investigation-of-sexual-violence-in-conflict/International_ Protocol_2017_2nd_Edition.pdf

Гора Ірина Віталіївна,
головний науковий співробітник науково-організаційного центру Національної академії Служби безпеки України, доктор юридичних наук, професор

ЗАСТОСУВАННЯ ПОЛОЖЕНЬ ЦИФРОВОЇ КРИМІНАЛІСТИКИ В ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

Питання кіберзлочинів, кіберзлочинності, протидії та боротьби з цими видами суспільно небезпечних діянь хвилюють суспільство, працівників практично всіх сфер виробництва, фінансів, бізнесу, надання послуг, законодавців, а разом з тим і викликають інтерес у науковців та практиків. Виявлення й розслідування кіберзлочинів залишається доволі складним завданням для працівників оперативних підрозділів та органів досудового розслідування, що зумовлене специфікою даного виду злочинів. Традиційні підходи до боротьби з такими кримінальними правопорушеннями не дають можливості повною мірою протидіяти якісно новому виду загроз. Необхідною умовою успішної роботи в цьому напрямі є розуміння слідчими, детективами, прокурорами, спеціалістами й експертами специфіки функціонування кіберсфери, її транскордонного характеру, вміння працювати в інформаційному середовищі, комунікувати з представниками IT-компаній та іншими фахівцями. Правоохоронцям потрібні знання того, де і як шукати докази, як їх фіксувати, вилучати, досліджувати й оцінювати, правильно будувати діалог з учасниками кримінального провадження під час допиту свідків, підозрюваних, потерпілих тощо. Окремою особливістю кіберзлочинів, що істотно впливає на організацію розслідування, є їх транскордонність. Ситуація, коли суб'єкт злочину та об'єкти посягання знаходяться в різних містах, країнах, а інколи й на різних континентах, потребує міжнародного співробітництва. На даний час багатьма державами вже здійснені успішні спроби укладання міжнародних угод щодо співробітництва при запобіганні вчиненню та розслідуванні злочинів у кіберпросторі, розробляються рекомендації з організації роботи при виявленні й розслідуванні кіберінцидентів.

Так, наприклад, на сьогодні вже розроблені міжнародні стандарти з розслідування кіберзлочинів. Технічним комітетом 272 «Криміналістика» (*англ.* – «Forensic sciences») Міжнародної організації із стандартизації (ISO) започатковано розроблення стандарту ISO 21043, що має 5 частин. Перша частина – ISO 21043-1:2018 «Криміналістика. Частина 1: Терміни та визначення». Друга частина – ISO 21043-2:2018 «Криміналістика. Частина 2: Виявлення, фіксування, вилучання, транспортування та зберігання об'єктів» присвячена загальним питанням розслідування. Три наступні частини цієї серії: – ISO 21043-3 «Криміналістика. Частина 3: Аналізування»; – ISO 21043-4 «Криміналістика. Частина 4: Інтерпретування»; – ISO 21043-5 «Криміналістика. Частина 5: Звітування» перебувають на остаточних етапах розробки [1].

Багато які з доказів, що стосуються кіберзлочинів, часто надаються в електронно-цифровій формі. Ці дані можуть зберігатися або бути транзитними й існувати у вигляді комп'ютерних файлів, повідомлень, робочих журналів чи мережевих даних. Для отримання таких доказів необхідно об'єднання традиційних і нових методів роботи слідчого, застосовування комп'ютерно-орієнтованих підходів до їх збирання, оцінки й використання в доказуванні. До їх числа можуть входити: пошук, огляд, вилучення або копіювання комп'ютерних даних, які знаходяться на пристроях, що належать підозрюваним або потерпілим; отримання комп'ютерних даних від третіх осіб, таких як розробники програмного забезпечення, постачальники послуг – оператори Інтернет-зв'язку та ін.; за необхідності оперативним працівником та слідчим має бути здійсненим перехоплення електронних повідомлень.

