна інформація, до якої здійснено неправомірний доступ (Web-сервер, персональний комп'ютер, мобільний телефон, електронна кредитна карта), що визначить напрямок всього подальшого розслідування; встановлення типу операційної системи комп'ютера (сервера), до якого здійснено неправомірний доступ (Unix, Linux, Netware, Windows), 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 (Бурбело, 2013: 179).

Кіберзлочини вчиняються підготовленими особами, які мають високий інтелектуальний рівень та відмінні знання у сфері використання комп'ютерних технологій. Важливо для розслідування таких злочинів залучати експертів та спеціалістів у вказаній галузі, які сможуть провести експертизу. Висновком експерта можна вважати докладний опис проведеного дослідження та зробленого висновку уповноваженим суб'єктом. Такою особою є експерт, який володіє спеціальними знаннями у галузі, відповідно до якої призначається експертиза. Експертиза є різновидом доказів, а тому займає особливе місце в процесі доказування кіберзлочинів.

Розслідування кіберзлочинів встановлює необхідність проведення гласних та негласних слідчих (розшукових) дії з метою отримання доказів з різноманітних джерел. 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 («Заходи забезпечення...», 2018: 98).

Необхідною дією при розслідуванні кіберзлочинів можна вважати проведення тимчасового доступу до речей та документів як заходу забезпечення кримінального провадження (у разі необхідності вилучення документів). Під тимчасовим доступом до речей і документів розуміється 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, вилучити їх (провести виїмку). Проведення вказаного заходу забезпечує отримання речей або документів, які можна використати в якості доказів, встановивши їх причетність до кіберзлочину.

Потрібно зазначити про можливість проведення таких дій як огляд приміщення, житла тощо або його обшук. Зазначені слідчі (розшукові) дії проводяться з метою відшукання знарядь та засобів вчинення кіберзлочину (комп'ютерної техніки) або особи, яка вчинила злочин. Тільки проведення усіх заходів в сукупності допоможе особі, яка проводить досудове розслідування притягти винних до кримінальної відповідальності за кіберзлочини, відшкодувати шкоду, заподіяну злочином.

Висновки і перспективи.

Кіберзлочини займають особливе становище у системі інших злочинів та набувають суспільного резонансу у

зв'язку із швидким розвитком комп'ютерних технологій та мережі Інтернет. Конвенція Ради Європи поділяє кіберзлочини на наступні групи: 1) злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему); 2) злочини, пов'язані з використанням комп'ютера як засобу скоєння злочинів, а саме – для маніпуляції з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення); 3) злочини, пов'язані з контентом (змістом даних); 4) злочини, пов'язані з порушенням авторського права і суміжних прав; 5) акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж.

Процес доказування становить собою шлях відтворення реальної картини події кримінального правопорушення, з'ясування її сутності та вироблення на підставі цього відповідних процесуальних рішень. Саме налагодження механізму розслідування кіберзлочинів необхідно для вчинення їх активної протидії. 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.

Можемо зазначити, що кіберзлочини носять латентний характер, а тому їх виявлення та розслідування становить цілу програму поетапно здійснених заходів, передбачених кримінально-процесуальним законодавством. З однієї сторони є особа, яка володіє знаннями та навичками у сфері ІТ-технологій, а з іншого боку – уповноважена службова особа (слідчий, прокурор), які можуть і не знати тонкощі розслідування таких злочинів. Важливим є залучення експертів та спеціалістів на стадії досудового розслідування з метою отримання консультацій, а в подальшому проведення експертиз та складання висновків.

Список використаних джерел

1. 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.
2. Заходи забезпечення кримінального провадження. Зразки та бланки процесуальних документів: практичний посібник-коментар. Київ: «Центр учбової літератури», 2018. 160 с.
3. Кабмін пропонує посилити відповідальність за кіберзлочини у сфері критичної інформаційної інфраструктури. URL: https://ua.interfax.com.ua.
4. Конвенція про кіберзлочинність: Закон України від 07 вересня 2005 р. 2824-IV (ратифікація). URL: https://zakon.rada.gov.ua/laws/show/994_575.
5. Кримінальний кодекс України: чинне законодавство із змінами та доповненнями на 18 лютого 2016 р.: офіц. текст. Київ: Алерта, 2016. 202 с.
6. Кримінальний процесуальний кодекс України: станом на 6 липня 2018 р. Харків: Право, 2018. 366 с.
7. Стратегія розвитку системи Міністерства внутрішніх справ України до 2020 р. URL: https://cyberpolice.gov.ua/strategy-2020.

