

УДК 343.98

Галина Костянтинівна АДЄЄВА,

*кандидат юридичних наук, старший науковий співробітник, провідний науковий співробітник Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса
Національної академії правових наук України*

ПРОБЛЕМИ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

На тлі стрімкого розвитку і поширення в усьому світі інформаційних технологій і телекомунікаційних систем злочини у сфері використання інформаційних технологій набули глобального характеру. Створюються міжнародні злочинні угруповання, члени яких діють узгоджено, хоча й перебувають в різних країнах світу. При цьому кількість кіберзлочинів щорічно зростає.

Провідною міжнародною компанією з кібербезпеки Cybersecurity Ventures надано прогноз щодо збільшення глобальних збитків від кіберзлочинності від трьох трильйонів доларів США в 2015 році до шести трильйонів доларів США у 2021 р. [1]. В таких умовах жодна країна світу, державна чи приватна установа не в змозі самостійно ефективно протидіяти кіберзлочинності і спонукає різні країни світу до міжнародної взаємодії та співробітництва.

Команда CERT-UA Держспецзв'язку в період з 18 по 24 квітня 2020 р. зареєструвала 2882 кіберінциденти, зафіксувала 17 фактів DDoS-атак (в т.ч. на сайти Офісу Президента України, ДБР, Держспецзв'язку) та 10761 підозрілих дій у кіберпросторі. Серед них: спроби викрадення інформації – 9, мережеве сканування – 2803, виявлення мережевого трояна – 1574, Web-атаки – 458, виявлення нестандартних протоколів або подій – 4344, спроби отримання прав адміністратора – 1531, спроби отримання прав користувача – 42 [2].

Правопорушники у кіберпросторі залишають не лише матеріальні сліди, а й електронні (цифрові). Виявлення, фіксація і використання електронних доказів у процесі доказування викликає певні труднощі через стрімкий розвиток інформаційних технологій, швидкі зміни поко-

лінь цифрової техніки та відсутність визначення поняття «електронні докази» у Кримінальному процесуальному кодексі України (КПК). У ч. 2 ст. 99 КПК України зазначено, що електронні носії інформації вважаються документами.

Електронні докази відрізняються від інших джерел доказів (показань, речових доказів, документів, висновків експертів) тим, що вони створені за допомогою електронних пристроїв, зберігаються та розповсюджуються лише за допомогою електронних носіїв інформації та комп'ютерних або телекомунікаційних мереж. Вони стають доступними для сприйняття людиною лише після обробки засобами електронної техніки з відповідним програмним забезпеченням. Електронні докази легше змінити чи підробити, ніж традиційні форми доказів, тому питання забезпечення їх належності і допустимості є вкрай актуальними.

У законодавстві України чітко не визначені порядок збирання та забезпечення електронних доказів, способи їх дослідження, механізми ідентифікації особи, яка створила або поширила інформацію в електронній формі.

В усіх країнах світу час від часу виникають проблеми визнання електронних (цифрових) доказів судом [3]. Складність їх використання в суді виникає через те, що до моменту дослідження в суді інформація в електронній формі може бути видалена або змінена, що значно знижує шанси довести факт її достовірності.

Чимало проблем виникає при дослідженні у вітчизняному суді навіть копій електронних листів. Суд вважає, що роздруковка з електронної скриньки не може вважатися належним доказом, оскільки неможливо ідентифікувати автора електронного листа та незрозуміло, на яку електронну адресу було здійснено відправлення, а також неможливо визначити, чи був надісланий файл підписаним електронним цифровим підписом [4].

На відміну від України, у США згідно з правилом 901b (4) «Федеральних правил про докази для судів та магістратів США» ідентифікація автора електронного листа з метою визнання його належним доказом здійснюється за допомогою показань свідків, які бачили, як певна особа створювала та надсилала електронний лист. Допустимість електронного листа як доказу в США встановлюється за сукупністю таких ознак, як зовнішній вигляд, зміст, лінгвістичні та семантичні ознаки листа, наявність певних знаків, фірмових найменувань, написів тощо [5].

Тобто, в окремих країнах світу поступово розробляються підходи до спрощення вимог щодо визнання електронних доказів судом. Однак в Україні через ускладнений та недосконалий процесуальний порядок подання електронних доказів в суд, їх використання у судочинстві є проблематичним.

Подолання існуючих проблем щодо визнання допустимими доказами інформації у цифровій формі є можливим за умови внесення до Кримінального процесуального кодексу спеціальної дефініції – визначення поняття «електронні докази» та розроблення «спрощеного» процесуального порядку їх фіксації і подання до суду.

Список бібліографічних посилань

1. The 2020 Official Annual Cybercrime Report // Herjavec Group. URL: <https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/> (дата звернення: 29.04.2020).
2. Команда CERT-UA Держспецзв'язку з 18 по 24 квітня зареєструвала 2882 кіберінциденти // Державна служба спеціального зв'язку та захисту інформації України : офіц. сайт. 27.04.2020. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=320629&cat_id=317163 (дата звернення: 28.04.2020).
3. Arshad Humaira, Bin Jantan Aman, Abiodun Oludare Isaac. Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence. *Journal of information processing systems*. 2018. Vol. 14, No. 2. Pp. 346–376. URL: <http://xml.jips-k.org/full-text/view?doi=10.3745/JIPS.03.0095> (дата звернення: 25.04.2020).
4. Постанова Львівського апеляційного господарського суду від 10.09.2018 : справа № 914/2505/17 // ZakonOnline : сайт. <https://zakononline.com.ua/court-decisions/show/76542389> (дата звернення: 25.04.2020).
5. Зозуля Н. Електронні докази за кордоном: практика застосування // Українське право : сайт. 25.06.2018. URL: <https://ukrainepravo.com/scientific-thought/naukova-dumka/elektronni-dokazy-za-kordonom-praktyka-zastosuvannya/> (дата звернення: 25.04.2020).

Одержано 01.05.2020