Деякі з процесуальних положень, в основі яких лежить просторовий, часовий, об'єктно-орієнтований підхід, важко застосовувати у ситуаціях, пов'язаних із пошуком, збереженням, вилученням чи копіюванням конкретних електронних даних та інформаційних потоків даних у режимі реального часу й конкретного місця. Одна з важливих проблем досудового розслідування кіберзлочинів пов'язана з неможливістю безпосереднього застосування до них стандартного алгоритму здійснення розслідування. У певних випадках порядок підготовки, проведення й фіксації результатів слідчих дій, що закріплені в КПК України, при розслідуванні даного виду злочинів не будуть ефективними. Так, наприклад, огляд місця події, що має географічну прив'язку до конкретної місцевості і

котрому часто надається центральне значення, при розслідуванні злочинів у кіберпросторі буде мати низку особливостей. По-перше, виникає питання, що саме слід вважати місцем злочину з процесуальної і позиційно-географічної точки зору. Адже у випадках, коли злочинцем здійснена хакерська атака як спосіб вчинення кіберзлочину – місце знаходження хакера під час атаки, місце написання ним шкідливої програми, місце, в якому розташоване атаковане комп'ютерне обладнання та місце, де настали шкідливі наслідки атаки будуть різними і перебувають на значних відстанях одне від одного. Це може відбуватись навіть на різних континентах. Може істотно відрізнятись і час вчинення певних дій злочинцем та настання наслідків на кожному з таких місць. Враховуючи те, що кіберзлочини вчиняються у так званому віртуальному, кіберпросторі, пропонують вважати місцем події певний його діапазон. Але навіть якщо пристати до такої точки зору, то слідчий стикається з наступною проблемою: як взагалі провести огляд місця події і як вказати його координати, якщо на кіберпростір не розповсюджуються географічні константи, а отже й юридичні закони певної держави. Водночас місце розташування задіяного для вчинення злочину комп'ютерного обладнання, місце роботи чи мешкання підозрюваного хакера, місце розташування «потерпілої» від кібератаки системи будуть відомі і мають свою географічну та IP адресу.

Сама процедура огляду місця події також пов'язана з низкою особливостей. Адже традиційні методики і способи використання криміналістичних науково-технічних засобів тут можуть бути безрезультатними, оскільки йде робота з пошуку, фіксації, вилучення не звичних матеріальних слідів, а електронних, які до того ж можуть бути активними або пасивними. Для роботи з ними потрібне спеціальне комп'ютерне обладнання та його програмне забезпечення. Результат застосування таких криміналістичних засобів має бути зафіксованим і внесеним до протоколу слідчої дії у прийнятній для розуміння будь-ким з учасників судочинства формі.

Зарубіжним науковцем Дж. Горсманом (G. Horsman) звертається увага на те, що так названі «сучасні» місця злочину часто можна розглядати як гібриди між фізичними та цифровими технологіями, де важливо, щоб органи правопорядку не обмежували своїх можливостей. У свою чергу, кожен цифровий пристрій сам є гібридним, таким, що містить як нематеріальні цифрові сліди, так і потенційні фізичні докази на самому

пристрої, до того ж обидва можуть мати цінність для справи. Ним зазначається, що технологія електронних пристроїв зараз є такою, що дозволяє розробникам вбудовувати різні датчики, процесори та цифрову пам'ять у невеликі за розміром, але ємнісні електронні пристрої. Наявність будь-якого цифрового пристрою на місці події є новим завданням для слідчого не тільки з точки зору їх ідентифікації, але й розуміння того, яку цінність може мати інформація з цих пристроїв для ведення досудового розслідування та збору доказової бази. Цей вчений також звертає увагу на те, що фахівці, які беруть участь у огляді місця злочину, часто бувають першими в ланцюжку розслідування та несуть відповідальність за забезпечення і виконання будь-яких подальших дій для перевірки всіх «доступних» доказів, а також відповідають за те, щоб ці докази були вилучені та надані таким чином, щоб зберегти свою цінність. Важливо враховувати, щоб слідчий, який проводить і відповідає за огляд місця події, розпізнав наявність будь-яких цифрових пристроїв та встановив можливості, які ці пристрої можуть надати для подальшого ведення розслідування, й переконався, що вони вилучені належним чином, щоб надалі полегшити їхнє дослідження [2, с. 761, 763].

Звертають науковці й практики увагу і на огляд засобів комп'ютерної техніки, що проводиться під час обшуку, який також має певну специфіку. Це обумовлюється об'єктивною можливістю швидко знищувати інформацію, яка міститься на її електронних носіях чи циркулює в мережі. Усі дії щодо роботи з комп'ютером повинен виконувати тільки спеціаліст, щоб уникнути можливості знищення наявної інформації. Тому для запобігання негативних наслідків необхідно забезпечити охорону засобів комп'ютерної техніки, а також даних і цінної інформації, що знаходиться в операційній системі. Необхідно блокувати роботу виробничого процесу, припинити надходження та виток будь-якого роду інформації з операційної системи [3, с. 172–173].