8. Теорія судових доказів в питаннях та відповідях: навчальний посібник. Л.Д. Удалова, Д.П. Письменний, Ю.І. Азаров та ін. Київ: «Центр учбової літератури», 2018. 104 с.

References

1. Burbelo, B.A. (2013). Kryminalistychni osnovy protydii kiberzlochynnosti. Aktualni pytannia rozsliduvannia kiberzlochyniv [Forensic Foundations for Countering Cybercrime. Current Issues in the Investigation of Cybercrime]. Kharkiv: Kharkivskyi natsionalnyi universytet vnutrishnikh sprav, 179–182.
2. Zakhody zabezpechennia kryminalnoho provadzhennia. Zrazky ta blanky protsesualnykh dokumentiv [Measures to ensure criminal proceedings. Samples and forms of procedural documents] (2018). Kyiv: «Tsentr uchbovoi literatury», 160.
3. Kabmin proponuie posylyty vidpovidalnist za kiberzlochyny u sferi krytychnoi informatsiinoi infrastruktury [The Cabinet of Ministers proposes to strengthen responsibility for cybercrime in the field of critical information infrastructure]. Available at: https://ua.interfax.com.ua.
4. Konventsiia pro kiberzlochynnist [Convention on Cybercrime] (2005): Zakon Ukrainy 07.09.2005 2824-IV. Available at: https://zakon.rada.gov.ua.
5. Kryminalnyi kodeks Ukrainy: chynne zakonodavstvo iz zminamy ta dopovnenniamy na 18.02.2016 [The Criminal Code of Ukraine: current legislation with amendments and supplements. on February 18, 2016] (2016). Kyiv: Alerta, 202.
6. Kryminalnyi protsesualnyi kodeks Ukrainy [The Criminal Procedural Code of Ukraine] (2018): stanom na 06.07.2018. Kharkiv: Pravo, 366.
7. Stratehiia rozvytku systemy Ministerstva vnutrishnikh sprav Ukrainy do 2020 [Strategy of development of the system of the Ministry of Internal Affairs of Ukraine up to 2020]. Available at: https://cyberpolice.gov.ua/strategy-2020.
8. Teoriia sudovykh dokaziv v pytanniakh ta vidpovidiakh [Theory of evidence in questions and answers] (2018). L.D., Udalova, D.P., Pysmennyi, Yu.I., Azarov ta in. Kyiv: «Tsentr uchbovoi literatury», 104.

***G.V. Muliar & O.S. Khovpun (2019). Features of evidence of cybercrime. Law. Human. Environment**, 10(3): 132-138. https://doi.org/10.31548/law2019.03.017*

***Summary.** The article deals with the issue of collecting, using and using evidence in proving crimes committed through the Internet (cybercrime). Particular attention is paid to carrying out a comprehensive, complete, objective and prompt pre-trial investigation into criminal proceedings for committing cybercrime, collecting and securing all necessary evidence, preserving the legal properties of evidence, and subsequently establishing the presence or absence of a person's fault. The stage of the process of proof (collection, verification and evaluation of evidence) of cybercrime and the possible difficulties that the investigator / prosecutor may face during the investigation is considered in stages. Establishing the necessity of carrying out investigative (search) actions and secret investigative (search) actions, carrying out of expert assessments, involving experts and specialists for consultations, application of measures for ensuring criminal proceedings and establishing international cooperation aimed at bringing the perpetrators to criminal responsibility for cybercrime. Particular attention is given to persons who commit cybercrime, since the latter have a rather high intellectual level and possess knowledge and skills in the use of computer technologies and programs.*

***Keywords:** evidence, proofing process, cybercrime, cybercrime, investigation, criminal proceedings*