Навіть така проста на перший погляд процесуальна дія як допит підозрюваного має низку складнощів, якщо допитують підозрюваного у вчиненні кіберзлочину. Головна проблема полягає в тому, що така особа в процесі допиту практично завжди висловлюється специфічними термінами, котрі важко сприймаються слідчим і можуть бути мало зрозумілими для людей без відповідної освіти, знань та досвіду роботу у сфері ІТ. Слідчому під час підготовки до допиту важливо отримати максимально повну інформацію щодо допитуваної особи, а саме:

вивчити її навички володіння комп'ютером, мережевими програмами, встановити мету проникнення у систему, знищення програм, впровадження вірусних шкідливих програм, заволодіння різноманітною інформацією та ін.

Важливе значення для виявлення й розслідування таких злочинів має використання оперативними працівниками й слідчими допомоги спеціалістів у галузі інтернет-технологій. Пошук, виявлення, фіксація й дослідження та оцінка електронних доказів й цифрових даних та інших слідів у комп'ютерних мережах не можливі без залучення відповідних фахівців. Слід погодитися з С.С. Чернявським та Ю. Ю.Орловим, що дослідження змісту електронного відображення та інформації в сервісних опціях операційної системи про це відображення в загальному випадку дозволяє встановити: подію кримінального правопорушення (наприклад, виявляючи сайт із забороненим контентом або з контентом, оприлюднення якого обмежено за законом); особу правопорушника (зокрема, вивчаючи дані його аккаунта, встановлюючи IP-адресу комп'ютера); спосіб та обставини вчинення злочину (наприклад, аналізуючи зміст електронного листування, результати моніторингу банківських рахунків тощо); характер і розмір шкоди, завданої злочином (які можуть полягати у порушенні функціонування певних електронних відображень, неправомірному перерахуванні електронних грошових коштів, передплаті ненаданих послуг (товарів), підробці документів, порушенні авторських прав тощо) [4, с. 118].

Такими є окремі і безумовно, що не всі питання, відповіді на які можна отримати з використанням можливостей сучасного і на сьогодні ще нового для нас напряму криміналістичної науки – цифрової криміналістики.

Список використаних джерел

1. International Organization for Standardization (ISO). URL: https://www.iso.org/standard/.

2. Horsman G. Digital evidence and the crime scene. *Science & Justice*. 2021. Volume 61, Issue 6. November. P. 761-770. URL: https://doi.org/10.1016/j.scijus.2021

3. Чаплинська Ю.А. Особливості проведення обшуків під час розслідування кіберзлочинів. *Актуальні питання розслідування кіберзлочинів*: *матеріали Міжнародної науково-практичної конференції*. Харків, 2013, С. 172-174.

4. Чернявський С.С., Орлов Ю.Ю. Електронне відображення як джерело доказів у кримінальному провадженні. *Вісник кримінального судочинства*. 2017. № 2. С. 112-124.

Шевчук Віктор Михайлович,
завідувач кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого, доктор юридичних наук, професор, головний науковий співробітник НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, заслужений юрист України

СУЧАСНІ ПРОБЛЕМИ Й ЗАВДАННЯ КРИМІНАЛІСТИКИ В УМОВАХ ВОЄННОГО СТАНУ ТА ЄВРОІНТЕГРАЦІЙНИХ ПРОЦЕСІВ

Повномасштабна збройна агресія Російської Федерації вплинула на всі сфери життєдіяльності нашої держави, в тому числі і на діяльність органів кримінальної юстиції. Російські окупаційні війська, порушуючи норми Міжнародного гуманітарного права, закони та звичаї ведення війни, завдають ударів по критичній інфраструктурі та житлу цивільного населення, вчиняють масові вбивства мирних людей, гвалтування жінок і дітей, мародерство [1, с. 896]. Фактично російські окупанти ведуть війну проти цивільного населення. Крім жахливих руйнувань цивільних об'єктів, вбивств мирного населення, агресор систематично пошкоджує енергетичну інфраструктуру та природоохоронну мережу України, завдаючи значних збитків нашій державі.

На сьогодні одним із головних завдань України є відсіч збройної агресії РФ та поновлення порушених прав і свобод українських громадян, а також забезпечення принципу невідворотності відповідальності винних осіб у вчинені злочинів, пов'язаних із вторгненням російських загарбників на терени нашої країни. Відомо, що докази та доказування – основа будь-якого процесу, і від того, наскільки якісно та повно під час досудового розслідування буде зібрана доказова база, залежить ефективність розгляду кримінального провадження в суді і швидкість досягнення мети правосуддя [2].